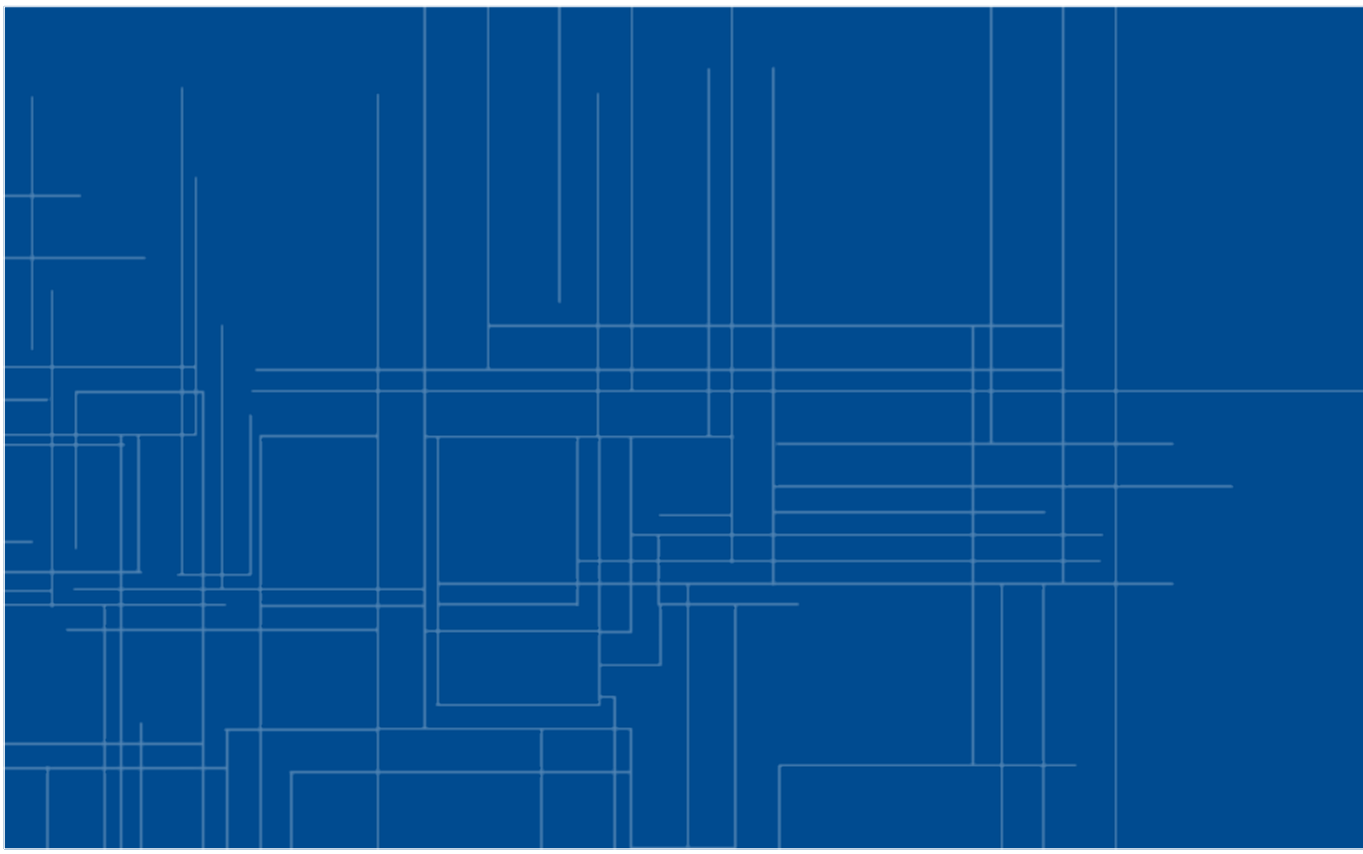
Informe Anual de Seguridad Nacional

2019



GOBIERNO DE ESPAÑA
PRESIDENCIA DEL GOBIERNO

Catálogo de publicaciones de la Administración General del Estado

htttp://cpage.mpr.gob.es

Edita:

NIPO (edición en línea): 08920006X
DL: En trámite (segundo trimestre)
Fecha de edición: marzo 2020
Imprime: imprenta Fragma Reprografía, S.L.

Informe Anual de Seguridad Nacional

2019

Este informe ha sido elaborado por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, en su condición de Secretaría Técnica y Órgano de Trabajo Permanente del Consejo de Seguridad Nacional, con la participación del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, el Ministerio de Justicia, el Ministerio de Defensa, el Ministerio de Hacienda, el Ministerio del Interior, el Ministerio de Fomento, el Ministerio de Educación y Formación Profesional, el Ministerio de Trabajo, Migraciones y Seguridad Social, el Ministerio de Industria, Comercio y Turismo, el Ministerio de Agricultura, Pesca y Alimentación, el Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad, el Ministerio de Política Territorial y Función Pública, el Ministerio para la Transición Ecológica, el Ministerio de Cultura y Deporte, el Ministerio de Economía y Empresa, el Ministerio de Sanidad, Consumo y Bienestar Social, el Ministerio de Ciencia, Innovación y Universidades y el Centro Nacional de Inteligencia. En el Análisis de Riesgos para la Seguridad Nacional 2019/2022 han participado ciento dieciséis expertos provenientes de la Administración, del sector privado y de los campos de la ciencia y la investigación. El informe fue aprobado por el Consejo de Seguridad Nacional en su reunión de 4 de marzo de 2020.

SUMARIO

INTRODUCCIÓN

El Informe Anual de Seguridad Nacional se articula en torno a los quince ámbitos de actuación que contempla la Estrategia de Seguridad Nacional vigente aprobada en 2017.

Junto a sectores tradicionales, como la Defensa Nacional o la lucha contra el terrorismo, a los que ya se suma la ciberseguridad en cuanto elemento nuclear del hibridismo actual de la seguridad, se incluyen el espacio aéreo y ultraterrestre, las pandemias y epidemias y la preservación del medio ambiente, materias abarcadas por la Estrategia de 2017 y cuyo estado fue tratado por primera vez en el Informe Anual de 2017.

Todos estos ámbitos se abordan desde tres dimensiones complementarias: la tendencia de la evolución de cada materia, el estado de los retos y las realizaciones llevadas a cabo para hacerles frente mediante la cooperación interdepartamental, e incluso de otros actores competentes en la materia.

Se completa todo lo anterior con una novedad: un análisis de riesgos para la Seguridad Nacional 2019/2022 que se basa en la valoración informada y colectiva de una red de expertos funcionales. Este entorno de conocimiento cualificado se está construyendo alrededor de los profesionales especializados, representantes de departamentos ministeriales de la Administración General del Estado y otros organismos, que participan en el Sistema de Seguridad Nacional, a su vez articulado en torno al Consejo de Seguridad Nacional y sus órganos de apoyo.

Respecto del mapa de tendencias que se dibuja en el Informe, se trata de un enfoque iniciado en la edición anterior, que basándose en la evolución de los datos recogidos desde 2013, nos permite identificar muchos de los índices que impactan en el entorno de seguridad y su mutación.

Estos índices, en una suma agregada y perfilada, pueden operar como indicadores relevantes para el diseño de políticas públicas útiles, todo sobre la base de la anticipación, un principio rector de la Seguridad Nacional, y la prospectiva. Es la preparación del Estado ante los cam-

bios que acontezcan un elemento inherente a la política pública de Seguridad Nacional.

Los procesos de cambio más significativos y marcados se categorizaban ya en la Estrategia en sus dimensiones geopolítica, económica, social, tecnológica y medioambiental y se reflejan en el Informe en la pendiente de ascenso que han experimentado.

El entorno de seguridad es cada vez más complejo, enmarcado en un espacio global, el ciberespacio, que modifica las relaciones geopolíticas. El ritmo acelerado de su transformación, impulsado por la tecnología, sigue siendo una constante.

El incremento de la gravedad de las ciberamenazas, la mutación del terrorismo internacional, o las implicaciones de fenómenos que afectan tan directamente a la sociedad, como puede ser el cambio climático, son tres ejemplos que ilustran esta evolución del entorno de la seguridad.

Especial mención merecen las amenazas híbridas, uno de cuyos componentes es la desinformación, que mediante la manipulación de la información a través de Internet y las redes sociales provoca la polarización y radicalización de la ciudadanía, lo que demanda el refuerzo de capacidades para luchar contra los procesos de desinformación.

Se ha asentado la consolidación de la "zona gris" en el tablero de juego estratégico. La nueva normalidad registra con cotidianeidad operaciones de información, subversión, presión económica y financiera junto a acciones militares, para movilizar y llevar a posiciones de extremo a la opinión pública, y desestabilizar y desprestigiar a las instituciones que sustentan los regímenes políticos de las democracias liberales.

Las amenazas híbridas y la desinformación han sido elementos de atención prioritaria en 2019 de forma general, como vector de preocupación para la ciudadanía; y con carácter concreto, en lo que se refiere a la protección de la integridad de los procesos electorales europeos, nacional y autonómicos.

El *Plan de Acción de la Unión Europea contra la desinformación*, de diciembre de 2018, y los *procedimientos de protección de los procesos electorales y la actuación contra la desinformación,* aprobados el 15 de marzo de 2019 en el seno del Consejo de Seguridad Nacional, son iniciativas orientadas a reforzar las garantías para la continuidad de la normalidad democrática sin interferencias indebidas.

Los retos que se consignan en el Informe Anual repercuten tanto en los dominios materiales y geográficos, como en los funcionales de la seguridad. Se desarrollan pormenorizadamente respecto de las amenazas que socavan la Seguridad Nacional y los desafíos que abren horizontes de oportunidad y vulnerabilidad. Entre los primeros permanecen los conflictos armados, el terrorismo, el crimen organizado, la proliferación de armas de destrucción masiva, el espionaje, las ciberamenazas y las amenazas sobre las infraestructuras críticas. Y entre los segundos, se encuentran desafíos como la economía digital, la transformación energética, los espacios globales, marítimo y aeroespacial, los movimientos migratorios, los fenómenos meteorológicos extremos, la

salud y sus vectores de propagación y, por supuesto, el fenómeno del cambio climático.

El caleidoscopio de retos es múltiple y cambiante, pues se retroalimentan y mudan en su morfología, forma de manifestarse, probabilidad de ocurrencia e impacto.

La constante competición geo(tecno)política y la inestabilidad regional que vivifica los conflictos armados; la incesante amenaza del terrorismo internacional en sus distintas ramificaciones; la fuerza de intersección del crimen organizado con otras amenazas y desafíos; la carrera de armamentos que sigue en la agenda global; la agresividad de los servicios de inteligencia extranjeros contra objetivos estratégicos nacionales; o las complejas y sofisticadas ciberamenazas que recuerdan a diario que se está inevitablemente expuesto, máxime cuando comprometen las infraestructuras críticas que aseguran los servicios esenciales a la sociedad, son ejemplos del dilatado paisaje de las amenazas en 2019.

Y junto a lo anterior, la proliferación de estas amenazas en el dominio marítimo, donde encontramos buques dedicados al contrabando y los tráficos ilícitos, sin olvidar el proceso de degradación al que el ser humano somete a los mares por el uso indebido de su explotación. O el aéreo y ultraterrestre, que conoce un uso extendido, una eclosión, de aeronaves pilotadas remotamente y la militarización progresiva de su dominio.

También completan el cuadro de situación de la Seguridad Nacional la ralentización económica, los retos de la transición energética que trae aparejada oportunidades, el flujo de inmigración irregular que ha requerido un gran esfuerzo para disminuir la inmigración irregular con el debido respeto a los derechos humanos y poniendo especial énfasis en la inclusión, los cambios meteorológicos que acrecientan la probabilidad de emergencias y catástrofes, la lucha contra el cambio climático en un año, 2019, que fue el más cálido después de 2016, y la media de la temperatura global estuvo 1,1° C por encima de la era preindustrial, o los grandes retos para la salud pública.

Por lo que se refiere a los medios disponibles para hacer frente a las amenazas y desafíos de Seguridad Nacional, el Informe de 2019 es coincidente con los diagnósticos que se decantan de otras semblanzas anuales. España dispone de un excelente catálogo de capacidades que se deben mantener, pero también es necesario reforzar e incrementar en algunos campos donde existen carencias, como son el de Ciberseguridad, o el remplazo de capacidades militares en las que debe primar la industria nacional y la innovación tecnológica, siempre con la finalidad de estar mejor preparados y adaptados a las exigencias de seguridad. Esto implica también la capacitación de profesionales y la sensibilización de los ciudadanos. Y supone el reconocimiento de la profesionalidad de todos los actores comprometidos con vocación de servicio público en un desempeño de excelencia silente y discreta, no por esto invisible al proyecto compartido de edificar una sólida, robusta y resiliente Seguridad Nacional.

Para todo lo anterior, el Sistema de Seguridad Nacional se fundamenta en la premisa de la integración de medios, fusión de información y adopción de procedimientos y protocolos de trabajo útiles para pro-

mover sinergias, y dotar de coherencia y consistencia a la política de Seguridad Nacional que tiene vocación social y de servicio. En 2019 se avanzó en este proceso tanto en el desarrollo político-estratégico como en el de gestión de las situaciones de crisis que superan las competencias de un solo ministerio o Administración.

En 2019 se han aprobado cinco nuevas estrategias de segundo nivel: La Estrategia Nacional de Ciberseguridad, la Estrategia Nacional de Seguridad Aeroespacial, la Estrategia Nacional contra el Terrorismo, la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave y la Estrategia Nacional de Protección Civil.

Además, la arquitectura del Sistema de Seguridad Nacional se extiende de forma natural y progresiva. Tal y como está configurada, esta estructura funcional y orgánica, liderada por el Presidente del Gobierno, cuya piedra angular está constituida por el Consejo de Seguridad Nacional, se completará próximamente con dos nuevos órganos de apoyo: el Comité Especializado contra el Terrorismo y el Consejo Nacional de Seguridad Aeroespacial, que se unirán a los actualmente existentes próximamente.

El Comité de Situación ha impulsado el desarrollo del modelo integral de gestión de crisis, primer objetivo general establecido en la Estrategia de Seguridad Nacional 2017. Modelo de referencia en Europa como se puso de manifiesto en la primera reunión de asesores nacionales de seguridad con el Secretario General de la OTAN. Entre las iniciativas novedosas se encuentra la aprobación de la realización del primer ejercicio de gestión de crisis de Seguridad Nacional de ámbito nacional que inició su preparación en el segundo semestre de 2019 y que verá su culminación en abril de 2020. Dentro de las funciones asignadas al Comité de Situación, en 2019 se activó, a partir del día 10 de octubre y de manera preventiva, una célula de coordinación interministerial con la función de hacer seguimiento de los acontecimientos de inseguridad que se produjeron tras la Sentencia del Tribunal Supremo sobre los hechos acaecidos el 1 de octubre de 2017 en Cataluña.

Este Informe presenta por primera vez un análisis de riesgos para la Seguridad Nacional 2019/2022, un desarrollo analítico novedoso, que cuantifica el nivel de impacto y el grado de probabilidad de las amenazas a la Seguridad Nacional. Es un elemento que complementa las tendencias de los indicadores de seguridad. Este trabajo será útil para la revisión de la Estrategia de Seguridad Nacional en 2022. Este estudio ha sido confeccionado mediante una encuesta de percepción de amenazas y desafíos a la Seguridad Nacional, documento en el que han participado más de cien expertos procedentes de la Administración Pública, el sector privado, la academia y los centros de pensamiento.

El Informe Anual de Seguridad Nacional es un instrumento al servicio de la política pública de Seguridad Nacional. Su propósito es ofrecer una visión integral de los retos a los que nos enfrentamos y hacerlo con ambición constante de mejora en su planteamiento, como instrumento vehicular de una cultura de Seguridad Nacional cercana al ciudadano.

Este Informe es un ejercicio de cohesión de visiones por parte de todos los departamentos ministeriales, el Centro Nacional de Inteligencia y el

Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, que dirige y coordina su proceso de elaboración, con la intención que sirva para fomentar el debate público y la finalidad última de que sea presentado en la sede parlamentaria que ofrece la Comisión Mixta Congreso-Senado de Seguridad Nacional, cuya participación discursiva ahonda en la relevancia de una política pública de Seguridad Nacional de todos y para todos articulada en la cooperación leal.

ÁMBITOS DE LA SEGURIDAD NACIONAL: TENDENCIAS, RETOS Y REALIZACIONES

DEFENSA NACIONAL

OBJETIVO:

Asegurar la defensa de la soberanía e integridad de España y la protección de la población y el territorio frente a cualquier conflicto o amenaza proveniente del ámbito exterior, de forma autónoma o junto a socios y aliados. Asimismo, contribuir a crear un entorno internacional más estable y seguro mediante la proyección de estabilidad y el refuerzo de la cooperación con los socios, particularmente en las áreas de especial interés para España.

Tendencias

La principal tendencia en el periodo 2018-2019 es la consolidación progresiva de la contribución de España a la paz y seguridad internacionales en un contexto donde la relación entre sus dimensiones interior y exterior es cada vez más permeable.

España ha mantenido su firme compromiso con la solución pacífica de controversias por la vía multilateral

España ha mantenido en este periodo su firme compromiso con la solución pacífica de controversias por la vía multilateral a través de la promoción del papel protagonista de las organizaciones internacionales más importantes en el ámbito de la seguridad y la defensa, como la Organización de las Naciones Unidas (ONU), la Unión Europea (UE), la Organización del Tratado del Atlántico Norte (OTAN) y la Organización para la Seguridad y Cooperación en Europa (OSCE). Asimismo, ha participado en la Coalición Internacional contra el DAESH.

España se manifiesta como un socio fiable y comprometido mediante la participación en el exterior de las Fuerzas Armadas (FAS) en misiones y operaciones relacionadas con la disuasión y defensa y de apoyo a la lucha contra el terrorismo, así como a través del despliegue de efectivos de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) en misiones de gestión civil de crisis y de mantenimiento de la paz.

En el marco de la UE, una de las prioridades es el fomento de la autonomía estratégica. Los desarrollos de la Cooperación Estructurada Permanente (PESCO en sus siglas en inglés correspondientes a la denominación *Permanent Structured Cooperation*) y del *Plan de Acción Europeo de la Defensa*, facilitador financiero de la cooperación industrial europea, han seguido materializándose para consolidar la cooperación europea.

En lo que respecta a la OTAN, el año 2019 marcó el 70º aniversario del Tratado de Washington. En la reunión de líderes celebrada en Londres el 3 y 4 de diciembre de 2019, el Presidente del Gobierno señaló a la Alianza como un instrumento de consenso y cohesión para alcanzar la paz, la estabilidad y la seguridad en el área euroatlántica. La realidad geoestratégica o nuevos desafíos a la seguridad, como el cambio climático, son abordados en este seno desde una perspectiva de adaptación y transformación continua. (Figura 1-1)

La apuesta de España por el multilateralismo en el marco internacional se completa con una política de refuerzo de las capacidades nacionales de respuesta a las amenazas actuales en todos los niveles, que además de las FAS y FCSE, comprende a los Servicios de Inteligencia y la Diplomacia española.

Además, para España resulta prioritaria la seguridad humana y concede especial atención a la *Agenda Mujeres, Paz y Seguridad* como motor de transformación de las sociedades en conflicto. (Figura 1-2)

Figura 1-1
Proceso de adaptación de la OTAN

Fuente: Informe Anual del Secretario General de la OTAN, 2018

Figura 1-2
Resoluciones del Consejo de Seguridad de Naciones Unidas sobre "Mujeres, Paz y Seguridad"

Fuente: "Mujeres, paz y seguridad por una Agenda eficaz y sostenida", DSN 2019

Retos

La Estrategia de Seguridad Nacional 2017 identifica la persistencia de focos de inestabilidad en zonas próximas al territorio español, y particularmente en el continente africano y Oriente Próximo, como factor de especial afectación a la Seguridad Nacional.

La crisis en Libia ha puesto de manifiesto la fragmentación de la comunidad internacional y agudizado las rivalidades regionales. El proceso de diálogo político liderado por la Misión de Apoyo de las Naciones Unidas en Libia (UNSMIL), tras el inicio de la operación militar dirigida por Khalifa Hafter, en abril de 2019, permanecía bloqueado al finalizar el año. La toma de la ciudad de Sirte por el Ejército Nacional de Libia alteró la situación en el territorio libio y aumentó la presión sobre Trípoli. Rusia y Turquía incrementaron su influencia en el conflicto en detrimento del papel de la UE y Estados Unidos.

En 2019 ha continuado el deterioro de la situación de seguridad en el Sahel

En 2019, en línea con la tendencia de los últimos años, continúa el deterioro de la situación de seguridad en el Sahel, sobre todo en la zona de la triple frontera entre Mali, Níger y Burkina Faso. Pese a los esfuerzos internacionales, la iniciativa regional de seguridad del G5 Sahel enfrenta serios desafíos para mejorar la situación en la región. El firme compromiso de los países del Sahel occidental junto con una mayor asistencia internacional podría aportar resultados esperanzadores, así como contener la expansión de la amenaza a medio plazo.

En Oriente Próximo, la tensión sigue aumentando. Dos son las dinámicas más relevantes que afectan a la seguridad internacional en esta zona geográfica de especial interés estratégico: la evolución del siempre complicado equilibrio de poder entre los dos principales actores, Arabia Saudí e Irán, y la persistencia del conflicto en Siria.

La relación entre Arabia Saudí e Irán dibuja el contexto regional principal que influye en el bloqueo a Catar, la guerra en Yemen, el aumento de la intensidad de los enfrentamientos entre las minorías iraníes y las fuerzas de seguridad del país o la intermitente inestabilidad en Bahrein.

En Siria, el incremento de la influencia de Turquía y Rusia, unido a la disminución de la presencia estadounidense, han modificado la dinámica del conflicto. Turquía llevó a cabo tres operaciones militares en la frontera con Siria: las operaciones Escudo del Éufrates (2016), Rama de Olivo (2019) y Manantial de la Paz (2019). Tras la tercera ofensiva, la situación en la zona es de alta inestabilidad, algo que podría afectar a la seguridad del despliegue militar español en Turquía que contribuye al Plan Permanente de Defensa Aérea y Antimisil de la OTAN.

En su conjunto, el incremento de la tensión en la zona, y particularmente el deterioro de la situación entre Estados Unidos e Irán, aumenta la probabilidad de eventuales consecuencias concretas para los intereses españoles en la región, tales como el aumento de los precios del petróleo, los ataques a infraestructuras construidas o gestionadas por empresas españolas, acciones sobre contingentes militares españoles o la aparición y expansión de grupos radicales. El sector marítimo también se ve afectado. La seguridad del tráfico que transita por dos de las principales rutas de abastecimiento a nivel mundial, el golfo Pérsico, a través del estrecho de Ormuz, y la línea de comunicación marítima que

conecta el Mediterráneo con el océano Índico, es altamente vulnerable a eventuales incidentes en el mar.

Dos países de la región albergan precisamente los despliegues españoles en el exterior más numerosos (alrededor de mil doscientos efectivos): el Líbano, en la Fuerza Provisional de las Naciones Unidas para el Líbano (UNIFIL por sus siglas en inglés correspondientes a la denominación *United Nations Interim Force in Lebanon*); e Irak, en la Coalición Global contra el DAESH y la NATO Mission Irak (NMI).

En cuanto a la reconstrucción y estabilización de Afganistán, la seguridad de sus ciudadanos e instituciones supone uno de los mayores retos para los aliados de la OTAN y otros miembros de la comunidad internacional. El tercer trimestre de 2019 resultó especialmente violento. La Misión de Asistencia de las Naciones Unidas en Afganistán (UNAMA por sus siglas en inglés correspondientes a la denominación *United Nations Assistance Mission in Afghanistan*) expresó su grave preocupación por los niveles de violencia sin precedentes contra la población civil. La expansión progresiva del control territorial por parte de la insurgencia, y las negociaciones para la retirada de las tropas internacionales apuntan hacia una mayor presencia del movimiento talibán en las instituciones afganas. El reto será conseguir que este retorno se realice de manera consensuada con el resto de fuerzas y no conduzca a un deterioro de la situación.

En clave global, la postura cada vez más asertiva de Rusia, su presencia activa en Oriente Próximo, entendimiento con China, venta de misiles a Turquía y política en Siria representan un reto para Europa. Además, el uso de las nuevas tecnologías y técnicas de distribución de la información es un desafío al que hay que hacer frente y que guarda relación directa con nuevos modelos de conflicto. (Figura 1-3)

En otro orden de consideraciones y desde un punto de vista funcional, se identifican dos retos: alcanzar y mantener una capacidad de disuasión creíble y lograr una posición de mayor liderazgo en el sistema de seguridad internacional.

Con respecto al primer reto, se trata de ser capaces de hacer frente a cualquier amenaza o desafío que afecte a la Seguridad Nacional mediante la adquisición y el mantenimiento de las capacidades adecuadas. A tal fin resulta necesario disponer de un marco de financiación estable y progresivamente creciente, que permita mantener el esfuerzo actual de los medios desplegados en operaciones, tanto en el exterior como en las operaciones permanentes de carácter nacional. (Figura 1-4)

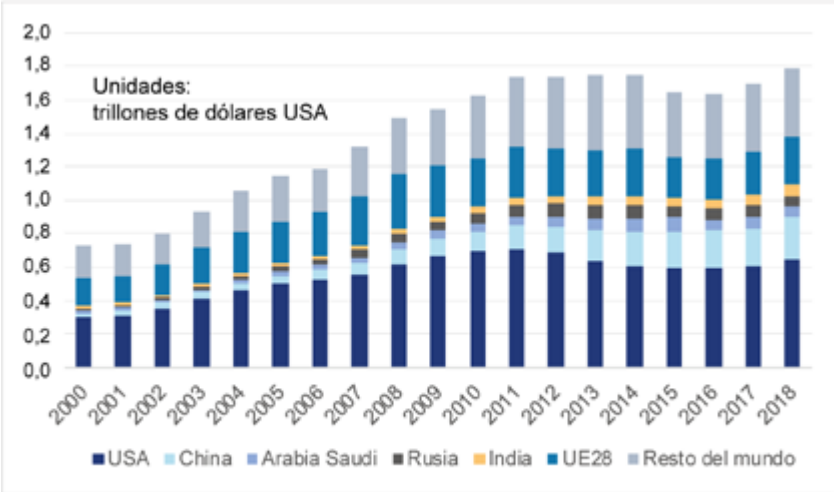
España está comprometida en mantener el impulso para la construcción de la Europa de la Defensa

En lo que respecta al mayor liderazgo en las organizaciones internacionales, España está comprometida en mantener el impulso para la construcción de la Europa de la Defensa en sus tres principales acciones: la participación en las misiones y operaciones de la Política Común de Seguridad y Defensa (PCSD), el Plan de Acción Europeo de la Defensa y la PESCO.

En el marco de la OTAN, resulta necesario preservar la unidad y cohesión interna de la propia organización, como foro fundamental para el diálogo transatlántico y elemento clave para la seguridad y estabilidad en Europa, uno de cuyos pilares fundamentales son los tratados de

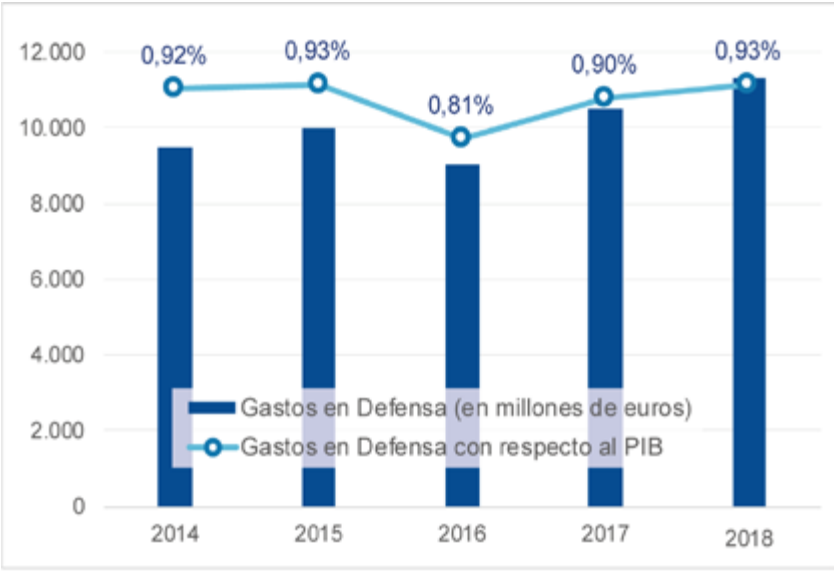
control de armamento y contra la proliferación de misiles. En ese sentido, sería clave renovar el Tratado de Reducción de Armas Estratégicas (START III por sus siglas en inglés correspondientes a la denominación *Strategic Arms Reduction Treaty)*, que vence en 2021, y sustituir al recientemente expirado Tratado sobre Fuerzas Nucleares de Rango Intermedio por otro acuerdo multilateral que necesariamente deberá tener en consideración a China, como actor global de creciente peso en la escena internacional.

Figura 1-3
Evolución del gasto en defensa a nivel mundial



Fuente: Instituto Internacional de Estudios para la Paz de Estocolmo (SIPRI)

Figura 1-4
Evolución del gasto en defensa en España 2014-2018



Fuente: Elaboración del DSN con datos del Ministerio de Defensa

Realizaciones

Se cumplen 30 años de la participación de España en misiones internacionales de paz y seguridad

Se cumplen 30 años de la participación de España en misiones internacionales de paz y seguridad. La contribución de más de 177.000 mujeres y hombres en despliegues fuera de las fronteras nacionales en este periodo es el mejor indicador de la firme y sostenida contribución a la construcción de un sistema internacional más seguro. También se cumplen 30 años de la caída del Muro de Berlín. Desde entonces, el mundo ha experimentado una transformación, por lo que las FAS y las FCSE se han visto obligadas a un proceso continuo de adaptación para hacer frente a los nuevas amenazas y desafíos a la Seguridad Nacional.

Capacidades de defensa autónoma y apoyo a la industria nacional

El Consejo de Ministros, en su reunión de 30 de noviembre de 2019, autorizó la suscripción de un convenio con la entidad NAVANTIA S.A., para el programa de desarrollo de las cinco fragatas F110 por un importe de 1.638 millones de euros en 7 años (de 2019 a 2025).

El programa de las fragatas F110 comporta un elevado contenido tecnológico y contribuye a la continuidad de la apuesta de la industria nacional por este sector. El programa supone una contribución al Producto Interior Bruto (PIB) español de 590 millones de euros anuales y un impacto de aproximadamente 7.000 empleos.

Por otra parte, cabe destacar la firma, el 17 de junio de 2019, del Acuerdo Marco que formaliza la entrada de España, junto a Alemania y Francia, en el programa del sistema de armas de siguiente generación en el seno del Futuro Sistema de Combate Aéreo *(New Generation Weapon System/Future Combat Air System)*.

En cuanto al proyecto del vehículo blindado VCR 8x8, desarrollado de forma íntegra en España, en 2019 se declaró desierta la licitación del contrato de suministro de los primeros 348 vehículos. Este hecho obliga a la redefinición del proceso contractual.

En materia de capacidades operacionales, en 2019 se certificó el avión A400M para el transporte de vehículos anfibios Piraña IIC y de helicópteros Cougar, mejorando significativamente el transporte estratégico y la capacidad de proyección de las FAS. Cabe recordar que, desde mediados de 2018, los helicópteros Cougar están desplegados en la operación *Inherent Resolve*, en Irak.

En 2019 tuvo lugar en Madrid la primera edición de la Feria Internacional de Defensa y Seguridad (FEINDEF 2019), apoyada institucionalmente por el Ministerio de Defensa en coordinación con la Administración General del Estado, la industria y las delegaciones oficiales.

Posición de España en el sistema de seguridad internacional

España ha mantenido su participación en todas las misiones internacionales comprometidas para este periodo en el seno de las organizaciones de seguridad en las que participa, un esfuerzo importante para los actores de la Seguridad Nacional dado el actual contexto presupuesta-

rio, que se justifica por el claro compromiso de España con la respuesta colectiva al diagnóstico y tratamiento de los conflictos.

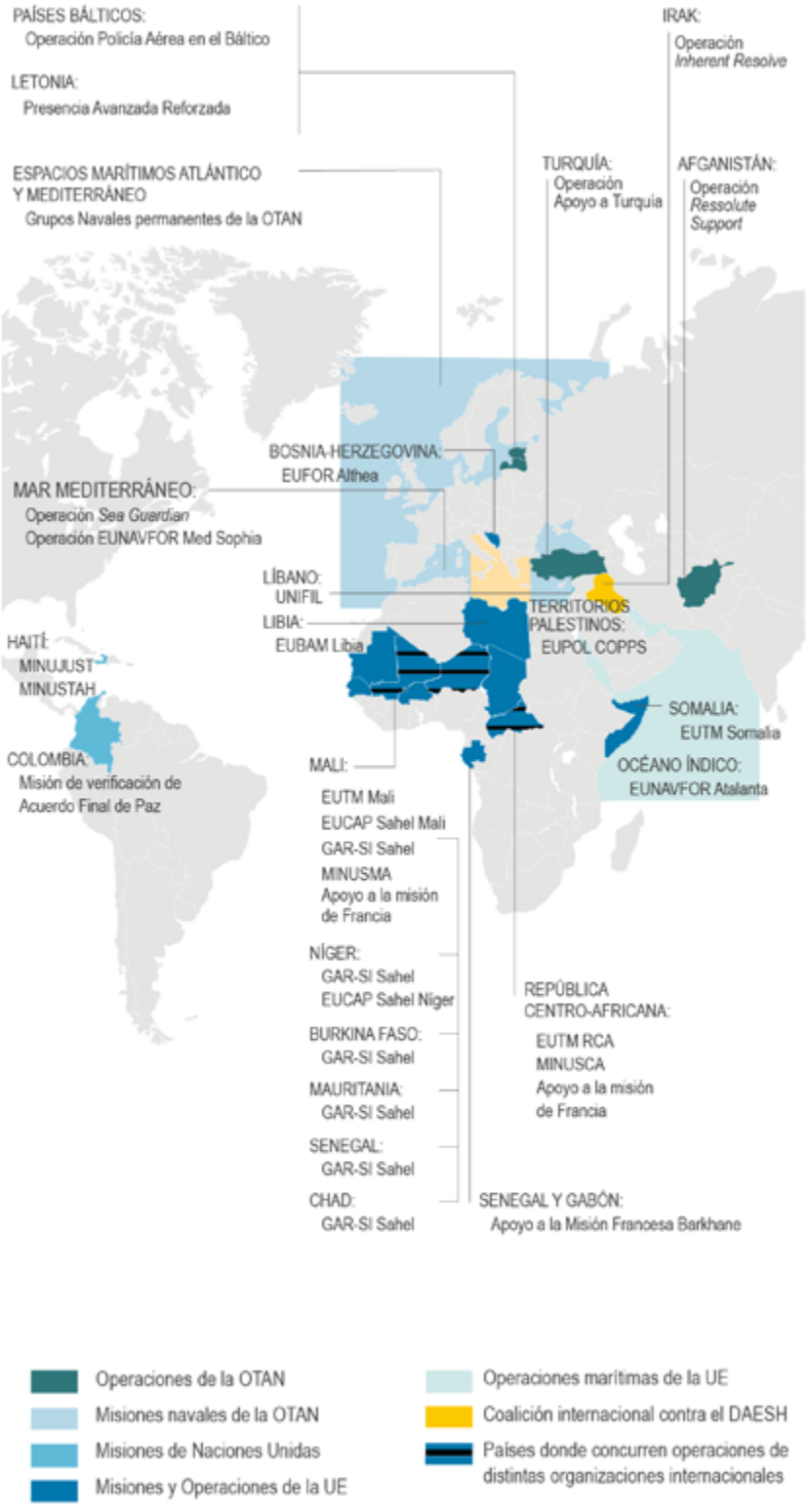
Las operaciones y misiones de gestión de crisis y para proporcionar estabilidad y seguridad en las que han participado las FAS, las FCSE y personal español de otros organismos, se han desarrollado en Bosnia-Herzegovina (operación *Althea*), Kosovo (*EULEX Kosovo*, misión civil de la PCSD), Georgia (*EUMM Georgia*, misión civil de la PCSD), Ucrania (*EUAM Ucrania*, misión civil de la PCSD), Colombia (donde un oficial general español ocupa el puesto de asesor militar principal del Representante Especial del Secretario General para la misión de verificación de Naciones Unidas), Libia (*EUBAM Libia*, misión civil de gestión de crisis de la PCSD), Líbano (*Libre Hidalgo*, de la Fuerza Provisional de Naciones Unidas), Macedonia del Norte (misión de la OSCE), Malí (*MINUSMA*, de Naciones Unidas, *EUTM Mali* y *EUCAP Sahel Mali*, misión civil de la PCSD, *Operación Marfil* de apoyo a Francia), Níger (*EUCAP Sahel Niger*), República Centroafricana (*MINUSCA* y *EUTM RCA*), Somalia (*EUTM Somalia* y *EUCAP Somalia*, misión civil de la PCSD), Senegal y Gabón (desde los destacamentos aéreos de apoyo a la misión francesa *Barkhane*, a las misiones de Naciones Unidas y la UE en Mali y RCA y a la Fuerza Conjunta G5 Sahel), en los Territorios Palestinos (*EUPOL Copps*), en el océano Índico (*EUNAVFOR Atalanta*) y el mar Mediterráneo (*EUNAVFOR Med Sophia*). (Figuras 1-5, 1-6 y 1-7)

Por otro lado, el 15 de octubre de 2019 concluyó su mandato la Misión de Apoyo a la Justicia en Haití (*MINUJUST*), sucesora a su vez de la Misión de Estabilización de las Naciones Unidas en Haití (*MINUSTAH*), poniendo fin a quince años consecutivos de presencia de la ONU en ese país, a la que España ha contribuido consecutivamente con efectivos de sus FAS y FCSE.

Dentro del proyecto europeo multinacional GAR-SI Sahel (por sus siglas en francés correspondientes a la denominación *Groupes d'Action Rapides – Surveillance et Intervention au Sahel*), liderado por la Guardia Civil, en colaboración con la Gendarmería Nacional Francesa, la Guardia Nacional Republicana de Portugal y el Arma de Carabinieri de Italia, y que tiene como finalidad contribuir a la estabilización de la zona del Sahel mediante la creación de unidades policiales robustas en todos los países del G5 Sahel (Malí, Mauritania, Chad, Níger y Burkina Faso) y Senegal, cabe señalar que en 2019 finalizó la fase de formación (810 efectivos). Actualmente, todas las unidades están operativas, salvo la del Chad que se encuentra en periodo de monitorización. Se obtuvieron los primeros resultados operativos, como la incautación de armamento ilegal, explosivos y drogas, entre otros.

En cuanto a las operaciones de lucha contra el terrorismo, se encuentran la operación *Inherent Resolve* de la Coalición Internacional contra el DAESH, en Irak, la operación *Resolute Support* en Afganistán y la operación *Sea Guardian*, en el Mediterráneo.

Las operaciones de disuasión y defensa en las que España participa son el despliegue de fuerzas terrestres en los países Bálticos y Polonia a través de la iniciativa de Presencia Avanzada Reforzada de la OTAN (apoyo al flanco Este de la Alianza en Letonia), y la contribución de la OTAN a la defensa antimisil de Turquía. Todo ello se complementa con el despliegue de fuerzas navales permanentes con especial interés en



Fuente: Elaboración del DSN con datos del Ministerio de Defensa

Figura 1-5
Misiones y operaciones en el exterior en 2019

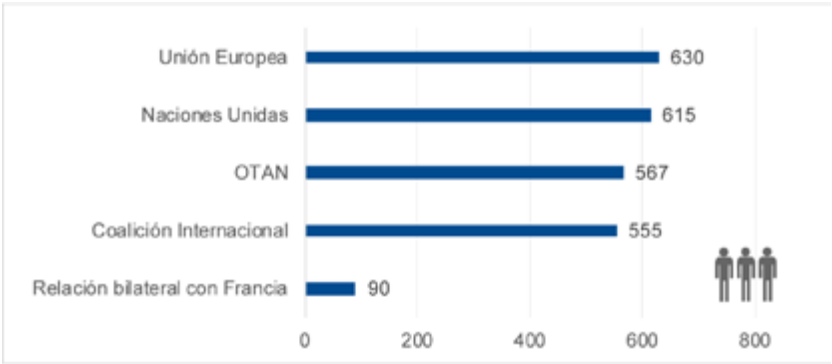
los mares Báltico, Negro y Mediterráneo. De forma periódica, se participa en la misión de policía aérea de los países Bálticos.

Se mantienen además esfuerzos dirigidos a las actividades bilaterales de seguridad cooperativa (Senegal, Mauritania, Túnez, Cabo Verde) y cooperación militar (otros países del norte de África y golfo de Guinea) en el marco de la diplomacia de Defensa.

Dentro del compromiso de España con la paz, la seguridad humana y la protección de los sectores más vulnerables de la población en zonas de conflicto, se ha realizado un intenso esfuerzo en apoyo a las Resoluciones del Consejo de Seguridad de las Naciones Unidas sobre "Mujeres, Paz y Seguridad" (1325) y "Lucha contra la Explotación y el Abuso Sexual" (2272), así como a la iniciativa "Escuelas Seguras".

El esfuerzo que España realiza en el ejercicio de su compromiso con los países y aliados internacionales a través de las FAS y las FCSE se complementa con el trabajo activo de los Servicios de Inteligencia en la identificación de retos y tendencias, el asesoramiento a la toma de decisión por parte de las autoridades políticas y el apoyo directo al personal español desplegado en la zona.

Figura 1-6
Número de efectivos de las Fuerzas Armadas desplegados en operaciones en el exterior en 2019



Fuente: Ministerio de Defensa

Figura 1-7
Operaciones de las Fuerzas Armadas en el exterior en 2019

OPERACIÓN MILITAR	
EUFOR ALTHEA	UE
EUTM SOMALÍA	UE
EUTM MALI	UE
EUNAVFOR ATALANTA	UE
EUNAVFOR MED SOPHIA	UE
EUTM RCA	UE
RESOLUTE SUPPORT	OTAN
SEA GUARDIAN	OTAN
PRESENCIA AVANZADA EN LETONIA (EFP)	OTAN
A/T APOYO A TURQUÍA	OTAN
GRUPOS NAVALES PERMANENTES DE LA OTAN	OTAN
NMI IRAK	OTAN
POLICÍA AÉREA DEL BÁLTICO (BAP)	OTAN
LIBRE HIDALGO	ONU
MONITORIZACIÓN NNUU ACUERDO DE PAZ COLOMBIA	ONU
APOYO MALI	
APOYO REPÚBLICA CENTRO AFRICANA	

Fuente: Ministerio de Defensa

Protagonismo activo en la PCSD, compromiso con la OTAN y colaboración internacional con Estados Unidos

España se mantiene en el núcleo duro de los Estados miembros en el desarrollo de la PCSD

España se mantiene en el núcleo duro de los Estados miembros en el desarrollo de la PCSD, tanto respecto de su formulación, como en lo que concierne a su vertiente práctica, como demuestra la continuación de la participación española en la PESCO liderando el proyecto de "Sistema Aéreo de Protección Electrónica Activa (AEA)" y participando en otros siete dentro de los nuevos trece aprobados en 2019. (Figura 1-8)

El Grupo de Combate de la UE (EUBG por sus siglas en inglés correspondientes a la denominación *European Union Battle Group*) constituye una de las herramientas de respuesta rápida de la UE capaz de llevar a cabo operaciones de forma independiente o también la fase inicial de operaciones de más envergadura. Con un elevado nivel de disponibilidad (5-10 días), el EUBG puede desplegarse en cualquier zona con un radio máximo de acción estimado de 6.000 kilómetros desde Bruselas.

España ha liderado el EUBG durante el primer semestre de 2019. Aportó la estructura de mando y control, un grupo de combate terrestre, un grupo de helicópteros, un grupo de operaciones especiales, una fuerza anfibia y otros apoyos en los ámbitos aéreo y naval. El Ejército de Tierra aporta la mayor parte de las capacidades y personal en los Cuarteles Generales. También contribuyen con capacitadores la Armada Española, el Ejército del Aire, la Unidad Militar de Emergencias (UME)y la Guardia Civil. Además, la UE dispondrá de otro EUBG en alerta, liderado en este caso por Francia.

Es de destacar que, desde 2004, la Guardia Civil forma parte de la Fuerza de Gendarmería Europea, organización multinacional capaz de realizar funciones policiales de gestión de crisis en zonas de conflicto. Esta organización, que puede actuar bajo mando militar o de una autoridad civil, es una herramienta europea idónea para contribuir al desarrollo de la PCSD y poder garantizar la seguridad y mantener el orden público en operaciones de gestión de crisis.

En el ámbito de la OTAN, se realiza una importante contribución nacional a las Fuerzas de Respuesta Mejorada (eNRF en sus siglas en inglés correspondientes a la denominación *Nato Response Force*), en particular a la Fuerza Conjunta de Muy Alta Disponibilidad (VJTF en sus siglas en inglés correspondientes a la denominación *Very High Readiness Joint Task Force*), así como a las operaciones de seguridad marítima en el Mediterráneo. Durante este periodo España mostró también su compromiso aportando un significativo paquete de capacidades a la nueva iniciativa de la OTAN denominada *NATO Readiness Initiative* (NRI). Por otra parte, España lidera la creación de las unidades de operaciones especiales de Túnez, en el marco del *Planning and Review Process* (PARP), proceso que se extenderá hasta el 2021.

Desde agosto de 2015, la Guardia Civil participa en el Centro de Excelencia OTAN de Policía de Estabilización (NATO *Stability Policing Centre of Excellence*), organismo militar de la OTAN, con estatus de organización internacional, que tiene por objeto proveer a la OTAN y a sus Estados miembros de capacidades en materia de policía de estabilidad, que comprenden el conjunto de actividades policiales realizadas con el

objetivo de establecer un entorno seguro y estable, así como de mantener el orden público en zonas en conflicto.

La Guardia Civil ha continuado participando en el *Regional Hub South* de la OTAN, en Nápoles (Italia), ocupando un puesto de especial relevancia, como es el de *Police Advisor* del Jefe del Cuartel General. Esta estructura, encuadrada en el Cuartel General Conjunto de la OTAN, concentra capacidades para contribuir a la recolección, manejo y distribución de información, facilitar el seguimiento análisis y comprensión de amenazas, retos y oportunidades en el Sur y contribuir a la coordinación de las actividades aliadas en el flanco sur de la OTAN, centradas en luchar contra la inestabilidad, la amenaza terrorista y el resto de desafíos y crisis existentes, emergentes o potenciales provenientes del flanco sur de Europa.

Figura 1-8
Proyectos PESCO 2019

	Proyecto	Miembros del proyecto
1	Centro común europeo integrado de formación y simulación (Eurosim)	Hungría, Alemania, Francia, Polonia, Eslovenia
2	Centro de la Unión Europea para el mundo académico y la innovación en el ámbito del ciberespacio (UE CAIH)	Portugal, **España**
3	Centro de Formación Médica de las Fuerzas de Operaciones Especiales (SMTC)	Polonia, Hungría
4	Polígono de entrenamiento para la defensa ante ataques químicos, biológicos, radiológicos y nucleares (QBRN) (CBNDTR)	Rumanía, Francia, Italia
5	Red de Centros de Buceo de la Unión Europea (EUNDC)	Rumania, Bulgaria, Francia
6	Sistema Marítimo no Tripulado Antisubmarinos (MUSAS)	Portugal, **España**, Francia, Suecia
7	Corbeta Europea de Patrulla (EPC)	Italia, Francia
8	Sistema Aéreo de Protección Electrónica Activa (AEA)	**España**, Francia, Suecia
9	Centro de coodinación del ámbito del ciberespacio y de la información (CIDCC)	Alemania, Chequia, **España**, Hungría, Países Bajos
10	Alerta rápida e interceptación con vigilancia espacial de los teatros de operaciones (TWISTER)	Francia, **España**, Italia, Países Bajos, Finlandia
11	Materiales y componentes para la competitividad tecnológica de la UE (MAC-UE)	Francia, **España**, Rumanía
12	Capacidades militares colaborativas de la UE (ECoWAR)	Francia, Bégica, **España**, Hungría, Rumanía, Suecia
13	Sistema de arquitectura europea global de integración en materia de Sistemas de Aeronaves Pilotadas a Distancia (RPAS)	Italia, Francia, Rumanía

Fuente: Diario Oficial de la Unión Europea. 14.11.2019

LUCHA CONTRA EL TERRORISMO

OBJETIVO:

Neutralizar la amenaza que representa el terrorismo contra los ciudadanos y los intereses españoles dentro y fuera de las fronteras, reduciendo la vulnerabilidad de la sociedad y haciendo frente a los procesos de radicalización violenta.

Tendencias

El terrorismo yihadista sigue constituyendo una amenaza persistente y real para España

El terrorismo yihadista sigue constituyendo una amenaza persistente y real para España. Frente a la decadencia estructural del DAESH, con la pérdida de territorio en la zona de Siria e Irak y la muerte de su líder Al-Baghdadi en 2019, hay que considerar el contrapunto que supone la adhesión al DAESH de grupos yihadistas de carácter local, el asentamiento en Libia, el incremento de la amenaza terrorista en el Sahel, Oriente Próximo y el sudeste asiático y la persistente amenaza de Al Qaeda y sus franquicias de carácter local. Las organizaciones terroristas yihadistas están adaptándose al nuevo escenario, constituidas en estructuras cada vez más horizontales y en red, en detrimento de formaciones verticales o jerárquicas. (Figura 2-1)

En este contexto, por lo que respecta al DAESH, no se prevé que su nuevo líder, Abu Ibrahim al-Hashimi al-Quraisi, suponga un cambio en sus planteamientos. Se estima que continúe su actividad criminal en el escenario sirio-iraquí y que se acentúe el tránsito de combatientes entre escenarios de yihad. En territorio sirio, el anuncio de retirada de las tropas de Estados Unidos y la ofensiva turca en el noroeste del país han contribuido a incrementar la incertidumbre sobre la evolución de la situación, así como a generar una nueva crisis humanitaria y migratoria en una región ya desestabilizada. (Figura 2-2)

La pérdida del control territorial del DAESH en Siria e Irak y su consolidación como insurgencia, conlleva algunos cambios significativos en la lucha contra el terrorismo internacional que se producirán a corto plazo, centrados principalmente en el eje Irak-Afganistán, donde, en línea con los esfuerzos de la Coalición Internacional contra el DAESH, ya se está llevando a cabo una redistribución de los esfuerzos entre las correspondientes áreas de operaciones.

España mantiene y prioriza sus esfuerzos en la región del Sahel

Las acciones terroristas se están incrementando en el Sahel y norte de África, entre otras circunstancias, por la debilidad de sus estructuras estatales. En el Sahel, la creciente inestabilidad de países como Mali, Chad, Níger o Burkina Faso, así como la permeabilidad existente en sus fronteras, favorece la expansión de grupos terroristas y el tráfico ilegal de personas, utilizado a su vez por estos como medio de financiación, con consecuencias directas para España, debido a su proximidad con el continente africano. Por este motivo, España mantiene y prioriza sus esfuerzos en esta región.

Por su parte, Al-Qaeda, que con el surgimiento del DAESH perdió el liderazgo de la llamada yihad global, ha mantenido inalterables sus planteamientos, buscando infligir a Occidente el mayor daño posible con la ejecución de ataques terroristas de gran impacto que requieren una mayor planificación. A su vez, ha materializado su actividad terrorista a través de las diversas ramas locales con las que cuenta, entre las que destaca Al-Qaeda en el Magreb Islámico (AQMI) por su potencial relevancia contra los intereses españoles en el Magreb-Sahel.

Todas estas circunstancias han creado una mayor conciencia sobre la necesidad de hacer de la cooperación el auténtico motor para la mitigación de la amenaza, tanto en el seno de la comunidad de Inteligencia internacional, como en las operaciones internacionales en el marco de la OTAN o la UE. En este aspecto la cooperación europea está consiguiendo debilitar la capacidad de las organizaciones terroristas para actuar fuera de su zona de influencia, lo que no descarta que se puedan producir actos llevados a cabo por los denominados *Homegrown Terrorist Fighters*, individuos crecidos en algún país occidental que, previamente radicalizados, atacan en su propia área de residencia.

En Europa, aunque inicialmente algunos ataques tuvieron algún tipo de vinculación con el exterior, bien fuera por la experiencia yihadista de los autores o por el apoyo recibido desde zonas de yihad, al dañarse significativamente las capacidades del DAESH para atentar fuera del autodenominado "califato", se ha producido un incremento de células autóctonas y actores solitarios autoradicalizados, que operan principalmente sin contacto o dirección por parte del DAESH.

En ocasiones, estas células autóctonas han sido capaces de desarrollar sus propios explosivos, recurriendo a materiales comerciales disponibles y a la formación a través de vídeos tutoriales que circulan por la red, pero en la mayoría de los casos continúan empleando medios no sofisticados, de reducido coste económico y de fácil acceso en el mercado. El fin principal de sus actos violentos sigue siendo generar inseguridad en la sociedad, por lo que sus objetivos potenciales son las fuerzas y cuerpos de seguridad, el personal militar y la población civil.

Aún persiste el riesgo del retorno de Combatientes Terroristas Extranjeros desde las zonas en conflicto, con el factor añadido de la convulsa situación en el norte de Siria, así como el de sus familiares e hijos, que representan un reto para los países de origen, pero también el riesgo de radicalización en centros penitenciarios de otros internos y la posible activación de terroristas autónomos tras los continuos llamamientos a atentar contra Occidente.

Mención especial merece el empleo por los grupos terroristas de las redes sociales y la creación de aparatos profesionales de propaganda que contribuyen al adoctrinamiento y al reclutamiento de combatientes, a la formación en técnicas, tácticas y procedimientos y a inspirar ataques en los países de origen o residencia de los terroristas (en lo que se conoce como califato virtual). En este sentido, una tendencia clara es el aumento progresivo de la propaganda terrorista en español orientada a incitar ataques terroristas.

El aumento progresivo de la propaganda terrorista en español es una tendencia clara

Se considera que en los próximos años el terrorismo yihadista mantendrá su actividad en redes sociales y el ciberespacio, y seguirá suministrando información para la fabricación artesanal de explosivos y el empleo de nuevas tecnologías, entre las que es previsible que los vehículos no tripulados ocupen un papel destacado.

Asimismo, continuará la ejecución de atentados sobre objetivos blandos (aquellos accesibles y con poca o ninguna capacidad de respuesta), llevando a cabo acciones no complejas mediante el empleo de medios de circunstancia.

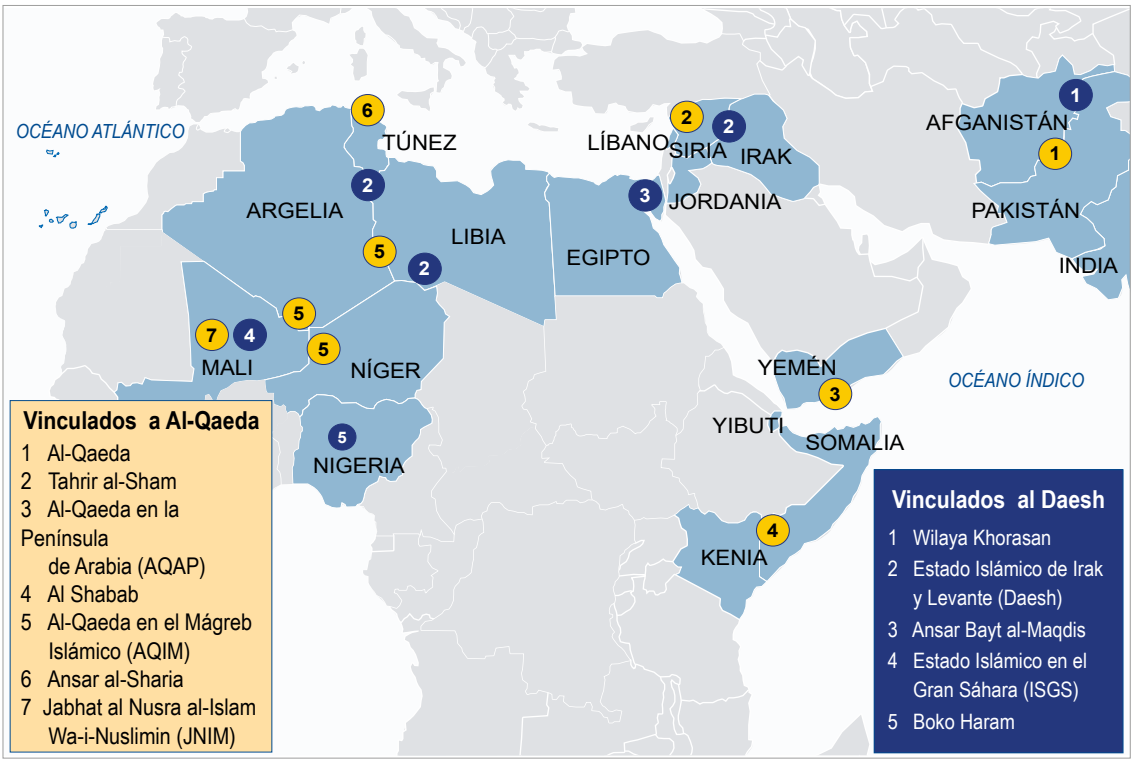
Desde el punto de vista de la financiación, esta ha evolucionado sustancialmente desde los atentados del 11-S cuando existían movimientos de fondos de cierta relevancia a través del sistema financiero internacional. En contraste, los recientes ataques en Europa, la mayoría de escasa planificación y dificultad, han necesitado poco respaldo económico para su ejecución.

Los grupos yihadistas suelen operar a través de pequeñas células que se autofinancian, obteniendo sus fondos en España o en países cercanos, sin necesidad de contar con el apoyo de la matriz del grupo terrorista. Generalmente, estas células utilizan cantidades económicas pequeñas para su funcionamiento y actividades, siguiendo un sistema de microfinanciación, tratando de evitar el sistema financiero formal. Algunos de los procedimientos utilizados son el envío de remesas, las donaciones a entidades con fines supuestamente humanitarios o el sistema *hawala* (un sistema para enviar dinero de un lugar a otro sin que exista un movimiento físico de fondos).

Respecto del número de detenidos en España en el ámbito del terrorismo yihadista, en 2019 se recuperó la tendencia al alza que se venía observando entre 2015 y 2017 y que en 2018 experimentó un considerable descenso.

En relación con el terrorismo nacional, las actuaciones policiales y judiciales están consolidando cada vez más la desarticulación efectiva de organizaciones como Resistencia Galega o GRAPO, mientras que el terrorismo de corte anarquista sigue siendo residual. Al mismo tiempo, continúan los esfuerzos en la investigación de atentados con víctimas mortales cometidos por ETA (*Euskadi Ta Askatasuna*) y que permanecen sin resolución judicial.

Figura 2-1
Principales grupos yihadistas vinculados al Daesh y a Al-Qaeda



Fuente: Elaboración del DSN

Figura 2-2
Presencia del Daesh en Siria e Irak en 2019

Fuente: Elaboración del DSN con datos del Servicio Europeo de Acción Exterior

Retos

En enero de 2019 el Consejo de Seguridad Nacional aprobó la nueva *Estrategia Nacional contra el Terrorismo* (*ENCOT*). La *ENCOT* es el documento marco a partir del cual se desarrollan líneas de acción y planes específicos para la lucha contra el terrorismo. Entre esos planes, cuyo reto consiste en su desarrollo efectivo y pleno, cobran especial relevancia los planes de prevención de la radicalización violenta, protección antiterrorista y lucha contra la financiación del terrorismo. (Figura 2-3)

En 2019 el Consejo de Seguridad Nacional aprobó la nueva Estrategia Nacional contra el Terrorismo

La amenaza terrorista, especialmente la de naturaleza yihadista, está asociada a factores inestables, volátiles, que requieren una reacción rápida. La utilización de medios poco sofisticados en los ataques terroristas, los rápidos procesos de paso a la acción de los radicalizados y el riesgo de emulación de atentados, así como las consecuencias de los cambios geoestratégicos en zonas de conflicto, son solo algunos de los indicadores de la transformación del fenómeno terrorista, que obligan a una continua adaptación de dispositivos de seguridad, sistemas de alerta y detección temprana, medidas preventivas y líneas de acción de la lucha contra el terrorismo.

El desarrollo de los Reglamentos relativos al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración, hará posible la búsqueda simultánea en varios sistemas de información y facilitará la detección de las alertas incluidas en ellos, a través de una única consulta de impresiones dactilares e imágenes faciales (datos biométricos).

Uno de los retos más significativos es la identificación y neutralización de los actores solitarios en las fases inmediatamente previas a que se realice el ataque. Por ello, el Centro Nacional de Inteligencia (CNI) y las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) trabajan en la mejora de sus procedimientos para permitir la correcta identificación de posibles actores solitarios y la detección precoz de vectores de comportamiento, pudiendo así actuar antes de que se cometa un acto terrorista.

Además, el previsible retorno de los combatientes europeos y de sus familias (desde Siria e Irak), pondrá a prueba los sistemas de alerta temprana que se han ido implementando en Europa con este fin. El seguimiento de la actividad de los simpatizantes de los grupos terroristas en el Magreb y el retorno de los combatientes de esta zona será un elemento de constante atención por el impacto que puede tener en España.

También los "viajeros frustrados", individuos que tenían la intención y determinación de viajar a alguna de las zonas de conflicto pero que por distintos motivos no lo hicieron se convierten en un foco de amenaza para los intereses españoles. La progresiva puesta en libertad de condenados por delitos de terrorismo o presos comunes radicalizados en prisión constituye otro foco de riesgo, habiéndose detectado casos de individuos que, tras cumplir su condena, continúan manifestando su adhesión a la ideología yihadista.

Fuera del territorio nacional, Siria e Irak seguirán siendo objeto de atención, no solo por el posible retorno de combatientes, sino porque la evolución de la situación en el terreno va a definir modelos de actuación de Al-Qaeda y del DAESH. Ambos grupos tienen una agenda internacional que se verá afectada por la evolución de los acontecimientos. La detección de sus relaciones con simpatizantes en Europa o del envío de terroristas para la ejecución de atentados serán un reto de primera magnitud.

En ciertos países del Sahel y el Magreb, la defensa de intereses españoles, ya sean empresas o personas españolas desplegadas en el terreno, requerirá que España fomente más apoyo y coordinación por parte de las autoridades locales. Libia y Mali seguirán siendo los focos de desestabilización más importantes.

En este sentido, continuará el esfuerzo de las Fuerzas Armadas (FAS), la Guardia Civil y el CNI en la lucha contra el terrorismo global en operaciones de asistencia militar en el exterior, aumentando así la capacidad de los países para combatirlo.

Es necesario adoptar una actitud proactiva para desmontar las falsedades del mensaje radical

En términos de la lucha contra el radicalismo violento, la coordinación y cooperación institucional, el enfoque multidisciplinar, la comunicación estratégica y el compromiso de la sociedad son objetivos fundamentales. Es necesario adoptar una actitud proactiva para desmontar las falsedades del mensaje radical que impide la integración y la convivencia. Como resultado de estas preocupaciones, el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), perteneciente al Ministerio del Interior, con la participación de diversos departamentos ministeriales y organismos implicados, está trabajando en el desarrollo de un Plan Nacional de lucha contra la Radicalización Violenta. La eliminación de la propaganda terrorista en la red es un elemento ineludible en la prevención de la amenaza terrorista, que seguirá demandando un importante esfuerzo en la dotación de personal y de capacidades técnicas.

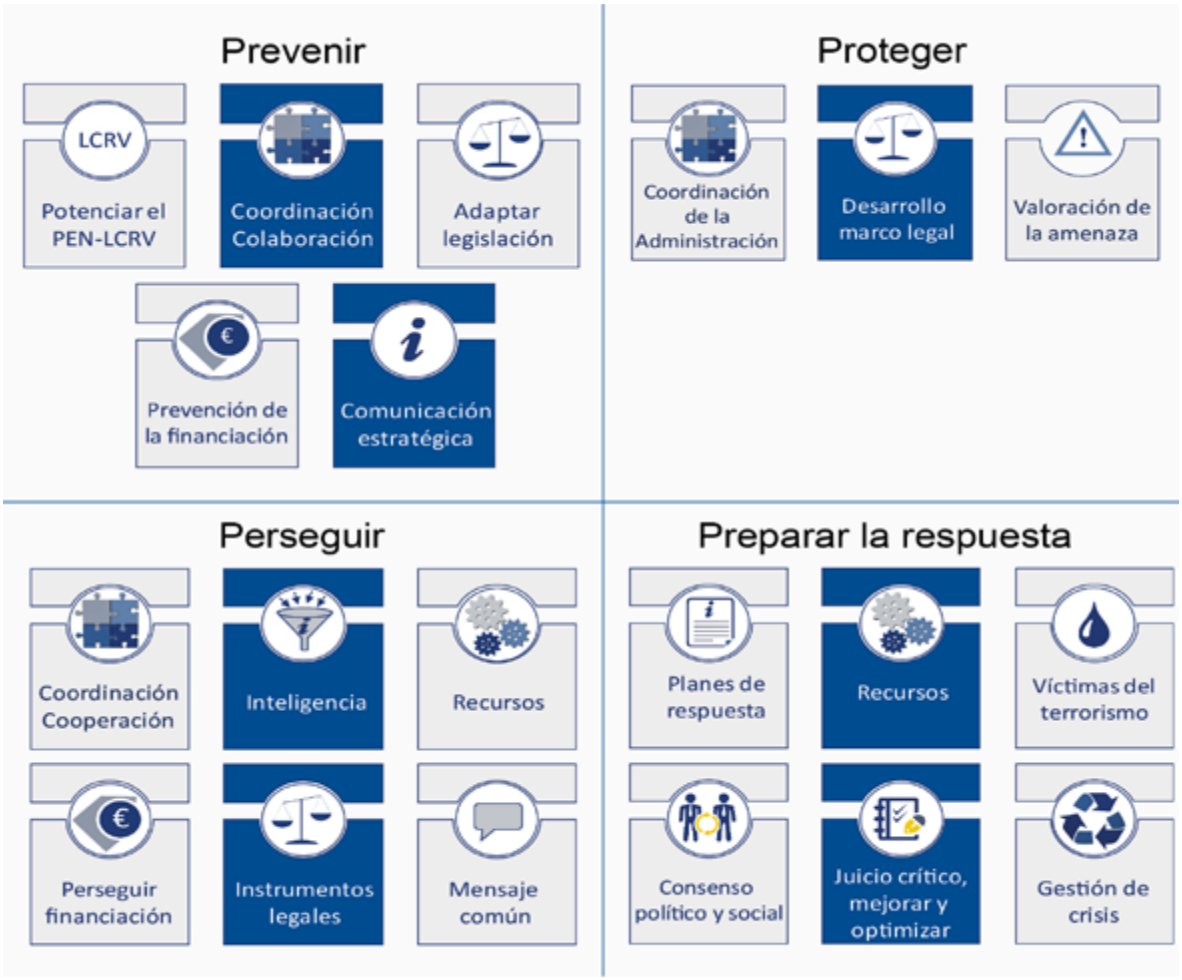
También es importante establecer cauces nacionales para la cooperación en materia de terrorismo entre la Dirección Adjunta de Vigilancia Aduanera y las FCSE durante el desarrollo del análisis de riesgo de seguridad de las mercancías. En este sentido se han realizado varias reuniones con el CITCO encaminadas a encontrar fórmulas para una colaboración efectiva en la identificación de envíos de mercancías que pudieran tener relación con objetivos terroristas.

Asimismo, la identificación e implementación de reglas de riesgo AVSEC (por sus siglas en inglés correspondientes a la denominación *Aviation Security Committee*) sobre la declaración PLACI (por sus siglas en inglés correspondientes a la denominación *Pre-loading Advance Cargo Information*) encaminada a la identificación de mercancías que pudieran contener artefactos explosivos en aviones (*bomb in a box*) constituye un reto para las aduanas y los cuerpos policiales con competencias en la materia.

En términos de financiación, es importante mantener operativos y profundizar en los mecanismos para la prevención, detección y control de los flujos financieros relacionados con la financiación del terrorismo, en línea con las Resoluciones del Consejo de Seguridad de Naciones

Unidas y los Reglamentos de la UE. En este sentido, las dificultades en la aplicación directa e inmediata de las Resoluciones de Naciones Unidas han puesto de manifiesto la necesidad de una reforma de la actual *Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo*. Uno de los aspectos más relevantes de dicha reforma será la necesaria inclusión para tareas de prevención de nuevos sujetos obligados, especialmente en el contexto del fenómeno *fintech* (industria financiera que aplica nuevas tecnologías a actividades financieras y de inversión) y del uso de activos virtuales.

Figura 2-3
Pilares de la Estrategia Nacional contra el Terrorismo 2019



Fuente: Estrategia Nacional contra el Terrorismo 2019

Realizaciones

El Consejo de Seguridad Nacional aprobó la *ENCOT* el 21 de enero de 2019, marco estratégico de la lucha contra el terrorismo en España. En su elaboración han participado además del Ministerio del Interior, el CNI, los ministerios de Defensa, Asuntos Exteriores, Unión Europea y Cooperación, Justicia, así como el Departamento de Seguridad Nacional (DSN) del Gabinete de la Presidencia del Gobierno.

Siguiendo el criterio establecido en la *Estrategia de Seguridad Nacional* 2017 para la lucha contra el terrorismo, la *ENCOT* se apoya en cuatro pilares básicos: prevención, protección, persecución y preparación de la respuesta. Además, contempla como líneas prioritarias, el reforzamiento de la actuación preventiva en el ámbito local a partir de una aproximación multilateral, la formación de los distintos actores implicados, el control y la supervisión de manera concertada de los individuos radicalizados, la coordinación efectiva de la persecución de terroristas y sus redes de apoyo, la cooperación internacional y la sensibilización del conjunto de instituciones y la sociedad civil.

Además, el CITCO, con la participación de diversos departamentos y organismos ministeriales, está trabajando en un Plan Nacional de lucha contra la Radicalización Violenta y otro Plan Nacional contra la Financiación del Terrorismo.

Prevención

El Nivel de Alerta Antiterrorista en España en 2019 se ha mantenido en un Nivel 4 sobre 5

El Nivel de Alerta Antiterrorista en España durante todo el 2019 se ha situado en un Nivel 4 (riesgo ALTO) sobre 5 (riesgo MUY ALTO), vinculado al riesgo derivado de manera fundamental de la amenaza yihadista. Paralelamente, este nivel de riesgo 4 se ha visto reforzado con medidas especiales de seguridad en cinco ocasiones, con motivo de acontecimientos diversos en cuyo marco se había apreciado un incremento del nivel de la amenaza. En general, se ha tratado de refuerzos puntuales de medidas de seguridad, incorporando a las mismas las capacidades de las Policías Autonómicas, los Cuerpos de Policía Local y del personal y empresas de Seguridad Privada en virtud de los mecanismos de colaboración y coordinación contemplados en el Ordenamiento Jurídico.

España contribuye a la prevención del terrorismo a través de su implicación en misiones y operaciones en el exterior, enfocadas al fortalecimiento institucional y a la formación y capacitación de las fuerzas de seguridad locales, y en colaboración con los organismos y Servicios de Inteligencia locales.

El Magreb es la región con mayor impacto sobre España, dada su proximidad geográfica y la gran comunidad magrebí residente en el país. Las desarticulaciones de células terroristas en el norte de Marruecos, una zona muy relacionada con España y que rodea las Ciudades Autónomas españolas de Ceuta y Melilla, demuestran la existencia de un número significativo de seguidores yihadista que pueden proyectar la amenaza sobre intereses españoles. La colaboración con los organismos antiterroristas marroquíes y el desarrollo de operaciones conjuntas ha sido clave, siendo de reseñar la detención en Rabat, en colaboración con la Policía Nacional española, de un estudiante marroquí de la Universidad

de Sevilla que estaba planeando cometer un ataque durante la celebración de la Semana Santa.

La Policía Nacional lidera el proyecto regional de la UE contra el terrorismo en el Cuerno de África y Yemen y participa en el proyecto de la UE *Apoyo a la lucha contra el terrorismo en Túnez*. También en la región de Oriente Próximo y norte de África, el Ministerio de Justicia participa, junto con el Ministerio del Interior, en el *Proyecto de la Unión Europea contra el Terrorismo en los países MENA (*siglas en inglés correspondientes a la denominación *Middle East and North Africa,* que se corresponden con Oriente Próximo y norte de África) y ambos han formulado en 2019, el proyecto *ACT* (en sus siglas en inglés correspondientes a la denominación *Action counterterrorism for Lebanon*), dirigido al fortalecimiento de la defensa antiterrorista del Líbano, la mejora de su sistema judicial antiterrorista y la aplicación de un enfoque de derechos humanos.

En Irak, España contribuye a la operación *Inherent Resolve* de la Coalición Internacional contra el DAESH con un máximo de 530 soldados y 25 efectivos de la Guardia Civil proporcionando labores de adiestramiento y formación a las fuerzas de seguridad iraquíes.

España contribuye a la operación Inherent Resolve de la Coalición Internacional contra el DAESH y a la misión NMI de la OTAN en Irak

Por otra parte, destaca la nueva misión de la OTAN en el país, denominada NATO *Mission Iraq* (NMI), centrada en la Reforma del Sector de la Seguridad.

España también participa en la misión *Resolute Support* de la OTAN en Afganistán y en la operación *Sea Guardian* de la OTAN en el Mediterráneo, así como en los despliegues de Fuerzas Navales Permanentes, instrumento de presencia, disuasión y reacción inmediata de la Alianza en el mar.

Por su parte, la Secretaría General de Instituciones Penitenciarias del Ministerio del Interior lidera un proyecto de hermanamiento en Turquía, cuyo objeto es la mejora de la gestión de terroristas y delincuentes peligrosos en prisión, así como la prevención de la radicalización.

En el escenario actual de Siria e Irak, donde hay presencia de activistas yihadistas con vínculos con España, donde podrían retornar, los Servicios de Inteligencia realizan un seguimiento permanente de estas personas. Además, también requiere atención la evolución de la situación en el Kurdistán sirio.

En la región del Sahel, la Guardia Civil lidera el proyecto GAR-SI Sahel, en el marco del cual se han creado Grupos Rápidos de Intervención en los diferentes países de la zona. Además, las FCSE participan en las misiones de capacitación de la UE en Malí y Níger (*EUCAP Sahel Mali* y *EUCAP Sahel* Níger) y tienen una participación destacada en proyectos de la UE como el *Programa de cooperación para la seguridad interior entre Senegal y la Unión Europea* (SECSEN-UE) y el proyecto *Apoyo a la cooperación regional de los países del G5 Sahel* y al Colegio Saheliano de Seguridad. Destaca también, la participación de las FAS en la operación *EUTM Mali*, así como en los esfuerzos de fortalecimiento de capacidades militares de países como Senegal, Cabo Verde, Mauritania y Túnez. (Figura 2-4 y 2-5)

España continúa apoyando a Francia en la Operación Barkhane en el Sahel

Respecto a los compromisos bilaterales, España continúa apoyando a Francia en la *Operación Barkhane* en el Sahel con el despliegue de dos destacamentos aéreos de transporte, que además apoyan a las misiones de UE y Naciones Unidas, así como a la Fuerza Conjunta G5 Sahel.

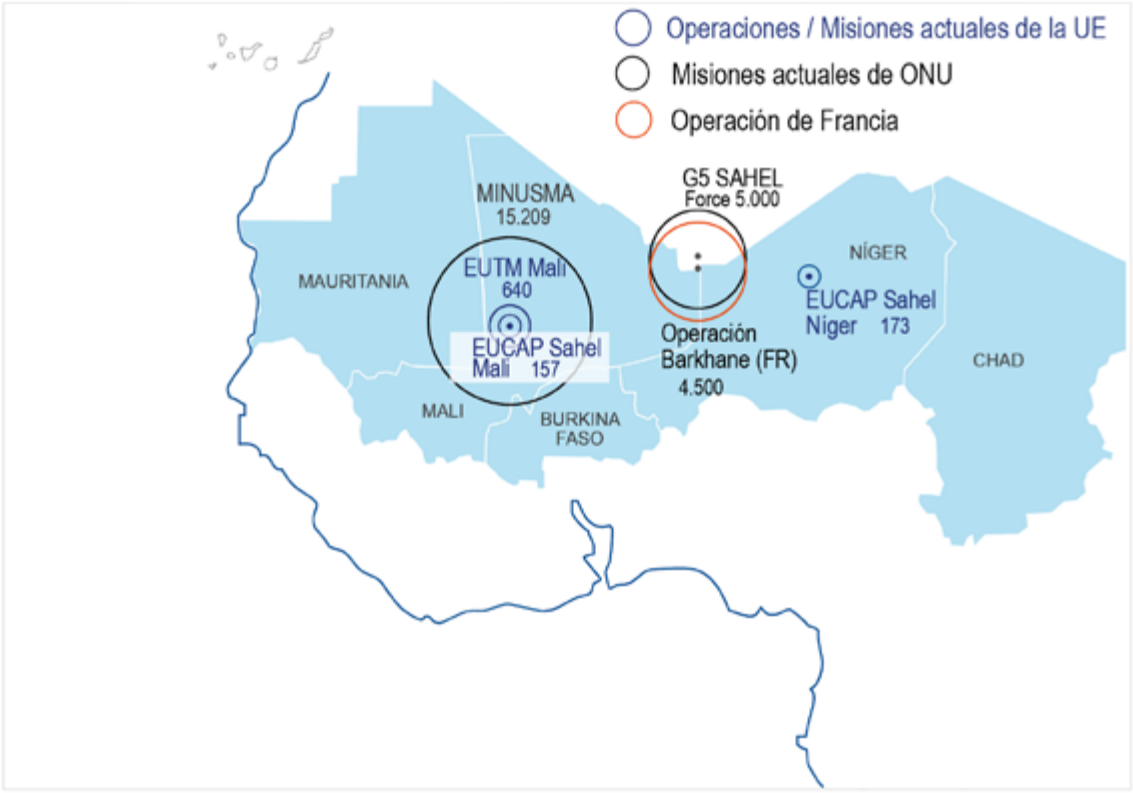
Las Fuerzas y Cuerpos de Seguridad de los Estados miembros y las instituciones de la UE, especialmente Europol (Oficina Europea de Policía), han potenciado y mejorado la cooperación y el intercambio de información, permitiendo mejoras en la investigación de los atentados sufridos en Europa. Asimismo, los Servicios de Inteligencia han incrementado su colaboración para la prevención de atentados, que en muchos casos tienen vínculos en más de un país europeo.

Además, se ha avanzado en la identificación de grupos terroristas y radicales, así como sus procedimientos de actuación y capacidades, que podrían ser una amenaza para las FAS y las FCSE, junto con aquellos grupos o personas que, tanto en zonas de operaciones como en territorio nacional, podrían estar apoyándolos.

A nivel nacional, el intercambio de información ha permitido desmantelar grupos que, en su mayor parte, se dedicaban a la captación de combatientes y a la diseminación de propaganda yihadista radical y contraria a la integración. En este sentido hay que subrayar la excelente cooperación en esta materia entre el CNI, la Policía Nacional, Guardia Civil, Mossos d'Esquadra y Ertzaintza, con objeto de aumentar la eficacia de la lucha contraterrorista a nivel nacional.

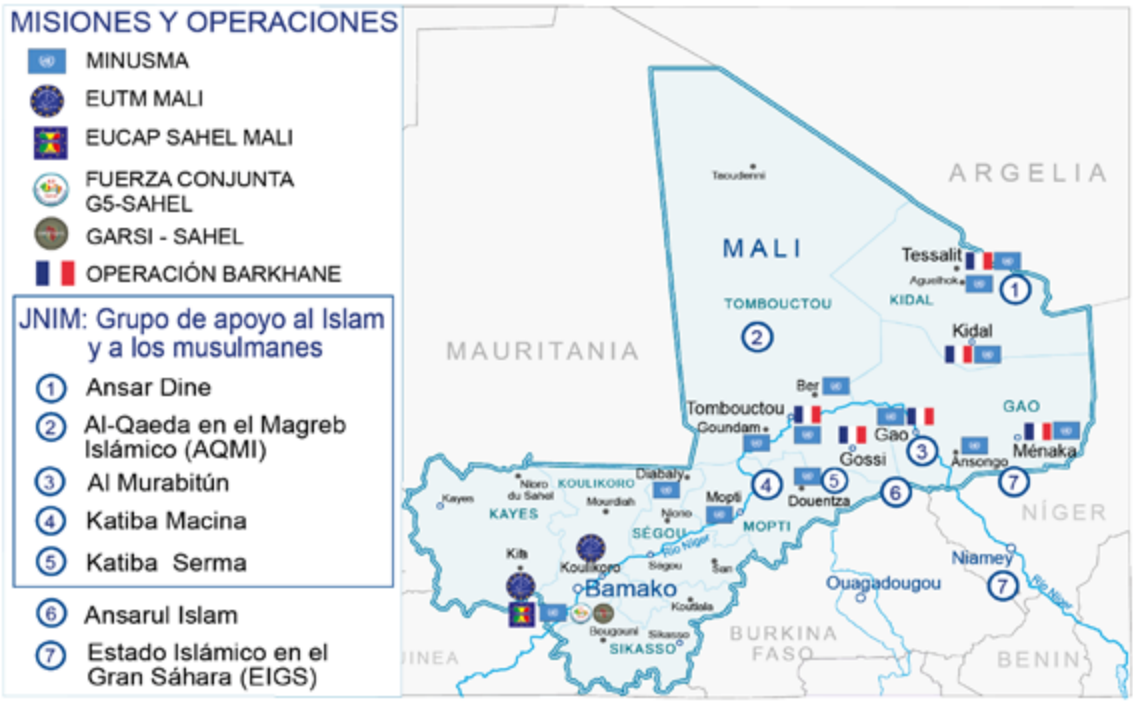
Por otro lado, la Fundación Víctimas del Terrorismo y el Centro Memorial de las Víctimas del Terrorismo han realizado cursos, seminarios, publicaciones y actuaciones de sensibilización, como el testimonio de las víctimas en las aulas, que contribuyen a la prevención del discurso terrorista a través de una narrativa eficaz protagonizada por sus víctimas directas.

Figura 2-4
Misiones y operaciones internacionales en las que participa España en el Sahel



Fuente: Documento de la EUISS "What if...? 14 futures for 2014", Chaillot Paper 157

Figura 2-5
Misiones y operaciones internacionales y grupos yihadistas en Mali 2019



Fuente: Elaboración del DSN con datos del Servicio Europeo de Acción Exterior

Protección

En el ámbito nacional, un nuevo convenio entre el Ministerio de Defensa y el Ministerio del Interior, que garantiza mecanismos más eficaces de activación de capacidades e intercambios de información, ha permitido mejorar la cooperación.

Por su parte, las FAS han revisado su Plan de Actuación, que les permite actuar como apoyo en la protección de las Infraestructuras Críticas cuyas capacidades han sido identificadas por el Ministerio del Interior, Autoridad competente, como susceptibles de ser reforzadas.

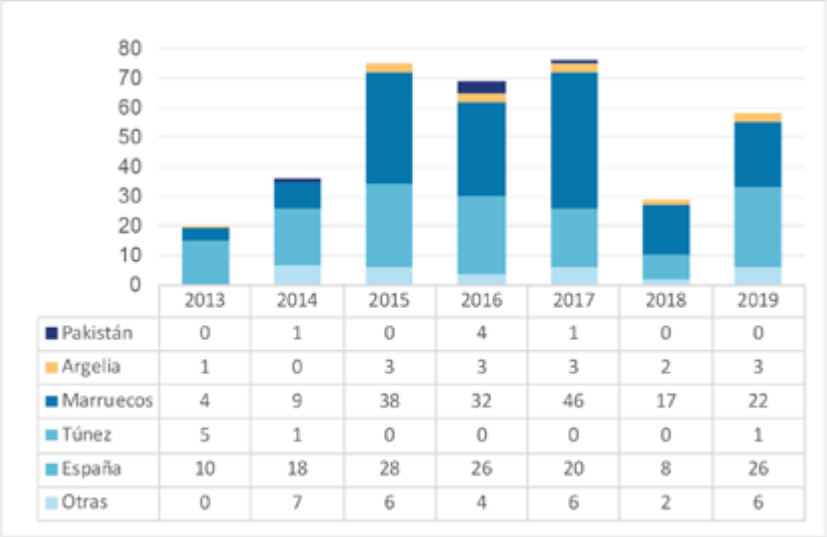
A nivel europeo, desde el año 2011 las aduanas europeas realizan de forma coordinada, tareas de análisis de riesgo de seguridad y protección de los ciudadanos de la UE en relación a las mercancías transportadas que transitan por territorio europeo comunitario. El sistema de análisis de riesgo abarca los riesgos y amenazas que tienen implicaciones en la seguridad como armas, explosivos, mercancías de doble uso, productos radioactivos, químicos y biológicos, y materiales que pudieran ser utilizados para la elaboración de artefactos explosivos o para propósitos relacionadas con terrorismo u otra actividad delictiva. Así, las últimas modificaciones europeas en materia de control aduanero están dirigidas al análisis de seguridad de las mercancías introducidas por vía postal y aéreo *exprés*, y también a la aplicación de reglas de seguridad específicas para la identificación de artefactos explosivos entre las mercancías trasportadas en los aviones (*bomb in a box*).

En 2019 se realizaron 58 detenciones en España en el ámbito del terrorismo yihadista

Persecución

En 2019, se realizaron 58 detenciones en España, en 32 operaciones en la lucha contra el terrorismo yihadista, volviendo a cifras de años anteriores, duplicando el número de detenidos de 2018. A estas cifras habría que añadir otras 10 detenciones, en operaciones policiales realizadas en otros países, en colaboración con las FCSE españolas. (Figura 2-6)

Figura 2-6
Evolución del número de detenidos en España por su vinculación con el terrorismo yihadista 2013-2019



	2013	2014	2015	2016	2017	2018	2019
Pakistán	0	1	0	4	1	0	0
Argelia	1	0	3	3	3	2	3
Marruecos	4	9	38	32	46	17	22
Túnez	5	1	0	0	0	0	1
España	10	18	28	26	20	8	26
Otras	0	7	6	4	6	2	6

Fuente: Ministerio del Interior

En el ámbito del terrorismo autóctono, se continuó con las labores de investigación tendentes a esclarecer los atentados cometidos por la organización terrorista ETA. En este sentido, cabe destacar la detención, el 16 de mayo en Francia, del fugado José Antonio Urrutikoetxea Bengoetxea, alias Josu Ternera. Por otra parte, la detención por la Guardia Civil el pasado 16 de junio de cuatro miembros de la organización terrorista Resistencia Galega ha ahondado en la derrota operativa de este grupo, aún no disuelto formalmente.

En términos normativos, la Ley Orgánica 1/2019, de 20 de febrero, que modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, transpone Directivas de la Unión Europea en los ámbitos financiero y de terrorismo, al tiempo que aborda cuestiones de índole internacional. Mediante esta Ley Orgánica se ha modificado la redacción del tipo penal relativo al viaje con fines terroristas, permitiendo así la sanción de la conducta sin necesidad de exigir que el viaje tuviere por destino un territorio controlado por terroristas.

La constante mejora de la cooperación judicial internacional es clave

En paralelo, es capital la actividad de España en favor de la necesaria y constante mejora de la cooperación judicial internacional, actividad en la que se incluye la contribución española al *Plan de Acción de Contraterrorismo del Consejo de Europa*, reflejada en el seminario organizado por el Ministerio de Justicia y el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación en junio de 2019 sobre cooperación internacional judicial.

A nivel europeo también, el Comité del Consejo de Europa contra el Terrorismo (CDCT) celebró una serie de debates preliminares sobre la necesidad y la viabilidad de elaborar una definición jurídica de terrorismo aplicable entre las Partes del Convenio del Consejo de Europa para la prevención del terrorismo y su Protocolo adicional. Los debates desembocaron en la decisión de abordar dicha tarea, revisando la redacción del artículo 1 de la Convención con el objetivo de ampliar su ámbito de aplicación. Para ello se constituirá un grupo de trabajo del que formará parte un representante del Ministerio de Justicia.

El CDCT también ha creado un grupo de trabajo dirigido a promover y desarrollar una mayor investigación sobre el terrorismo y las técnicas y vínculos entre el terrorismo y la delincuencia organizada transnacional. Desde el Ministerio de Justicia se colabora con el Ministerio del Interior para la elaboración de unas guías en la materia. Asimismo, el CDCT ha conformado un grupo de trabajo, en el que participa el Ministerio de Justicia, dirigido a alcanzar un conjunto de recomendaciones y líneas directrices para la recopilación de pruebas en zona de operaciones, así como la forma de adecuarlas al protocolo penal.

En relación con esta última cuestión, se constituyó, a iniciativa del Ministerio de Justicia, un grupo de trabajo para abordar la problemática sobre el uso de las pruebas obtenidas en el campo de batalla, llamado *Proyecto Battlefield*. Su finalidad consiste en la redacción de un protocolo/guía de actuación con el fin de establecer las pautas y canales que se deben seguir para solicitar a las autoridades estadounidenses la información relativa a las pruebas que obran en su poder.

Por otra parte, el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación y el Ministerio de Justicia colaborarán con el Foro Global

contra el Terrorismo en dos proyectos, uno relativo al desarrollo de un Manual Práctico para la elaboración de Listas de Observación (*Watch-Lists*) sobre elementos terroristas y otro relativo a la celebración en España de un seminario sobre la aplicación práctica de los puntos claves del Memorando de Nueva York sobre "Impedimento de Viajes de Terroristas" y su control judicial.

En análogo orden de ideas y acciones destaca la organización en Málaga, en marzo de 2019, del Comité de Coordinación del Foro Global de Contraterrorismo.

En el ámbito de Naciones Unidas, se creó junto con Afganistán el Grupo de Amigos de Víctimas del Terrorismo, el 25 de junio de 2019.

En términos de financiación, el Ministerio de Economía y Empresa mantuvo encuentros con el sector privado para la sensibilización y puesta en común de las amenazas en el ámbito de la financiación del terrorismo sobre la base del documento al respecto elaborado por el Grupo de Acción Financiera Internacional (GAFI). Además, es motivo de general satisfacción poder destacar que la Evaluación Mutua de España en el Plenario GAFI de octubre de 2019 en París alcanzó muy buenos resultados.

En cumplimiento de la recomendación 1 del GAFI, se ha elaborado un Análisis Nacional de Riesgos, en el que se incluye un análisis específico y completo sobre la situación de las organizaciones sin fines de lucro y su papel como posibles canalizadoras de fondos a actividades terroristas. En este sentido, se ha distribuido, a través de la Asociación Española de Fundaciones, un documento para resolver las preguntas frecuentes que las organizaciones sin fines de lucro se plantean en relación con las obligaciones de identificación de las personas de las que reciben fondos que les impone la normativa en materia de blanqueo de capitales.

Asimismo, el Ministerio de Economía y Empresa participó en otros foros internacionales sobre financiación, incluyendo en la Comisión Europea para la elaboración de Directivas de obligada trasposición en España, en la Coalición Internacional contra el DAESH para la puesta en común de información no confidencial sobre la lucha en el ámbito de la financiación del DAESH y para la previsión de nuevos comportamientos generadores de financiación del terrorismo y en la Conferencia de *No Money for Terror*, del Egmont Group (el Egmont Group agrupa a 164 unidades de inteligencia financiera para intercambiar conocimientos e inteligencia para para combatir el blanqueamiento de capitales y la financiación del terrorismo).

Preparación de la respuesta

Las FCSE han colaborado de forma activa durante este año en numerosos foros y grupos de trabajo relacionados con los explosivos, materiales nucleares, radiológicos, biológicos y químicos (NRBQ) tanto en el ámbito nacional como en el internacional.

Asimismo, han realizado diversos simulacros de atentado terrorista, con diferentes escenarios, con el objetivo de poner a prueba las capacidades de actuación y coordinación con otros actores implicados.

LUCHA CONTRA EL CRIMEN ORGANIZADO

OBJETIVO:

Neutralizar las amenazas relacionadas con el crimen organizado mediante estrategias dirigidas a desarticular grupos ya existentes, prevenir la implantación de otros nuevos y contrarrestar su confluencia con el terrorismo.

Tendencias

El crimen organizado representa una amenaza en permanente evolución

El crimen organizado representa una amenaza en permanente evolución. Debido a su carácter trasnacional, flexible y con gran potencial de adaptación y de obtención de beneficios ilícitos, repercute muy negativamente en la vida de los ciudadanos. La diversificación de las actividades criminales, la apertura de nuevas rutas y mercados, la creciente especialización y la adopción de nuevas técnicas, métodos y procedimientos evidencian su continua capacidad de adaptación. (Figura 3-1)

Las organizaciones criminales se dotan de medidas de seguridad cada vez más complejas para protegerse de la acción de los Estados y buscan alianzas entre sí para compartir recursos. Proliferan los grupos de carácter policriminal (que combinan el tráfico de drogas con el tráfico de personas o con la trata de seres humanos) y se consolida la dinámica del "crimen como servicio", con el empleo de plataformas y estructuras específicas que facilitan a los grupos criminales diversos apoyos especializados para blanquear capitales, desarrollar comercio por Internet o proporcionar medios e infraestructuras logísticas.

Las principales amenazas del crimen organizado siguen siendo el tráfico de sustancias estupefacientes, el blanqueo de capitales, el cibercrimen y el tráfico ilícito de armas. (Figura 3-2)

Con respecto al tráfico de drogas, las aprehensiones de cocaína, heroína y hachís muestran una tendencia lineal más o menos constante, si bien las incautaciones de marihuana y de plantas de *Cannabis sativa* presentan una progresión al alza. Se aprecia, asimismo, un incremento de casos de interceptaciones de metanfetamina procedente de México.

La vía principal de introducción de la cocaína sigue siendo el contenedor marítimo, oculta entre mercancías o mediante la técnica del *rip off* o "gancho perdido", consistente en introducir de forma clandestina la droga en contenedores con mercancías lícitas, para ser extraída posteriormente, en los puertos de destino, por los denominados "rescatadores". Los puertos principales para su introducción son, además de Algeciras y Valencia, Barcelona y Las Palmas. Esto es debido a que son los puertos con mayor tráfico de contenedores de España y, por tanto, de mayor dificultad de inspección. Continúa el uso de la técnica *drop-off*, con buques de línea regular que arrojan droga cerca de la costa para ser recogida por embarcaciones menores y se ha visto reactivado el uso de veleros en la ruta atlántica. (Figura 3-3, 3-4 y 3-5)

Debido a la intensificación del control e inspección sobre las llamadas "RHIBS" (embarcaciones semirrígidas de alta velocidad) en el estrecho de Gibraltar, el tráfico de hachís procedente de Marruecos se ha visto desplazado hacia las provincias de Málaga y Huelva. Por otro lado, la ruta del Mediterráneo oriental se ha desplazado al noroeste de Argelia, destacando también el uso de veleros.

En lo referente a la marihuana, es de señalar el crecimiento significativo del denominado cultivo *indoor* (plantaciones en naves industriales o viviendas particulares).

Es importante hacer un seguimiento de los métodos para el blanqueo de los beneficios que genera el tráfico de estupefacientes

En relación a los beneficios que genera el tráfico de estupefacientes, es importante hacer un seguimiento de los métodos para su blanqueo. Los grupos de origen latinoamericano o magrebí introducen los fondos generados por el tráfico de drogas en el sistema financiero español a través de personas y establecimientos que proporcionan justificación al envío del dinero. Es también frecuente el transporte de dinero en efectivo a través de correos humanos.

En cuanto al contrabando de tabaco, las principales modalidades son la introducción en contenedores, pequeñas embarcaciones procedentes de Gibraltar, alijos clandestinos de grandes cargas en contenedor (en Menorca y Huelva) o a través de la venta ilegal por Internet. Las falsificaciones y la fabricación clandestina son otra constante en toda la UE destacando los grupos especializados del este de Europa.

En los territorios de la Comarca del Campo de Gibraltar, donde se concentra gran parte del tráfico ilícito de sustancias estupefacientes, las medidas impulsadas con la entrada en vigor del *Plan Especial de Seguridad para el Campo de Gibraltar*, conjunto para la Policía Nacional y la Guardia Civil, han contribuido a paliar, por un lado, el importante deterioro de las condiciones objetivas de seguridad debido al impacto del narcotráfico, y por otro, las conductas violentas ligadas a la actividad de los grupos de delincuencia organizada, algunas de ellas dirigidas contra miembros de las FCSE.

Este Plan, unido a medidas adoptadas en el ámbito judicial, como la apertura de una nueva Unidad Administrativa de la Oficina de Recuperación y Gestión de Activos (ORGA) en Algeciras, y en el ámbito legislativo, como la entrada en vigor del *Real Decreto-ley 16/2018, de 26 de octubre, por el que se adoptan determinadas medidas de lucha contra el tráfico ilícito de personas y mercancías en relación con las embarcaciones*

utilizadas, está contribuyendo a la desarticulación de cada vez más organizaciones y grupos criminales.

Así, el incremento sostenido de la presión policial ha provocado una reacción por parte de las organizaciones criminales que operan en los territorios de la comarca, llevándolos a utilizar otras rutas de entrada de la droga, destacando las zonas costeras de la provincia de Huelva y Málaga, así como la desembocadura y cauce del río Guadalquivir. Igualmente, les ha movido a explotar otras actividades para mantener la financiación de las infraestructuras, como el contrabando de tabaco y a utilizar nuevos *modus operandi*, como la utilización de embarcaciones de recreo de doble fondo para transportar la droga, en lugar de las conocidas embarcaciones semirrígidas o narcolanchas.

En términos de cibercriminalidad, los fraudes informáticos representan la principal amenaza tanto para el consumidor como para el desarrollo del comercio electrónico, seguidos del cibercrimen asociado a amenazas y coacciones a través de las tecnologías de la información y la comunicación (TIC).

España ha realizado un importante esfuerzo respecto de la lucha contra el tráfico ilícito de armas de fuego

Es preciso prestar especial atención a la evolución de la violencia, principalmente entre grupos, y al desarrollo de las modalidades criminales más recientes, como el tráfico de opioides sintéticos o el fraude y la corrupción en el ámbito deportivo y las apuestas *online*.

Son relevantes también los grupos de delincuencia china que llevan a cabo su actividad a través de redes de establecimientos comerciales que generan enormes cantidades de dinero para su envío a China (a través de operaciones de ingreso de efectivo y transferencia o correos humanos) o inversión en España (a través de la compra de locales comerciales).

Por lo que respecta a la lucha contra el tráfico ilícito de armas de fuego, cabe señalar el importante esfuerzo que en España se ha realizado durante los últimos años, tal y como se desprende de la evolución del número de armas incautadas por todos los operadores de Seguridad y depositadas a disposición judicial en las Intervenciones de Armas de la Guardia Civil por la comisión de ilícitos penales, que han ascendido de 7.649 armas en 2013 a 14.996 en 2019. (Figura 3-6)

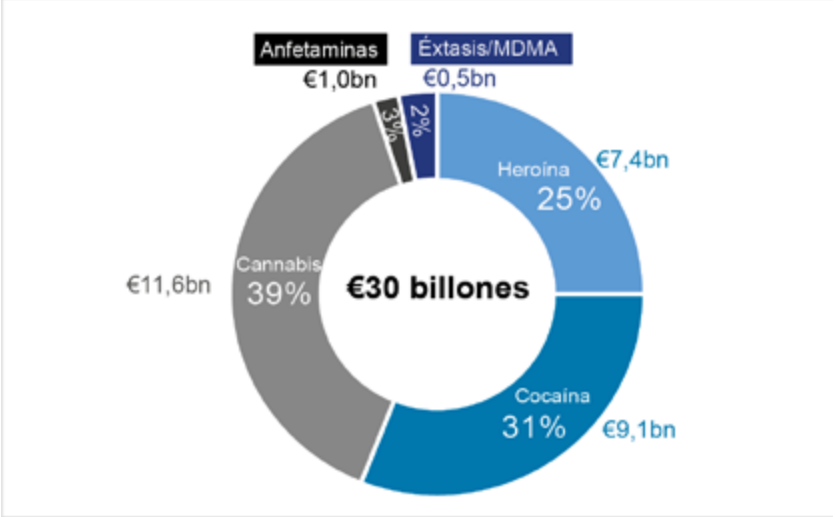
Fuente: Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023

Figura 3-1
Características principales del crimen organizado

Figura 3-2
Objetivos prioritarios del crimen organizado en la UE 2018-2021

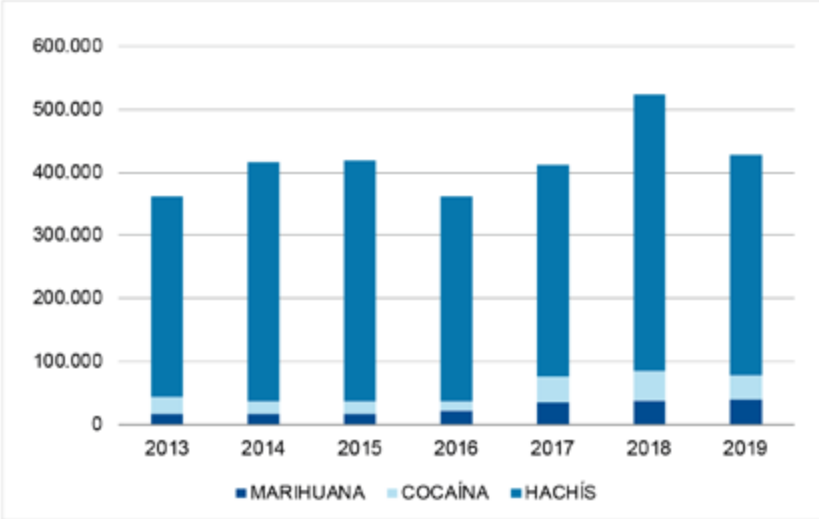
Fuente: Informe de Europol "EU Drug Markets Report 2019", EMCDDA

Figura 3-3
Estimación del mercado ilícito de drogas en la UE



Fuente: Informe de Europol "EU Drug Markets Report 2019", EMCDDA

Figura 3-4
Evolución de la droga intervenida en España (en Kilogramos) 2013-2019

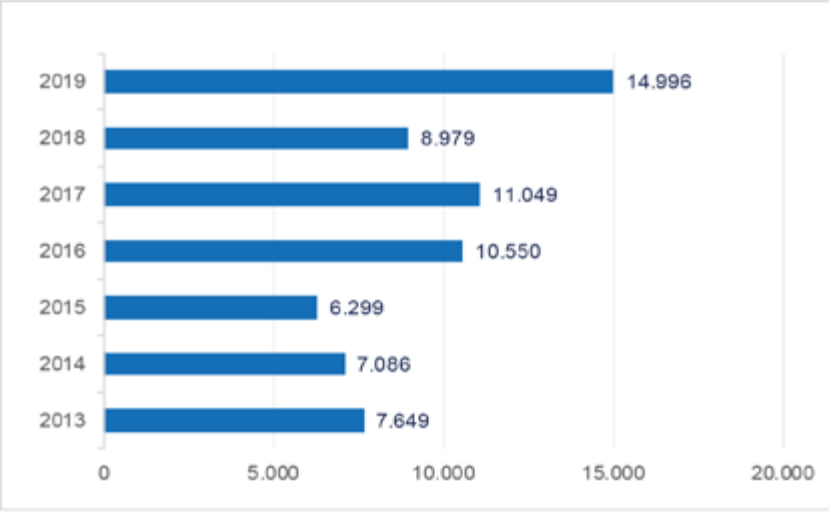


Fuente: Ministerio del Interior

	2018	2019	Variación
Hachís (kg)	436.963	349.489	-20%
Cocaína (kg)	48.453	37.868	-22%
Heroína (kg)	251	234	-7%
M.D.M.A. (uds)	300.571	267.632	-11%
M.D.M.A. (kg)	258	278	8%
Metanfetamina (uds)	227.530	93.779	-59%
Metanfetamina (kg)	23	1.559	6678%
Sulfato anfetamina (kg)	281	437	56%
Plantas de cannabis (uds)	981.148	1.538.995	57%
Marihuana (kg)	37.220	39.861	7%

Fuente: Ministerio del Interior

Figura 3-5
Droga intervenida en España
2018-2019



Fuente: Ministerio del Interior

Figura 3-6
Armas incautadas y depositadas a disposición judicial por la comisión de un delito en las Intervenciones de Armas de la Guardia Civil
2013-2019

Retos

En un mundo globalizado, las drogas, armas, residuos peligrosos, especies protegidas y los beneficios económicos del crimen organizado fluyen rápidamente a través de países y continentes, proporcionando nuevas oportunidades para esta amenaza a la Seguridad Nacional. En particular, el comercio electrónico ha experimentado un crecimiento exponencial.

Los avances tecnológicos facilitan la utilización por el crimen organizado de la Internet profunda y oscura

Por otro lado, los avances tecnológicos facilitan la utilización por el crimen organizado de la Internet profunda y oscura (conocida como *deep y dark* web respectivamente) para el tráfico y comercio de todo tipo de bienes ilícitos, así como el empleo de criptoactivos como medios de pago.

Para abordar estos retos resulta necesario incrementar la formación de todos los operadores implicados en la lucha contra el crimen organizado sobre los aspectos logísticos y operativos del comercio internacional. Asimismo, es imprescindible la adaptación a los nuevos métodos utilizados por las organizaciones criminales, el intercambio de información y la cooperación internacional, así como la formación del personal de las unidades policiales operativas, para que estén actualizados respecto de los *modus operandi* utilizados.

En particular, para hacer frente al reto que supone el incremento del tráfico de cocaína, cuya vía principal de entrada es el contenedor marítimo a través de puertos españoles, belgas y neerlandeses, es necesario potenciar el análisis de riesgos, la cooperación internacional y la coordinación entre servicios aduaneros y policiales.

Por otra parte, el tráfico de cocaína por vía aérea requiere un esfuerzo adicional, y por ello la Organización Mundial de Aduanas y la UE han desarrollado el Proyecto Colibri, financiado por la UE en el marco del Programa de la Ruta de la Cocaína y en el que participa el Departamento de Aduanas e Impuestos Especiales de la Agencia Tributaria (AEAT). Aunque las medidas de seguridad y control están establecidas en los aeropuertos civiles, muchos aeródromos secundarios no están sujetos a tarifas de administración, cargos de aterrizaje o estacionamiento, restricciones operativas o controles, y las medidas de seguridad en general se relajan sustancialmente, situación que supone una oportunidad para los traficantes y el crimen organizado. (Figura 3-7)

La problemática de la trata de seres humanos y el blanqueo de capitales se aborda en el tercer eje de la recientemente aprobada *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (2019-2023)* sobre lucha contra los mercados criminales y las graves formas delictivas. Para hacer frente a estas importantes amenazas, y siguiendo las líneas de acción de la citada Estrategia, se pretende desarrollar, por un lado, un plan estratégico específico nacional contra la trata y la explotación de seres humanos, y por otro, un plan estratégico de lucha contra el enriquecimiento ilícito de las organizaciones criminales y los delincuentes, que incluya el blanqueo de capitales, y la recuperación y localización de activos. En su elaboración, coordinada por el Ministerio del Interior, se contará con la participación de todos los organismos implicados. (Figura 3-8, 3-9 y 3-10)

Asimismo, continúan los esfuerzos en el ámbito normativo, con trabajos preparatorios para la reforma de la *Ley de Enjuiciamiento Criminal* y para la elaboración de una nueva ley de protección de colaboradores con la Administración de Justicia (tanto testigos y peritos como investigados), que sustituirá a la actual *Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales*. Se pretende así abordar el tratamiento de las personas (víctimas/testigos) implicadas en los fenómenos criminógenos unidos a los flujos migratorios para mejorar su asistencia y evitar su victimización secundaria, a través de una regulación a fondo de la protección a dispensar a dichas personas por los tribunales y la creación de planes de protección específicos.

También en relación a la lucha contra el blanqueo de capitales, se espera que los nuevos convenios de colaboración entre la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias y los distintos supervisores contribuyan a una mejor coordinación, de tal forma que se favorezca una actuación conjunta destinada a potenciar la supervisión de los sujetos obligados en materia de prevención del blanqueo de capitales de acuerdo con un enfoque de riesgo y en línea con los resultados del Análisis Nacional de Riesgos elaborado en cumplimiento de la recomendación 1 del GAFI.

Se debe perseverar en el trabajo de coordinación y cooperación recíproca entre instituciones que se ejerce a través de la ORGA, para la localización de activos vinculados a la actividad criminal de los grupos y organizaciones dedicadas al narcotráfico, así como a través de mecanismos como la Comisión Nacional y las Comisiones Provinciales de Coordinación de Policía Judicial, de cara a concretar y agilizar procedimientos que, en el marco del auxilio de las FCSE a las autoridades fiscales judiciales, permitan destruir determinados efectos judiciales, en aplicación de las previsiones recogidas en este ámbito en la *Ley de Enjuiciamiento Criminal*. Se impedirá así, por un lado, la readquisición de los mismos fruto de su realización en subasta pública por personas o entidades vinculadas a las organizaciones y grupos criminales, y por otro, el almacenamiento innecesario que se produce en las instalaciones policiales y otros espacios destinados al almacenamiento provisional de los efectos judiciales.

La cooperación internacional ha mejorado sustancialmente en los últimos años, como pone de manifiesto el importante incremento de las operaciones policiales transnacionales con resultados óptimos contra el crimen organizado. No obstante, se necesita mejorar en aspectos como el desarrollo de investigaciones trasnacionales o la incautación de bienes situados en otros países, de forma que se refuerce el gran avance que se ha producido en España en los últimos años en el desarrollo de mecanismos destinados a la lucha contra el blanqueo de capitales y a la incautación de activos procedentes de actividades criminales.

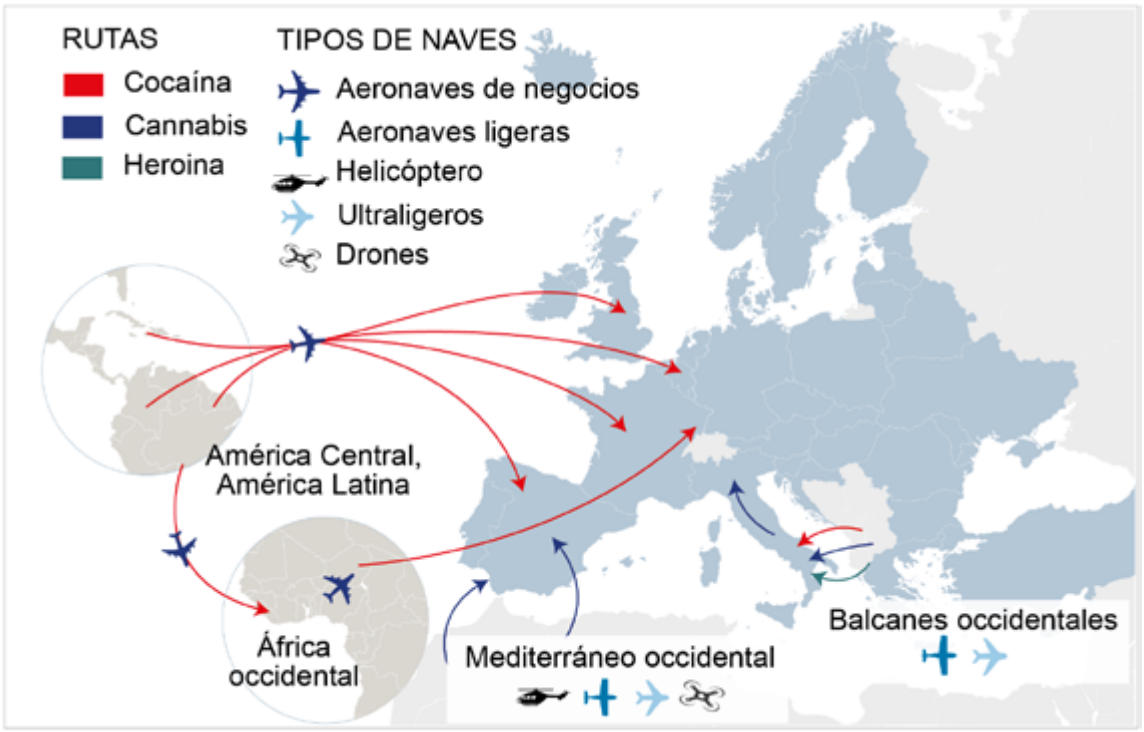
Resulta necesaria la regulación legislativa de los criptoactivos

En el caso concreto de los criptoactivos, resulta necesaria la regulación legislativa tanto en el ámbito conceptual (si se considera activo o medio de pago) como en el tributario. Además, se requiere la consideración como sujetos obligados en relación a la prevención del blanqueo de capitales a determinados proveedores de servicios con criptoactivos, como consecuencia de la transposición de la *Directiva 2018/843*

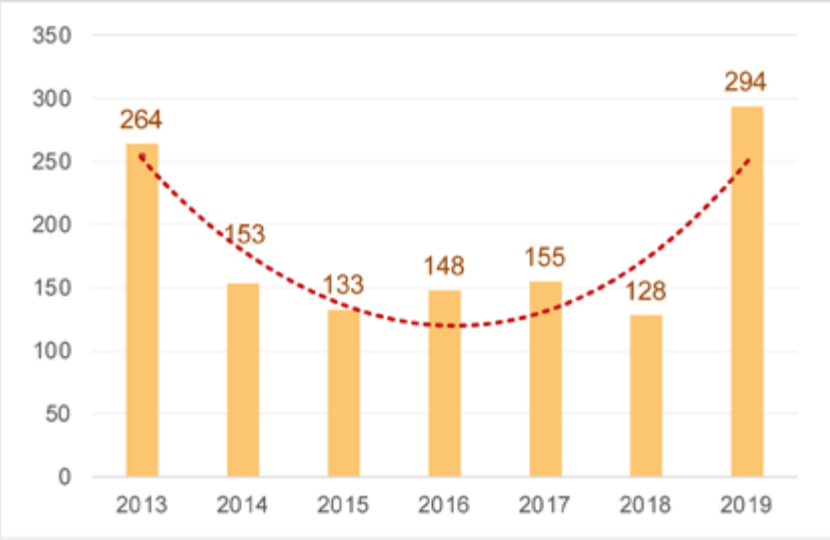
del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo y la Recomendación 15 del Grupo de Acción Financiera Internacional.

Finalmente, en relación con el uso ilícito de explosivos, el 20 de junio de 2019 entró en vigor el nuevo *Reglamento (UE) 2019/1148 del Parlamento Europeo y del Consejo, de 20 de junio, sobre la comercialización y la utilización de precursores de explosivos*, cuya aplicación en los diferentes países de la UE, entrará en vigor a partir de febrero de 2021. En este sentido, se hace necesaria la transposición nacional, estableciendo grupos de trabajos para la redacción de un anteproyecto de Ley que sirva como instrumento en el control de los precursores de explosivos a nivel nacional, tanto en el ámbito del crimen organizado como de la lucha contra el terrorismo.

Figura 3-7
Tráfico de drogas por vía aérea: rutas y tipos de aeronaves empleados

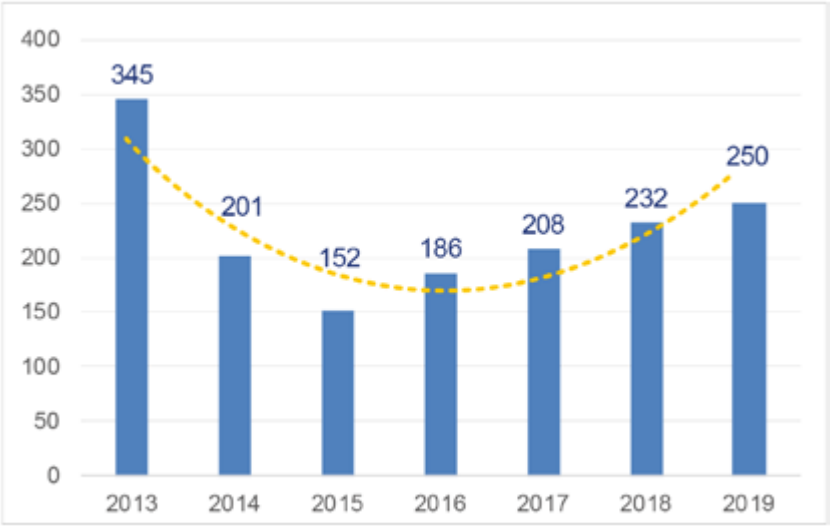


Fuente: Informe de Europol "EU Drug Markets Report 2019", EMCDDA



Fuente: Ministerio del Interior

Figura 3-8
Víctimas de trata sexual
2013-2019



Fuente: Ministerio del Interior

Figura 3-9
Detenidos por trata sexual
2013-2019

Fuente: Ministerio del Interior

Figura 3-10
Víctimas y detenidos por trata laboral
2015-2019

Realizaciones

En 2019 el Consejo de Seguridad Nacional aprobó la nueva Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023

Para hacer frente a esta importante amenaza y teniendo en cuenta los cambios experimentados, especialmente en determinados aspectos delincuenciales y tecnológicos, en 2019 el Consejo de Seguridad Nacional aprobó la nueva *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023*, cuyo objetivo principal es minimizar las consecuencias negativas de las amenazas que presentan el crimen organizado y la delincuencia grave para la Seguridad Nacional, articulando una serie de ejes de actuación encaminados a disminuir el impacto de tales amenazas en la sociedad. (Figura 3-11)

Las diferentes dimensiones del crimen organizado exigen que sea abordado desde un enfoque de respuesta integral y multidisciplinar, como el adoptado en la Estrategia.

La Estrategia se configura como un elemento de prevención y reacción frente al crimen organizado y la delincuencia grave; además, recoge aspectos de carácter asistencial y de sensibilización social, que contribuyen a mejorar el apoyo y protección a las víctimas.

Figura 3-11
Ejes troncales y transversales de la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023

Fuente: Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019 - 2023

Formación

Durante el año 2019 se llevaron a cabo actividades formativas, tanto en América Latina y América Central, como en territorio nacional.

El Ministerio del Interior, en colaboración con la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), organizó una serie de seminarios en los que participaron especialistas de distintos países de América Latina y América Central. Concretamente, se realizaron seminarios sobre "Inteligencia policial y análisis en la lucha contra la delincuencia organizada" (Bolivia), "Actuación policial en la lucha contra la trata de personas" (Guatemala), "Actuación policial contra el blanqueo de capitales, investigación patrimonial y recuperación de activos" (Uruguay) e "Investigación interna en los servicios policiales" (Colombia).

Asimismo, las FCSE lideraron la ejecución de diferentes programas formativos de CEPOL (la agencia de la UE que promueve la cooperación policial europea e internacional a través de la formación) en el ámbito de la UE y proyectos financiados por la UE, dirigidos al fortalecimiento institucional y a la formación y capacitación de las fuerzas de seguridad locales en materia de lucha contra el crimen organizado en diferentes áreas geográficas.

Inteligencia estratégica e intercambio de información

Un aspecto importante en la lucha contra el crimen organizado y la financiación del terrorismo es el control del ciclo de circulación del dinero. En este sentido, en 2019 se llevaron a cabo dos operaciones de control de movimientos de efectivo (GLOBAL y DAPHNE, esta última en el marco del Plan de Acción del Grupo de Cooperación Aduanera de la UE y liderada por la Agencia Italiana de Aduanas y con Europol como colíder). Este tipo de operaciones permiten potenciar la investigación de operaciones de movimiento de efectivo sospechosas, conforme a la normativa de prevención de blanqueo de capitales y financiación del terrorismo.

Además, se realizaron reuniones de coordinación en el ámbito operativo a través del Grupo Operativo de Inteligencia Financiera (GOIF), dependiente del Comité de Inteligencia Financiera, con representantes, entre otros, de las FCSE, Ministerio Fiscal y la Agencia Tributaria - Aduanas, para la puesta en común de informaciones de interés que pueden dar lugar a la elaboración de operativos coordinados o individuales.

Asimismo, el Ministerio de Economía y Empresa elaboró un Análisis Nacional de Riesgos en materia de blanqueo de capitales, en cumplimiento de la recomendación 1 del GAFI, donde se unifican los análisis y evaluaciones de riesgo sectoriales realizados hasta la fecha, con la participación de las distintas autoridades públicas vinculadas a la lucha contra el blanqueo de capitales y la financiación del terrorismo. También participó en el proceso de evaluación del GAFI del 5° año, en el que la calificación de cumplimiento de España en el apartado Resultado Inmediato 4 (Medidas preventivas) mejoró de "*moderate*" a "*substantial*."

En 2019 se ha elaborado un Análisis Nacional de Riesgos en materia de blanqueo de capitales

Por otro lado, en 2019 entró en vigor el nuevo modelo de inteligencia marítima del Servicio de Vigilancia Aduanera de la Agencia Tributaria

para una mayor integración de la actuación de sus servicios marítimos y de investigación, utilizando un nuevo modelo de difusión de la información y empleando nuevas técnicas de análisis de la información y vigilancia marítima. Además, se crearon las Oficinas de Información Marítima y se impulsó un plan de formación en la materia. Este nuevo sistema permitirá, además, una mejor coordinación del intercambio de información e inteligencia marítima con otros servicios nacionales e internacionales.

En este sentido, el Departamento de Aduanas e Impuestos Especiales de la Agencia Tributaria lidera, junto con Puertos del Estado y con el apoyo de la Fiscalía Especial Antidroga y la Guardia Civil, una iniciativa de colaboración público–privada para el incremento de la seguridad en los puertos españoles, con la finalidad de prevenir la penetración en las instalaciones y servicios portuarios de los grupos y organizaciones criminales dedicados al tráfico de drogas y otros delitos.

En relación con la zona del Campo de Gibraltar, se puso en marcha el *Plan Especial de Seguridad para el Campo de Gibraltar*, fijado para los años 2018 y 2019, destinado a restablecer las condiciones de seguridad y a reforzar las capacidades operativas y de inteligencia de las FCSE. En el marco de este Plan, el Ministerio del Interior estableció una serie de medidas en materia de recursos humanos, económicos, materiales y técnicos, así como de coordinación y cooperación, para potenciar la lucha contra el narcotráfico, entre las que se encuentra el intercambio constante de información e inteligencia entre las FCSE en coordinación con Vigilancia Aduanera de la Agencia Tributaria.

Los resultados obtenidos hasta el momento demuestran la eficacia del Plan y de una estrategia de trabajo coordinada entre las FCSE y con Vigilancia Aduanera de la Agencia Tributaria. En particular, se ha incrementado en un 77,8% el número de operaciones contra el tráfico de drogas y en un 86,9% las operaciones contra el blanqueo de capitales e investigación patrimonial; se han realizado 4.852 detenciones; se han aprehendido 145,16 toneladas de hachís, 4,67 toneladas de cocaína, 1 kilogramo de heroína y 177 kilogramos de marihuana, así como 758.999 cajetillas de tabaco de contrabando; y se han incautado 750 vehículos utilizados para transportar mercancías ilegales, de los cuales 133 son embarcaciones, fundamentalmente lanchas semirrígidas dedicadas al narcotráfico.

Entre los logros del plan destaca además la consolidación de una mayor actividad en el ámbito de la prevención y de la colaboración con sectores de la sociedad civil y entidades afectadas por el narcotráfico.

Asimismo, es importante resaltar la coordinación con otros organismos e instituciones. En este sentido, se han constituido diversos órganos de coordinación de los que forman parte la Policía Nacional, la Guardia Civil, la Dirección Adjunta de Vigilancia Aduanera de la Agencia Tributaria y los Cuerpos de Policía Local, además de una Mesa Técnica Comarcal y una Mesa Técnica en La Línea de la Concepción.

El Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC) también ha contribuido a la ejecución del *Plan Especial de Seguridad para el Campo de Gibraltar* a través de actuaciones de concienciación de los sujetos obligados; de la

intensificación de la supervisión, incluyendo en el plan de inspección del SEPBLAC para 2019 acciones específicas en este ámbito territorial; el reforzamiento de las capacidades del sector privado; y el refuerzo de la cooperación con otras unidades, a través del envío de informes de inteligencia financiera.

Otra herramienta eficaz para la lucha contra el contrabando y el narcotráfico en la zona del Estrecho de Gibraltar es el *Real Decreto-ley 16/2018, de 26 de octubre, por el que se adoptan determinadas medidas de lucha contra el tráfico ilícito de personas y mercancías en relación con las embarcaciones utilizadas*, cuyo periodo transitorio de aplicación finalizó en abril de 2019.

En este sentido, hasta mediados de noviembre de 2019 se tramitaron 972 solicitudes de inscripción de operadores y 767 solicitudes de autorización de uso de embarcaciones semirrígidas. En ese mismo periodo se realizaron 165 expedientes de contrabando por uso de este tipo de embarcaciones sin estar previamente inscritos en el Registro del Departamento de Aduanas e Impuestos Especiales de la Agencia Tributaria.

Cooperación y Coordinación Internacional

La Europol publicó en febrero de 2018 el Informe SOCTA (por sus siglas en inglés correspondientes a la denominación *Serious and Organized Crime Threat Assessment*), principal documento de análisis de la UE sobre la amenaza que supone la criminalidad grave y la delincuencia organizada. A partir de los resultados obtenidos y las conclusiones del SOCTA, el Consejo de Justicia y los ministros de interior de la UE trazaron las líneas de investigación y actuación prioritarias para luchar contra el crimen organizado de cara al segundo Ciclo Político 2018-2022 (*EU Policy Cycle*). Las valoraciones y conclusiones de este informe se tienen en cuenta en los trabajos del Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (COSI) para el Ciclo Político 2018-2021.

El Director del CITCO actúa como el coordinador nacional de todas las actuaciones que España realiza en el contexto del Ciclo Político (proyectos EMPACT), lo que supone garantizar la participación efectiva de las autoridades nacionales pertinentes en la aplicación de las prioridades y en la coordinación de actividades, facilitando y apoyando la implicación de España, para lograr consolidar su actual posición de liderazgo en la lucha contra el crimen organizado en Europa.

En este sentido, el papel de España en el Ciclo Político es muy activo. En 2019, de un total de 244 acciones operativas, España participó en 193, asumiendo un rol director en 20 y co-liderando 58. Además, la Policía Nacional lidera la prioridad de tráfico de cocaína, cannabis y heroína y la Guardia Civil, la de tráfico de armas y explosivos. Asimismo, la Policía Nacional es co-lider en facilitación de la inmigración ilegal y, en el marco de la prioridad de ciberdelincuencia, en explotación sexual infantil. Por su parte, la Guardia Civil es co-líder en dos prioridades: delito medioambiental y delincuencia organizada contra la propiedad.

En este marco, con financiación europea y como ejemplo de buenas prácticas, se podrían incluir el exitoso Equipo Conjunto de Investigación creado entre España y Francia con sede en Niamey (Níger), cuyo

objetivo es la lucha contra las redes criminales vinculadas a la inmigración ilegal y el tráfico de personas, así como el recientemente creado equipo conjunto en Senegal en el que, en estrecha colaboración con las autoridades francesas, la Policía Nacional contribuye, ejerciendo funciones de liderazgo en la lucha contra la inmigración irregular, el tráfico de inmigrantes y la trata de seres humanos.

España participa en varios programas de la UE dirigidos a la cooperación con América Latina y América Central en materia de crimen organizado

España también participa en varios programas de la UE dirigidos a la cooperación con América Latina y América Central.

El Ministerio del Interior, con participación del Ministerio de Justicia, co-lidera con Francia el Programa de la UE "Europa Latinoamérica - Programa de Asistencia contra el Crimen Transnacional Organizado" (EL PAcCTO). Su finalidad es contribuir a reforzar el Estado de Derecho y la seguridad ciudadana en América Latina, actuando en los tres pilares que conforman la cadena penal (sistema policial, de justicia y penitenciario) y cinco ejes transversales (derechos humanos, género, cibercrimen, corrupción y lavado de activos).

España también lidera el proyecto de la UE de "Cooperación en materia de investigación penal en Centroamérica para la lucha contra la delincuencia organizada y el tráfico de drogas" (ICRIME), dirigido a los países del SICA (América Central); el proyecto (EU-ENLCD) de "Apoyo contra el tráfico de drogas y el crimen organizado", en Perú, y el proyecto (EU-FELCN) de "Apoyo europeo a las fuerzas especiales de lucha contra la droga en la aplicación de la ley" en Bolivia, participando en todos ellos el Ministerio del Interior y el Ministerio de Justicia.

Asimismo, el Ministerio del Interior lidera el proyecto de la UE "EL-PAcCTO apoyo a AMERIPOL", en el cual se está trabajando para lograr la personalidad jurídica plena de la Comunidad de Policías de América (AMERIPOL), como organización de cooperación policial internacional de referencia en América Latina.

La Policía Nacional y la Guardia Civil participan en el Proyecto de Cooperación Portuaria (SEACOP), financiado por la Comisión Europea, cuyo objetivo es apoyar la lucha contra el tráfico marítimo ilícito (sustancias estupefacientes) y las redes criminales internacionales en países de África occidental y meridional, así como América Latina y el Caribe.

Por otro lado, a través de la Oficina de Naciones Unidas contra la droga y el delito (UNODC por sus siglas en inglés correspondientes a la denominación *United Nations Office on Drugs and Crime*) y con idéntico ámbito territorial, la Policía Nacional mantiene desplegado a un Inspector en el marco del proyecto AIRCOP, cuyo fin es el fortalecimiento de las capacidades de las fuerzas policiales aeroportuarias en la lucha contra el tráfico de estupefacientes y la detección de pasajeros de alto riesgo.

España también tiene un papel destacado en el proyecto EU-ACT, destinado a la mejora de la cooperación y refuerzo de las capacidades para hacer frente al crimen organizado relacionado con la droga a lo largo de la ruta de la heroína, desde Asia hacia Europa.

En el ámbito europeo, el Ministerio del Interior participa en el proyecto de la UE *Euromed Police*, que tiene como objetivo incrementar la segu-

ridad de los ciudadanos, a través del fortalecimiento de la cooperación en materia de seguridad entre países del sur de la cuenca mediterránea y los países de la UE.

La Policía Nacional lidera el Proyecto EURASIAN con Polonia y Lituania, en cuyo marco se han desarrollado algunas de las operaciones más importantes en Europa en 2019 contra el crimen organizado euroasiático, con la colaboración estrecha de Europol y del resto de países europeos. La Policía Nacional es también el punto nacional de contacto del Project Millennium de Interpol, foro internacional especializado en los Ladrones en Ley o máximos dirigentes de la Criminalidad Organizada rusa y georgiana, asistiendo también a dicho foro la Guardia Civil. Ambos cuerpos participan asimismo en el Project Limes, liderado por Alemania, contra el crimen organizado transnacional.

Por su parte, la Guardia Civil lidera la plataforma del EMPACT FIREARMS mediante la que se pretende hacer frente a las principales amenazas en materia de armas de fuego, focalizando su actuación en el largo plazo contra la reactivación ilegal de armas de fuego, la transformación ilegal de armas detonadoras, el desvío de tráfico lícito al mercado negro, el uso de la paquetería intracomunitaria o el uso de la red para transacciones ilegales (en todo el internet, incluyendo la darknet o internet oscura).

En el ámbito normativo, la *Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave*, es en sí misma un punto de inflexión en la lucha contra el terrorismo y el crimen organizado.

Desde el CITCO se ha desarrollado ya, en la denominada "Fase I del Sistema de Alerta del Registro de Pasajeros", un plan inicial, mediante el uso de los datos API (por sus siglas en inglés correspondientes a la denominación *Advanced Passenger Information*) de los vuelos que llegan a España desde fuera del espacio Schengen, que ha aglutinado todo el potencial de inteligencia del Centro en materia de lucha contra el terrorismo y el crimen organizado, favoreciendo con ello el desarrollo e intercambio de información entre diferentes Estados miembros y con Europol, así como la coordinación y el apoyo operativo no solo entre las Fuerzas y Cuerpos de Seguridad del Estado, sino también con los Servicios de Inteligencia, las Policías Autonómicas y los servicios de Aduanas.

A lo largo de la presente legislatura se realizará la completa transposición de esta Directiva europea al ordenamiento jurídico nacional, elaborando una Ley Nacional para el tratamiento de datos PNR.

En materia de lucha contra la trata, la Policía Nacional lidera el proyecto de la UE "Acción contra la trata de seres humanos y las redes de favorecimiento de la inmigración irregular" (A-TIPSOM), en Nigeria.

La fructífera cooperación con Marruecos ha contribuido a la desarticulación de redes de tráfico de personas y a la detención de traficantes, resultando siempre necesario perseverar en la detección de nuevos *modus operandi* por parte de las organizaciones delictivas.

En el marco de Naciones Unidas, el Ministerio de Justicia participó en el 28º periodo de sesiones de la Comisión de Prevención del Delito y Justicia Penal con el objetivo de realizar seguimiento e intervenir en los debates relativos a las resoluciones que fueron aprobadas. La Comisión es el órgano principal del sistema de las Naciones Unidas para formular políticas y recomendaciones sobre cuestiones de justicia penal, incluida la trata de seres humanos, los crímenes transnacionales y los aspectos de la prevención del terrorismo. Desde el Ministerio de Justicia, en coordinación con el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, se está llevando a cabo la preparación del XIV Congreso de las Naciones Unidas para la Prevención del Delito y Justicia Penal (Kyoto, 20 al 27 de abril de 2020).

Por otro lado, dentro de las actividades que en España se llevan a cabo para erradicar la fabricación, transferencia y circulación ilícita de armas pequeñas y ligeras en el marco del Programa de Acción de Naciones Unidas sobre su comercio ilícito, la Guardia Civil destruyó más de 42.234 armas de fuego durante 2019, lo que implica que desde el año 2013 se han destruido 436.646 armas de fuego en España.

En lo que se refiere a los amaños deportivos y la corrupción en el deporte, el Ministerio de Cultura y Deporte cuenta con instituciones como el Consejo Superior de Deportes y sus respectivas federaciones, a través de las que obtiene información sobre hechos que pudieran ser delictivos dentro del entorno deportivo y las apuestas que se generan en el mismo. En julio se creó la Comisión Nacional para combatir la manipulación de las competiciones deportivas y el fraude en las apuestas cuyo objetivo es detectar, prevenir y combatir las actuaciones ilícitas en el ámbito de las competiciones deportivas y el fraude en las apuestas a través de la acción coordinada de los ministerios de Hacienda, Interior y Cultura y Deporte.

NO PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA

OBJETIVO:

Combatir la proliferación de armas de destrucción masiva, sus vectores de lanzamiento, materiales conexos y tecnología asociada, así como impedir su acceso a actores no estatales, y en particular a organizaciones terroristas.

Tendencias

La proliferación de armas de destrucción masiva supone una grave amenaza para la paz y seguridad internacionales y afecta directamente a la Seguridad Nacional.

Con los mecanismos creados desde mediados del siglo XX hasta la actualidad se ha conseguido retrasar el proceso de proliferación. Sin embargo, la globalización y el desarrollo tecnológico favorecen la transferencia de conocimiento en este ámbito y facilitan la adquisición de componentes y materiales estratégicos. Los riesgos derivados del desvío y el contrabando de materiales sensibles y de precursores de explosivos están aumentando considerablemente.

Es necesario reforzar los mecanismos de control de la tecnología y del material necesario para fabricar armas de destrucción masiva

Además, existe una parálisis en prácticamente todos los foros tradicionales de no proliferación debido a la desconfianza, rivalidad y lógica obsolescencia de parte de los tratados fruto de la evolución de las tecnologías y la aparición de nuevos e importantes actores, principalmente China. Se ha vuelto a una política de bloques en lugar de a la búsqueda de consenso y cooperación, de manera que los Estados como entidades independientes se están viendo desplazados. Es por ello que se hace necesario continuar reforzando los mecanismos, tanto nacionales como internacionales, de control de la tecnología y del material necesario para fabricar este tipo de armas, buscando fórmulas de equilibrio entre seguridad, confianza y progreso técnico.

En el ámbito de las armas químicas, la incorporación de Siria en 2013 a la Organización para la Prohibición de las Armas Químicas (OPAQ) supuso un importante avance, prontamente fallido tras el uso de armas

químicas tanto por parte del sector rebelde como por fuerzas gubernamentales. Además, la polarización existente ha obstaculizado las investigaciones de atribución de estos ataques, retrasando o impidiendo que se lleven a cabo.

Sin embargo, en la última reunión de la OPAQ se observó un tono de mayor distensión y se aprobó el presupuesto anual, aunque hubo menor consenso al abordar los trabajos de inspección en Siria, que continúan siendo cuestionados tanto por Siria como por Rusia.

Se consiguió la inclusión de los Novichok en la lista de la OPAQ. Dicha inclusión contó con el voto de Rusia a pesar de su reticencia previa. Rusia también incluyó otros compuestos de forma puramente testimonial y que no afectan a España.

Respecto a los depresores del sistema nervioso central (entre los que se encuentran los fentanilos), Estados Unidos decidió retirar su propuesta de que se aprobara una decisión prohibiendo su uso por Fuerzas y Cuerpos de Seguridad a la espera de contar con mayores apoyos. Previsiblemente será presentada al próximo Consejo Ejecutivo. España ha expresado su apoyo a la propuesta, aunque ha pedido que se especifiquen algunos de sus puntos.

En el marco de los tratados internacionales de no proliferación de armas de destrucción masiva ha habido una polarización política. Esto complica que avancen las propuestas para afrontar los nuevos desafíos. Se valora que esta tendencia se mantendrá mientras existan conflictos de intereses entre los diferentes grupos de países implicados en esos tratados.

En 2020 el START III quedará como el único acuerdo de control de armas nucleares en vigor

En 2020 comienza un nuevo escenario donde el Tratado de Reducción de Armas Estratégicas (START III por sus siglas en inglés correspondientes a la denominación *Strategic Arms Treaty*) queda como el único acuerdo de control de armas nucleares en vigor. Por tanto, las relaciones bilaterales entre Estados son claves. El contexto geopolítico ha venido marcado por la retirada de Estados Unidos del Plan de Acción Integral Conjunto (JPCOA por sus siglas en inglés, correspondientes a la denominación *Joint Comprehensive Plan of Action*) y por la posibilidad de que la República Popular Democrática de Corea se consolide como un Estado Nuclear *de facto*, lo que ha generado un aumento de la incertidumbre respecto del modelo de no proliferación.

En el caso de la República Popular Democrática de Corea, es altamente probable que continúe desarrollando su programa nuclear, considerado clave para la supervivencia de su Estado. La financiación de su programa mediante ciberactivos le permite conseguir los fondos y la tecnología militar necesarios, pudiendo evadir las sanciones financieras.

En cuanto a Irán, tras la ruptura del JPCOA por parte de Estados Unidos en 2018, la situación ha continuado deteriorándose hasta que en enero de 2020 el Gobierno iraní se desvinculó de los límites fijados en el Plan relativo al enriquecimiento de uranio. En consecuencia, tres de los firmantes del Plan (Alemania, Francia y Gran Bretaña) han activado el mecanismo de resolución de disputas (previsto en los artículos 36 y 37 del JPCOA),

Todo ello hace del nuevo escenario iraní un medio desestabilizador regional y global que afecta a varios ámbitos de actuación como es el comercio de hidrocarburos y el tránsito marítimo de mercancías.

En el marco del Régimen de Control de Tecnologías de Misiles, se ha observado una polarización política similar, derivada del conflicto comercial entre Estados Unidos y China. La inestabilidad de algunos países seguirá favoreciendo los avances de sus respectivos programas de misiles, incrementando su arsenal y mejorando la precisión y el alcance de sus sistemas. Las adquisiciones de materiales y tecnologías de doble uso por parte de estos países seguirán exigiendo mayores esfuerzos para su detección y control debido al empleo de métodos cada vez más sofisticados.

Continúan constituyendo una importante amenaza para la seguridad internacional el incremento de la aparición de patógenos emergentes a nivel global y la utilización potencial de agentes biológicos por grupos terroristas y criminales. De igual manera, el rápido desarrollo de las técnicas de edición genética, que permiten la modificación del genoma de toda clase de seres vivos, supone un importante avance en el tratamiento de enfermedades y en la investigación biomédica, agropecuaria y en ciencias ambientales, pero a su vez constituye una preocupación por el potencial doble uso de estas tecnologías.

El incremento de la aparición de patógenos emergentes constituye una importante amenaza para la seguridad internacional

En este sentido, la Seguridad Nacional requiere permanecer vigilante frente a las nuevas amenazas, asumiendo las responsabilidades que incumban a España en cuanto al establecimiento de controles para mitigar la proliferación de armas de destrucción masiva atendiendo a los estándares internacionales basados en los tratados, convenciones y demás instrumentos internacionales en el ámbito de la no proliferación, conforme a lo previsto en la *Estrategia de Seguridad Nacional 2017* y la estrategia de la UE contra la proliferación.

A pesar de los obstáculos, se han adoptado medidas para dar respuesta a esta amenaza tanto en el ámbito internacional, como el regional y el nacional.

El Consejo de Seguridad de las Naciones Unidas ha adoptado distintas Resoluciones que prohíben la financiación de actividades relacionadas con la proliferación por agentes no estatales y otras específicas contra la República Democrática Popular de Corea e Irán.

En el marco de la UE, en 2003 se aprobó la Estrategia de la UE contra la proliferación de armas de destrucción masiva y, desde entonces, se vienen adoptando una serie de Decisiones de actualización y seguimiento.

España ha reiterado durante 2019 su compromiso político con el Tratado de Prohibición completa de los Ensayos Nucleares adoptado en 1996 que no ha entrado todavía en vigor.

Retos

Las armas de destrucción masiva constituyen una de las mayores amenazas que, por su potencial riesgo e impacto, debe afrontar la humanidad en las próximas décadas. (Figura 4-1)

En relación a las armas de naturaleza biológica, teniendo en cuenta el riesgo que supone que agentes biológicos escapen al control y puedan caer en manos de agentes no estatales y en particular de organizaciones terroristas, resulta necesario disponer de un inventario de patógenos susceptibles de custodia; identificar las instalaciones que los contengan, con el objeto de implantar en ellas las medidas de seguridad adecuadas y su transporte; así como definir y controlar los requisitos de habilitación del personal con acceso a dichas sustancias.

En el ámbito nuclear deben mejorarse los sistemas de protección y seguridad de las instalaciones nucleares y radiactivas ante la amenaza del *insider* (persona que puede llevar a cabo ataques desde el interior de una empresa o institución) mediante la implantación de un sistema de chequeo del personal.

Los foros internacionales son contextos propicios a la colaboración para hacer frente a la amenaza de la proliferación de armas de destrucción masiva, por eso constituye un desafío perfeccionar los mecanismos multilaterales de intercambio de información entre los Servicios de Inteligencia internacionales en este ámbito, potenciando la confianza y la transparencia entre los Estados que buscan erradicar su proliferación.

Tras la expiración del Tratado INF es necesario fortalecer los mecanismos internacionales de control de armas, desarme y no proliferación

Es especialmente conveniente fortalecer los mecanismos internacionales de control de armas, desarme y no proliferación tras la expiración del Tratado INF y el futuro incierto del START III, que vence en 2021.

En el año 2020 se deberá llevar a cabo la Conferencia de Revisión del Tratado de No Proliferación de armas nucleares (TNP). El TNP es uno de los instrumentos más antiguos con los que se dotó la comunidad internacional para evitar o minimizar los riesgos de la proliferación de armas de destrucción masiva (en este caso, de las armas nucleares). La actual situación de dificultad por la que atraviesa el multilateralismo como marco internacional de resolución hace que el desarrollo de esta Conferencia pueda resultar especialmente importante. (Figura 4-2)

Además, se han de revisar las necesidades de los futuros marcos regulatorios de control de armamentos tras la aparición de nuevos vectores de armas, tanto de origen como en nuevas aplicaciones.

Dentro de las competencias de la Subdirección General de Energía Nuclear en relación a la aplicación del TNP, en cumplimiento de artículo 14 del Protocolo Adicional al TNP, y tras un largo proceso negociador, se aceptó por parte de España la implementación de la Transmisión Remota de los datos (conocida por sus siglas en inglés como RDT- *Remote Data Transmission*). El RDT consiste en el envío remoto de los datos y señales de los equipos de salvaguardias que el Organismo Internacional de Energía Atómica (OIEA) y la Comisión Europea tienen instalados en los reactores nucleares españoles (como cámaras o sellos electrónicos). Se ha iniciado el envío oficial de datos de forma remota a Luxem-

burgo desde el almacén temporal individualizado de la central nuclear de Trillo. Quedaría, por tanto, como reto pendiente dicha implantación en el resto de centrales nucleares españolas.

En definitiva, se debe colaborar con las organizaciones internacionales involucradas en la No Proliferación, como la OPAQ o el OIEA, y en regímenes de control como el Grupo de Australia (relativo a material químico y biológico), el Grupo de Suministradores Nucleares GSN o el Régimen de Control de Tecnología de Misiles (MTCR, en sus siglas en inglés correspondientes a la denominación *Missile Technology Control Regime*).

En relación a los países proliferadores, se trabaja en detectar y verificar sus avances, intentos de adquisición de material y tecnología, y su colaboración con otros países en programas de armas de destrucción masiva, sobre todo en los ámbitos nuclear y de misiles balísticos.

Un factor de suma importancia son las exportaciones y tránsitos de productos y tecnologías (incluidas las intangibles) de doble uso que pudieran utilizarse con fines ilícitos en contravención de la normativa internacional o nacional aplicables.

Estos movimientos han de estar bajo control siempre que intervengan personas físicas o jurídicas españolas o radicadas en España, se utilice el territorio nacional o afecten a la seguridad de España o a sus intereses. Para ello, será necesario reforzar la sensibilización y colaboración de los organismos nacionales e internacionales y de los países comprometidos con la prevención y lucha contra la proliferación de las armas convencionales y las de destrucción masiva, fortaleciendo la seguridad de la cadena logística internacional y el control fronterizo aduanero. Ha de extenderse esa labor dentro de España a autoridades, empresas, laboratorios, centros de investigación, etc.

La gestión efectiva de los riesgos es una tarea que concierne a los distintos organismos representados en la Junta Interministerial reguladora del comercio exterior de Material de Defensa de Doble Uso (JIMDDU) y por tanto exige una estrecha cooperación entre ellos, con el fin de garantizar la adecuada vigilancia y controles aduaneros de las mercancías estratégicas seleccionadas que entren y salgan del territorio. En la estrategia aduanera deben quedar identificados los parámetros de evaluación de la amenaza y los bienes estratégicos de ámbito nacional que van a ser objeto de control.

Dentro del régimen existente en materia de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso, y teniendo en cuenta las recomendaciones realizadas por el GAFI, uno de los retos a afrontar es la modificación del *RD 679/2014, de 1 de agosto, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso*, que regula la composición y competencias de la JIMDDU, con objeto, entre otros aspectos, de integrar al SEPBLAC.

Igualmente, se han de mantener activos y profundizar en los mecanismos para la prevención, detección y control de los flujos financieros relacionados con la proliferación, en línea con las Resoluciones del Consejo de Seguridad de Naciones Unidas y los Reglamentos de la UE.

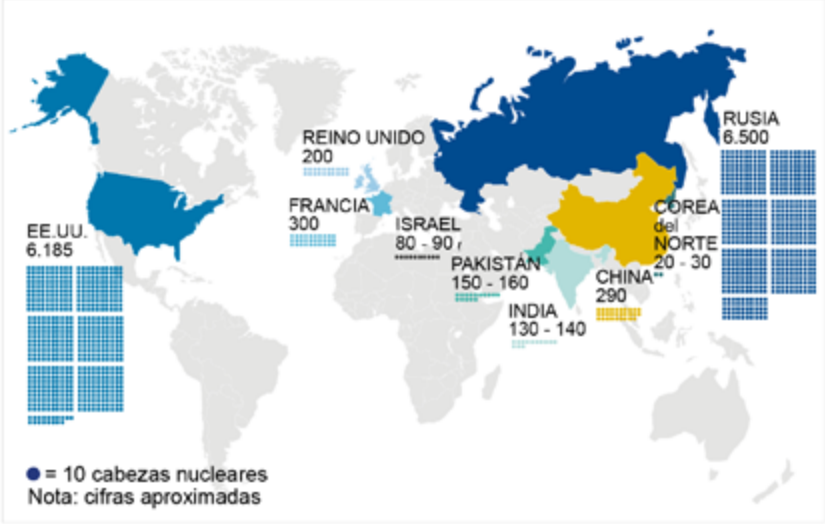
En este sentido, el reto fundamental es la aplicación directa e inmediata de las Resoluciones de Naciones Unidas, para lo cual se plantea como necesidad la reforma de la actual *Ley 10/2010 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo*.

En cuanto al *Real Decreto 1308/2011, de 26 de septiembre, sobre la protección física de las instalaciones nucleares, y de las fuentes radiactivas*, habiendo transcurrido ocho años desde su publicación en el Boletín Oficial del Estado (BOE), y teniendo en cuenta la práctica adquirida, se hace necesaria la modificación de determinados aspectos de este Real Decreto.

Garantizar la seguridad física de los materiales e instalaciones nucleares y radiactivos es un aspecto de gran relevancia. En este sentido, para el Departamento de Aduanas e Impuestos Especiales de la Agencia Tributaria supone un reto permanente el mantenimiento del nivel de control basado en la tecnología y el análisis de riesgos.

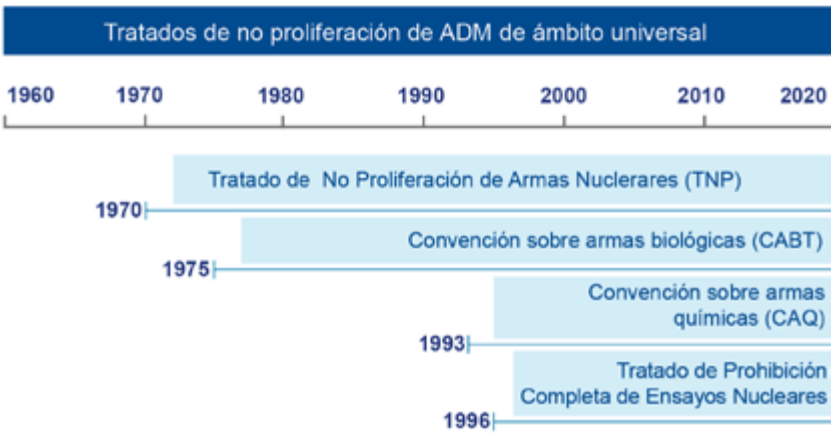
En relación a las Fuerzas Armadas (FAS), se quiere desarrollar procedimientos para la participación de sus capacidades en las iniciativas y operaciones de interceptación de armas de destrucción masiva y poner en práctica y mejorar el proceso de toma de decisiones y coordinación de actores implicados en una situación de crisis de estas características.

Figura 4-1
Inventario estimado de cabezas nucleares en el mundo



Fuente: Instituto Internacional de Estudios para la Paz de Estocolmo (SIPRI)

Figura 4-2
Principales Tratados de no Proliferación de Armas de Destrucción Masiva



Fuente: Elaboración del DSN

Realizaciones

El Comité Especializado de No Proliferación de Armas de Destrucción Masiva constituye un impulso de primer orden en la no proliferación de armas de destrucción masiva. El Comité, que apoya al Consejo de Seguridad Nacional en el desempeño de sus funciones, posee una visión omnicomprensiva de los campos, nuclear y radiológico, químico y biológico, al tiempo que armoniza y refuerza la coordinación y actuación del Gobierno en dichas materias.

Multilateralismo eficaz y refuerzo del régimen internacional de no proliferación

España mantiene un fuerte compromiso respecto de todos los esfuerzos internacionales de desarme convencional y es parte de los tratados fundamentales, como la Convención sobre ciertas armas convencionales, el *Tratado para la Prohibición de Minas Antipersonal*, la Convención sobre municiones de racimo, el *Tratado sobre Fuerzas Armadas Convencionales en Europa*, el *Tratado de Cielos Abiertos* (conocido como *Open Skies)*. También se mantiene un compromiso activo con los objetivos de la *Convención sobre las Armas Químicas*. En este sentido, a lo largo de 2019 el Ministerio de Defensa, a través del Laboratorio de Verificación de Armas Químicas del Instituto Nacional de Técnica Aeroespacial (INTA), contribuyó a la formación dirigida al Grupo de países de Latinoamérica y del Caribe. También en 2019 las Fuerzas Armadas han revisado su aportación a la *Proliferation Security Initiative* (PSI).

España está comprometida con los esfuerzos internacionales de desarme convencional y es parte de los tratados fundamentales

Por otra parte, España participó en la operación de seguridad marítima *Sea Guardian*, entre cuyos cometidos adicionales, sujetos a la aprobación política por parte del Consejo Atlántico, figura la lucha contra la proliferación de armas de destrucción masiva.

Las FCSE fueron parte del *2019 Global Congress on Chemical Security and Emerging Threats*, organizado por Interpol con la finalidad de ampliar y afianzar las enseñanzas y procedimientos de actuación sobre respuesta ante atentados o incidentes con agentes químicos.

Además, es importante señalar que la Estación Primaria del Sistema Internacional de Vigilancia de Naciones Unidas de la Comisión del Tratado de Prohibición Completa de Ensayos Nucleares (CTBTO) en Sonseca (Toledo), no registró durante el año ninguna explosión nuclear declarada como tal por la CTBTO.

La participación española también fue muy activa en la coordinación con los servicios que integran la comunidad de Inteligencia occidental, con los que se comparte cada vez más y mejor información, y se ejecutaron con eficacia acciones conjuntas.

En la UE, España forma parte de las Estrategias de desarme y no proliferación desde su adopción en 2003 y 2005 respectivamente, así como de todas las iniciativas y decisiones adoptadas por el Consejo de la Unión Europea.

Desde principios de 2018, España, a través del Ministerio del Interior, participa activamente en el Grupo Asesor NRBQ (Nuclear, Radiológico, Biológico y Químico) de la UE, creado para la aplicación del *Plan de*

acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares de la UE. Este Plan tiene la finalidad de aumentar la cooperación europea para reforzar la seguridad NRBQ, poniendo el acento en la prevención, la preparación y la respuesta a estas amenazas y los atentados terroristas. En este ámbito, para coordinar la implantación del citado Plan, en España se creó el Grupo de trabajo interministerial liderado por el Ministerio del Interior. España contribuyó a la elaboración de un listado de productos químicos que pueden ser empleados como agentes químicos.

Desde la Secretaría de Estado de Energía se realizaron las acciones oportunas de cara a la preparación del sector nuclear ante el escenario de *brexit*. Parte de las implicaciones tienen relación con el cumplimiento *del Real Decreto 1308/2011, de 26 de septiembre, de protección física de las instalaciones y los materiales nucleares, y de las fuentes radiactivas*, en su aplicación para los transportes de material nuclear entre el Reino Unido y la fábrica de combustible nuclear de Enusa, en Salamanca.

Cooperación internacional en la lucha contra el tráfico ilícito reforzando las políticas y prácticas de control de las exportaciones

Las herramientas para controlar las exportaciones de material de doble uso se ampliaron y reforzaron, y se potenciarán más aun con la aplicación de controles *ex post* y la puesta en marcha de un protocolo de actuación ante casos de interceptaciones de dicho material.

Cabe destacar la participación en las reuniones del GAFI en materia de proliferación de armas de destrucción masiva, colaborando con la elaboración de documentación, como el documento sobre Financiación de la Proliferación elaborado por el *Policy Development Group* (*think tank* privado norteamericano). En 2019, España estuvo involucrada en el proceso de evaluación periódica (5° año) del GAFI en el que se comprueba el nivel de cumplimiento de sus 40 recomendaciones. El resultado para España fue positivo, pasando de *moderate* a *substantial* en su nivel de cumplimiento.

A fin de reforzar la coordinación de actuaciones de investigación, persecución y delitos de contrabando sobre productos que sean susceptibles de ser destinados a la proliferación de armas de destrucción masiva, se creó, dentro de la Subdirección General de Operaciones del Departamento de Aduanas e Impuestos Especiales de la Agencia Tributaria, una nueva área denominada "Seguridad y Protección" que desarrolla, entre otras, tareas de coordinación de investigaciones policiales que instruyan las unidades territoriales de vigilancia aduanera, detección y análisis de bienes que pudieran ser de riesgo o el análisis y propuesta de perfiles de riesgo para poder establecer filtros de identificación de movimientos sospechosos de tráfico ilícito de estos productos.

España también intensificó su actividad en los distintos foros internacionales de contra Proliferación, especialmente en la Iniciativa para la Seguridad contra la Proliferación de carácter global para prevenir el tráfico ilícito de armas de destrucción masiva, hacia y desde actores no estatales, entendida como marco de referencia en materia de coordinación internacional e intercambio de prácticas y capacidades frente a

dicho reto, especialmente en lo referente a actuaciones específicas de interdicción en distintos escenarios: marítimo, terrestre y aéreo.

Las FCSE participaron en la segunda fase de las actividades desarrolladas por la UE en Santiago de Chile y en Valparaíso (Chile), en el proyecto de promoción del *Tratado de Comercio de Armas -ATT-* (EU P2P *Export Control Programme for Arms*), organizado por la Oficina Federal de Economía y Control de Exportaciones de Alemania y el *Expertise France* con el fin de capacitar a personal de los organismos implicados en el proceso de incorporación del mencionado Tratado en Chile.

También contribuyeron a la elaboración del borrador final relativo a emergencias, preparación y respuesta a incidentes nucleares o radiológicos y participaron en la reunión del Grupo de Trabajo de Detección Nuclear, desarrollada en Tánger (Marruecos), dentro de las actividades de la Iniciativa Global contra el Terrorismo Nuclear y con la finalidad de estudiar diferentes procedimientos y actividades operativas de detención de materiales nucleares y radiológicos en su paso clandestino por pasos fronterizos habilitados o no.

Fortalecer las capacidades nacionales en no proliferación y contra proliferación

El Plan Nacional de Biocustodia fue aprobado por el Consejo de Seguridad Nacional en 2019

Destaca la formación de un grupo de trabajo para la creación y puesta en marcha de la Comisión Nacional de Biocustodia creada en el seno del Comité Especializado de No Proliferación de Armas de Destrucción Masiva, para dar cumplimiento al mandato del Plan Nacional de Biocustodia (PCI/168/2019), elaborado por dicho Comité y aprobado por el Consejo de Seguridad Nacional en enero de 2019. Con el desarrollo de estos trabajos España se pondría al nivel de los países más avanzados para el control del uso de material biológico con fines terroristas o ilícitos.

La Red de Laboratorios de Alerta Biológica (RE-LAB), coordinada por el Instituto de Salud Carlos III (ISCIII), dio respuesta a las alertas por envíos postales conteniendo posibles agresivos biológicos producidas durante este año. La RE-LAB es una infraestructura de apoyo científico-técnico al Sistema de Seguridad Nacional ante situaciones de riesgo biológico, formada por una serie de laboratorios especializados en microbiología, entre los que se encuentran el laboratorio biológico del INTA en calidad de laboratorio de referencia, y el Laboratorio de Verificación Rápida (LABIR) de la UME, como laboratorio colaborador dentro de sus competencias en el ámbito de la protección civil. (Figura 4-3)

Por otra parte, el riesgo de desvío a programas de armas de destrucción masiva se detectó y evitó en varios casos gracias a la obtención de inteligencia por medios propios y por la estrecha colaboración con otros servicios, a la eficaz coordinación con Vigilancia Aduanera de la Agencia Tributaria y las FCSE y a la acción de la JIMDDU. Se tiene un mejor conocimiento de los programas de armas de destrucción masiva de los países objetivo, con lo que se está en una mejor posición para asesorar a las autoridades sobre ellos cuando así lo requieran.

Si bien las transacciones de materiales estratégicos están sujetas a controles tanto nacionales, como internacionales, la cada vez más ágil interconexión en los nodos portuarios y aeroportuarios, unida a un

volumen cada vez mayor de mercancías, permite explotar las ventajas de los transbordos para evadir los controles nacionales. Por ello, se creó un Grupo de Trabajo de Interceptación para casos de desvío de Armas de Destrucción Masiva, sus vectores o materiales conexos, dependiente del Comité Especializado de No Proliferación de Armas de Destrucción Masiva del Consejo de Seguridad Nacional, grupo en el que participaron las FAS mediante personal experto.

Las FCSE reforzaron la preparación de su personal mediante acciones formativas que contemplan, de forma específica, el conocimiento de tecnologías y materiales de doble uso. En este sentido, participaron en la planificación del ejercicio de Seguridad Nacional CRISEX 2020, donde se abordó, entre otros supuestos, un escenario relativo al hallazgo de material nuclear en la frontera y participaron en los cursos de formación de operadores MEGAPORT, desarrollados en Valencia y organizados por la Agencia Tributaria con el apoyo del Servicio de Aduanas de Estados Unidos, así como en el ejercicio de campo relativo a la evaluación de los protocolos y procedimientos del sistema MEGAPORT, que tuvo lugar en el Puerto de Barcelona.

Por su parte, desde el CNI se llevaron a cabo sesiones divulgativas de sensibilización e información en la Administración central, con la finalidad de fortalecer las capacidades nacionales de aplicación de la legislación nacional e internacional. En esta línea de sensibilización, se realizaron labores de difusión y concienciación del sector privado sobre sus obligaciones en materia de cumplimiento, tanto presencialmente como a través de la web del Ministerio de Economía y Empresa.

Para una mejor coordinación institucional, se realizaron reuniones con los representantes de ministerios y organismos públicos competentes en materia de sanciones adoptadas en el marco de Naciones Unidas y de la Unión Europea en temas de lucha contra la proliferación, para mejorar el Mecanismo de Coordinación Interministerial y la actualización de la red de puntos focales. También se actualizaron las guías en materia de proliferación de armas de destrucción masiva en relación con Irán y la República Popular Democrática de Corea.

Igualmente se está potenciando la actividad del Grupo de Trabajo de Interceptación de ADM, impulsado por el Consejo de Seguridad Nacional. Todo ello al objeto de crear un cuerpo legislativo y mecanismos de coordinación interministerial para hacer frente al reto de la Proliferación de Armas de Destrucción Masiva siguiendo las recomendaciones de la Resolución del Consejo de Seguridad de Naciones Unidas 1540.

Garantizar la seguridad física de los materiales e instalaciones nucleares y radiactivos

En 2016 se publicó en el BOE la Instrucción de Seguridad IS-41, del Consejo de Seguridad Nuclear, por la que se aprobaron los requisitos sobre protección física de fuentes radiactivas. En su disposición transitoria, se concedía hasta marzo de 2018 para que sus titulares adaptaran los correspondientes sistemas de protección física requeridos, algo que implicaba presentar una solicitud de aprobación del Plan de Protección Física. Dado que en el ámbito de aplicación de las instalaciones y fuentes radiactivas existe una variedad de autoridades competentes impli-

cadas, desde la Subdirección General de Energía Nuclear se ejerció la labor de coordinación con el Consejo de Seguridad Nuclear, Ministerio del Interior y aquellas Comunidades Autónomas con competencias transferidas (todas excepto Andalucía y Castilla La Mancha), de cara a aplicar una gestión de expedientes armonizada.

Desde marzo de 2018 hasta la actualidad se recibieron, en el ámbito de competencias de la Dirección General de Política Energética y Minas, 30 solicitudes de aprobación de los Planes de Protección Física de dichas instalaciones.

RED DE LABORATORIOS DE ALERTA BIOLÓGICA "RE-LAB"

Laboratorios de referencia:

- Laboratorios del Centro Nacional de Microbiología del Instituto de Salud Carlos III, adscrito al Ministerio de Ciencia e Innovación.
- Laboratorios del Centro Nacional de Sanidad Ambiental del Instituto de Salud Carlos III.
- Laboratorio del Centro Nacional de Alimentación de la Agencia Española de Seguridad Alimetaria y Nutrición, adscrito al Ministerio de Sanidad.
- Laboratorios del Centro de Vigilancia Sanitaria Veterinaria de la Universidad Complutense de Madrid.
- Laboratorios del Centro de Investigación en Sanidad Animal del Instituto Nacional de Investigación y Tecnología Agraria y Alimentaria, adscrito al Ministerio de Ciencia e Innovación.
- Laboratorio Biológico "La Marañosa", integrado en el Instituto Nacional de Técnica Aeroespacial "Esteban Terradas", Organismo Público adscrito al Ministerio de Defensa.
- Laboratorio Central de Veterinaria del Ministerio de Agricultura, Ganadería, Pesca y Alimentación.
- Laboratorios del Centre de Recerca en Sanitat Animal del Instituto de Investigación y Tecnología Agroalimentarias, adscrito al Departamento de Agricultura, Ganadería, Pesca y Alimentación de la Generalitat de Cataluña.
- Laboratorios del Instituto Vasco de Investigación y Desarrollo Agrario NEIKER-Tecnalia, del Gobierno Vasco.
- Laboratorios del Centro de Rickettsiosis y Enfermedades transmitidas por Artrópodos Vectores, del Centro de Investigación Biomédica de La Rioja, del Gobierno de La Rioja.
- Laboratorios del Instituto Universitario de Enfermedades Tropicales y Salud Publica de Canarias, dependiente de la Universidad de La Laguna.
- Laboratorios de Virología y Bacteriología del Centro de Protección Vegetal y Biotecnología del Instituto Valenciano de Investigaciones Agrarias, de la Generalitat Valenciana.

Laboratorio colaborador:

Laboratorio de Identificación Rápida del Grupo de Intervención de Emergencias Tecnológicas y Medioambientales de la Unidad Militar de Emergencias del Ministerio de Defensa.

Figura 4-3
Red de laboratorios de alerta biológica RE-LAB

Fuente: Ministerio de Ciencia e Innovación

CONTRAINTELIGENCIA

OBJETIVO:

Adoptar medidas en la defensa de los intereses estratégicos, políticos y económicos de España para prevenir, detectar y neutralizar las agresiones encubiertas, incluidas las efectuadas desde el ciberespacio, procedentes de otros Estados, de sus Servicios de Inteligencia o de grupos o personas, y que estén dirigidas a la obtención ilegal de información.

Tendencias

En los últimos años se han detectado intentos de aproximación y captación sobre ciudadanos españoles y extranjeros, vinculados con actividades desarrolladas en los ámbitos políticos, religiosos y empresariales o bien relacionados con instituciones de las que España forma parte.

En 2019 varios Servicios de Inteligencia han ampliado su presencia en España

En concreto, varios Servicios de Inteligencia han ampliado su presencia en España, cambio que ha provocado un notable incremento de sus actividades. Asimismo, se ha observado un aumento en sus intentos de adquisición de información en los ámbitos científico y tecnológico. Es destacable la utilización de coberturas diplomáticas, empresariales o periodísticas. Este hecho obliga a realizar un importante esfuerzo en la detección y neutralización de sus actividades. (Figura 5-1)

Del mismo modo, y enmarcado en el concepto TESSCO (Terrorismo, Espionaje, Sabotaje, Subversión y Crimen Organizado) de la OTAN, se ha producido un notable incremento en operaciones relacionadas con subversión, dirigidas a deteriorar la imagen que tiene la ciudadanía española sobre las Fuerzas Armadas (FAS).

El ciberespionaje se está convirtiendo en una práctica habitual. Por ello, las actividades de determinados Servicios de Inteligencia plantean la necesidad de seguir reforzando la cooperación internacional y desarrollando capacidades técnicas que permitan prevenir aquellos casos de ciberataques en contra de organismos ministeriales y entidades económicas nacionales, en su mayoría realizados desde el exterior y utilizando complejos sistemas de ataque informático, de manera que se dificulta su neutralización.

Igualmente, se ha detectado un incremento en las actividades realizadas por otros Estados, que tienen como objetivo influir en los procesos políticos y sociales que se desarrollan en Europa y también en España. A este fin, utilizan toda clase de iniciativas, tanto en el mundo físico como en el virtual.

Las acciones de desinformación son de especial importancia por su potencial de desestabilización política

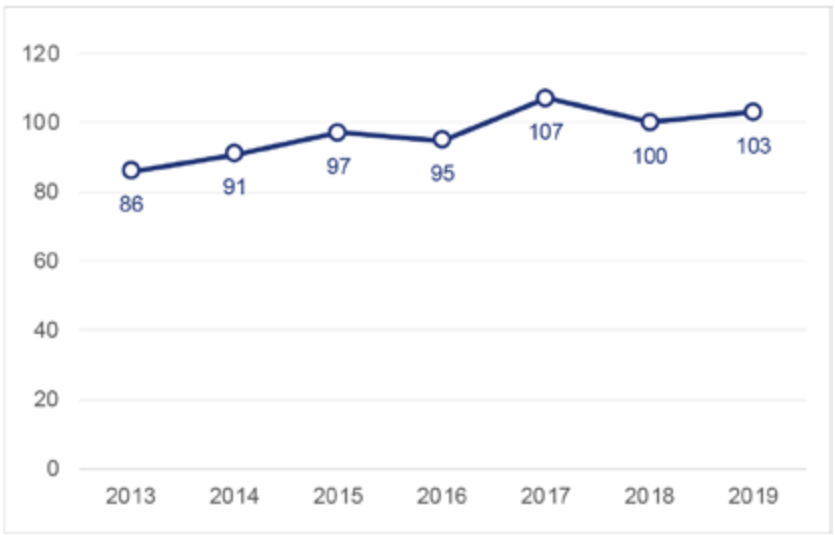
De especial importancia son las acciones de desinformación desplegadas principalmente en las grandes plataformas de comunicación online, redes sociales y también en espacios digitales. (Figura 5-2)

Esto es así por su potencial de desestabilización política, pues pretenden en general desacreditar a las instituciones democráticas a través de la generación de desconfianza y polarización social, que alientan respuestas radicales e ideologías extremistas. En las diversas convocatorias electorales de 2019 se han detectado actividades de manipulación informativa, que, sin embargo, no han constituido campañas sostenidas o masivas de desinformación.

Por lo que respecta a la responsabilidad de la Oficina Nacional de Seguridad (ONS), se ha producido una notable intensificación en la atención prestada a la protección de la información clasificada en las instituciones europeas motivada, especialmente, por el desarrollo de proyectos en los ámbitos de seguridad y del espacio. Cabe destacar el incremento producido en la promoción y gestión de numerosos programas clasificados de la mano de organismos y consorcios internacionales, como son la Agencia de Defensa Europea, la Agencia Espacial Europea, la Organización para la Cooperación Conjunta de Armamento y la Agencia OTAN de Gestión del *Eurofighter* y del *Tornado*, principalmente.

En el ámbito empresarial se han incrementado las solicitudes de acreditaciones de seguridad para participar en las licitaciones de contratos clasificados promovidos por la Administración Pública, en particular por el Ministerio de Defensa.

Figura 5-1
Índice de actividad de los Servicios de Inteligencia extranjeros



Fuente: Centro Nacional de Inteligencia

Retos

España como actor geopolítico, tanto en el marco de la UE como a escala internacional, es un sujeto de interés para otros Estados que pueden tratar de minar su estabilidad o influir en cuestiones de su política interna haciendo uso de los Servicios de Inteligencia. La motivación subyacente es el favorecimiento de sus intereses a través de actuaciones que más allá del ámbito económico y empresarial, merman la propia cohesión y fortaleza de la UE como sujeto internacional.

La transversalidad de las operaciones híbridas hace que haya que prestar una especial atención a las actividades de los Servicios de Inteligencia extranjeros, una de las principales herramientas de los Estados para ejecutar este tipo de acciones.

Especialmente relevante es el caso de los denominados Servicios de Inteligencia Hostiles (HOIS por sus siglas en inglés correspondientes a la denominación Hostile Intelligence Services), en sus distintas vertientes, que habrían comenzado a incrementar su actividad en España con anterioridad a la crisis en Cataluña, en coherencia con un mayor dinamismo advertido en otros países occidentales (Alemania, Estados Unidos, Francia y Reino Unido), centrando sus acciones en campañas de desinformación que ponen el foco en cuestiones de política interna, especialmente desarrolladas en el ámbito cibernético.

Otro de los riesgos es la posible confluencia entre la actividad de los HOIS y el crimen organizado, pudiendo operar los primeros a través de elementos criminales y negando, en caso de ser detectados, cualquier vinculación con actividades dirigidas por un tercer Estado.

Para las Fuerzas Armadas (FAS) y las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), la principal amenaza detectada en relación a los HOIS es el acceso a la información de alto valor contenida en las bases de datos militares y policiales mediante la aproximación a miembros de estas organizaciones. Por su parte, para el CNI el reto es la detección de los intentos de reclutamiento y captación de ciudadanos españoles, sobre todo en instituciones vinculadas con la Seguridad Nacional y con organismos supranacionales fuera de España.

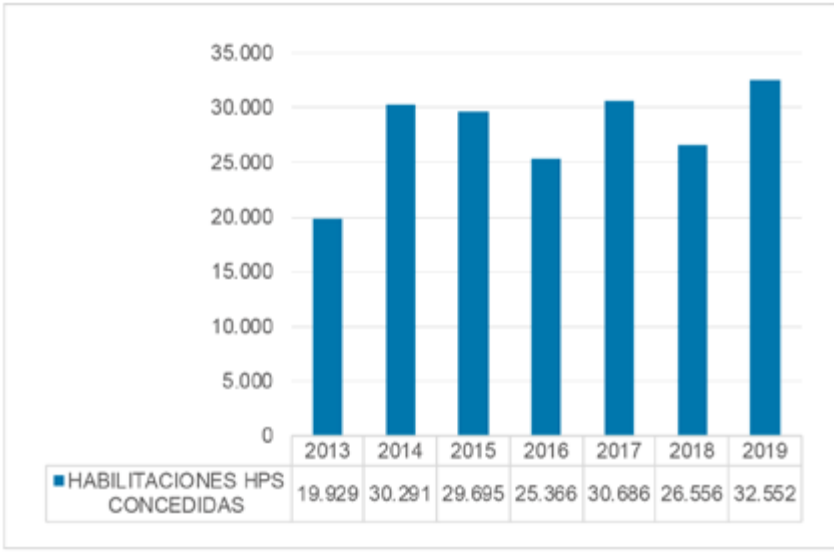
En el ámbito de la ONS, la mejora del marco normativo, especialmente con la actualización de la Ley 9/1968, de 5 de abril, sobre secretos oficiales, es uno de los principales retos. Es necesaria su adaptación a la nueva estructura orgánica y funcional del Estado, acorde a las necesidades que demandan hoy en día los nuevos procedimientos y técnicas.

Son tres los asuntos principales objeto de actualización: los procedimientos que regulan la concesión/denegación de las habilitaciones de seguridad para el acceso a la información clasificada por las empresas y las personas; la regulación referida a la licitación y ejecución de los contratos clasificados celebrados por el sector público, incluyendo aquélla específica respecto a las inversiones y participaciones extranjeras en empresas con habilitación de seguridad para el acceso a la información clasificada; y los procedimientos normativos que permiten integrar el manejo de la información clasificada en el ámbito de la administración electrónica del Estado. (Figura 5-3)

Figura 5-2
Características de las campañas de desinformación

Fuente: Centro Criptológico Nacional

Figura 5-3
Número de Habilitaciones Personales de Seguridad concedidas por la Oficina Nacional de Seguridad 2013-2019



Fuente: Centro Nacional de Inteligencia

Realizaciones

En un contexto en el que se produce la utilización de estrategias híbridas, las actividades de Inteligencia de los Servicios Hostiles se prevalen de la complejidad que ofrecen las tecnologías digitales para ejercer influencia en contra de la confianza de la sociedad en los procesos libres y democráticos.

Por estos motivos, de especial relevancia ha sido la aprobación por el Consejo de Seguridad Nacional, el 15 de marzo de 2019, del *Procedimiento de actuación contra la desinformación*, documento que da respuesta a las exigencias marcadas por el *Plan de acción contra la desinformación* aprobado por la UE en diciembre de 2018, y supone un refuerzo de las garantías para el desarrollo de unos procesos democráticos sin interferencias indebidas.

En 2019 el Consejo de Seguridad Nacional aprobó el Procedimiento de actuación contra la desinformación

Refuerzo de capacidades

El seguimiento y control de las actividades que llevan a cabo los Servicios de Inteligencia extranjeros en España es una de las prioridades establecidas en el CNI a la hora de prevenir acciones de injerencia de terceros Estados en la estabilidad política, social y económica, así como en la defensa de la soberanía e integridad territorial.

Por parte del CNI se ha incrementado de manera sustancial la sensibilización y la divulgación sobre esta amenaza a otros organismos de la Administración Pública y empresas de sectores estratégicos, haciendo especial énfasis en la importancia de intensificar las medidas de seguridad ante determinados ciberataques y actuaciones de captación sobre miembros de sus organizaciones.

Se han mejorado, por una parte, los procedimientos de control sobre personal extranjero no aliado (militar o civil) y, por otra parte, se han perfeccionado los procedimientos de coordinación entre diversos organismos armados específicos y conjuntos.

La incorporación de un Oficial de Enlace de la Guardia Civil en el Centro de Inteligencia de las Fuerzas Armadas (CIFAS) ha mejorado sustancialmente el intercambio de información e inteligencia en beneficio de las misiones de las FAS.

Protección de la información clasificada

La información clasificada es un activo cuya protección se articula en distintas dimensiones, que comprenden actividades formativas y de concienciación del personal, así como procesos funcionales y normativos que aportan solidez estructural.

En el campo de la concienciación sobre la importancia de proteger la información clasificada, cabe destacar la adopción de medidas de mejora a través de jornadas formativas realizadas para personal que desempeña los cometidos de inspectores de seguridad respecto de contratos clasificados, responsables de seguridad de los programas y personal de los órganos de contratación y los órganos de control de la documentación clasificada

En lo que respecta a la ONS, se ha incrementado el nivel de actuaciones dirigidas a la formación y concienciación en materias de protección de la información clasificada, mediante la realización de cursos a responsables de la seguridad de la información en organismos y empresas, y de sesiones especiales, dirigidas a altos cargos de la Administración.

Desde el punto de vista de la solidez funcional, es destacable la adopción de medios seguros para el intercambio de información con las empresas y los órganos del Ministerio de Defensa con los que se relacionan en el marco de su participación en contratos clasificados.

Asimismo, se identifica personal, así como estructuras de información y tácticas, técnicas y procedimientos de Servicios de Información de determinados países que podrían estar realizando labores de información en territorio nacional, tratando de individualizar aquellos que pudiesen resultar hostiles y que tienen objetivos informativos sobre las FAS.

Además, se han mejorado los sistemas de intercambio de información en todo lo relacionado con los procesos y procedimientos de habilitación, acceso, manejo y control de la información clasificada a nivel nacional e internacional; se ha incrementado, tanto en el sector público como en el sector privado, el número de instalaciones acreditadas para la protección y manejo de información clasificada; se ha implementado un sistema de inspección continua de la infraestructura de protección de información clasificada en empresas habilitadas para su manejo; y se han establecido nuevos procedimientos para la supervisión y control de los contratos clasificados, así como de las empresas participantes.

Cooperación internacional

En la ONS se trabaja en la constitución de nuevos grupos de seguridad en el marco de los programas internacionales, al tiempo que se mantiene constante la participación en los ya existentes.

En cuanto a la conclusión de acuerdos bilaterales para la protección de la información clasificada, la ONS gestiona 49 tratados internacionales, 44 de ellos bilaterales y 5 multilaterales, y otros 37 en distintas fases de negociación o tramitación, 5 de ellos pendientes de firma o de ratificación parlamentaria.

En el marco del seguimiento de las actividades de los Servicios de Inteligencia considerados hostiles el CNI lleva a cabo un esfuerzo por redoblar la cooperación con países amigos y aliados, con los que se trabaja conjuntamente en operaciones e investigaciones.

El CNI proyecta también su actuación fuera de España en la protección de los intereses nacionales y en apoyo a inversiones de empresas españolas en el exterior, con el objeto de anticipar las amenazas que se pudieran detectar y, a su vez, favorecer los intereses comerciales y empresariales españoles en el exterior.

Se reforzó la cooperación con la UE en la lucha contra las amenazas híbridas mediante la creación de un nuevo grupo de trabajo horizontal en el seno del Consejo de la UE, en el que España ha participado activamente, entre otras cuestiones, presentando el modelo nacional de protección de infraestructuras críticas. El Consejo de Seguridad Nacio-

nal, a través del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, asegura la coordinación entre los órganos y organismos con competencia en la materia y la adopción de las posiciones nacionales sobre esta cuestión ante el Grupo Horizontal para la mejora de la resiliencia y para hacer frente a las amenazas híbridas.

España también participa activamente en el Centro Europeo de Excelencia contra las Amenazas Híbridas de Helsinki (Finlandia), centro de conocimientos especializados que, auspiciado por la UE y la OTAN, apoya los esfuerzos individuales y colectivos de los países participantes para mejorar sus capacidades civiles-militares, resistencia y preparación para hacer frente a amenazas híbridas. Dentro del marco general de actuación de este Centro de Excelencia de Helsinki, la participación española contribuye a proporcionar una visión integral con un enfoque que contemple de forma equilibrada a todas las amenazas a la seguridad europea.

España participa activamente en el Centro Europeo de Excelencia contra las Amenazas Híbridas de Helsinki

Ha continuado el desarrollo de los mecanismos previstos en el *Plan de Acción contra la Desinformación de la UE*, reforzando las células o agrupaciones operativas dedicadas a las vecindades oriental, sur y Balcanes occidentales y manteniendo la necesaria coordinación de acciones con las autoridades nacionales con el objetivo de proteger la confianza de los ciudadanos, salvaguardar el prestigio de las instituciones democráticas y la integridad de los procesos electorales.

CIBERSEGURIDAD

OBJETIVO:

Garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socioeconómico.

Tendencias

El ciberespacio se consolida como entorno de relevancia estratégica, geopolítica, económica, social e individual con importantes implicaciones para la Seguridad Nacional.

Es un ámbito sin fronteras ni nítidas demarcaciones jurisdiccionales, de débil regulación, más allá de los códigos de buenas prácticas sobre comportamiento responsable, donde resulta difícil la trazabilidad y atribución de las acciones delictivas llevadas a cabo con diferentes objetivos tanto por actores estatales -o sus posibles intermediarios-, como no estatales –organizaciones terroristas, *hacktivistas* y grupos de ciberdelincuencia organizada-, dada la fácil accesibilidad a un amplio abanico de técnicas y la extensión del cibercrimen como modelo de negocio.

La hiperconectividad amplía la superficie de vulnerabilidad a las amenazas complejas

Si bien la transformación digital presenta grandes posibilidades de emprendimiento tecnológico, desarrollo científico, y progreso socioeconómico, acompañados de las necesarias inversiones e investigación, desarrollo e innovación (I+D+i), la creciente dependencia de tecnologías digitales, la hiperconectividad de los ciudadanos, organizaciones e instituciones públicas amplía la superficie de vulnerabilidad a amenazas complejas. (Figura 6-1)

Estas amenazas retan la posibilidad de ofrecer servicios electrónicos cada vez más seguros y resilientes, que generen y mantengan la confianza del usuario, junto a las dimensiones de la confidencialidad y privacidad. (Figura 6-2, 6-3 y 6-4)

El número de ciberincidentes, su alcance, continua y rápida evolución, sofisticación y severidad de su impacto sigue aumentando anualmente a escala global, tendencia a la que contribuye la falta de concienciación y formación en ciberseguridad.

En 2019 han proliferado los incidentes de ransomware

Siguen proliferando los incidentes de secuestro de información (*ransomware*), adaptados al tipo de víctima y a la forma de intrusión y rescate solicitado. Afectan tanto a sectores críticos, servicios esenciales y organismos estatales, como a empresas y ciudadanos. Las campañas de *Emotet*/*Riuk,* de alto impacto en operadores tanto públicos como privados, son un ejemplo de esta ciberamenaza.

Existe también en España un crecimiento significativo de direcciones del protocolo de Internet (más conocidas como IP por sus siglas en inglés correspondientes a la denominación *Internet Protocol*) comprometidas o vulnerables por *botnets* (red de robots informáticos o bots que se ejecutan de manera autónoma y automática, cuyo artífice puede controlar todos los ordenadores y servidores infectados de forma remota), del mismo modo que un incremento de los ataques distribuidos de denegación de servicios (DDoS, por sus siglas en inglés correspondientes a la denominación *Distributed Denial of Service*).

Igualmente, se ha observado una creciente tendencia en la explotación de vulnerabilidades para lanzar operaciones colectivas de *spear-phishing* (ataques personalizados con el objetivo de infectar los equipos de sus víctimas). Prolifera el conocido como "fraude al CEO", dirigido a los empleados con acceso a los recursos de la empresa. También se ha detectado un aumento de amenazas persistentes avanzadas (APT por sus siglas en inglés correspondientes a la denominación *Advanced Persistent Threat*) que, de forma permanente, actúan contra entornos móviles y de servicios en la nube (*cloud*), o contra sistemas de control industrial, que suscitan siempre el complejo problema de la atribución de su autoría.

Aunque se ha producido un descenso significativo de las amenazas e incidentes relacionados con el fraude electrónico, se ha elevado el número de incidentes en el ámbito de las redes académicas y de investigación, debido al mayor nivel de exposición de sus sistemas.

Además, se prevé que, en los próximos años, la ciberamenaza se agrave por la irrupción de las nuevas tecnologías de progresiva implantación, como la computación cuántica, el *blockchain*, el *Internet de las cosas* (IoT), el *Cloud*, el 5G y la inteligencia artificial.

La computación cuántica ha surgido en los últimos años como una tecnología disruptiva que, además de sus múltiples aplicaciones, tiene especial relevancia en la ciberseguridad, por cuanto se ha demostrado que disponer de un ordenador cuántico con la suficiente capacidad supone la vulneración de la mayor parte de los sistemas de cifrado actuales y sus aplicaciones (firma, identificación, autenticación, integridad, etc.), algo que demandará el desarrollo de nuevos sistemas criptográficos resistentes a la computación cuántica.

La tecnología *blockchain*, que permite un almacenamiento distribuido, auditable e inmutable de la información, está en continuo crecimiento. Sus aplicaciones en ciberseguridad han sido muy variadas, tanto en la industria como en el terreno científico. Es preciso sentar las bases que permitan una adecuada aplicación de este paradigma en materia de ciberseguridad, al tiempo que posibiliten aprovechar al máximo sus capacidades, incluyendo el desarrollo de contratos inteligentes.

El IoT permite la interconexión de dispositivos limitados en capacidad de cómputo y almacenamiento. Su irrupción en la vida diaria está siendo exponencial y entraña riesgos de seguridad que afectan directamente a los ciudadanos, sobre todo los relacionados con su privacidad.

La plena implantación del *cloud* en España supondrá una revolución digital para todos los sectores económicos, equivalente a la revolución de Internet, y tendrá un impacto muy positivo en toda la ciberseguridad del sistema económico y social.

La implantación del cloud en España supondrá una revolución digital para todos los sectores económicos

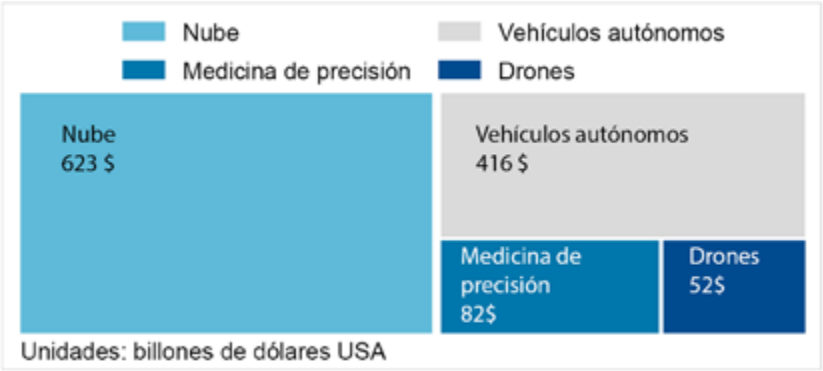
La futura dependencia de estas tecnologías y de otras como la inteligencia artificial o la tecnología 5G, que aumentará la velocidad de conexión y de dispositivos conectados, va a crecer significativamente (conducción autónoma, domótica inteligente, sistemas de control industrial, etc.), por lo que los ciberataques podrían tener un alto impacto no solo en el tejido económico o en la Administración Pública, sino en el ciudadano.

Por otro lado, será significativa su utilización como herramienta en las acciones híbridas que combinan el uso de capacidades tradicionales, con otros instrumentos como la manipulación de la información en Internet y redes sociales y los ciberataques.

Ante la nueva configuración de la ciberamenaza, los sistemas clásicos de ciberdefensa, basados principalmente en acciones reactivas tras el ataque, de defensa y mitigación de daños, están evolucionando hacia nuevos modelos que se complementan por medio de la llamada "defensa activa", centrada en la prevención, los prototipos predictivos y la disuasión del adversario.

El *hacktivismo*, tal y como se viene comprobando desde 2017, es una tendencia creciente vinculada a actos reivindicativos concretos con fines esencialmente políticos, que muestra no solo más actividad, sino también más efectividad en su búsqueda de notoriedad pública. Se acompaña con acciones que intentan manipular la opinión de la sociedad a través del uso de noticias falsas y desinformación. Entre las acciones de *hacktivismo* se incluye la autoatribución de ciberataques que nunca fueron perpetrados con éxito.

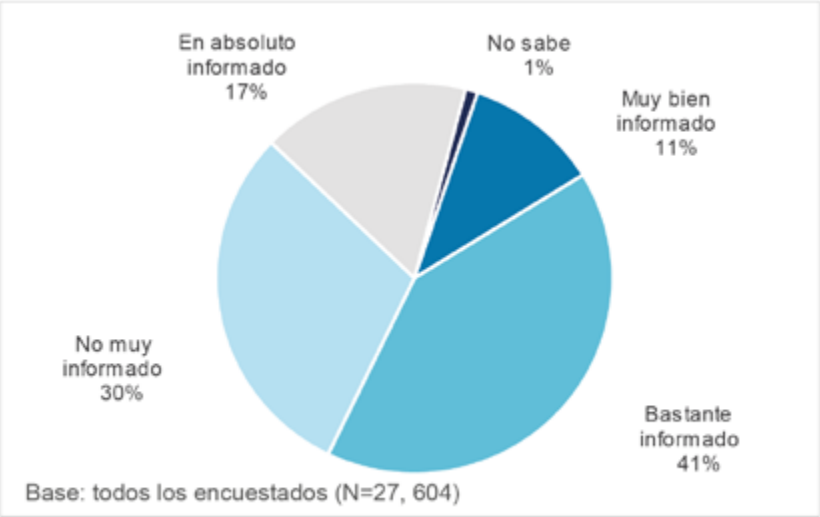
En otro orden de consideraciones, se está produciendo el acercamiento de las comunidades investigadora e industrial con los agentes finales, como las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), las unidades de Protección Civil y emergencias, y otros usuarios de los resultados de la I+D+i en seguridad, con objeto de fomentar la colaboración en esta materia.



Fuente: Elaboración del DSN con datos del Foro Ecónomico Mundial

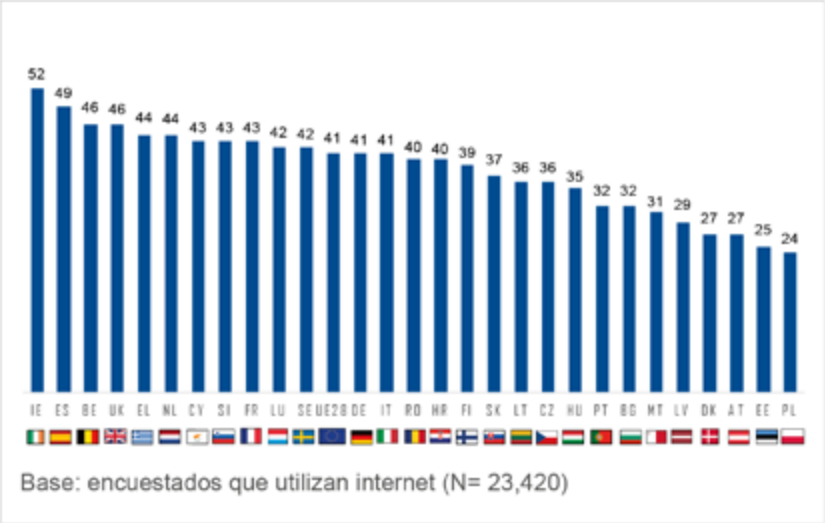
Figura 6-1
Proyecciones del mercado de tecnologías de la IV Revolución Industrial a 2025

Figura 6-2
Porcentaje de personas encuestadas que se consideran bien informadas sobre los riesgos del cibercrimen



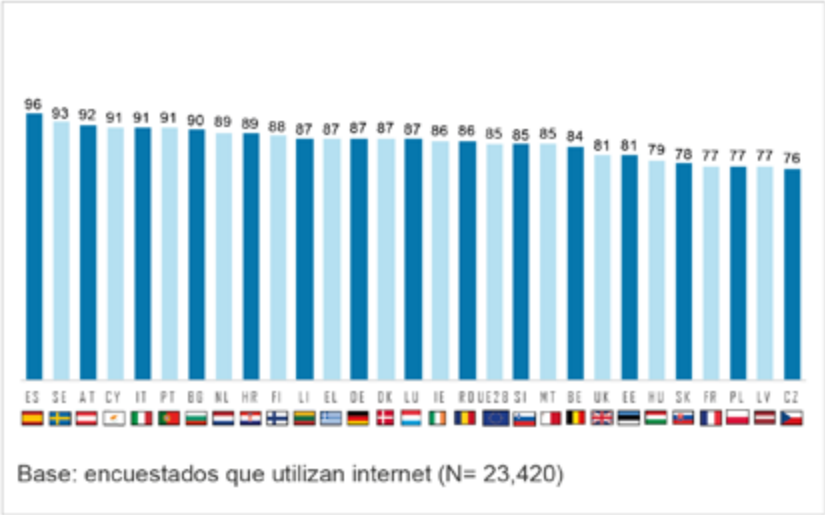
Fuente: Eurobarómetro 499 de Octubre 2019 (Comisión Europea)

Figura 6-3
Porcentaje de personas encuestadas que muestran preocupación sobre la seguridad de los medios de pago on line



Fuente: Eurobarómetro 499 de Octubre 2019 (Comisión Europea)

Figura 6-4
Porcentaje de personas encuestadas que utilizan el teléfono móvil para acceder a internet



Fuente: Eurobarómetro 499 de Octubre 2019 (Comisión Europea)

Retos

Uno de los principales retos de la ciberseguridad es la valoración precisa de la amenaza, para lo que es necesario la correcta atribución de los ciberataques, la detección del *modus operandi* y de las técnicas, tácticas y procedimientos de los autores, así como determinar el interés del agresor en las víctimas reales o potenciales, para detectar patrones que permitan la prevención de futuros ataques.

Es preciso reforzar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y defensa activa frente a las ciberamenazas, así como potenciar la coordinación a todos los niveles del Sistema de Seguridad Nacional. Se ha de avanzar en la mejora de las infraestructuras y la capacitación del personal destinado a las funciones de ciberseguridad, apostando por acciones encaminadas a la identificación y retención del talento. (Figura 6-5)

Debido a la especial relevancia que los ciberataques pueden tener como parte de actos de sabotaje, ciberespionaje, ciberterrorismo y operaciones híbridas, se requiere una mayor cooperación de las organizaciones de ciberdefensa, Servicios de Inteligencia, FAS, FCSE, otras Administraciones públicas y organismos internacionales y de estos con el sector privado, enfocada a incrementar las capacidades que contribuyan a mejorar la seguridad del ciberespacio. (Figura 6-6)

Esto implica incrementar la difusión de alertas tempranas, así como el intercambio de información sobre ciberamenazas y ciberincidentes entre todos los organismos competentes y la industria de la ciberseguridad y con el sector privado en general, tanto a nivel nacional como internacional, e implantar los mecanismos para que estos colectivos puedan establecer las medidas de ciberdefensa activa para la mejor protección de las redes y los sistemas de información.

En relación con la cooperación policial y judicial internacional, dada la natural dimensión transfronteriza de los ciberataques y la inexistencia de una legislación común que ampare en algunas ocasiones la persecución de los autores, los principios de cooperación y reciprocidad internacional son cardinales, para garantizar un espacio común seguro y fiable.

En este sentido, el refuerzo de la cooperación y la solidaridad con los miembros de la UE resulta fundamental en materia de lucha contra las amenazas híbridas y cibernéticas, y se ha de basar en el aumento del intercambio mutuo de información a través de los mecanismos y protocolos operativos establecidos.

La creación del Centro Europeo de Competencias Tecnológicas, Industriales y de Investigación para impulsar la ciberseguridad del mercado interior digital debería integrar reglas de gobernanza y financiación que resulten satisfactorias para todos los Estados miembros. Una resiliencia compartida en el ámbito europeo frente a las amenazas comunes de la ciberseguridad y la desinformación constituye un objetivo esencial, debiendo mantenerse los esfuerzos para neutralizar los ataques de desprestigio de la Unión.

La Directiva NIS ha contribuido a armonizar el nivel de ciberseguridad de los Estados miembros de la UE

Adicionalmente, la *Directiva 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión* (más conocida como *Directiva NIS*) ha contribuido a armonizar el nivel de ciberseguridad de los Estados miembros, sobre todo en lo referente a construcciones de capacidades, gobernanza y respuesta a incidentes en sectores considerados esenciales, sobre los que hay que continuar avanzando para alcanzar un grado de madurez óptima. A la vez, estas propuestas deben complementarse con el desarrollo y armonización de los modelos de gestión de crisis a nivel europeo.

El nuevo *Marco Europeo de Certificación de Ciberseguridad* elevará la exigencia de cumplimiento de productos y servicios con los más altos estándares internacionales.

El incremento en la gravedad y el número de ciberataques, unido a la creciente digitalización de la información en la Administración, supone un reto que obliga a mejorar el sistema de acreditación propio de la Administración General del Estado para el manejo de información clasificada entre los distintos ministerios.

En el ámbito normativo, es preciso culminar la revisión del *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad,* a la luz de la generalizada actuación electrónica de las entidades del sector público, la evolución de las amenazas, los nuevos vectores de ataque y el desarrollo de mecanismos de respuesta, así como la necesidad de mantener la conformidad y el alineamiento con las recientes regulaciones nacionales y europeas de aplicación en materia de seguridad de las Tecnonologías de la Información y la Comunicación (TIC).

Avanzar en la generación de confianza de los servicios ofrecidos a los ciudadanos por las Administraciones públicas es clave. Se debe potenciar la obtención de certificaciones de cumplimiento con el Esquema Nacional de Seguridad, así como con otras certificaciones internacionalmente reconocidas y seguir avanzando en materia de formación y concienciación de la seguridad. Además, progresivamente se han de ofrecer más y mejores servicios que incluyan nuevos modos de interrelación con las Administraciones públicas haciendo uso de las nuevas oportunidades que las tecnologías ofrecen de manera segura y confiable.

Las medidas a implantar suponen un reto respecto del marco organizativo y operacional, así como en cuanto a las medidas de protección contempladas en el Esquema Nacional de Seguridad, que afectan a las políticas de seguridad departamentales.

Por otra parte, la integridad y confidencialidad de los datos y transacciones telemáticas que realizan los usuarios-ciudadanos de los servicios electrónicos y el cumplimiento del *Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales* supondrá un incremento de las medidas de seguridad necesarias para su integridad, confidencialidad y trazabilidad.

El adecuado cumplimiento de las normativas anteriores exigirá el establecimiento de planes de continuidad y la monitorización constante de

los procesos establecidos con el objetivo final de alcanzar un sistema de gestión de la seguridad de la información maduro, coordinado de forma sistemática y conocido por toda la organización.

Igualmente, será necesaria la dotación de los necesarios recursos técnicos, humanos, económicos y presupuestarios para la mejora continua y el cumplimiento del Esquema Nacional de Seguridad y de la nueva *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, así como del *Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones*.

Por otra parte, es especialmente importante aprobar el Reglamento de desarrollo del *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*.

Además, se deben incrementar las acciones de colaboración público-público y pública-privada enfocadas a mejorar la concienciación, la formación y la capacitación de todos los colectivos. El cultivo y desarrollo del talento para proteger las instituciones y organismos públicos y privados, el refuerzo de la base tecnológica e investigadora nacional y la visibilidad de la industria de la ciberseguridad en España, apoyando su expansión internacional, son metas a las que se debe seguir contribuyendo.

Será necesario también impulsar las reformas normativas necesarias a nivel nacional e internacional que permitan mejorar la cooperación y el acceso de las agencias y organismos encargados de hacer cumplir la ley a la información que puedan facilitar los gestores de las plataformas, operadores y proveedores de servicios de Internet, en especial en lo relativo a la conservación y obtención de datos informáticos almacenados fuera del territorio del Estado requirente.

Desde una perspectiva orgánica, se ha de implementar el Acuerdo de Consejo de Ministros por el que se consolida el servicio compartido de seguridad gestionada a través de la constitución del Centro de Operaciones de Ciberseguridad para la Administración General del Estado. Además, se prevé que el Organismo de Certificación asuma las funciones de Autoridad Nacional de Certificación de la Ciberseguridad.

Otros retos consisten en potenciar la investigación en el ámbito de la computación cuántica y el desarrollo de soluciones criptográficas y de *blockchain* para la gestión distribuida de la confianza.

Del mismo modo, se considera necesario la progresiva inclusión en las listas de control de los regímenes de control multilateral de productos de *software* y *hardware* dirigidos a la intrusión en equipos informáticos y vigilancia de las comunicaciones, particularmente aquellos de doble uso destinados a cibervigilancia. En este caso particular, la supervisión de las transferencias de tecnología desde la UE a terceros Estados requiere la aplicación de la diligencia debida por parte de todos los actores y usuarios implicados en el mundo tecnológico.

Así y, en un sentido más amplio, la implantación de una cultura de ciberseguridad, que incremente el nivel de concienciación en seguridad

de la información y basada en la aplicación de medidas, servicios, buenas prácticas y planes de continuidad para la protección, seguridad y resiliencia en el sector público y empresarial, los sectores estratégicos, así como la ciudadanía, de manera que se garantice un entorno digital seguro y fiable, se mantiene como reto de atención prioritaria.

Figura 6-5
Estructura de la Ciberseguridad en el Sistema de Seguridad Nacional

Fuente: Estrategia Nacional de Ciberseguridad 2019

Figura 6-6
Ciberamenazas y acciones que usan el ciberespacio con fines maliciosos

Fuente: Estrategia Nacional de Ciberseguridad 2019

Realizaciones

La nueva *Estrategia Nacional de Ciberseguridad* se aprobó en la reunión del Consejo de Seguridad Nacional de 12 abril de 2019. Los avances tecnológicos y normativos surgidos en los últimos años requerían de una revisión y actualización urgentes. (Figura 6-7)

La nueva Estrategia Nacional de Ciberseguridad fue aprobada por el Consejo de Seguridad Nacional en 2019

El proceso de elaboración, según el mandato del Consejo de Seguridad Nacional dirigido al Consejo Nacional de Ciberseguridad, estuvo coordinado por el DSN del Gabinete de la Presidencia del Gobierno, y contó con una amplia participación. El sector público intervino a través de un comité técnico integrado por representantes de la Administración. Además, un comité de expertos independientes, formado por más de 40 personas de reconocido prestigio, aportó su visión. El documento a su vez fue compartido con la Conferencia Sectorial para Asuntos de Seguridad Nacional. Asimismo, se incorporaron las conclusiones realizadas en la ponencia de ciberseguridad de la Comisión Mixta Congreso-Senado de Seguridad Nacional. España se ha dotado de una Estrategia apoyada en un amplio consenso político y social.

Una Estrategia más colaborativa y más inclusiva e integrada que se desarrolló entendiendo al ciudadano como eje central de la seguridad y corresponsable en su preservación, involucrando de manera directa a la sociedad civil y, particularmente, al sector privado. Una estrategia menos técnica y más dirigida a ser entendida por la sociedad con el fin de contribuir a la cultura de ciberseguridad.

La Estrategia contempla actuaciones de prevención y acción constante en el ciberespacio tales como la ciberdefensa activa, la respuesta o la resiliencia y propone la creación de un *Foro Nacional de Ciberseguridad* para potenciar la participación de la sociedad civil en el ámbito de la ciberseguridad y mejorar la eficiencia en la colaboración y cooperación.

Fuente: Estrategia Nacional de Ciberseguridad 2019

Figura 6-7
Objetivos de la Estrategia Nacional de Ciberseguridad 2019

Reforzar las capacidades ante las amenazas provenientes del ciberespacio

En su labor diaria, el Centro Criptológico Nacional (CCN) gestionó en 2019 un total de 42.997 incidentes, de los cuales el 7,46% fueron clasificados por el Equipo de Respuesta a Incidentes de la Seguridad de la Información Gubernamental Nacional (CERT por sus siglas en inglés correspondientes a la denominación *Computer Emergency Response Team*) con una peligrosidad muy alta o crítica, para el sector público o para empresas de interés estratégico en base a diversos parámetros (tipo de amenaza, origen, perfil del usuario o sistemas afectados, etc.). (Figura 6-8 y 6-9)

El CCN gestionó en 2019 un total de 42.997 incidentes y el CERT de INCIBE más de 107.397 incidentes

El CERT del Instituto Nacional de Ciberseguridad (INCIBE) gestionó más de 107.397 incidentes. De estos, más de 72.858 corresponden a ciudadanos y empresas y 33.743 a la red académica. En esta labor de prevención cabe destacar tanto la realización de más de 83.401 notificaciones a proveedores de servicios de Internet, operadores de red que proporcionan acceso a Internet, como el alta en la base de datos de vulnerabilidades gestionada por INCIBE de más de 18.937 de estos incidentes. (Figura 6-10 y 6-11)

En la línea de refuerzo, impulso y promoción de los mecanismos para garantizar un entorno digital seguro y fiable, ha de destacarse especialmente la actividad de la línea de ayuda en ciberseguridad, que atendió más de 8.440 consultas. Este canal de ayuda de la Secretaria de Estado para el Avance Digital, dispondrá próximamente del número telefónico 017 para atender de manera gratuita, confidencial y accesible las dudas o consultas sobre ciberseguridad, privacidad, confianza digital, uso seguro y responsable de Internet y de la tecnología, a los ciudadanos usuarios de Internet en general y al colectivo de empresas y profesionales que utilizan Internet y las tecnologías en el desempeño de su actividad y deban proteger sus activos y negocios.

Por otra parte, se mejoró el desarrollo de las capacidades de defensa y respuesta, avanzando en la integración y dependencia operativas de los Centros Operativos de Seguridad (COS) de las FAS, todo esto mediante la reasignación de cometidos, sistemas, funciones y tareas, así como de los medios para ejercer el mando y control y los procedimientos de coordinación, manteniendo el compromiso de colaboración con diversas entidades públicas nacionales e internacionales. Se continúa avanzando en la obtención de recursos para apoyar las capacidades de explotación y respuesta del Mando Conjunto de Ciberdefensa (MCCD) y de las FAS.

En febrero de 2019, el Consejo de Ministros aprobó la creación del Centro de Operaciones de Ciberseguridad (COCS), como instrumento de la Administración General del Estado y sus organismos públicos vinculados o dependientes para la consolidación del Servicio Compartido de Seguridad Gestionada, con el objetivo de reforzar las políticas de seguridad y las infraestructuras tecnológicas y organizativas que permitan prevenir y combatir las amenazas en los sistemas informáticos de las Administraciones públicas. En 2019 la Secretaría General de Administración Digital, que ejerce la dirección técnica y estratégica, y el CCN, a quien corresponde la operación, avanzaron en la preparación del COCS.

Asimismo, se puso en servicio el Centro de Operaciones de Seguridad (SOC) en el que el CCN actúa como prestador del servicio y la Subdirección General de Nuevas Tecnologías del Ministerio de Justicia asume su dirección y gestión con disponibilidad 24 horas, 7 días a la semana, 365 días al año. Desde el SOC se realiza la monitorización de los sistemas, servicios y redes TIC del Ministerio de Justicia con el objetivo de detectar incidentes de seguridad, diagnosticar vulnerabilidades y amenazas, bloquear ciberataques y mejorar la prevención y respuesta a los posibles incidentes de seguridad.

Otro servicio de seguridad gestionada 24x7x365 ha iniciado su actividad: el Centro de Operaciones de Seguridad para la prevención, monitorización, detección, respuesta y recuperación relativos a incidentes en los entornos de sistemas y redes de comunicaciones del Administrador de Infraestructuras Ferroviarias (Adif). Su objetivo es ir incrementando sus capacidades operativas y alcanzar un grado de madurez adecuado en el medio plazo.

El Ministerio del Interior ha elevado las exigencias que, en materia de seguridad, se han incluido en la contratación de la difusión del escrutinio provisional de resultados en los distintos procesos electorales celebrados en 2019. Así, por primera vez, se ha optado por la celebración de un Acuerdo Marco, entre otras razones, porque ello permite incluir, como requisito imprescindible para los licitadores, la superación de una auditoría previa en materia de seguridad de los sistemas que ha llevado a cabo el CCN-CERT; asimismo se dispuso de un equipo de seguridad del Ministerio del Interior, compuesto por personal de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad junto con personal del CCN-CERT. Con ello, se ha pretendido dar cumplimiento a las recomendaciones formuladas por el propio CCN para mejorar la seguridad y estabilidad del sistema electoral ante las vulnerabilidades detectadas en procesos anteriores.

En 2019 se ha creado una Red Nacional para la gestión de los procesos electorales

Por otro lado, se ha creado una Red Nacional para la gestión de los procesos electorales, siguiendo la citada Recomendación de la Comisión Europea *ELECTION PACKAGE* del pasado 12 de septiembre de 2018. Dicha Red se articula en torno a cuatro grandes bloques conceptuales:

a. Garantizar que el proceso electoral se lleve a cabo con transparencia y objetividad y acorde con el principio de igualdad, respetando las reglas del juego previstas en el procedimiento electoral a través de la Subdirección General de Política Interior y Procesos Electorales del Ministerio del Interior, junto con la Junta Electoral Central, y las Juntas Autonómicas, Provinciales y de Zona y las Mesas Electorales.

b. Proteger contra la utilización indebida de datos personales a través de la Agencia Española de Protección de Datos.

c. Establecer procedimientos frente al riesgo que representan los ciberataques para los sistemas informáticos de las elecciones, las campañas, los partidos políticos, los candidatos o las administraciones públicas, velando por la seguridad de todos los aspectos informáticos del proceso electoral a través de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad y del Centro Nacional de Protección de Infraestruc-

turas y Ciberseguridad (CNPIC) de la Secretaría de Estado de Seguridad, y con el apoyo del CCN.

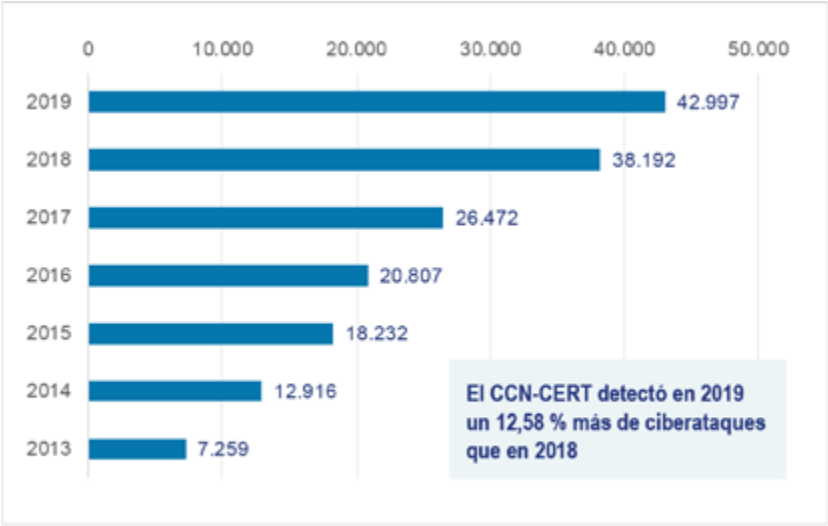
d. Combatir la desinformación en línea y las noticias falsas a través de la Secretaría de Estado de Comunicación y del Departamento de Seguridad Nacional, ambos de la Presidencia del Gobierno.

Este dispositivo tiene por objeto principal llevar a cabo una vigilancia efectiva y un seguimiento proactivo de las diversas acciones y hechos que pudieran ocurrir en el ámbito cibernético, para proceder a la difusión de la información a los actores implicados.

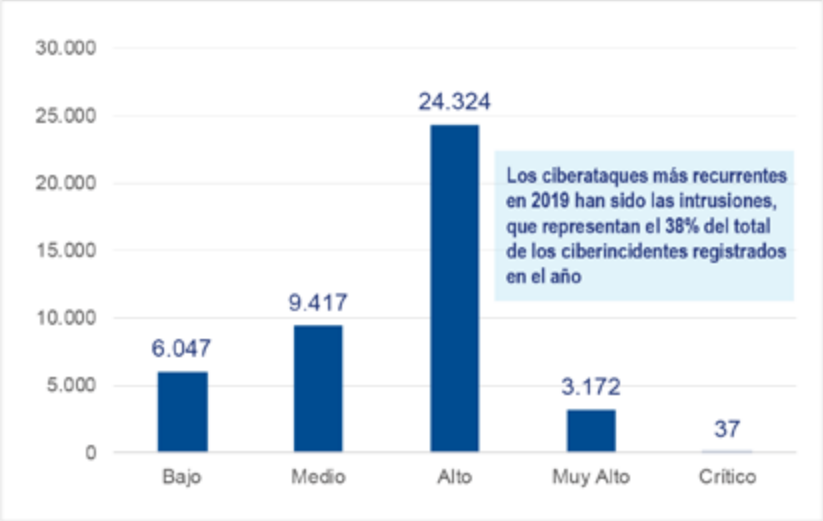
Por primera vez en España, las instrucciones elaboradas por el Ministerio del Interior para garantizar la seguridad de los comicios electorales, han contado con un apartado específico dedicado expresamente a la ciberseguridad.

En el seno de la Guardia Civil se ha considerado oportuno la creación de una unidad que coordine y optimice el potencial disponible para hacer frente a las amenazas procedentes de medios cibernéticos o transmitidas a través de ellos, que se constituya como punto de referencia en aspectos relacionados con la ciberseguridad y que fije determinados procedimientos de armonización en la gestión de los recursos humanos, materiales y financieros relacionados con esta materia.

Figura 6-8
Número de cibertaques registrados por el CCN-CERT 2013-2019

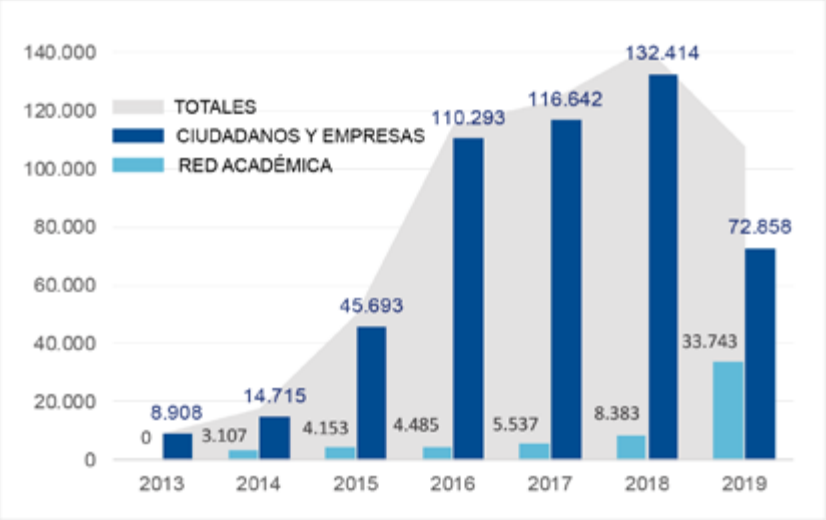


Fuente: Centro Nacional de Inteligencia



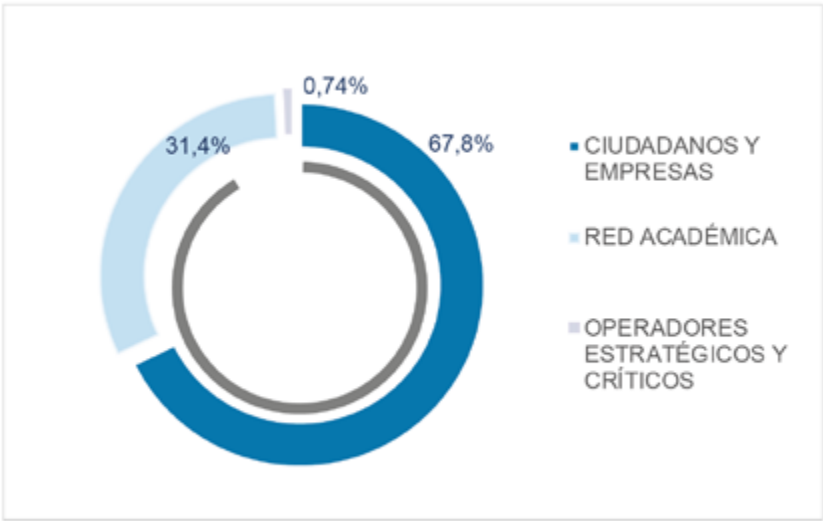
Fuente: Centro Nacional de Inteligencia

Figura 6-9
Número de ciberataques detectados en 2019, clasificados por nivel de peligrosidad



Fuente: Instituto Nacional de Ciberseguridad

Figura 6-10
Evolución del número de ciberincidentes gestionados por el Instituto Nacional de Ciberseguridad



Fuente: Instituto Nacional de Ciberseguridad

Figura 6-11
Tipología de los ciberincidentes gestionados por el Instituto Nacional de Ciberseguridad en 2019

Garantizar la seguridad y resiliencia de los activos estratégicos para España

En 2019 se publicó el Informe Nacional del Estado de la Seguridad de los Sistemas de las Tecnologías de la Información y la Comunicación

Se ha progresado en la elaboración del proyecto de modificación del Esquema Nacional de Seguridad. Con carácter general, los distintos departamentos ministeriales han llevado a cabo las revisiones del cumplimiento y la adecuación de los nuevos sistemas al esquema, así como implementado los diferentes planes de acción y políticas de seguridad de la información a la luz de lo recogido en el *Informe Nacional del Estado de la Seguridad de los Sistemas de las Tecnologías de la Información y la Comunicación*, publicado en 2019 con datos de 2018. Por otra parte, se ha avanzado en la preparación de los proyectos de instrucciones técnicas de seguridad de interconexión de sistemas y de criptología de empleo en el ENS.

Cabe subrayar la aprobación de la *Política de Seguridad de la Información de la Administración Judicial Electrónica*, aplicable a todos los sistemas de información y comunicación utilizados por toda la Administración de Justicia con inclusión de las Comunidades Autónomas que tienen transferidas las competencias en esta materia, avance que aporta uniformidad y homogeneidad a la adopción de las decisiones.

También el Ministerio de Hacienda llevó a cabo la revisión de su política de seguridad de la información para incluir la nueva legislación de protección de datos -cuestión ligada a las adecuaciones correspondientes sobre la responsabilidad en materia de protección en los convenios de cesión de datos de la Agencia Tributaria (AEAT) y aspectos de continuidad de negocio; se abordó un estudio transversal en el Ministerio de la situación actual de la continuidad de los servicios esenciales y se propusieron iniciativas de revisión a partir de 2020.

En el ámbito de las infraestructuras, Adif está implantando un Sistema de Gestión de Seguridad de la Información, que comprende el diseño, implantación y mantenimiento de un conjunto de procedimientos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos y amenazas de seguridad de la información, cuya madurez se irá incrementando a medida que se implementen y desarrollan sus capacidades con el tiempo.

Por parte de Aeropuertos Españoles y Navegación Aérea (Aena), siguiendo la línea marcada en el año anterior, tras conseguir con éxito la certificación en la norma ISO 27001:2014 en el entorno de los servicios centralizados para todos los centros, se sigue trabajando en la certificación del SGSI (Sistema de Gestión de Seguridad de la Información) ampliando el alcance al aeropuerto *Adolfo Suárez Madrid Barajas*, así como en incrementar el nivel de madurez en toda la organización. La Agencia Estatal de Seguridad Aérea (AESA) realizó la primera inspección de ciberseguridad en el ámbito del *Reglamento (UE) 2017/373 para la protección de la prestación de servicios ATS/CNS* (*Air Traffic Service / Communications Navigation Surveillance*) y Puertos del Estado diseñó un esquema general de ciberseguridad portuaria de mejora de las capacidades de prevención, vigilancia y respuesta a incidentes.

Con el objetivo de facilitar la adquisición de productos y servicios de seguridad TIC que dispongan de un nivel mínimo de confianza para

la Administración Pública, es decir cuyas funcionalidades de seguridad relacionadas con el objeto de su adquisición han sido certificadas, el CCN publicó el *Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación para aquellos sistemas afectados por el ENS de categoría alta*.

La utilidad del catálogo ha motivado el desarrollo por el CCN de una nueva metodología ligera, LINCE, con la finalidad de evaluar y certificar productos de seguridad TIC para la categoría media y básica del Esquema Nacional de Seguridad. Entre los ámbitos que han mejorado sus modelos de certificación de acuerdo a los nuevos procedimientos se encuentra la aviación.

El *Informe Nacional del Estado de la Seguridad de los Sistemas de las Tecnologías de la Información y la Comunicación*, publicado en 2019 con datos de 2018, incluye 768 organismos, con un total de 20.158 sistemas TIC declarados (5.514 sistemas de categoría básica, 10.483 sistemas de categoría media y 4.161 Sistemas de categoría alta) que dan servicio a 4.790.777 usuarios. El incremento respecto de 2017 ha sido del 11,72% en la Administración General del Estado, del 43,66% en las Comunidades Autónomas, del 35,14% en las entidades locales y en las universidades del 5,88%. Estas cifras suponen un incremento global del 28%.

Por otra parte, el Servicio de Respuesta a Incidentes en TI para Infraestructuras Críticas y Operadores Estratégicos, prestado por el CNPIC e INCIBE, proporciona a los operadores estratégicos nacionales un canal de respuesta a incidentes cibernéticos. Para la prestación de este servicio es necesaria la existencia de un acuerdo de confidencialidad suscrito entre todas las partes implicadas, CNPIC, INCIBE y cada operador. Hasta el momento se dispone de 126 acuerdos de confidencialidad.

La resiliencia no se improvisa, es necesario ejercitarla. Se participó en dos ciberejercicios en el contexto de la OTAN: *Locked Shields* 2019 y *Cyber Coalition Exercise* 2019, así como en diversos ejercicios prácticos basados en escenarios de crisis organizados por la presidencia finlandesa del Consejo de la UE. Dichos ejercicios, así como la elaboración de un documento estratégico de conclusiones, están dirigidos a reforzar la conciencia sobre este tipo de amenazas y a la necesidad de hacerles frente mediante una respuesta coordinada y eficaz.

Se reforzó la conciencia de la necesidad de mantener una respuesta coordinada entre los Estados miembros de la UE y las instituciones comunitarias mediante la realización de ejercicios de ciberseguridad en los que se ha practicado la operatividad de la denominada *toolbox,* o caja de herramientas diplomática de la UE.

España participó en el ejercicio *BlueOlex*, cuyo objetivo es identificar y elaborar procedimientos de cooperación para el nivel operacional del *Blueprint,* un proyecto liderado por España y Francia para desarrollar los aspectos relativos a la implementación de las recomendaciones de la Comisión Europea (JOIN (2017) 450 final) sobre una respuesta coordinada a incidentes y crisis a gran escala. Estas medidas están orientadas a sentar las bases para un Marco Europeo de Respuesta a Crisis de Ciberseguridad.

Impulsar la ciberseguridad de ciudadanos y empresas

En 2019 desde INCIBE se siguió potenciando la colaboración con distintos socios como el Instituto de Comercio Exterior (ICEX) o la Agrupación Empresarial Innovadora en Ciberseguridad y Tecnologías Avanzadas, así como con universidades, instituciones regionales y locales o entidades de capital riesgo. Fruto de esta colaboración se han podido llevar a cabo acciones de capacitación, cooperación en materia de servicios y contenidos e impulso de iniciativas de concienciación, relativas al uso seguro y responsable de Internet por los ciudadanos y los menores.

Cooperación público-público y pública-privada

La *Estrategia Nacional de Ciberseguridad 2019* expone que la ciberseguridad se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social.

El futuro Foro Nacional de Ciberseguridad incrementará las sinergias público-privadas en el Sistema de Seguridad Nacional

Asimismo, la Estrategia señala que, ante esta visión renovada de un ámbito que se entiende extendido funcionalmente, la colaboración público-privada es un elemento clave. En el marco de dichas orientaciones, se creará el Foro Nacional de Ciberseguridad. Una iniciativa liderada por el Consejo de Seguridad Nacional y dependiente del Consejo Nacional de Ciberseguridad dirigida a incrementar las sinergias público-privadas en el Sistema de Seguridad Nacional y cuyo objetivo es generar conocimiento sobre oportunidades, desafíos y amenazas a la seguridad en el ciberespacio.

En lo que respecta a la colaboración y coordinación en materia de ciberseguridad con las FCSE, así como con organismos europeos, se activaron por parte del CNPIC, a través de la Oficina de Coordinación Cibernética, varios dispositivos extraordinarios de ciberseguridad respecto de la alerta terrorista, actualmente establecida en el Nivel 4 (alto); los procesos electorales con motivo de la celebración de las Elecciones Generales de 28 de abril y 10 de noviembre, las elecciones municipales, autonómicas y europeas de 26 de mayo; la cumbre del G7 en Biarritz entre el 24 y el 26 de agosto; o el seguimiento de campañas de desinformación e incidentes de ciberseguridad con incidencia especialmente en infraestructuras críticas, tras la reunión de la Comisión Permanente de lucha contra la desinformación convocada por el DSN del Gabinete de la Presidencia del Gobierno el 4 de octubre.

También se activó un sistema extraordinario con ocasión de la XXV Conferencia de Naciones Unidas sobre el Cambio Climático celebrada del 2 al 13 de diciembre en Madrid, bajo la presidencia de Chile y con el apoyo del Ejecutivo español, mediante la coordinación permanente del CNPIC con los CSIRT de referencia INCIBE-CERT, CCN-CERT y ESPDEFCERT (MCCD), las FCSE y los operadores críticos y de servicios esenciales.

En los operativos especiales, INCIBE ha identificado más de 170 movimientos *hackivistas* importantes.

En otro orden de realizaciones, para dar respuesta a la exigencia de disponer de un documento de carácter técnico que recoja y desarrolle

los contenidos mínimos en relación al conocimiento, gestión y notificación de ciberincidentes, bien sea por requerimiento del *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*, o por cualquier otra disposición legal, en enero de 2019, el Consejo Nacional de Ciberseguridad validó la *Guía Nacional de Notificación y Gestión de Ciberincidentes*.

La Guía es considerada como un hito a nivel nacional e internacional en el contexto de la ciberseguridad y la protección de infraestructuras críticas. Actualmente se encuentra en revisión por parte del grupo de trabajo encargado de su elaboración, conformado por las principales instituciones de ciberseguridad en España a nivel estatal (CCN, INCIBE, MCCD y CNPIC, que lideró el grupo de trabajo referenciado).

Existen además foros de cooperación de interés como el Comité Técnico de Normalización 320 - Ciberseguridad y protección de datos personales en el que participan más de 40 entidades públicas y privadas. Su Subcomité SC2 - Criptografía y mecanismos de seguridad, bajo presidencia del CCN y secretaría del Consejo Superior de Investigaciones Científicas (CSIC), contribuye al desarrollo de estándares internacionales en apoyo al nuevo marco regulatorio europeo, como el *Reglamento General de Protección de Datos* o la *Directiva NIS*.

Por otra parte, el Comité del Convenio sobre la Ciberdelincuencia del Consejo de Europa, que representa a las Partes en el Convenio de Budapest, acordó la negociación de un Segundo Protocolo Adicional al Convenio de Budapest sobre la mejora de la cooperación internacional en cibercrimen. El Ministerio de Justicia participa periódicamente en las reuniones del grupo de redacción del protocolo, que incluirá previsiones que darán base jurídica a una asistencia judicial recíproca más eficaz, la cooperación directa con proveedores de otras jurisdicciones y la ampliación de las búsquedas transfronterizas, todo ello con las debidas salvaguardias en materia de protección de datos.

Potenciar la industria española de ciberseguridad y la generación y retención de talento

Entre las acciones para el impulso de la industria española de la ciberseguridad cabe mencionar las acciones efectuadas para la mejora de su competitividad. INCIBE continuó su apoyo a la expansión, atrayendo el talento tanto internacional como nacional a efectos de impulsar la innovación tecnológica. (Figura 6-12 y 6-13)

Las entidades españolas, incluyendo unidades de la Administración General del Estado -como usuarios finales de los proyectos-, participaron intensamente en distintos órganos de gobierno y grupos de trabajo de la Organización Europea de Ciberseguridad (ECSO), asociación industrial que da soporte a la *Contractual Public Private Partnership* de ciberseguridad.

El Centro de Desarrollo Tecnológico e Industrial (CDTI) ha sido muy activo defendiendo los intereses españoles en seguridad en el marco de los comités de seguridad TIC del programa *Horizonte 2020*. En relación con los resultados españoles en el Programa de Sociedades Seguras para el periodo 2014-2018, los retornos obtenidos son satisfactorios. Las entidades españolas están presentes en 136 de 212 proyectos,

coordinando 25 de ellos. Los retornos económicos suponen el 9,94% de la UE-28. Los retornos españoles se reparten entre las empresas (46,6%), seguidas por las universidades (19,3%) y las administraciones públicas (13,2%).

En el futuro Programa Marco Horizonte Europa, toda la I+D+i de ciberseguridad, hasta ahora disgregada entre los Programas de Sociedades Seguras, pasará a abordarse a partir de 2021 de manera conjunta en el futuro Clúster de Seguridad Civil para la Sociedad.

También en el ámbito de la capacitación, se creó un grupo de trabajo para la elaboración de cursos de especialización de la Formación Profesional del Sistema Educativo en el ámbito de la Industria 4.0; se elaboró el curso de especialización para titulados de Formación Profesional de Grado Superior *Ciberseguridad en el ámbito de las tecnologías de la información y las comunicaciones*, destinado principalmente a los titulados de las familias profesionales más directamente relacionadas con las competencias genéricas en cuanto a las redes de comunicaciones; y el curso *Ciberseguridad en el ámbito industrial*, para titulados de las familias profesionales más directamente relacionadas con las redes de comunicación específicas del ámbito industrial.

En los organismos públicos de investigación y universidades, se han continuado realizando avances científicos y tecnológicos en el ámbito de la ciberseguridad financiados, entre otras entidades, por la Agencia Estatal de Investigación.

Entidades como el CSIC participan en diversos cursos de formación de singular relevancia para la generación de perfiles profesionales especializados en el ámbito de la ciberseguridad: *Curso de Especialidades Criptológicas* (del CCN), *Curso de Protección de Datos* (Fundación Ortega y Gasset), *Curso de Evidencias Digitales y Ciberseguridad* (Instituto de Ciencias Forenses de la Universidad Autónoma de Madrid), másteres en ciberseguridad en universidades, etc.

Contribuir a la seguridad del ciberespacio en el ámbito internacional

El 17 de abril fue aprobado el *Reglamento (UE) 2019/991 del Parlamento Europeo y del Consejo relativo a ENISA (Agencia Europea para la Seguridad de las Redes y de la Información) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 (Reglamento sobre la Ciberseguridad).* Este nuevo Reglamento otorga un nuevo mandato a ENISA y le asigna mayores recursos y más responsabilidad, consolidándola como Agencia de la Unión en materia de ciberseguridad.

En el marco de la colaboración a nivel europeo, la Secretaría de Estado para el Avance Digital continuó participando activamente en el grupo de cooperación conformado por los Estados miembros, la Comisión Europea y ENISA, cuyo objetivo es facilitar la cooperación estratégica, intercambiar información, compartir experiencias y desarrollar buenas prácticas para la implementación de la *Directiva NIS*.

En este grupo de cooperación existen líneas de trabajo específicas sobre operadores de servicios esenciales y proveedores de servicios digitales, que analizan aspectos como los criterios para la identificación de dichas entidades, y el ámbito y alcance de los servicios incluidos en el marco de la Directiva.

En otros ámbitos de la cooperación internacional, España participa en el Grupo de Trabajo de Composición Abierta de Naciones Unidas sobre Tecnologías de la Información y la Comunicación en el contexto de la Seguridad Internacional y el proceso de creación de Medidas de Fomento de la Confianza en la OSCE, así como en el Foro de Gobernanza de Internet, el Foro para la Libertad en Internet y el Foro Global de Ciber Experiencia. España participa en la Comisión informal de expertos de Naciones Unidas para estudiar la posible integración de la ciberguerra en el ámbito de los delitos que conoce el Tribunal Penal Internacional. También cabe destacar la organización en España, con la colaboración de la Organización de Estados Americanos, de la cuarta edición del *Cybersecurity Summer Bootcamp*.

El reglamento de exportaciones de doble uso de la UE fue objeto de revisión en los últimos tres años; los conceptos de asistencia técnica y transferencia de tecnología son de gran importancia. Se han incluido los controles exhaustivos para impedir el uso de la nube, así como la transferencia hacia empresas no europeas de conocimiento de ciber-vigilancia.

Además, AESA continuó con el liderazgo del Grupo de Trabajo Nacional de Ciberseguridad para la Aviación Civil, creado por el Comité Nacional de Seguridad para la Aviación Civil, con la finalidad de fijar las líneas de acción precisas frente a las ciberamenazas. La Agencia ejerce la representación de España en diversos programas europeos de ciberseguridad para aviación.

Desarrollar una cultura de ciberseguridad

El CCN celebró las XIII Jornadas STIC CCN-CERT, que bajo el lema "Comunidad y confianza, bases de nuestra ciberseguridad", reunió a más de 2.800 profesionales del sector de la ciberseguridad. Además, en junio de 2019, en colaboración con el Ministerio de Política Territorial y Función Pública y la Fundación Círculo de Tecnologías para la Defensa y la Seguridad, tuvo lugar el I Encuentro del Esquema Nacional de Seguridad: Tendencias y Políticas de Seguridad, con el objetivo de hacer balance del desarrollo e implantación del Esquema. Más de 350 responsables de seguridad, tanto del sector público como privado, asistieron a este encuentro, que contó con la participación de las principales empresas del sector.

Con el propósito de promover el alcance y mantenimiento de los conocimientos, habilidades, experiencias, así como capacidades tecnológicas y profesionales, INCIBE realizó en 2019 diversos eventos entre los que destacan la 6ª edición del *Cybercamp*, en Valencia, el 13º Encuentro Internacional de Seguridad de la Información, la 4ª edición del *Cyber-Security Summer BootCamp* o el Foro MujeresCiber, estos tres últimos celebrados en León.

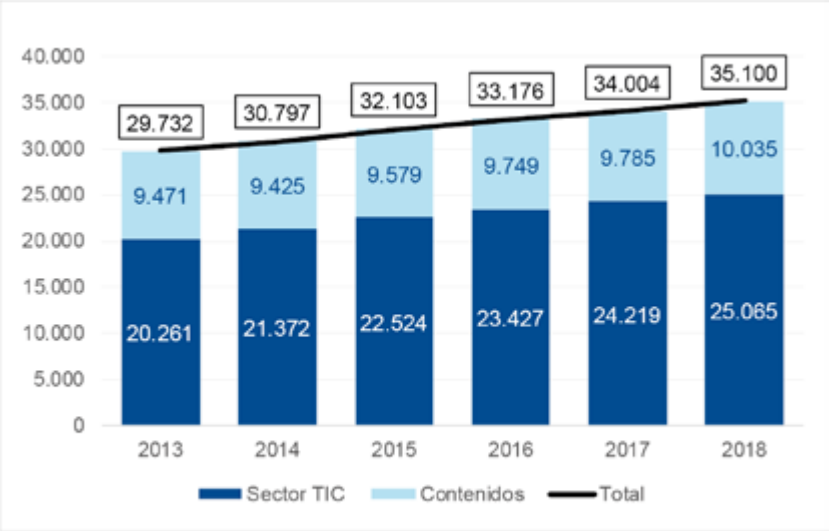
En junio, se celebró en la Escuela Nacional de Policía el I Congreso de Seguridad Digital y Ciberinteligencia. El evento, organizado por la Policía Nacional, sirvió para reforzar los lazos entre la comunidad de la ciberseguridad en España.

Asimismo, el CCN sumó a su oferta formativa, más orientada al personal técnico, diversos servicios enfocados a la sensibilización de todo tipo de usuarios para que, en su día a día, adopten procedimientos adecuados y buenas prácticas en el uso de las nuevas tecnologías como mejor manera para reducir la superficie de exposición a los riesgos que las mismas implican. Organizó, en noviembre de 2019, una nueva edición de los desayunos tecnológicos dirigido a personal de las Administraciones públicas, dedicado a las soluciones que permiten incorporar dispositivos móviles en cualquier organismo con el mantenimiento de los niveles de seguridad requeridos. Igualmente, desde mayo de 2019, recopiló algunos de los principales consejos que pueden darse a la hora de concienciar y facilitar el uso seguro de las TIC, que pueden visitarse en el apartado "ciberconsejos" del portal del CCN.

Por otra parte, las FCSE consolidaron las relaciones con el ámbito universitario mediante la participación en diversos programas formativos, dirigidos a empresas y particulares. En este sentido cabe resaltar la coorganización de una nueva edición, junto con el Centro Nacional de Excelencia en Ciberseguridad (CNEC), de un Máster en Evidencias Digitales y Lucha contra el Cibercrimen, orientado a miembros de las FCSE, así como la presentación por el Ministro del Interior, el 4 de junio, de la primera edición de la Liga Nacional Interuniversitaria de retos en el ciberespacio, iniciativa organizada por la Guardia Civil con el objeto de impulsar el talento de jóvenes especializados en materia de ciberseguridad entre estudiantes universitarios y de ciclos formativos de grado superior. La Policía Nacional desarrolló y puso en marcha un máster de ciberdelincuencia para su personal.

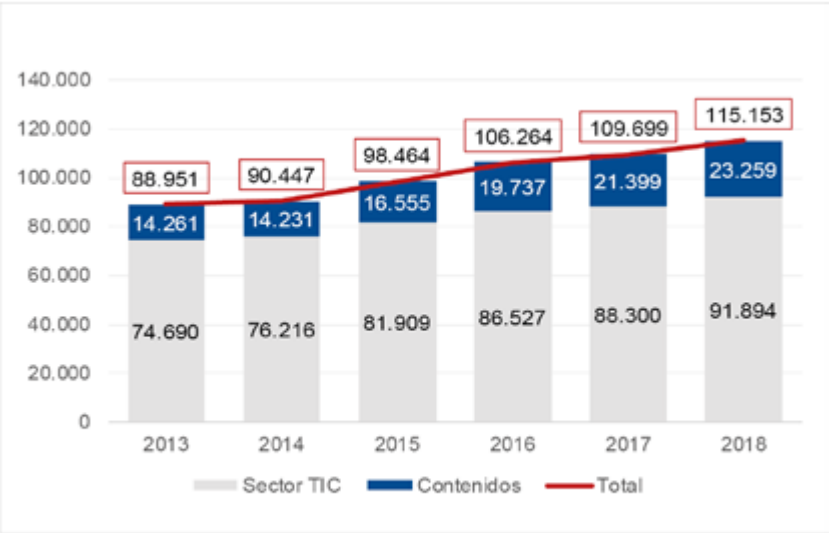
Adicionalmente, los departamentos ministeriales se implicaron en el diseño de una estrategia de concienciación y formación que permita progresivamente avanzar en una cultura de seguridad fundamentada en la prevención. En este sentido y a modo de muestra, el Ministerio de Justicia implementó el *Plan de Concienciación en Seguridad* dirigido tanto a personal de la Administración de Justicia como a los equipos técnicos del Ministerio, para sensibilizar a los usuarios de la importancia de la seguridad y además capacitarles para aplicar la seguridad a su entorno. En ENAIRE (Gestor de la navegación Aérea en España y el Sáhara Occidental) se desarrolló una estrategia de ciberseguridad corporativa, así como un plan de adaptación como Operador de Servicio Esencial y en el Ministerio de Hacienda se ha desarrollado un plan de formación y concienciación de la normativa de seguridad.

El Ministerio de Defensa continúa avanzando en la elaboración de la normativa específica relativa a acreditación de sistemas e informes de evaluación. Dentro de este ámbito, se realizaron diversas inspecciones de seguridad a sistemas TIC clasificados del ámbito conjunto; auditorías para la mejora de la seguridad, verificaciones técnicas de seguridad de sistemas clasificados para su acreditación y apoyo a las acreditaciones realizadas por las ONS de seguridad a sistemas TIC desplegados en zonas de operaciones.



Fuente: Ministerio de Economía y Empresa

Figura 6-12
Evolución del número de empresas del sector TIC
2013-2018



Fuente: Ministerio de Economía y Empresa

Figura 6-13
Evolución de la cifra de negocio del sector TIC
2013-2018

SEGURIDAD MARÍTIMA

OBJETIVO:

Impulsar una política de seguridad en el espacio marítimo, tanto a nivel nacional como en el marco internacional y, especialmente, en la UE, con el fin de proteger la vida humana en el mar; mantener la libertad de navegación y proteger el tráfico marítimo y las infraestructuras marítimas críticas; prevenir y actuar ante actividades criminales y actos terroristas que se desarrollen en ese medio; proteger y conservar el litoral, los recursos del medio marino, el medio ambiente marino y el patrimonio cultural subacuático; y prevenir y responder en casos de catástrofes o accidentes en ese medio.

Tendencias

El dominio marítimo se caracteriza por ser un espacio geográfico de interés estratégico; un medio de transporte de personas, bienes e información; un área que proporciona recursos y riqueza; y un sistema cuyo estado es clave para el medioambiente.

La situación en las principales líneas de comunicación marítima afecta notablemente a la Seguridad Nacional

España, un país con marcado carácter marítimo, se encuentra en una de las zonas con más tráfico a nivel mundial. La situación en las principales líneas de comunicación marítima afecta notablemente a la Seguridad Nacional.

En el marco internacional, la degradación de la seguridad en la periferia de Europa afecta tanto a la ribera atlántica como a la mediterránea. La creciente tensión con Rusia a partir de la anexión ilegal de Crimea en 2014 ha reactivado el interés de la OTAN por los asuntos marítimos. Actualmente, frente a las capacidades navales rusas las autoridades de la OTAN y numerosos países aliados abogan por una potenciación del poder naval. El Mediterráneo es asimismo un escenario estratégico de influencia geopolítica, clave para la seguridad de Europa.

La inestabilidad en la zona de Oriente Próximo ha tenido su reflejo en las aguas que la rodean. La región comprende un paso marítimo de alto interés para el comercio internacional, especialmente el de hidrocarburos. Las crisis vividas en el golfo Pérsico como consecuencia de las tensiones con Irán, de forma intensa durante el segundo semestre

de 2019, han afectado al tráfico por el estrecho de Ormuz. Igualmente, la inestabilidad en la península Arábiga ha tenido repercusiones en la navegación en el golfo de Adén y el mar Rojo.

Son dos las principales iniciativas internacionales de seguridad marítima en el golfo Pérsico: la primera, liderada por Estados Unidos, es la operación denominada *International Maritime Security Construct*. Su creación obedece a la creciente tensión en aguas del Golfo. Participan Arabia Saudí, Albania, Australia, Bahrein, Emiratos Árabes Unidos y Reino Unido. De forma paralela, Francia lidera una coalición denominada *European Maritime Surveillance Mission in the Strait of Hormuz* (EMASoH) en la que participan, además, Dinamarca y Países Bajos.

Por otra parte, y por su relevancia, es de destacar el reciente desarrollo, en el mes de diciembre de 2019, del primer ejercicio naval conjunto entre Irán, Rusia y China en aguas del golfo Pérsico.

En la región del Cuerno de África, la inestabilidad en Somalia y el conflicto de Yemen son las principales causas para la inseguridad marítima en el golfo de Adén y en el estrecho de Bab el-Mandeb, donde, además, las características geográficas, el alto volumen del tráfico marítimo y el desarrollo de tráficos ilícitos elevan los riesgos para la navegación. La piratería de origen somalí sigue suponiendo una amenaza para el tráfico marítimo y en particular para las embarcaciones españolas, o con tripulantes nacionales a bordo, dedicadas a la pesca, principalmente del atún.

El número de secuestros en la región empezó a descender drásticamente a partir del año 2012. No obstante, no se pueden descartar incidentes en los que se vean afectadas embarcaciones españolas o con tripulantes españoles, principalmente de pesca. A modo de ejemplo se puede mencionar el ataque al atunero de bandera española *Txori Argi* por un esquife el día 21 de abril de 2019. La agresión fue repelida por el equipo de seguridad privada embarcada. Dos días después de este incidente, medios navales españoles integrados en la operación *EUNAVFOR Atalanta* liberaron el *dhow* yemení *Al–Azham*, que había sido utilizado como "nodriza" por los piratas para atacar al atunero español y a otro buque taiwanés ese mismo día. En los últimos años, las medidas adoptadas por los barcos que navegan por aguas próximas a Somalia y la presencia de las fuerzas navales internacionales, y en concreto las de la operación *EUNAVFOR Atalanta* de la UE, han sido decisivas para la contención de este fenómeno criminal. (Figura 7-1)

La operación EUNAVFOR Atalanta de la UE ha sido decisiva para la contención de la piratería en el Cuerno de África

Cabe destacar también la entrada en vigor de la nueva delimitación del Área de Alto Riesgo (HRA por sus siglas en inglés correspondientes a la denominación *High Risk Area*) el 1 de mayo de 2019, que, una vez más, ha vuelto a reducirse con respecto a los límites establecidos en 2015. Esto evidencia que el sector marítimo en general percibe que esta amenaza se encuentra relativamente controlada. Sin embargo, la amplitud de la zona de operaciones y el relajamiento de las medidas de autoprotección podrían facilitar el éxito de alguno de los esporádicos ataques de grupos piratas, principalmente en los periodos de bonanza meteorológica. Además, las autoridades somalíes han primado los acuerdos y equilibrios entre clanes en su lucha contra la piratería marítima, algo que afecta a la erradicación del problema.

Por su parte, y en lo que respecta al golfo de Guinea, la tendencia principal es el incremento de los actos delictivos en el medio marítimo. Esta área de interés estratégico para España continúa siendo uno de los puntos más peligrosos para la navegación internacional y en sus aguas se siguen sucediendo actos de piratería, robos a mano armada con secuestros de tripulación y *bunkerización* de petróleo en la fuente, todo ello a pesar de todos los esfuerzos de la comunidad internacional para apoyar a los Estados ribereños en su lucha contra estos fenómenos. En el golfo de Guinea, España debe continuar su apoyo los Estados ribereños mediante la seguridad cooperativa, asumiendo un papel preeminente en el marco del *G7++ Amigos del golfo de Guinea*. La mayor parte de las incidencias se originan en la costa nigeriana.

Finalmente, en el Pacífico continúan los focos de tensión que afectan a la seguridad marítima. La UE, en la *Comunicación Conjunta al Parlamento Europeo, el Consejo Europeo y el Consejo "UE-China – Una Perspectiva Estratégica*" de la Comisión Europea de 12 de marzo de 2019, ha reconocido por primera vez a la República Popular de China como un "rival sistémico". El poder creciente de China tiene su reflejo en sus pretensiones, cada vez más firmes, de soberanía sobre el mar del sur de China, con consecuencias para la seguridad de la región. Esto está provocando un enfrentamiento geoestratégico y el incremento en la tensión entre Estados Unidos y China, algo que afecta a la seguridad marítima a nivel global.

Alrededor del 60% de las exportaciones y del 85% de las importaciones se efectúan por vía marítima

En otro orden de consideraciones, el sector portuario, principio y fin de toda la actividad marítima y punto especialmente crítico dentro del sistema, es el eslabón principal de las cadenas logísticas y de transporte, por el que circula cerca del 60% de las exportaciones y del 85% de las importaciones españolas. Las cifras de tráfico portuario, y en particular, las relativas a contenedores, muestran tendencias crecientes. (Figura 7-2, 7-3 y 7-4)

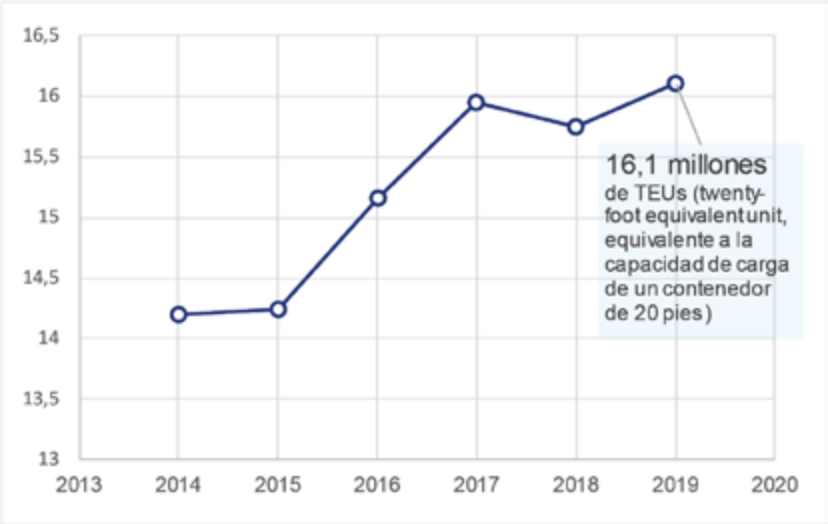
Además, gracias a las mejores técnicas de análisis científico, se constata la tendencia de aumento de la frecuencia e intensidad de fenómenos extremos. Este factor implica un mayor número de temporales, más violentos y con periodos de retorno menores. También se observa una tendencia de aumento del nivel del mar, factor que hace prever un incremento en los riesgos asociados a los impactos de erosión e inundación en el litoral.

La aplicación de la *Estrategia de Adaptación al Cambio Climático de la Costa Española* y el avance en la consolidación de la Red de Espacios Marinos Protegidos son las principales referencias para las actuaciones en este ámbito.

Fuente: EUNAVFOR

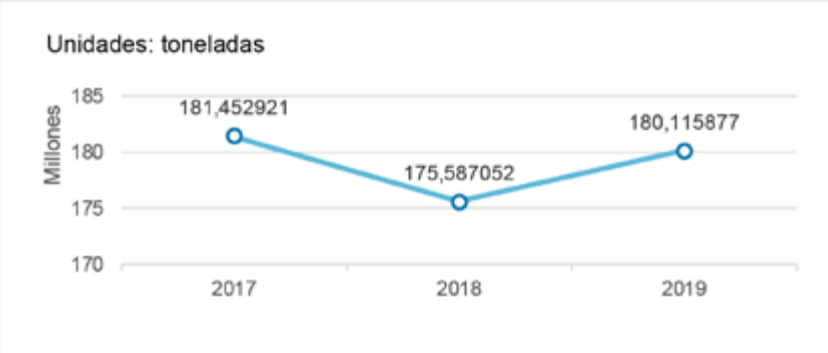
Figura 7-1
Evolución del número de ataques piratas en el Cuerno de África

Figura 7-2
Evolución del número de contenedores (medidos en TEUs) en los puertos españoles



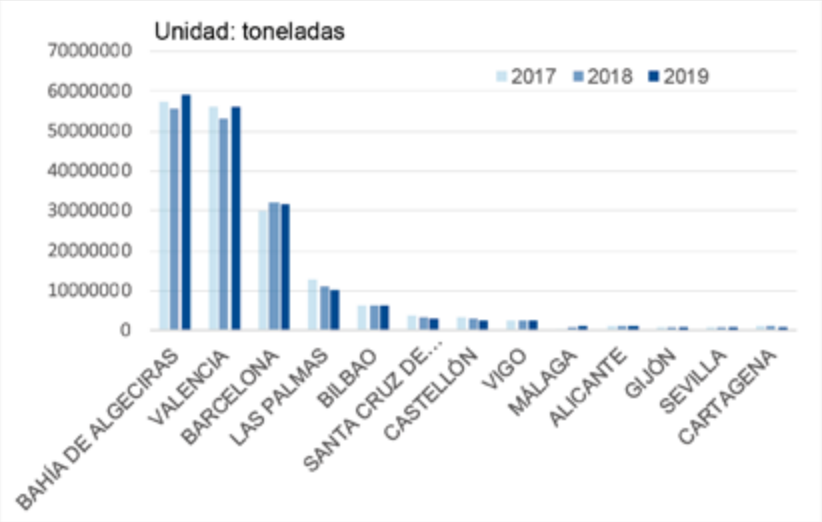
Fuente: Puertos del Estado

Figura 7-3
Mercancías por vía marítima gestionadas en los puertos españoles 2017-2019



Fuente: Puertos del Estado

Figura 7-4
Mercancías gestionadas en los principales puertos españoles 2017-2019



Fuente: Puertos del Estado

Retos

El objetivo establecido en la *Estrategia de Seguridad Nacional 2017* de fortalecer la proyección internacional de España se manifiesta en su dimensión marítima a través del adecuado posicionamiento en materias como la delimitación de los espacios marítimos de conformidad con el Derecho Internacional, el refuerzo de la actuación de la UE en asuntos marítimos o una Alianza Atlántica adaptada a una visión más acorde al contexto actual de seguridad marítima.

En lo relativo a la migración irregular por vía marítima, las cifras de 2019 reflejan una disminución importante del número de llegadas de aproximadamente un 50% con respecto al año anterior, invirtiendo la tendencia al alza de los últimos cinco años. No obstante, dada la posición geográfica de España, la migración irregular es un desafío permanente para la Seguridad Nacional, especialmente en el Levante y la costa meridional, así como en las islas Canarias.

Con respecto al contrabando por vía marítima, la penetración clandestina en aguas nacionales de toda clase de buques es el principal reto. Se trata de embarcaciones de recreo (veleros, yates, motos de agua), pesqueros, mercantes, remolcadores, narcolanchas (lanchas de alta velocidad), narcosubmarinos y pequeñas embarcaciones que transportan principalmente cocaína, hachís y cigarrillos. El contrabando por vía marítima afecta a todos los espacios marítimos de soberanía nacional, pero se manifiesta más intensamente en el estrecho de Gibraltar y mar de Alborán.

Además de su vínculo con el crimen organizado, el empleo de este tipo de embarcaciones, que navegan a alta velocidad y utilizan medios para no ser detectadas (ausencia de luces obligatorias o dispositivos de localización, navegación semisumergida, pinturas antirradar) resulta un serio peligro para la navegación.

La seguridad del transporte por vía marítima y su vínculo funcional con el sector portuario es uno de los pilares básicos de la seguridad marítima. El desarrollo de los sistemas de información marítima, las inspecciones de protección en buques, la aplicación de tecnologías específicas para reforzar las estructuras de seguridad, las capacidades de vigilancia, de prevención y de respuesta de los sistemas, son, entre otros, los medios que están en constante evolución.

Entre los riesgos contemplados en la *Estrategia de Seguridad Marítima Nacional* se encuentran la explotación ilegal de los recursos marinos y la destrucción y degradación del medio marino.

La lucha contra la Pesca Ilegal, No Documentada y No Reglamentada (INDNR) constituye un reto prioritario para la consecución de los objetivos de la Política Pesquera Común. También la pesca recreativa ha incrementado considerablemente, por lo que es necesario un nivel alto de vigilancia y control, con inspecciones en los desembarcos y en las importaciones de productos de la pesca, así como la colaboración con terceros países.

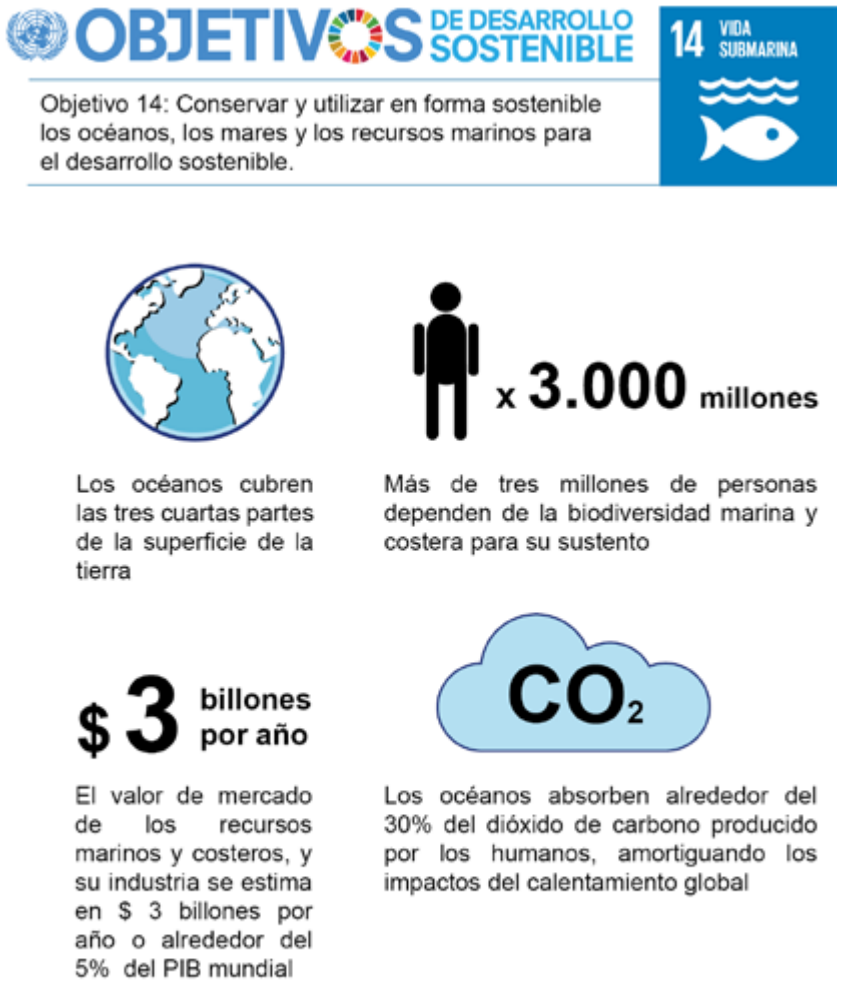
La explotación de los recursos mineros submarinos ha experimentado una tendencia al alza en los últimos años, en parte por la evolución

Los efectos del cambio climático sobre los ecosistemas marinos suponen una amenaza generalizada

de las tecnologías utilizadas. La Autoridad Internacional de los Fondos Marinos controla las actividades de exploración y explotación de los recursos en los fondos marinos y oceánicos y su subsuelo fuera de los límites de la jurisdicción nacional. En España se han identificado este tipo de recursos naturales en el área solicitada como ampliación de la plataforma continental española en las islas Canarias.

Uno de los grandes riesgos para la degradación del medio marino y su biodiversidad es la contaminación, incluyendo la contaminación por metales pesados, el lastre de los barcos, plásticos (y otros materiales) y fuentes de energía como el ruido submarino. Además, los efectos del cambio climático sobre los ecosistemas marinos suponen una amenaza generalizada, igual que los riesgos sísmicos y volcánicos, que potencialmente pudieran producirse en zonas sensibles, por sus características geológicas, como el mar de Alborán, el golfo de Cádiz o las islas Canarias. (Figura 7-5)

Figura 7-5
Objetivos de Desarrollo Sostenible 14: vida submarina



Fuente: Elaboración por DSN con datos de la ONU

Realizaciones

El Consejo de Seguridad Nacional, en su reunión de 15 de marzo de 2019, aprobó el *Plan de Acción de Seguridad Marítima*, documento que desarrolla la *Estrategia de Seguridad Marítima Nacional* conforme a sus cinco líneas de acción y orienta la acción hacia la consecución de su objetivo principal: impulsar una política de seguridad en el ámbito marítimo.

En 2019 el Consejo de Seguridad Nacional aprobó el Plan de Acción de Seguridad Marítima

Enfoque integral

Las acciones contempladas en el Plan de Acción se fundamentan en una optimización de la colaboración interdepartamental.

Con fecha 30 de mayo de 2019, se firmó el nuevo Acuerdo Marco entre el Ministerio de Agricultura, Pesca y Alimentación y el Ministerio del Interior en materia de inspección pesquera. Esta colaboración se materializa mediante un Programa Anual de Control Integral de la Actividad Pesquera (PACIAP) que incluye actuaciones coordinadas con los Servicios Aéreo, Marítimo y de Protección de la Naturaleza (SEPRONA) de la Guardia Civil.

El Ministerio de Defensa participa en las campañas de inspección de las organizaciones subregionales de pesca de las que España es miembro (NAFO y NEAFC, siglas que corresponden respectivamente a las denominaciones *North Atlantic Fishing Organization* y *North East Atlantic Fisheries Commission*) así como en campañas de inspección de los caladeros nacionales y apoyo a las flotas artesanales de pesca en el Cantábrico.

A su vez, con base en el acuerdo con el Ministerio de Educación, Cultura y Deporte, la Armada Española realiza tareas de vigilancia y apoyo sobre el Patrimonio Arqueológico Subacuático.

El Ministerio de Ciencia, Innovación y Universidades inició en 2019 la creación de un marco de trabajo para la planificación tecnológica conjunta en el que participen todos los ministerios y organismos públicos con flota y/o competencias marítimas en España. Este mecanismo mejorará la planificación y prospectiva tecnológica.

En el plano operacional cabe destacar la cooperación interdepartamental en la operación *Índalo*, de lucha contra delitos transfronterizos, que se desarrolla en aguas meridionales y del levante español y en la que participan la Armada Española, el Ejército del Aire, la Dirección Adjunta de Vigilancia Aduanera de la Agencia Tributaria (AEAT) y la Guardia Civil.

Durante el año 2019 se ha constituido el Comité Interministerial de Inspecciones de Protección Portuaria, órgano colegiado que tiene el objeto de la adopción de las medidas necesarias para coordinar las actuaciones que deriven del ejercicio de las competencias del Ministerio de Fomento y del Ministerio del Interior en relación con sus funciones y responsabilidades respecto a la normativa de protección marítima para el control y mejora del sistema de inspecciones.

Por último, un año más la Armada Española organizó el ejercicio de seguridad marítima *MARSEC*, que cuenta con la participación de casi todos los organismos nacionales con responsabilidades en el ámbito marítimo, y con un buen número de actores privados del sector.

Fortalecimiento de la capacidad de actuación del Estado

Conforme a las prioridades de la *Directiva Anual de Operaciones Marco*, las Fuerzas Armadas (FAS) mantuvieron una presencia permanente en todos los espacios marítimos de soberanía nacional y en aquellos en los que España ostenta derechos soberanos o ejerce jurisdicción. En el ámbito de las operaciones, y encuadradas en el Mando de Vigilancia y Seguridad Marítima, efectúan una vigilancia integral permanente de estos espacios en el ejercicio de la acción del Estado en el mar, a la que contribuye el apoyo de los Servicios de Inteligencia.

El Ministerio de Hacienda, a través de la Agencia Tributaria, desempeña también un papel clave en la seguridad marítima. Las operaciones desarrolladas en el transcurso del año 2019 para intensificar la vigilancia y control de tráficos ilícitos cubrieron buena parte de las zonas marítimas, con especial énfasis en el campo de Gibraltar. El despliegue de medios aeronavales se complementa con vigilancia vía satélite y sistemas tecnológicos.

La Agencia Tributaria asume un papel importante en operaciones internacionales en colaboración con la Agencia Europea de la Guardia de Fronteras y Costas (Frontex) y con Interpol. La operación *Pascal Atlántico 2019*, acción conjunta marítima regional entre las aduanas española y francesa, cuyo objetivo es la lucha contra el fraude aduanero por vía marítima, fue liderada por España para hacer frente al tráfico de estupefacientes procedentes del Caribe, realizado por barcos de recreo, barcos de comercio de poco tonelaje o barcos de pesca transformados, que transitan en el golfo de Vizcaya.

En el plano orgánico, en 2019 se creó la red de Oficinas de Inteligencia Marítima con el fin de incentivar e intensificar la investigación en la lucha contra el tráfico ilícito de estupefacientes.

El Ministerio del Interior elaboró en 2019 la *Estrategia Nacional de Gestión Integrada de Fronteras*, documento que establece medidas de coordinación y cooperación entre los diferentes actores concurrentes en el ámbito fronterizo español conformado, en gran medida, por su vertiente marítima.

Las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) han continuado el ejercicio de sus funciones permanentes. La Policía Nacional y la Guardia Civil lideran la ejecución del *Proyecto de Cooperación Portuaria* (*SEACOP*), financiado por la Comisión Europea y gestionado por la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP), cuyo objetivo es apoyar la lucha contra el tráfico marítimo ilícito (sustancias estupefacientes, especialmente cocaína) y las redes criminales internacionales en países de África occidental y meridional, así como América Latina y el Caribe.

En cuanto a la mejora del *Sistema Integrado de Vigilancia Exterior* (SIVE), operado por el Ministerio del Interior, en 2019 se ampliaron los medios

en la provincia de Las Palmas y se elaboró un Pliego de Prescripciones Técnicas para la modernización y ampliación en el estrecho de Gibraltar, todo ello con la finalidad de mejorar y asegurar su funcionamiento y alcanzar un adecuado nivel de eficacia en la vigilancia de las fronteras exteriores.

El Ministerio de Fomento, a través de la Dirección General de la Marina Mercante y su brazo operativo, la Sociedad Española de Salvamento Marítimo (SASEMAR), cubrió una superficie de vigilancia marítima superior a 157 millones de km^2, equivalente a 311 veces el territorio nacional. El número total de buques controlados por los centros de Salvamento Marítimo en los dispositivos de separación de tráfico de Finisterre, Tarifa, Cabo de Gata, Canarias oriental y occidental ascendió a 316.077 buques en 2019. Las cifras muestran una actividad incesante en materia de salvamento marítimo, coordinándose el rescate, la asistencia y búsqueda de 44.800 personas, datos que equivalen a 123 al día, y asistiendo a 945 embarcaciones. (Figura 7-6 y 7-7)

En 2019 SASEMAR cubrió una superficie de vigilancia marítima superior a 157 millones de km^2

En 2019 se realizaron más de 1.300 inspecciones a buques extranjeros bajo el ámbito del *Memorando de París*. De estas inspecciones, se produjeron 39 detenciones por incumplimiento de los requisitos establecidos en los convenios internacionales respecto a la seguridad marítima, protección marítima, protección del medio ambiente marino y/o condiciones de vida y trabajo a bordo.

En materia portuaria, la Dirección General de Marina Mercante y Puertos del Estado, junto a las Capitanías Marítimas y las Autoridades Portuarias, acordaron el texto del futuro convenio de actuación de respuesta ante emergencias portuarias que incluye el supuesto de la implicación de buques atracados en la emergencia.

En los últimos años, a través del Ministerio de Agricultura, Pesca y Alimentación se ha perfeccionado el sistema de inspección y control de la pesca de España. Como piedra angular del sistema de control se ha puesto en marcha el Sistema de Información Pesquero Español (SIPE) que integra a todos los sistemas de información anteriormente separados y que se completó el 7 de noviembre de 2018 con la puesta en marcha del Acta Electrónica, que sustituye las actas de inspección en papel por un sistema digital. La existencia de un control más eficiente ha conseguido implantar una cultura de cumplimiento entre los operadores, viéndose reducidas las incidencias en las pesquerías.

Para el desarrollo de la actividad se cuenta con 135 inspectores de pesca marítima, esperando la incorporación, en los primeros meses de 2020, de otros 28 inspectores. Como resultado de su labor se realizaron, en 2019, 8.617 actividades de inspección, que derivaron en 1.155 infracciones.

El sistema de inspección se complementa con el seguimiento vía satélite permanente de los buques españoles que faenan en caladeros repartidos por todo el mundo. También destaca el control mediante el diario electrónico de abordo, obligatorio para los buques de eslora superior a 15 metros, que funciona como un registro informático de los datos de las operaciones de pesca por los patrones de los buques pesqueros.

El Ministerio de Ciencia, Innovación y Universidades emprendió en 2019 campañas oceanográficas, observación y monitorización oceánica a lo largo de la costa y la Zona Económico Exclusiva española, para realizar análisis científicos y cartografía de los fondos marinos e identificación de yacimientos de recursos mineros y de hábitats sensibles susceptibles de ser protegidos.

Es de destacar la elaboración de la *Estrategia de Innovación en Economía Azul*, uno de cuyos ejes es la seguridad marítima. Además, se ejecutó el programa de monitorización de contaminantes a lo largo de toda la costa española y se iniciaron nuevos análisis de impacto sobre especies marinas de interés comercial. Se desarrollaron modelos de estudio de la propagación del ruido submarino y su efecto sobre la biodiversidad, y se acometieron proyectos de investigación para el control de especies alóctonas invasoras.

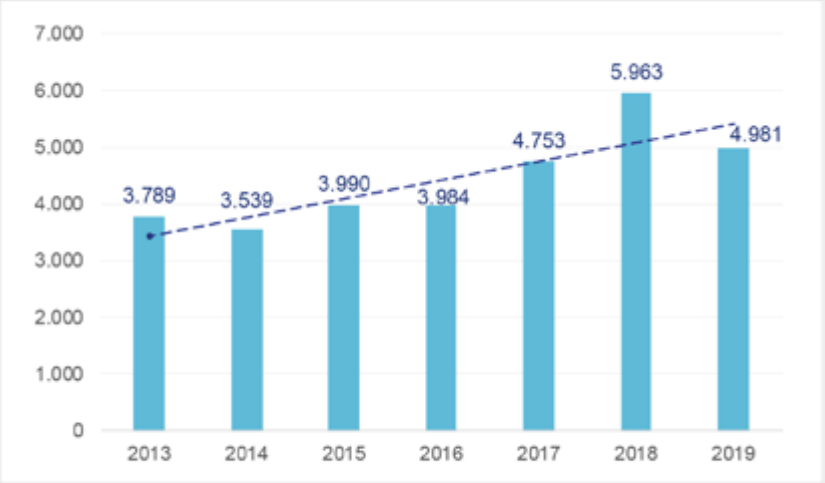
Por otra parte, cabe señalar la aprobación en 2019, por parte de la Comisión Europea, de una ayuda de 68,3 millones de euros a cargo del Fondo Europeo de Desarrollo Regional destinada a financiar el diseño, la construcción y el equipamiento de un nuevo buque oceanográfico para España.

En cuanto a la respuesta ante los temporales acaecidos en enero y febrero de 2019, y la depresión aislada en niveles altos (DANA) de septiembre de 2019, el Ministerio para la Transición Ecológica, a través de la Dirección General de Sostenibilidad de la Costa y del Mar, promovió en febrero y septiembre actuaciones de emergencia para paliar los daños provocados por temporales en el litoral. Se actuó en 11 provincias (Málaga, Granada, Almería, Murcia, Alicante, Valencia, Castellón, Tarragona, Asturias, Cádiz, Guipúzcoa), con una inversión total de 12,2 millones de euros.

Adicionalmente, se llevaron a cabo actuaciones dirigidas a la protección de la costa con cargo al presupuesto de inversión, que fue de casi 61 millones de euros. Cabe destacar la redacción de varias de las actuaciones previstas en las *Estrategias para la Protección de la Costa* de Huelva, Maresme (Barcelona), Castellón, Valencia y Granada. Se está avanzando en la elaboración de las *Estrategias para la Protección de la Costa* de Cádiz, Málaga, Almería, Baleares y del Delta del Ebro en Tarragona considerando los efectos del cambio climático, con financiación del Programa de Apoyo a las Reformas Estructurales de la Unión Europea. Se encuentra en su fase final de elaboración el *Plan para la Protección del Borde Litoral del Mar Menor*.

Se avanzó en la elaboración de los planes de ordenación del espacio marítimo con arreglo a lo establecido en el *Real Decreto 363/2017, de 8 de abril, por el que se establece un marco para la ordenación del espacio marítimo* y se ha iniciado el proceso de evaluación ambiental estratégica de dichos planes. También se continuó con la elaboración de planes de gestión de los espacios marinos protegidos de gestión estatal.

Con respecto a la materialización de la *Estrategia de Adaptación al Cambio Climático de la Costa Española*, en 2019 se presentaron las proyecciones regionales de cambio climático de variables marinas necesarias para el estudio de impactos costeros a lo largo de toda la costa española.



Fuente: Ministerio de Fomento

Figura 7-6
Evolución del número de barcos asistidos por Salvamento Marítimo 2013-2019

Fuente: Ministerio de Fomento

Figura 7-7
Estadística de Salvamento Marítimo 2019

Cooperación internacional

En el marco de la UE, ha continuado implementándose el *Plan de Acción de Seguridad Marítima* mediante la aportación de las iniciativas nacionales al proyecto común europeo de seguridad marítima.

España asumió el mando de la operación EUNAVFOR Atalanta en marzo de 2019

En lo relacionado con la PCSD de la UE, el elemento más destacable es la asunción, por parte de España, del mando de la operación *EUNAVFOR Atalanta*, por medio del recientemente creado ES-OHQ de Rota, en marzo de 2019. El mandato actual de la operación de lucha contra la piratería marítima en el Cuerno de África se extiende hasta el 31 de diciembre de 2020. En una eventual extensión de la operación entran en consideración aspectos como la lucha contra el tráfico de drogas, armas y seres humanos.

En cuanto a la operación *EUNAVFOR Med Sophia*, de desarticulación del modelo de negocio de los traficantes de migrantes y los tratantes de personas en el Mediterráneo central meridional, el Consejo Europeo prorrogó por seis meses, hasta el 31 de marzo de 2020, su mandato. El despliegue de los medios navales de la operación seguirá suspendido temporalmente

En 2019, el Servicio Europeo de Acción Exterior publicó el concepto sobre *Presencias Marítimas Coordinadas*, donde se presenta como caso piloto el golfo de Guinea. Esta iniciativa subraya la particular relevancia de España en este campo, toda vez que, como Estado miembro de la UE, ha venido prestando un apoyo sostenido mediante la cooperación bilateral con los países ribereños a través de actividades de cooperación militar realizada por buques de la Armada Española y aeronaves del Ejército del Aire.

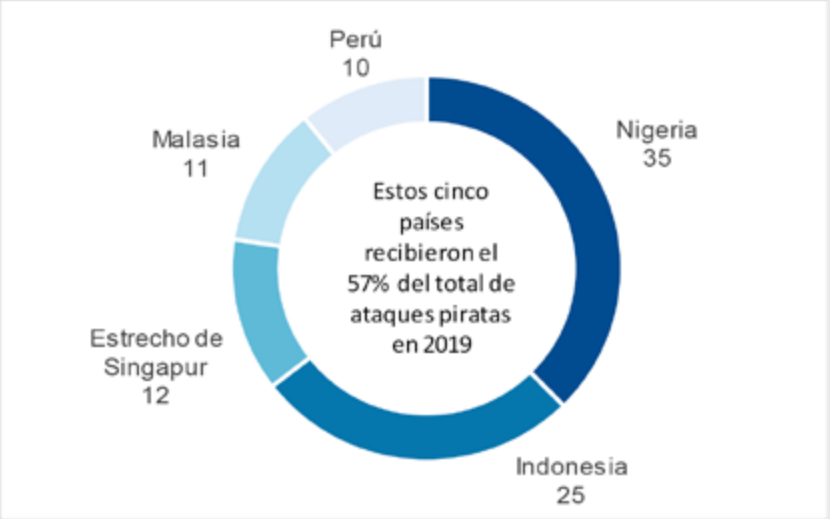
Con periodicidad semestral se despliega un buque de la Armada en el golfo de Guinea, para realizar actividades de adiestramiento con las marinas de los países ribereños y así incrementar su capacidad para afrontar los retos de seguridad marítima. Estas actividades se enmarcan en acuerdos de seguridad cooperativa (Cabo Verde, Mauritania, Senegal y Túnez) o en actuaciones de cooperación militar bilateral (Angola, Camerún, Costa de Marfil, Gabón, Ghana, Nigeria o Santo Tomé y Príncipe). Además, España continúa apoyando a los países ribereños en aplicación de la denominada *Arquitectura de Yaundé* para la lucha contra la piratería y a favor del desarrollo en el seno del grupo *G7++ Amigos del golfo de Guinea*. (Figura 7-8)

Por su parte, la Guardia Civil es un actor fundamental en cuanto a la seguridad marítima, colaborando para salvaguardar la vida de las personas en el mar, liderando la vigilancia de las fronteras exteriores de la UE, combatiendo a las redes criminales, así como garantizando el cumplimiento de la legalidad marítima por los distintos sectores que operan en el mar. Todo ello propicia la consolidación de su posición en el marco de la Guardia Europea de Fronteras y Costas, no solo en el desarrollo de operaciones conjuntas, sino también de actividades de formación, análisis de riesgos y proyectos de innovación tecnológica.

El 8 de noviembre de 2019, el Consejo aprobó un nuevo *Reglamento sobre la Guardia Europea de Fronteras y Costas*, un elemento importante del planteamiento general de la UE para la gestión de la migración y

las fronteras que refuerza el personal y los medios de Frontex y le otorga un mandato más amplio de apoyo a las actividades de los Estados miembros, especialmente en materia de control de las fronteras, retorno y cooperación con terceros países. Además, este nuevo reglamento incorporará el *Sistema Europeo de Vigilancia de Fronteras* al marco de la Guardia Europea de Fronteras y Costas con el fin de mejorar su funcionamiento.

En cuanto a la dimensión marítima de la OTAN, el Consejo Atlántico aprobó en 2019 su nueva política que busca revitalizar las capacidades de combate de la Alianza en el dominio marítimo y mejorar la eficiencia en el empleo de las fuerzas navales. España continua su aportación de unidades a las Fuerzas Navales Permanentes y mantiene su contribución a la Operación *Sea Guardian* en el Mediterráneo como muestra del compromiso con la seguridad en el dominio marítimo.



Fuente: Oficina Marítima de la Cámara Internacional de Comercio

Figura 7-8
Principales países y territorios objeto de ataques piratas en 2019

SEGURIDAD DEL ESPACIO AÉREO Y ULTRATERRESTRE

OBJETIVO:

Garantizar la seguridad del espacio aéreo y ultraterrestre en un marco 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 reacción ante los desafíos.

Tendencias

Una tendencia ascendente en el panorama de la Seguridad Nacional es la relevancia estratégica que está adquiriendo el dominio aeroespacial. Es un nuevo escenario de interés y cooperación que ofrece posibilidades y vías de progreso gracias a las nuevas tecnologías. También lo es de confrontación; su centralidad, junto a la del ciberespacio, está ensanchando los contornos de la arena internacional geopolítica y geotecnológica, tal y como se ha conocido en las últimas décadas. En este escenario proliferan las amenazas, creando nuevos desafíos.

Garantizar un acceso seguro al dominio aeroespacial es una prioridad para la Seguridad Nacional

Es, de hecho, un entorno de cuya seguridad dependen otros muchos ámbitos de la Seguridad Nacional, tal y como recoge la reciente *Estrategia de Seguridad Aeroespacial Nacional* aprobada en 2019. Garantizar un acceso seguro a este dominio dual, pero funcionalmente único, y su uso sostenible, es una prioridad para la Política de Seguridad Nacional de España, como país que se sitúa entre los principales socios europeos del sector aeroespacial y su industria.

En el espacio aéreo y ultraterrestre se producen situaciones de riesgo tanto para la vida y la salud humanas como para la seguridad del Estado. Existe una alta dependencia de los servicios, aplicaciones y productos proporcionados por el sector aeroespacial, que va a experimentar un uso creciente y consolidar su importancia para la sociedad. Cualquier alteración o denegación en su provisión afectan al ciudadano. Además, la seguridad de gran parte de los sistemas críticos del Estado depende del buen uso y funcionamiento de este dominio.

El crecimiento acelerado de tecnologías, que están ampliando la capacidad de acceso al espacio aéreo y ultraterrestre de manera global, aunque es fuente de importantes beneficios, se está produciendo en dos líneas de progresión, en ocasiones relacionadas. Por un lado, las capacidades de las tecnologías de la información y la comunicación (TIC), que permiten el acceso a sus sistemas de control y gestión. El abaratamiento de costes y las tecnologías de doble uso han "democratizado" su adquisición, y la "hiperconexión" en red ha facilitado su explotación por actores estatales y no estatales. Es relevante en este sentido el desarrollo de la industria ultraterrestre privada.

El crecimiento del uso de drones podría afectar al funcionamiento de las infraestructuras críticas y de los servicios esenciales

Y, por otro, la eclosión del uso de RPAS (por sus siglas en inglés correspondientes a la denominación *Remotely Piloted Aircraft*), que pueden emplearse para la comisión de actos negligentes, delictivos o en apoyo de estos últimos. El crecimiento del uso de aeronaves pilotadas remotamente cada vez más sofisticadas deberá ser tenido en especial consideración, dado que está afectando el pleno ejercicio de los derechos fundamentales y las libertades públicas. Sujetos individuales u organizaciones criminales recurren a su uso para sus fines delictivos en un amplio abanico de supuestos, que pueden conminar el funcionamiento de las denominadas infraestructuras críticas y los servicios esenciales para la comunidad.

La confluencia en este espacio de amenazas para la Seguridad Nacional se pone de manifiesto por la tendencia a consagrar a este dominio segmentos inicialmente defensivos de las Fuerzas Armadas en países como Estados Unidos, Francia, Reino Unido, Rusia o China. La accesibilidad a tecnologías de denegación de área y acceso (A2/AD por sus siglas en inglés correspondientes a la denominación *Anti-Access* y *Area-Denied* respectivamente) de posibles adversarios, pone en peligro la superioridad en el enfrentamiento de las Fuerzas Armadas (FAS) en escenarios externos al territorio nacional, por lo que habrá que reforzar estas capacidades en el futuro.

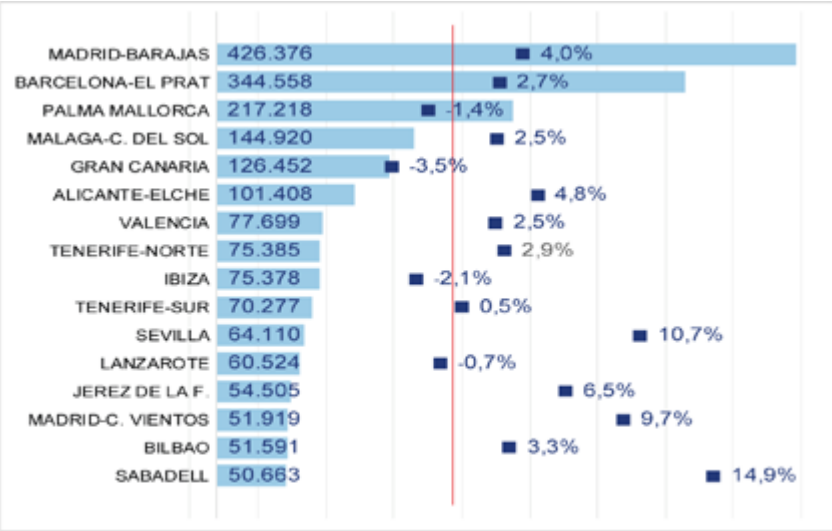
La evolución de los retos en el espacio aéreo y ultraterrestre ha ido marcando una tendencia hacia la búsqueda de una defensa aérea global, que incluya también la Defensa Antimisil, evolución a la que España presta la máxima consideración por el factor de escalada de la tensión con otros actores internacionales.

Se aprecia una evolución ascendente de los flujos aéreos y de nuevas amenazas a la aviación. Demandan medidas extensibles a todos los ámbitos que conforman el transporte aéreo, como las instalaciones aeroportuarias, los servicios de control de navegación, los sistemas de comunicaciones y las propias aeronaves, contemplando tanto la seguridad física, como la ciberseguridad y la adecuación y mejora de los procedimientos utilizados. (Figura 8-1, 8-2 y 8-3)

Ligado con este último aspecto, el dominio de la "información" juega un papel cada vez más importante para asegurar la superioridad en el ciclo de decisión de las crisis. El conocimiento de la situación "multidominio", casi en tiempo real, y el desarrollo de capacidades integrales de respuesta inmediata, son necesarios para la Seguridad Nacional y especialmente acuciantes en este campo, puesto que la elevada tecnificación, interconectividad y sincronización características del ámbito

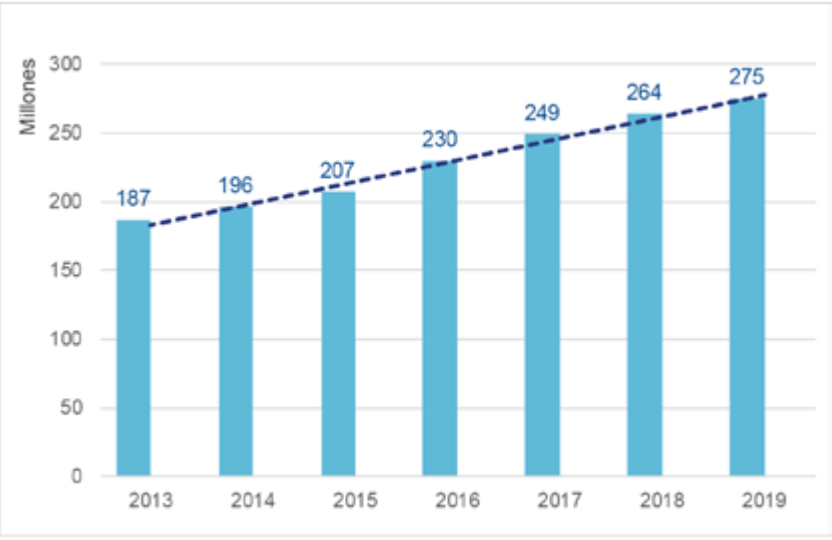
aeroespacial hacen que los efectos disruptivos se propaguen a gran velocidad, pudiendo desembocar en crisis ante las que el tiempo de reacción es muy escaso.

El ritmo de evolución de riesgos y amenazas exige una estrategia de "agilidad por diseño" de las estructuras de crisis, que facilite una integración transversal de capacidades entre departamentos y mayor autonomía de actuación vertical.



Fuente: Elaboración del DSN con datos de AENA

Figura 8-1
Número de operaciones en aeropuertos de España en 2019 (diferencia en términos porcentuales con respecto a 2018)



Fuente: Ministerio de Fomento

Figura 8-2
Número de pasajeros en los aeropuertos de España en 2013-2019

Figura 8-3
Número de pasajeros en los principales aeropuertos de España en 2019
(diferencia en términos porcentuales con respecto a 2018)

Fuente: Elaboración del DSN con datos de AENA

Retos

Proliferan en este ámbito las amenazas y los desafíos. Destacan la posible incidencia de los conflictos armados, el uso del espacio aéreo para producir atentados terroristas, el crimen organizado, el riesgo que suponen las armas de destrucción masiva usadas desde el espacio, el espionaje, las ciberamenazas, que constituyen fuente creciente de vulnerabilidad, las emergencias y catástrofes motivadas por la entrada de meteoritos, los efectos de la meteorología solar, los objetos espaciales que reingresan en la atmósfera, etc. Igualmente, la propagación atmosférica de enfermedades (epidemias, pandemias), o la contaminación atmosférica por fenómenos naturales como las cenizas volcánicas o artificiales son retos que se deben prevenir y afrontar.

Asegurar el conocimiento de la situación aeroespacial en tiempo casi real (vigilancia y control aeroespacial 24x7x365) es un reto que requiere sistemas redundantes y resilientes plenamente actualizados y operativos, la recuperación de capacidades pérdidas y/o degradadas, debido a la carencia de estabilidad presupuestaria en el marco de Defensa, así como la integración de Defensa Contra Misiles Balísticos (BMD), detección de drones o UAS (en sus siglas en inglés correspondientes a la denominación *unmanned aircraft systems*) o resiliencia ligada a la tecnología IP.

Además, resulta clave garantizar el uso correcto y control del espacio ultraterrestre para un adecuado funcionamiento de los servicios esenciales que presta a la sociedad, de tal forma que se proporcione un crecimiento económico y estratégico vital para el Estado. A este fin, se han de combatir los actos de interferencia ilícita contra la aviación civil y los sistemas de control de navegación aérea, con objeto de salvaguardar su normal funcionamiento. Igualmente, se debe proporcionar frente a estos actos una correcta protección a los elementos de tecnología satelital estratégica y asegurar la salvaguarda de pasajeros, tripulaciones, público y personal de aeropuertos, aeródromos e instalaciones de navegación aérea, tanto en tierra como en aeronaves, preservando el tránsito aéreo nacional e internacional en España y su espacio aéreo.

Garantizar el uso correcto y el control del espacio ultraterrestre es clave para un adecuado funcionamiento de los servicios esenciales

La dimensión anterior lleva aparejada la demostración de un eficaz empleo de la fuerza que disuada a las posibles amenazas al espacio aéreo de soberanía, profundizando en la ejecución coordinada de las operaciones permanentes y manteniendo el normal uso y funcionamiento del espacio aéreo de responsabilidad española y de aquellos servicios que, utilizando el ámbito ultraterrestre, permiten desarrollar los flujos de información y financieros básicos para el normal desarrollo de la sociedad.

Dada la tendencia referida del uso extendido de RPAS y debido a las amenazas emergentes que representan por su uso con fines terroristas o criminales o, incluso, debido a usos imprudentes, es un desafío el desarrollo de nuevas capacidades en el uso, control y gestión de todos los aspectos que puedan tener influencia en la Seguridad Nacional. En este sentido, por un lado, es necesario prevenir un uso no autorizado de RPAS y, llegado el caso, ser capaces de neutralizarlos, para lo que se ha de disponer de una herramienta que posibilite la identificación de los pilotos y las aeronaves ante cualquier circunstancia que amenace la seguridad pública. (Figura 8-4)

Por otro lado, se debe potenciar el empleo de los RPAS en labores de vigilancia y control en un uso más eficiente de los recursos disponibles y a través de la normalización del uso de la tecnología dron y antidron, hasta introducirla en los estándares de servicio como un elemento adicional en la dotación material de recursos operativos.

Es igualmente necesario disponer de un marco normativo nacional para la convivencia segura de aeronaves tripuladas por control remoto con el tráfico aéreo convencional, y el desarrollo económico del sector, con las adecuadas garantías desde el punto de vista de la seguridad pública y la seguridad ciudadana.

Desde el punto de vista normativo, se debe seguir desarrollando el Cielo Único Europeo (*Single European Sky*) para que el tráfico civil y militar pueda seguir operando en las mejores condiciones de seguridad, eficiencia y rapidez, así como recurrir a los mecanismos de financiación comunitarios con el fin de fortalecer la base industrial aeroespacial y la consolidación y mejora de un sector estratégico para la economía y la seguridad de España. Resulta importante la implementación de nuevos proyectos de valor, que garanticen la capacidad de las infraestructuras aeroportuarias para atender la demanda prevista y la calidad y seguridad en la prestación del servicio.

La colaboración internacional es imprescindible en los proyectos espaciales

En este sentido, resulta relevante disponer de capacidades espaciales europeas, que aporten mayor independencia para doble uso (civil y militar) respecto de los tradicionales países líderes en el empleo del espacio. La naturaleza global del espacio ultraterrestre y las características de los proyectos espaciales hacen imprescindible la colaboración internacional para abordarlos y para que países con posibilidades limitadas de inversión, como es el caso de España, puedan disponer de las capacidades y de las herramientas que aportan los sistemas espaciales.

Es también preciso asegurar la eficaz coordinación de España con sus aliados de la UE y la OTAN, vecinos como Francia, Portugal, Cabo Verde, Mauritania, Marruecos, Argelia, Italia y el resto de socios a través de la firma de convenios internacionales de cooperación bilateral y multilateral que contemplen las situaciones de crisis.

A estos efectos, se debe mantener y mejorar el nivel de 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 del espacio aéreo de soberanía nacional.

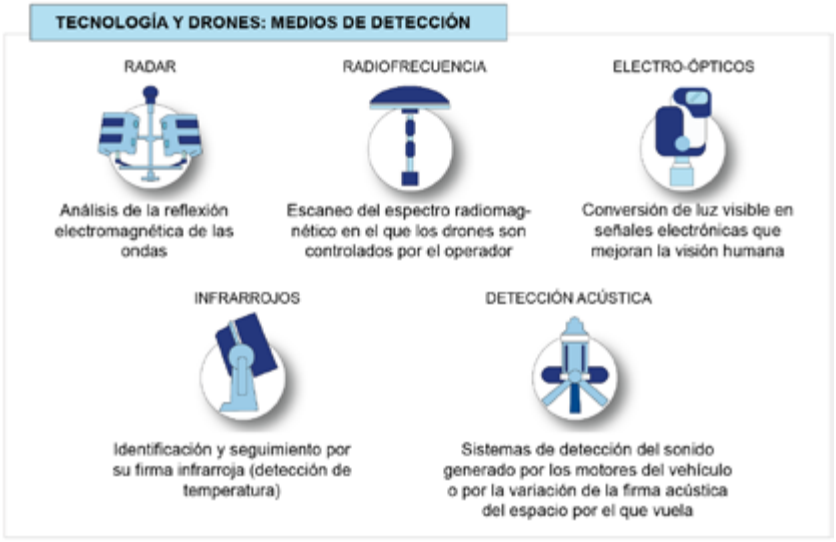
Además, es un objetivo fomentar la participación activa y representación de España en todas las organizaciones, comités, programas, foros y grupos de trabajo internacionales en materia de seguridad aeroespacial y, sobre esta base, fomentar el establecimiento de mecanismos de intercambio de información de vigilancia espacial con centros y organismos (civiles y militares) de otros Estados para complementar la monitorización de los activos espaciales nacionales fuera de la cobertura del sistema de vigilancia espacial.

Se debe progresar en la provisión de servicios meteorológicos de apoyo a la navegación aérea necesarios para contribuir a la seguridad, regularidad y eficiencia del tránsito aéreo, así como en la coordinación internacional para el desarrollo de protocolos internacionales de

prevención, alerta y actuación en caso de fenómenos meteorológicos adversos, principalmente aquellos de origen ultraterrestre, en línea con los estudios y planes de protección establecidos para los fenómenos de meteorología espacial.

Así, es esencial la información sobre meteorología espacial (condiciones físicas y fenomenológicas del entorno espacial) que puedan afectar a las comunicaciones, sistemas de navegación, salud de tripulantes de aeronaves, comportamiento de equipos electrónicos y redes de distribución de energía eléctrica.

Por lo demás, se ha de reforzar la coordinación internacional para la prevención y control de la propagación de enfermedades contagiosas a través del sistema de transporte aéreo internacional.



Fuente: Elaboración del DSN con datos del Centro de Estudios del Dron

Figura 8-4
Tecnología y drones: medios de detección

Realizaciones

En 2019 el Consejo de Seguridad Nacional aprobó la Estrategia de Seguridad Aeroespacial Nacional

El Consejo de Seguridad Nacional aprobó el 12 de abril la *Estrategia de Seguridad Aeroespacial Nacional* según el procedimiento aprobado por el Consejo que incluía la participación de una Comisión de Alto Nivel, un Comité Técnico, un amplio Comité de Expertos independientes del sector público y privado y la Conferencia Sectorial para asuntos de la Seguridad Nacional.

Esta Estrategia, novedosa en España, se suma a las otras dos que orientan la gobernanza de los llamados espacios comunes globales: el ciberespacio y el espacio marítimo. Recoge las principales amenazas y desafíos que se producen en este ámbito para posteriormente determinar, en las líneas de acción, las medidas necesarias para contrarrestarlas, reducirlas o neutralizarlas. Las amenazas se agrupan en seis epígrafes: conflictos armados, terrorismo, crimen organizado, proliferación de armas de destrucción masiva, espionaje y ciberamenazas. (Figura 8-5)

En cuanto a la dimensión orgánica, se contempla la previsión de crear un Consejo Nacional de Seguridad Aeroespacial como instrumento de apoyo al Consejo de Seguridad Nacional.

Figura 8-5
Líneas de acción de la Estrategia de Seguridad Aeroespacial Nacional 2019

	ESTRATEGIA DE SEGURIDAD AEROESPACIAL NACIONAL
1	Fomentar una actuación coordinada de todas las Administraciones Públicas y departamentos con competencias en el espacio aéreo y ultraterrrestre.
2	Fortalecer las capacidades de los organismos e instituciones nacionales, para hacer frente a las diversas amenazas y desafíos propios del espacio aéreo y ultraterrestre.
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.
4	Impulsar un desarrollo normativo del uso civil de aeronaves pilotadas remotamente.
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.

Fuente: Estrategia de Seguridad Aeroespacial Nacional 2019

Fomentar una actuación coordinada de todas las administraciones públicas

Se mantienen las coordinaciones necesarias entre los departamentos ministeriales y administraciones públicas con competencias en el espacio aéreo que posibilitan el adecuado control del espacio aéreo y la necesaria flexibilidad y rapidez de reacción.

La Secretaria de Estado de Seguridad y las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) han participado en las reuniones del Comité Nacional de Seguridad de la Aviación Civil, donde se coordinan los distintos aspectos relacionados con la seguridad. Igualmente, se participa en grupos de trabajo de la UE en materia de seguridad de la aviación civil, de la Organización Internacional de Aviación Civil (OACI), de la Conferencia Europea de Aviación Civil (CEAC) y del Consejo de Europa.

Se ha incrementado la colaboración público-privada y público-pública a través del INCIBE-CERT y CCN-CERT, para fortalecer las capacidades de respuesta ante incidentes de ciberseguridad cuyo objetivo sean infraestructuras críticas de los sectores Aéreo y del Espacio, y se ha puesto en marcha un Protocolo de colaboración entre el Ministerio de Ciencia, Innovación y Universidades y el Ministerio de Defensa, para la mejor coordinación de la planificación y prospectiva tecnológica y la financiación de tecnologías con uso dual.

Por otra parte, la Agencia Estatal de Meteorología (AEMET) proporciona información sobre condiciones meteorológicas en ruta para el desarrollo seguro del tránsito aéreo comercial durante ejercicios de entrenamiento militar.

Fortalecer las capacidades de los organismos e instituciones nacionales

En el plano normativo, la Agencia Estatal de Seguridad Aérea (AESA) ha participado en el desarrollo del *Reglamento de Ejecución (UE) 2019/947, de 24 de mayo de 2019,* de la Comisión, relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas y del *Reglamento Delegado (UE) 2019/945, de 12 de marzo de la Comisión, sobre los sistemas de aeronaves no tripuladas y los operadores de terceros países de sistemas de aeronaves no tripuladas*. La reglamentación define, entre otros aspectos, las características que debe tener un dron para volar de forma segura y estar identificado individualmente, con la finalidad de facilitar su seguimiento y rastreo cuando sea necesario.

En este sentido, el Centro de Operaciones Aéreas (AOC), situado en la Base Aérea de Torrejón, ha iniciado un proyecto para fortalecer y ampliar las capacidades. Dicho AOC deberá adaptarse teniendo en cuenta la transversalidad de las amenazas aeroespaciales; ya sea en el ámbito aéreo, ultraterrestre o ciber, y donde se contemple los mecanismos de control y coordinación centralizados y eficientes. Asimismo, deberá revisar sus protocolos de coordinación con otros organismos y entidades públicas o privadas del sector.

Respecto del Programa Nacional de Seguridad, se han incorporado los nuevos requisitos del *Reglamento de Ejecución (UE) 2019/103 de la Comisión, de 23 de enero de 2019, por el que se modifica el Reglamento de*

Ejecución (UE) 2015/1998 en lo que respecta a la aclaración, armonización y simplificación, así como al refuerzo de determinadas medidas de seguridad aérea específicas, que refuerza las medidas de seguridad para el estudio de antecedentes del personal y políticas de contratación para trabajar en el sector aéreo.

También se ha avanzado en la adaptación de los procedimientos de navegación aérea al *Reglamento de ejecución (UE) de la Comisión 2017/373, de 1 de marzo de 2017, por el que se establecen requisitos comunes para los proveedores de servicios de gestión del tránsito aéreo/navegación aérea y otras funciones de la red de gestión del tránsito aéreo y su supervisión.*

Por lo que se refiere a los medios, España aloja importantes infraestructuras espaciales nacionales e internacionales en su territorio: ESA-ESAC, NASA-Estación Robledo de Chavela, ESA-Estación de Cebreros y otras instalaciones, CESAEROB, EU SatCen, S3TOC, Centros de Control y Procesado de PNOTS, Hispasat, Hisdesat y Urthecast, Centro de Respaldo de Monitorización de la Seguridad de Galileo en La Marañosa y Centro de Servicios de EGNOS, Centro de Respaldo de EUMETSAT, Centros de Procesado, Archivado y Determinación Precisa de Órbitas para Copernicus, instalaciones de ensayo, etc.

En particular, España dispone de capacidades propias en telecomunicaciones por satélite, teledetección por satélite y vigilancia y seguimiento espacial, y es un país con un alto uso y dependencia de los sistemas espaciales en todos los segmentos (vuelo, tierra, lanzadores), desde la fabricación de equipos hasta la integración de sistemas complejos (satélites, centros de operaciones, etc.). Cuenta también con presencia en el sector de las aplicaciones y los servicios, y, así, dispone de varios operadores de satélites.

España dispone del satélite de órbita polar Paz con capacidad de observación óptica y por radar

Entre los activos de España en el sector se incluye un satélite de órbita polar y capacidad de observación óptica y por radar, uno de los pocos del mundo, el satélite Paz. Está previsto lanzar al espacio próximamente el segundo, Ingenio.

Se ha avanzado en la creación y activación del Centro de Operaciones de Vigilancia Espacial (COVE) en la Base Aérea de Torrejón, que recibirá los datos procedentes del radar de vigilancia espacial ubicado en la Base Aérea de Morón (Sevilla), la estación radionaval de Santorcaz, y los telescopios de Puertollano, Montsec, el Teide y San Fernando, y se integra en el Sistema de Mando y Control Aéreo. Su cometido es el apoyo a las capacidades espaciales, para el control y la vigilancia del espacio aéreo exterior en el cumplimiento de las misiones que les son encomendadas según el marco de las operaciones permanentes.

Se trata de un avance importante para desarrollar el segmento militar del programa nacional de Vigilancia y Seguimiento Espacial (S3T - *Spanish Space Surveillance & Tracking*), que permite el seguimiento de reentradas atmosféricas, el estudio de fragmentaciones, la prevención de colisiones y el apoyo a los lanzamientos hacia el espacio, en coordinación con el segmento civil que desarrolla este programa, maximizando las sinergias entre ambos centros y minimizando las duplicidades.

Esta capacidad posiciona a España entre los pocos países 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. España se encuentra preparada para participar en futuras iniciativas de mutualización de capacidades de vigilancia y control del espacio ultraterrestre.

España cuenta además con un extenso catálogo de medios espaciales, infraestructuras, centros de investigación, tejido industrial y sistemas espaciales, que sitúan al país entre los principales actores del sector espacial internacional. Se dispone, en particular, de sistemas de comunicaciones seguras, sistemas de observación de la Tierra y sistemas de posicionamiento por satélite. Esta situación se ha alcanzado gracias a la evolución que ha experimentado el sector respaldado por la inversión proveniente, en su gran mayoría, de las administraciones públicas.

En otro orden de consideraciones, se ha creado una nueva oficina de meteorología para dar soporte al aeropuerto de Murcia-Corvera y ha reabierto la oficina de soporte al aeropuerto de Ciudad Real. En colaboración con el prestador de servicios de navegación aérea ENAIRE se ha implantado un servicio de asesoría meterológica en el Centro de Control Aéreo de Barcelona como fase final de desarrollo de un proyecto para desplegar nuevos servicios de predicción en los centros de control de área.

Por último, las FAS continúan progresando en la de obtención de capacidades que contribuyan a la BMD.

Análisis de riesgos y evaluación de medidas contra ciberataques, actos terroristas o delictivos

Se han evaluado las distintas metodologías de análisis de riesgos contenidas en los planes del Sistema de Planificación de Protección de las Infraestructuras Críticas, revisando los riesgos inherentes a estas infraestructuras y adaptándolos a las actuales amenazas que afectan a las instalaciones aeroportuarias, de navegación aérea, y de las instalaciones del sector del espacio.

En este sentido, AESA realiza análisis de riesgos para evaluar estos nuevos desafíos en el sector aéreo y participa en el desarrollo de la Declaración de contexto de riesgo global de seguridad de la aviación de la OACI, que se actualiza periódicamente. Su objetivo es ofrecer a los Estados una metodología y un marco para realizar evaluaciones de riesgos a nivel nacional y proporcionar una visión general de la amenaza actual a la seguridad de la aviación mundial.

El Comité Nacional de Seguridad de la Aviación Civil ha liderado el Grupo de Amenazas y Riesgos, con objeto de evaluar los riesgos específicos que suponen los drones para el transporte aéreo. Este grupo de trabajo, organismo competente en la materia a nivel nacional, está siendo coordinado por AESA, con la participación del Ministerio del Interior, y se ha centrado en aportar la valoración de la amenaza.

En el ámbito de la seguridad de la aviación civil, se han realizado dos simulacros liderados por la Agencia Estatal de Seguridad Aérea en relación con la amenaza por artefacto explosivo en el aeropuerto de Fuerteventura y el secuestro aéreo en el aeropuerto de Málaga, con

participación en ambos de las FCSE, el Ejercito del Aire, así como de AESA, ENAIRE y Aena.

ENAIRE, dentro de su Plan Estratégico para el periodo 2017-2020, denominado *Plan de Vuelo 2020*, establece como primer objetivo estratégico aumentar los niveles de seguridad en sus tres ejes: seguridad operacional, seguridad física y prevención de riesgos laborales.

Impulsar un desarrollo normativo del uso civil de aeronaves pilotadas remotamente

El Comité Nacional de Seguridad de la Aviación Civil ha establecido el Protocolo coordinado de respuesta ante la amenaza de presencia de drones en el entorno aeroportuario

Se ha establecido en el seno del Comité Nacional de Seguridad de la Aviación Civil el *Protocolo coordinado de respuesta ante la amenaza de presencia de drones en el entorno aeroportuario*, de carácter nacional. El protocolo no solo tiene en cuenta las amenazas de seguridad (drones cuyo objetivo es ejecutar un acto de interferencia ilícita), sino también aquellas relativas a la seguridad operacional (drones no autorizados que podrían suponer un peligro para la operación aérea). Con estas consideraciones se establece el entorno a proteger, se especifican las medidas de coordinación entre los distintos implicados y se definen las líneas de actuación, tanto para la paralización de las operaciones como para la restauración de las mismas.

En la red de aeropuertos españoles de Aena, ya se ha implantado este protocolo en los aeropuertos con mayor carga operativa: Adolfo Suárez Madrid-Barajas, Josep Tarradellas Barcelona-el Prat, Palma de Mallorca, Málaga-Costa del Sol, Gran Canaria, Alicante-Elche, Ibiza y Tenerife Sur. Estos aeropuertos dan soporte a más del 60% de las operaciones en España y se está trabajando de manera coordinada con ENAIRE y con las Fuerzas y Cuerpos de Seguridad locales de cada aeropuerto, para lograr la implantación de este protocolo en el resto de aeropuertos con el objetivo de tener un procedimiento coordinado ante el avistamiento de drones en todos los aeropuertos.

La utilización por grupos terroristas o delincuentes del espacio aéreo para cometer actos ilícitos penales mediante el uso de aeronaves pilotadas por control remoto constituye una amenaza significativa. Para mitigar esta amenaza, el Ministerio del Interior está liderando el despliegue de "contra-medidas" frente a drones (C-UAS). De la misma manera, ante el posible uso imprudente de aeronaves pilotadas por control remoto, que puede suponer una amenaza tanto a la seguridad ciudadana como a la aviación civil, el Ministerio del Interior y el Ministerio de Fomento están impulsando y desarrollando el despliegue de estas "contra-medidas".

Además, tanto el Ministerio del Interior como Ministerio de Fomento están desarrollando una importante actividad a través de la participación en diferentes foros relacionados con la mitigación del riesgo que suponen las aeronaves pilotadas por control remoto. En este sentido, en el ámbito de Unión Europea, han participado en las reuniones de alto nivel sobre la amenaza que presentan los drones (*High-Level International Conference on countering the threats posed by unmanned aircraft systems*).

Por otro lado, desde febrero de 2019, el Ministerio de Fomento, a través de Aena, participa activamente en el grupo internacional *Drones*

Task Force de Airports Council International (ACI) que trata sistemas anti-drones y contramedidas.

La Secretaría de Estado de Seguridad ha puesto en marcha el *Proyecto Madrid Global*, cuyo objeto es la detección y neutralización de RPAS en el espacio aéreo de Madrid capital y alrededores. Los usuarios del sistema global son las FCSE en sus respectivos ámbitos competenciales, Servicio de Seguridad de la Casa Real de su Majestad el Rey y el Departamento de Seguridad de Presidencia del Gobierno. Además de Madrid capital y alrededores, el sistema se ha empezado a implantar en centros penitenciarios.

También cabe destacar la puesta en funcionamiento por parte de la Guardia Civil en todas las provincias de los denominados "Equipo PEGASO", encargados del control y supervisión de la aviación ligera y deportiva, de los campos eventuales e instalaciones aeronáuticas, así como de las aeronaves pilotadas por control remoto y de los "Equipos ÍCARO", que tienen la misión de estudiar y analizar el comportamiento de pasajeros y de otras personas en aras a detectar conductas anómalas y así mejorar la seguridad de determinados aeropuertos.

También la Policía Nacional ha reforzado sus capacidades de análisis de riesgos para los 25 aeropuertos más importantes de España mediante la creación del Grupo de Trabajo de Gestión de Riesgos en el Sistema Aeroportuario. Asimismo, la Policía Nacional ha incrementado sus actuaciones ante incidentes por uso irregular de aeronaves pilotadas por control remoto y aprobó el *Protocolo de Actuación Policial ante incidentes con d*rones en Madrid.

Apoyar el papel de España en el ámbito internacional

España es miembro de varias organizaciones internacionales dedicadas al espacio como UNOOSA, COPUOS, la ESA, EUMETSAT, INMARSAT, EUTELSAT, ITSO, y participa en los principales proyectos internacionales y europeos del ámbito espacial: ISS (Estación Espacial Internacional), Copernicus, Galileo, GOVSATCOM, EGNOS, Meteosat, lanzadores Ariane y Vega, EUSST (Vigilancia y Seguimiento Espacial de la Unión Europea), Sistema COSPAS-SARSAT, etc.

Además, y respecto de la membresía en la OTAN y la UE, se ha participado en la elaboración de la Política Espacial de la OTAN, que fue refrendada por los Ministros de Defensa en junio. La Alianza declaró el Espacio como dominio operacional, al igual que los dominios terrestre, aéreo, marítimo y cibernético, decisión que fue refrendada por los Ministros de Exteriores en noviembre. Por otra parte, España ha entrado oficialmente en el programa multinacional Sistema de Armas de Nueva Generación (*New Generation Weapon System*), junto a Alemania y Francia. Asimismo, lidera varios proyectos aeronáuticos en el marco de la PESCO. Dichos programas ayudarán a catalizar el desarrollo de la base tecnológica industrial nacional en áreas de alto valor añadido, actualmente deficitarias.

PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

OBJETIVO:

Asegurar la correcta provisión de los servicios esenciales para la sociedad, haciendo más robusto y resiliente el sistema de infraestructuras críticas sobre el que se sustenta.

Tendencias

En 2019 se registraron un total de 89 incidentes relacionados con la seguridad física en los sectores estratégicos

En 2019 se reportaron al Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) un total de 89 incidentes relacionados con la seguridad física en los sectores estratégicos, frente a los 22 registrados en 2018 y los 54 del año 2017.

En el ámbito de la ciberseguridad se gestionaron un total de 8.086 incidentes (818 incidentes en operadores de titularidad privada y 7.268 incidentes en operadores de titularidad pública) de distinta peligrosidad e impacto en operadores críticos, de servicios esenciales o estratégicos. Estos incidentes no llegaron a comprometer los servicios esenciales soportados por dichas infraestructuras, aunque su efecto sobre los servicios corporativos de los operadores críticos fue en algunos casos elevado. Los sectores más afectados fueron el financiero y tributario, energético y el de transporte, que contabilizan más del 50% de los incidentes gestionados. (Figura 9-1)

Los ataques dirigidos contra los sistemas que proporcionan los servicios esenciales de la sociedad, las injerencias en países, o los ciberataques enfocados hacia el Internet de las cosas, plantean un escenario de gran vulnerabilidad. En este sentido, el *hacktivismo*, tal y como se viene comprobando desde 2017, está teniendo no solo más actividad sino también más efectividad.

En los últimos seis años el número de incidentes de ciberseguridad ha crecido debido a la evolución de las ciberamenazas y a que las entidades que se encargan de gestionarlas han mejorado sus capacidades de respuesta, así como el intercambio recíproco de información.

Los ciberataques a los sectores estratégicos han aumentado tanto en número como en nivel de sofisticación

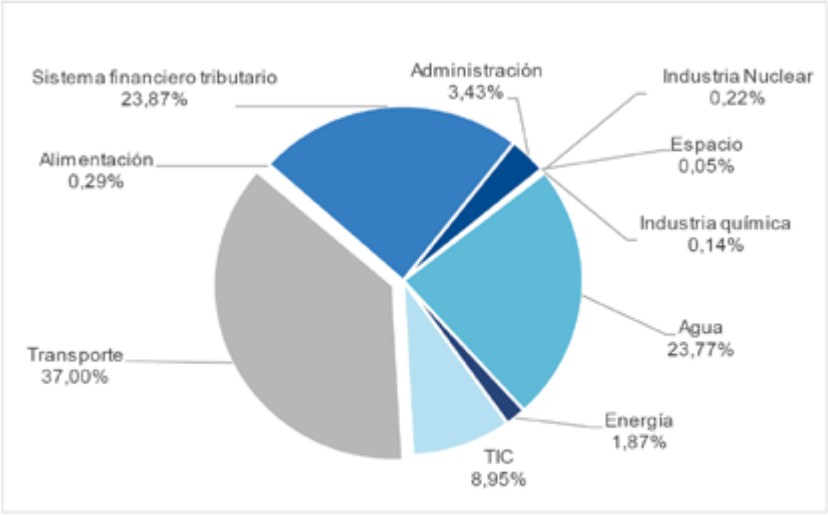
En este periodo, los ciberataques a los sectores estratégicos han ido aumentando, tanto en número, como en nivel de sofisticación. De esta forma, en 2013 se detectaron 17 ataques, pasando en el año 2014 a 50 ciberataques y 118 durante el año 2015. Esta cifra aumentó exponencialmente en el año 2016 con un total de 2.569 incidentes entre el ámbito público y privado, cifra que se situó en 4.056 en el 2017. El año 2018 registró un total de 6.954 incidentes.

En el ámbito de los operadores críticos, estratégicos o de servicios esenciales se aprecia una tendencia de diversificación en los ataques, focalizándose principalmente en el sector financiero y tributario, transporte, energía, agua, alimentación y sector de las tecnologías de la información y la comunicación (TIC), que han registrado incidentes de especial relevancia con riesgo alto, muy alto y crítico.

La seguridad de estas infraestructuras se tendrá que enfrentar a amenazas físicas y lógicas que, actuando de manera conjunta o separada, podrán materializarse en la negación de servicios. Las nuevas tecnologías permitirán que actores tanto estatales como no estatales puedan disponer de nuevas capacidades de actuación.

El espacio ultraterrestre será un dominio desde el que se proveerán servicios esenciales a la sociedad, como comunicaciones y acceso al ciberespacio, por lo que la protección de las infraestructuras espaciales (tanto desplegadas en el espacio ultraterrestre como las basadas en tierra) será una necesidad prioritaria.

Figura 9-1
Sectores estratégicos más afectados por ciberataques en 2019



Fuente: Ministerio del Interior

Retos

La implantación completa del Sistema Nacional de Protección de Infraestructuras Críticas es un reto de primera magnitud para los próximos años, toda vez que proporciona una eficaz protección y seguridad a instalaciones, redes y sistemas sobre los que descansa el funcionamiento de los servicios esenciales. Este objetivo se alcanza a través del desarrollo de proyectos que posibiliten responder eficazmente a las amenazas que se desarrollan en el ciberespacio, bien como medio, bien como objetivo, así como por medio del perfeccionamiento de los procedimientos y sistemas necesarios para evitar la interrupción en la prestación de los servicios proporcionados por las infraestructuras de sectores estratégicos. A su vez, se precisa aumentar la capacidad de resiliencia de los sistemas de infraestructuras estratégicas e infraestructuras críticas de los sectores estratégicos del Estado.

En este sentido, se debe continuar con la producción y revisión de planes inter-departamentales, mejorando los procedimientos de intercambio de información y poniendo a disposición del Estado un catálogo de capacidades civiles y militares para la protección, en su caso, de determinadas infraestructuras críticas. Cobra importancia el desarrollo de la capacidad "Contra-UAS", incluyendo los protocolos necesarios para el empleo y coordinación de todos los medios a disposición del Estado, que permita ejecutar una opción de respuesta rápida y eficaz ante esta amenaza.

El incremento de la complejidad de la protección de las infraestructuras, al evolucionar hacia infraestructuras conectadas, presenta la necesidad de potenciar y aumentar los servicios que han de permitir mejorar las capacidades en ciberseguridad de los operadores críticos y de servicios esenciales, procediendo de forma efectiva y eficaz a la notificación y gestión de incidentes. Estas cuestiones serán abordadas en el Reglamento de desarrollo del *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*, en el cual se está trabajando.

En este mismo sentido, cobra relevancia la mejora de la ciberresiliencia de los operadores críticos y de servicios esenciales a través de mediciones y autoevaluaciones sectorizadas, para elevar el nivel de protección ante ciberataques e incidentes, manteniendo la madurez y el grado de comparación con anteriores mediciones y elaborando guías de securización de sistemas de control industrial, tanto en lo referente a las tecnologías de la información, como a las tecnologías de operación.

Por otro lado, en el sector del transporte se mantiene la necesidad de lograr el pleno desarrollo del Sistema de Protección de las Infraestructuras Críticas como una prioridad.

Del mismo modo, es preciso lograr un sistema de respuesta que sea capaz de absorber el impacto de una amenaza sin por ello perder capacidad operativa, potenciando una Política General de Seguridad adecuada a las exigencias de los nuevos escenarios y requerimientos de las diversas organizaciones y la revisión y actualización del Proceso Gestión de la Seguridad.

Realizaciones

Avanzar en el cumplimiento normativo y la planificación escalonada

En 2019 ha continuado el proceso de implantación del Sistema de Protección de Infraestructuras Críticas

En 2019 se ha continuado con el proceso de implantación del Sistema de Protección de Infraestructuras Críticas (PIC) a nivel nacional. En este sentido se ha elaborado el *Plan Estratégico Sectorial de Instalaciones de Investigación* y se han revisado los *Planes Estratégicos Sectoriales de los sectores Espacio* e *Industria Química,* aprobándose por la Comisión Nacional PIC, que también aprobó la designación de ocho nuevos Operadores Críticos de los sectores afectados, las listas de servicios esenciales y de operadores de servicios esenciales, conforme a lo establecido en el *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*, identificando en total, 133 servicios esenciales y un total de 170 operadores de los mismos. Además, se han reanudado los trabajos correspondientes a la elaboración del Plan Estratégico del Sector de la Administración, previsto su aprobación en el primer semestre del año 2020. (Figura 9-2, 9-3, 9-4 y 9-5)

En línea con el proceso de planificación escalonada recogido en la normativa sobre protección de infraestructuras críticas, se ha avanzado en desarrollo del Plan Estratégico Sectorial del Subsector Marítimo, mediante la presentación a las Autoridades portuarias designadas como operadores críticos de una Guía de Redacción del Plan de Protección Específico. En este mismo sentido, Renfe Operadora ha continuado con la elaboración de los Planes de Protección Específicos de las Infraestructuras que fueron declaradas "críticas" en el Sector del Transporte, Subsector del Transporte Urbano e Interurbano, así como en la actualización del Plan de Seguridad del Operador en ambos Subsectores, el Ferroviario y el de Transporte Urbano e Interurbano. Además, INCIBE, Renfe y Adif han puesto en marcha en 2019 un grupo de trabajo para mejorar la ciberseguridad en el ferrocarril, en el que están presentes todas las empresas significativas del sector.

En el sector aéreo, el gestor de navegación aérea ENAIRE durante el año 2019 ha continuado con la gestión de diversos expedientes de mejora de los sistemas de seguridad existentes en las instalaciones de navegación aérea que prestan servicios esenciales, iniciados durante el año 2018, con el fin de mejorar su protección frente a actos ilícitos, dotando de esta manera a la organización de un mayor nivel de seguridad física frente a riesgos y vulnerabilidades. Asimismo, por parte de Aena se ha recibido la aprobación del *Plan de Seguridad del Operador Crítico* y se han finalizado los Planes de Protección Específicos de las infraestructuras consideradas como Críticas en el *Plan de Seguridad del Operador*.

En lo que respecta al ámbito legislativo, se está trabajado en la confección de un borrador de Proyecto de Real Decreto de Reglamento de Protección de las Infraestructuras Críticas, que implementará nuevos sistemas de supervisión y coordinación más eficientes y modernos, esto de forma acorde con lo requerido por *el Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información.*

Este proyecto de Real Decreto establece modificaciones importantes en relación al contenido de los Planes de Seguridad del Operador

(PSO) y los Planes de Protección Específicos (PPE), que pasan a estructurarse en dos bloques diferenciados, uno declarativo y otro demostrativo. El primero pasa a ser un documento de mera validación administrativa que verifica el CNPIC, sin embargo, el bloque demostrativo se constituye como la parte que debe ser acreditada a través de la norma de certificación. Este esquema de certificación integral y automatizada supondrá un valor añadido, puesto que todos los aspectos comunes a estos planes serán automáticamente validados y aprobados, con un ahorro de costes y tiempo tanto para la administración, como para los propios operadores afectados.

Se ha iniciado la elaboración de un nuevo Real Decreto sobre medidas de protección física que han de cumplir las instalaciones que alberguen materiales nucleares y fuentes radiactivas, así como su transporte, que vendrá a sustituir al actual *Real Decreto 1308/2011, de 26 de septiembre, sobre protección física de las instalaciones y los materiales nucleares, y de las fuentes radiactivas*. El nuevo Reglamento sobre protección física de las instalaciones y materiales nucleares y fuentes radiactivas abordará aspectos como la aprobación de los Planes de Protección Física, las evaluaciones de idoneidad del personal que trabaja en el sector, el transporte de material nuclear, la implementación de medidas de seguridad concretas que deben cumplir las centrales e instalaciones nucleares y los operadores del transporte y, por último, las Unidades de Respuesta.

Figura 9-2
Evolución del número de Planes Estratégicos Sectoriales

Fuente: Ministerio del Interior

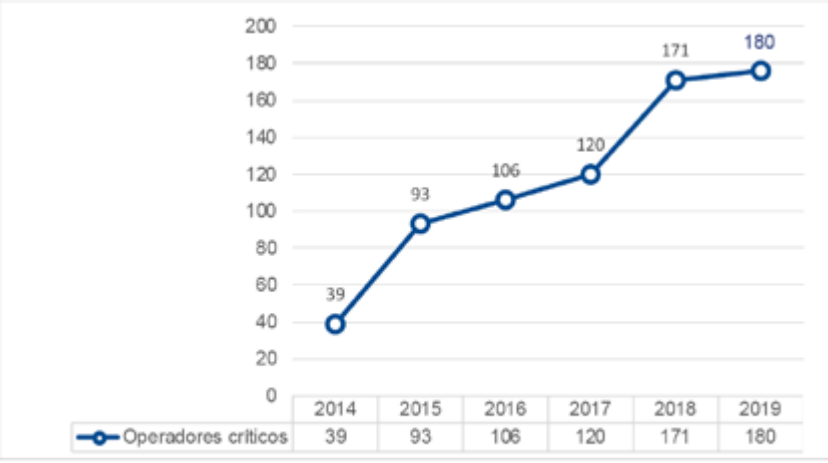


Figura 9-3
Evolución del número de operadores críticos 2014-2019

Fuente: Ministerio del Interior

Figura 9-4
Grado de avance del Sistema de Protección de las Infraestructuras Críticas

PLANIFICACIÓN ESTRATÉGICA	
Planes Estratégicos Sectoriales	17
Planes de Seguridad del Operador	148
Operadores Críticos	180
Planes de Protección Específicos	259

Fuente: Ministerio del Interior

Figura 9-5
Planes de Seguridad del Operador y Planes de Protección Específicos

Sector	Subsector	PSO	PPE
ENERGÍA	GAS	5	33
	PETRÓLEO	5	17
	ELECTRICIDAD	14	71
INDUSTRIA NUCLEAR		4	6
FINANCIERO		14	27
TRANSPORTE	AÉREO	2	7
	MARÍTIMO	18	9
	FERROVIARIO	3	5
	CARRETERA	2	2
	URBANO	10	0
AGUA		34	59
QUÍMICO		8	14
ESPACIO		2	0
TIC		6	8
ALIMENTACIÓN		19	1
SALUD		2	0
INVESTIGACIÓN		0	0
TOTALES		148	259

Fuente: Ministerio del Interior

Seguridad integral a través de un prisma amplio

Por lo que respecta al ámbito de la ciberseguridad, INCIBE-CERT localizó más de 53.345 equipos o recursos comprometidos en España, en el ámbito de los diferentes sectores definidos en *la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*. En este marco, además, se documentaron más de 506 avisos para los Sistemas de Control Industrial (sistemas informáticos para el control de procesos industriales).

En 2019, INCIBE y CNPIC llevaron a cabo una nueva medición de la capacidad de los operadores críticos y de servicios esenciales para soportar y sobreponerse a desastres y perturbaciones procedentes del ámbito digital. Participaron 71 operadores de hasta ocho sectores estratégicos y de 23 universidades y centros de investigación asociados a RedIRIS (red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional, gestionada por la entidad pública empresarial Red.es).

Por parte de las Fuezas Armadas (FAS) cabe destacar los trabajos de actualización de los planes de contingencia para la protección de las infraestructuras críticas, adiestramiento y capacitación de las unidades ejecutantes, al objeto de responder con eficacia ante este tipo de situaciones, ampliando el marco de actuación de las FAS en apoyo de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) frente a la amenaza terrorista. Además, mediante el Centro de Operaciones de Vigilancia Espacial (COVE) se ha contribuido al desarrollo de la Capacidad de Vigilancia Espacial que potencia la prevención, reacción y mitigación del daño que pudieran causar objetos procedentes del espacio sobre las infraestructuras críticas. En este mismo sentido, se han desarrollado y se están implementando unos procedimientos contra la amenaza de drones o RPAS de reducido tamaño en las bases aéreas y aeródromos del Ejército del Aire, de los cuáles también se beneficiarán aquellos aeródromos civiles a los que se permite el empleo de las infraestructuras aeronáuticas militares.

En el marco de lo dispuesto en la *Ley 5/2014 de seguridad privada*, se han llevado a cabo actuaciones de control de los servicios de seguridad de diferentes infraestructuras críticas, especialmente en la industria nuclear.

Capacidad y resiliencia de los sistemas asociados a las infraestructuras críticas

En 2019 se ha continuado también con los trabajos para mejorar las herramientas de detección proactiva de incidentes, a fin de prestar un mejor desempeño en el área de las infraestructuras críticas nacionales, y disponer de un conocimiento situacional de los incidentes acaecidos en el seno de la Administración Pública, y especialmente aquellos que revisten impacto en las infraestructuras críticas. De igual manera se prosigue con el análisis y estudio acerca de la implantación de una Guía de notificación de incidentes para operadores críticos.

Promover la coordinación en materia de protección de infraestructuras críticas

La Mesa de Coordinación PIC ha funcionado como órgano permanente de apoyo para el seguimiento y coordinación de las medidas de protección activadas por los operadores críticos, así como para el establecimiento de procedimientos de colaboración y comunicación entre los distintos agentes del Sistema de Protección de Infraestructuras Críticas. Se ha reunido cinco veces en 2019, a lo que hay que añadir una reunión más con motivo de la convocatoria de una Mesa Conjunta Extraordinaria.

Por su parte la Mesa de Coordinación de Ciberseguridad se reunió en cuatro ocasiones. Este órgano está constituido para dar soporte a la Mesa de Coordinación PIC, a la que está subordinada en aquellos asuntos relacionados con la ciberseguridad, y con el objeto de que esta pueda coordinar las acciones que se requieran en cada momento.

Coordinación y cooperación público-público y público-privada

Se han puesto en marcha en el año 2019 nuevas iniciativas para mejorar la cooperación tanto con el sector privado como entre los organismos del sector público responsables de la protección de las infraestructuras críticas. Prueba de ello ha sido la puesta a disposición de los operadores críticos y esenciales del ámbito privado de un nuevo portal de reporte y notificación en cumplimiento del *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*, así como el establecimiento de unos procedimientos para el intercambio de la información proveniente del sistema anti-UAS global del Ministerio del Interior y el Centro de Operaciones Aéreas del Ejército del Aire, que permitirán al Sistema de Defensa Aérea tener un mejor conocimiento de la situación en las capas más bajas del espacio aéreo.

Colaboración internacional y comunitaria

Desde el punto de vista internacional, se ha avanzado en la revisión de la Directiva Europea PIC y el Programa Europeo de Protección de Infraestructuras Críticas, además de otros temas como las amenazas internas, amenazas híbridas y los objetivos blandos, desde el punto de vista de su incidencia en la protección de las infraestructuras críticas. En este sentido, en el seno del CNPIC se creó el Centro de Coordinación y Alerta (CECOA) que conoce y trabaja la información que es remitida por operadores y las FCSE, relativa a las infraestructuras y personal que gestiona las mismas.

Se ha mantenido la actividad de los grupos de trabajo de la UE *Landsec* y *Railsec*, sobre seguridad del transporte terrestre y ferroviario. En este ámbito y cumpliendo con las recomendaciones del Grupo Railsec España, Renfe Operadora y Adif han mantenido una estrecha colaboración con el Ministerio del Interior en la capacitación de los formadores entre su personal para la prevención de la radicalización violenta.

Además, se han organizado ejercicios internacionales como el International CyberEx, que en su quinta edición ha contado con la participación de 80 entidades de 24 países.

SEGURIDAD ECONÓMICA Y FINANCIERA

OBJETIVO:

Promover un crecimiento económico equilibrado basado en la competitividad, como base de un modelo socioeconómico inclusivo, sostenible y resiliente, capaz de crear empleo de calidad, que favorezca la innovación y la productividad en la actividad económica y empresarial y refuerce la defensa de los intereses y compromisos nacionales de seguridad.

Tendencias

El periodo 2013-2019 se ha caracterizado por la intensa recuperación de la economía española. La tasa de variación interanual del PIB, tras alcanzar en 2015 su máximo registro tras la crisis (+4,2%), se ha desacelerado en los últimos años en línea con la esperada maduración del ciclo. (Figura 10-1)

El contexto internacional está agudizando la incertidumbre y ralentizando el crecimiento. Factores como las tensiones comerciales y geopolíticas o la salida del Reino Unido de la UE (*brexit*) representan serios desafíos para la economía y la seguridad.

El ritmo de crecimiento de la economía española se encuentra aún por encima del grueso de las economías avanzadas

Pese a la desaceleración, el ritmo de crecimiento de la economía española se encuentra aún por encima del grueso de las economías avanzadas y es líder en la zona euro. Así, según las últimas previsiones de la Comisión Europea, España cerraría 2019 con un crecimiento del PIB del 2,0%, frente a un 1,2% en el caso de la zona euro. (Figura 10-2)

La expansión está basada en la fortaleza de las exportaciones, el consumo y la inversión empresarial. La creación de empleo es especialmente vigorosa, con un recorte de la tasa de paro desde su máximo de 26,9% en 2013, hasta 13,8% del cuarto trimestre de 2019. (Figura 10-3)

Hay que destacar que desde 2014, y por primera vez en décadas, la economía española está siendo capaz de compatibilizar un sólido ritmo de crecimiento con superávit corriente (2019 marca el séptimo año consecutivo en positivo), elemento que apunta a un cambio estructural

derivado de la ganancia de competitividad. La evolución de los precios del petróleo, la mejora de las condiciones de financiación y el aumento de la competitividad, tras una notable corrección de los costes laborales unitarios, son factores que contribuyen a esta tendencia positiva, si bien a un ritmo de crecimiento más lento en los dos últimos años. Así, en 2019, el saldo por cuenta corriente se mantuvo en el 1,9%, fruto de las tensiones comerciales y el menor empuje de las principales economías europeas. (Figura 10-4)

A diferencia de anteriores fases expansivas, la actual está caracterizada por un aumento del gasto e inversión de familias y empresas compatible con el desapalancamiento, factor que provoca una expansión más sostenible y menos vulnerable. En concreto, el endeudamiento privado en España se ha reducido en 74 puntos porcentuales desde su máximo en 2010 de 205,8% del PIB a la actualidad de 132,1% del PIB. Además, las entidades de crédito han acometido un profundo proceso de reestructuración, recapitalización y reducción de activos dudosos. Estos factores tienen su reflejo en la evolución de la prima de riesgo, que desde los 400 puntos de 2013 ha mostrado una tendencia a la baja hasta el entorno de los 65 puntos a finales de 2019. (Figura 10-5)

El 14 de junio de 2019 el Consejo de la Unión Europea clausuró el procedimiento de déficit excesivo aplicado a España en abril de 2009

Además, cabe destacar que el 14 de junio de 2019, el Consejo de la Unión Europea clausuró el procedimiento de déficit excesivo aplicado a España en abril de 2009, con lo que confirma que el país ha reducido su déficit hasta un nivel inferior al 3% del PIB, valor de referencia de la Unión.

En cuanto al delito financiero, entre las actividades más relevantes que inciden de manera negativa en el tejido económico, destacan el blanqueo de capitales (que infiltra en la economía legal flujos de divisas procedentes de actividades ilícitas), el fraude a la seguridad social y la hacienda pública nacional o comunitaria, el contrabando, el comercio de productos falsificados, la evasión de divisas, las estafas a diversos sectores de importancia para la economía nacional (como el fraude al seguro, a las entidades bancarias, a las empresas con potencial exportador o a la pequeña y mediana empresa) o al ciudadano, la corrupción pública y privada o el fraude en las apuestas vinculado con la corrupción en el deporte.

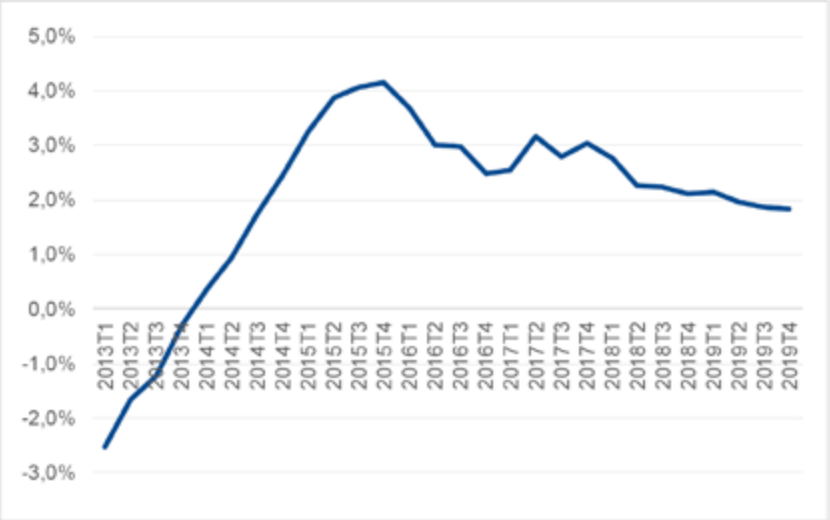
Especial transcendencia adquiere el crecimiento del uso de las nuevas tecnologías y la ingeniería social en la comisión de estafas, sobre todo las que afectan a las empresas o están relacionadas con los mercados de valores y de inversión; de delitos vinculados a cuestiones de competencia y que afectan incluso a sectores estratégicos; y del comercio ilícito de productos derivados del tabaco (especialmente la fabricación y distribución de hoja de tabaco) o de productos falsificados.

También adquiere un creciente interés el uso de medios alternativos de pago y de criptodivisas como medio de ocultación y transferencia de los beneficios obtenidos del delito.

Todas estas actividades ilícitas provocan que se reduzcan los índices de productividad, se detraigan recursos destinados al desarrollo de políticas públicas, se rebaje o elimine la competitividad en el mercado de bienes y servicios, se afecte al empleo de calidad y a los derechos de los

trabajadores y se produzca una pérdida de legitimidad de los poderes públicos.

Los ciberataques al sector financiero han ido aumentando, tanto en número, como en nivel de sofisticación. Los ciberdelincuentes han evolucionado dirigiendo sus ataques contra los sistemas de información de empresas, bancos y otras instituciones financieras, en lugar de dirigirse solo a los consumidores. De los 8.086 incidentes registrados en todos los sectores sobre operadores estratégicos en 2019, 1.930 (23,87% del total) fueron gestionados dentro del sector financiero.



Fuente: Instituto Nacional de Estadística

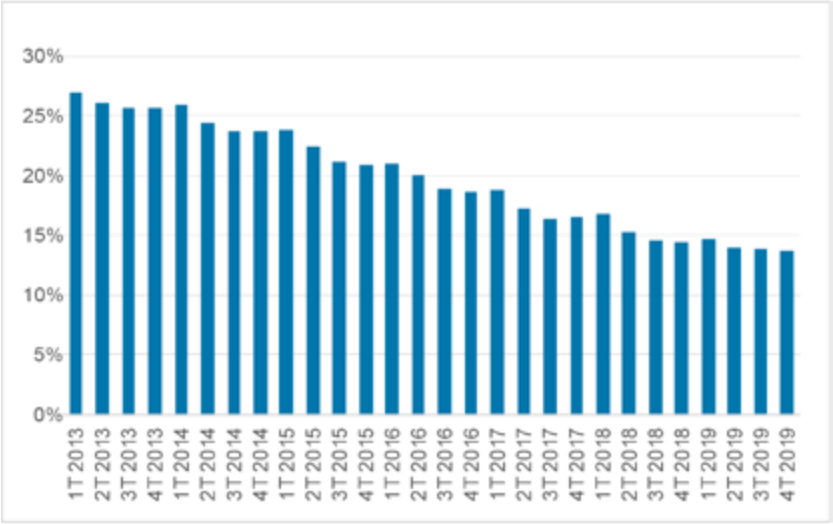
Figura 10-1
Tasa de variación interanual del PIB

Previsiones PIB (%)			
	2019	2020	2021
Comisión Europea (02/2020)	2,0	1,6	1,5
Fondo Monetario Internacional (01/2020)	2,0	1,6	1,6
Escenario Macroeconómico (02/2020)	2,0	1,6	1,5

Fuente: Ministerio de Economía y Empresa

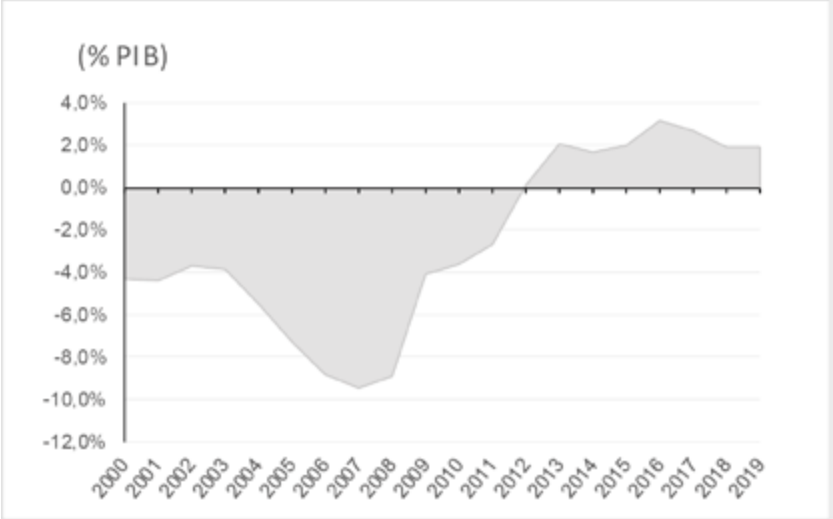
Figura 10-2
Previsiones económicas de los organismos internacionales

Figura 10-3
Evolución de la tasa de paro en España 2013-2019



Fuente: Instituto Nacional de Estadística

Figura 10-4
Saldo por cuenta corriente



Fuente: Banco de España

Figura 10-5
Evolución de la prima de riesgo en España 2008-2020

Fuente: Bloomberg

Retos

La actual fase de desaceleración de la economía mundial se produce en un contexto de fuerte incertidumbre geopolítica

La actual fase de desaceleración de la economía mundial se produce en un contexto de fuerte incertidumbre geopolítica, señaladamente por el conflicto comercial y el *brexit*. Aunque la economía española se ha fortalecido estructuralmente tras la crisis y muestra unas tasas y perspectivas de crecimiento superiores a las de gran parte de las economías avanzadas, no es ajena a este contexto internacional.

En el plano internacional, además de la incertidumbre marcada por las tensiones comerciales y el *brexit*, cabe destacar el cambio climático y la disrupción tecnológica.

La guerra comercial es un factor que está afectando al crecimiento económico a nivel global. Según estimaciones del Banco Mundial, el crecimiento económico global ha sido del 2,4%, la cifra más baja desde el fin de la gran recesión. Además, la imposición de aranceles afecta de forma directa a España. La autorización de la Organización Mundial del Comercio de imposición de aranceles a varios países de la UE por valor de 7.500 millones de euros es de aplicación a diversos bienes producidos en España.

Se confirma el 31 de enero de 2020 como la fecha de salida de Reino Unido de la UE. La exposición comercial y financiera de España con respecto al Reino Unido es significativa. En el ámbito del comercio bilateral, las exportaciones al Reino Unido, medidas en términos de valor añadido, representan alrededor del 10% del total. En cuanto a las importaciones, España es el quinto socio comercial del Reino Unido. Además, la inversión extranjera directa de las empresas españolas tiene como principal destino el Reino Unido, particularmente en el sector financiero y en el de las telecomunicaciones.

El cambio climático afecta significativamente al modelo productivo. Distintos estudios especializados, como el reconocido Informe Stern, estiman necesaria una cantidad equivalente al 2% del PIB global anual para llevar a cabo las acciones necesarias para hacer frente al calentamiento global.

El desarrollo tecnológico y la incorporación de las criptomonedas a los sistemas monetarios supone un reto desde la perspectiva de la seguridad internacional. El G7 formó un grupo especializado *ad hoc* para estudiar en profundidad cómo las *global stablecoins* (aquellas criptomonedas que poseen una gran base de clientes y tienen el potencial de escalar rápidamente) afectarían al sistema financiero internacional. El estudio concluyó que, por el momento, no es posible implementar ninguna moneda de esta naturaleza ya que no tiene cabida en el marco regulatorio actual y pueden ser empleadas eventualmente en actividades delictivas como el blanqueo de dinero y la financiación de actividades terroristas.

En la dimensión europea, el proceso de integración constituye otro pilar sobre el que se asienta la estabilidad económica. Para España es fundamental seguir impulsando los avances en la consecución de una Unión Económica y Monetaria real, a través de iniciativas como el reaseguro de desempleo común, el presupuesto para la eurozona, el fortalecimiento del papel internacional del euro y la lucha contra el fraude fiscal y el blanqueo de capitales a nivel europeo.

En el ámbito del sector financiero, el principal objetivo continúa siendo la conclusión de la Unión Bancaria. La puesta en marcha del esquema común de garantía de depósitos es un elemento clave para garantizar la estabilidad financiera de la Unión, reduciendo la fragmentación del mercado y reforzando su resiliencia.

En el plano nacional, se identifican cuatro retos principales: los niveles de deuda, el desempleo, la despoblación rural y la gestión de la actuación frente a acciones delictivas contra la seguridad económica.

En los últimos años la deuda pública ha continuado su senda descendente

En primer lugar, y en lo que respecta a la deuda pública, privada y externa, cabe señalar que los niveles actuales siguen representando una fuente de vulnerabilidad. No obstante, en los últimos años, la deuda pública consolida su senda descendente, el endeudamiento privado se ha visto fuertemente reducido y la posición deudora neta de la economía se ha reducido sensiblemente.

En segundo lugar, el desempleo en España, pese a haber disminuido en los últimos años, sigue siendo muy alto, especialmente en lo referente a la tasa de paro juvenil, con cifras superiores al 32%, siendo España el segundo país con la mayor tasa de la UE tras Grecia.

En tercer lugar, la despoblación es uno de los mayores retos a los que se enfrenta el medio rural, considerando que el 85% del territorio está ocupado por tan solo el 16% de la población, y su resolución debe formar parte de las prioridades de la agenda política y del conjunto de la sociedad. Para avanzar en esta tarea debe superarse la brecha de desigualdad entre los territorios rurales y las zonas urbanas.

De continuar este proceso, los problemas para la seguridad no vendrán solo por el abandono del territorio, la pérdida de actividad económica y un aumento de riesgos naturales, sino también porque el resultado del éxodo rural será la creación de grandes ciudades difíciles de gestionar y con graves problemas de vivienda o movilidad.

Con el objetivo de revitalizar el medio rural, se trabaja para fomentar el relevo generacional, favoreciendo la incorporación de jóvenes a las actividades agrarias y pesqueras, impulsando el papel de las mujeres e implementando medidas que favorezcan la modernización, la innovación y la digitalización.

En este sentido, es clave defender la incorporación de la perspectiva de género y el relevo generacional entre los objetivos estratégicos de la nueva *Política Agrícola Común* (PAC) de la UE post 2020 y su posterior desarrollo en el *Plan Estratégico Nacional de la PAC*. Otro eje de actuación para hacer frente a uno de los retos que afectan a la Seguridad Nacional desde una perspectiva socioeconómica es conceder una mayor relevancia y presupuesto a los programas de gestión de crisis.

En cuarto lugar, se identifica como reto la gestión de las situaciones que dificulten el normal funcionamiento de las políticas económicas y financieras o impidan maximizar su eficacia y continuidad. Así, es necesario luchar contra las actividades que supongan una interrupción o disminución en los sistemas de comercio y las acciones que minen la eficacia de los instrumentos económicos al servicio de los intereses y compromisos nacionales de seguridad.

La obtención y explotación eficiente de información con trascendencia tributaria y, más en concreto, el intercambio automático de información en el marco de la asistencia mutua internacional, la inteligencia, y la investigación patrimonial son importantes herramientas preventivas contra la evasión de capitales, el blanqueo de dinero y el fraude fiscal. El traslado de capitales fuera de las fronteras del país donde debieran tributar, para mantenerlos así ocultos a las autoridades fiscales, merma la recaudación de impuestos para el sostenimiento de los gastos públicos, y también tiene efectos financieros y en la economía real.

Desde el punto de vista de la inteligencia económica, el reto es facilitar la acción del gobierno en el mantenimiento de un crecimiento inclusivo y sostenible de la economía española en el actual contexto adverso y de transición ecológica.

El análisis de la información relativa a la seguridad económica, el análisis de riesgos, tanto internos como procedentes del exterior, y la sensibilización acerca de la estrategia de terceros países de utilización de sus sistemas de sanciones internacionales como herramienta de política exterior son actividades clave para la toma de decisiones sobre la protección y promoción de los intereses nacionales en los ámbitos económico y financiero.

En lo referente a la protección de las infraestructuras críticas del sector financiero, el reto es adoptar una posición de ventaja para incrementar la robustez y resiliencia de los procesos que soportan los servicios esenciales del sector, especialmente en la dimensión tecnológica y de ciberseguridad.

Realizaciones

Desarrollo de órganos, organismos, recursos y procedimientos de seguridad económica

En el plano orgánico, la publicación del *Real Decreto 102/2019, de 1 de marzo, por el que se crea la Autoridad Macroprudencial Consejo de Estabilidad Financiera, se establece su régimen jurídico y se desarrollan determinados aspectos relativos a las herramientas macroprudenciales* está orientada a la mejora de la coordinación de la supervisión macroprudencial a nivel nacional y ayuda a prevenir o mitigar los riesgos sistémicos, con la finalidad de redundar en una contribución más sostenible del sistema financiero al crecimiento económico.

En el ámbito de la protección de las infraestructuras críticas, se aprobaron las listas de servicios esenciales y operadores de servicios esenciales, conforme a lo establecido en el *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*, habiéndose evaluado y aprobado un plan de seguridad de nuevos operadores críticos del Subsector Financiero.

Además, continuó el análisis, evaluación y seguimiento de todos los instrumentos de planificación del *Plan Nacional de Protección de las Infraestructuras Críticas* en el ámbito del subsector financiero. Se potenció la colaboración y cooperación con entidades del sector para la resolución de incidentes y ciberincidentes, así como para dotarlos de mayor capacidad de resiliencia y mitigación ante la materialización de acciones de perturbación grave de los servicios esenciales.

Las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) potenciaron las relaciones con otras organizaciones e instituciones para mejorar el acceso e intercambio de información y la inteligencia en materia de blanqueo de capitales, entre las que destacan el Consejo General del Notariado y el Colegio de Registradores, con los que existen sendos protocolos suscritos y actualizados con dichas entidades.

Las FCSE participan asimismo en la Comisión Nacional para combatir la manipulación de las competiciones deportivas y el fraude en las apuestas. Entre sus objetivos figura la creación de un nuevo sistema de alertas tempranas sobre posibles manipulaciones de competiciones deportivas mediante información recabada de autoridades, instituciones, entidades deportivas y operadores de juego.

La proyección de las empresas españolas en el ámbito internacional y los programas de formación forman parte, asimismo, de las actividades acometidas. Destaca la celebración de la reunión anual del Grupo de Coordinación del Sector de Entidades Financieras, en la que toman parte los principales operadores del referido sector y en la que se abordan temas relacionados con la seguridad, y la colaboración con colectivos públicos y privados como el Notariado, los Registradores, la Universidad, la Agencia Tributaria (AEAT), el Tesoro, la Judicatura, la Fiscalía, la Comisión Nacional del Mercado de Valores o la Comisión Nacional de los Mercados y la Competencia.

Coordinación internacional

A nivel internacional, España participa en discusiones para la adopción de medidas y marcos para garantizar la seguridad económica y financiera. Entre otros esfuerzos, España ha seguido contribuyendo a los trabajos del Consejo de Estabilidad Financiera sobre prácticas supervisoras y de regulación en materia de ciberseguridad.

En la cumbre del G20, celebrada en Osaka (Japón), la participación española apoyó el compromiso con el multilateralismo como instrumento para lograr una globalización inclusiva y más justa. Como novedad, en la edición de 2019 se mantuvo -a iniciativa española-, un encuentro con los países iberoamericanos presentes en el G20 (Argentina, Chile y México).

En cuanto a la cooperación internacional en materia de intercambio de información con fines tributarios, en la actualidad, existen 109 países o jurisdicciones comprometidas con el estándar de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para el intercambio automático de información sobre cuentas financieras (*Common Reporting Standard*), de las cuales 106 han firmado el *Acuerdo Multilateral de Autoridades Competentes sobre Intercambio Automático de Información de Cuentas Financieras*. España recibe información detallada de las cuentas financieras de sus residentes fiscales mantenidas en 98 jurisdicciones.

Además, mediante el traslado a normativa nacional del Acuerdo Multilateral entre Autoridades Competentes sobre intercambio automático de información de cuentas financieras y el Acuerdo Internacional firmado entre España y Estados Unidos para la mejora del cumplimiento fiscal internacional y la implementación de la Foreign Account Tax Compliance Act (FATCA) se establece la obligación de identificar la residencia fiscal de las personas que ostenten la titularidad o el control de determinadas cuentas financieras y de informar acerca de las mismas en el ámbito de la asistencia mutua.

La Guardia Civil firmó un *Memorándum de Entendimiento para su participación en la Red Europea de Investigaciones Financieras*, red dinámica informal de investigadores financieros a nivel europeo implicada en la mejora de la calidad de las investigaciones de este tipo, que de por sí tienen una alta complejidad. En su seno se realizan intercambios de experiencias y grupos de trabajo orientados a la mejora de la calidad de las investigaciones financieras, las tecnologías y las técnicas de investigación.

Actuaciones frente al reto demográfico y la despoblación rural

El 29 de marzo de 2019, el Consejo de Ministros aprobó un acuerdo sobre las directrices generales de la *Estrategia Nacional frente al Reto Demográfico y la Estrategia de digitalización del sector agroalimentario, forestal y del medio rural*.

La *Estrategia Nacional frente al Reto Demográfico*, junto con los resultados del Foro Nacional contra la Despoblación, ofrecen el marco prin-

cipal para contribuir a la revitalización del medio rural, a partir del impulso de los sectores agroalimentario, y forestal, como fuente de riqueza y empleo en los territorios rurales. (Figura 10-6, 10-7 y 10-8)

La digitalización y las nuevas tecnologías son pilares para luchar contra la despoblación

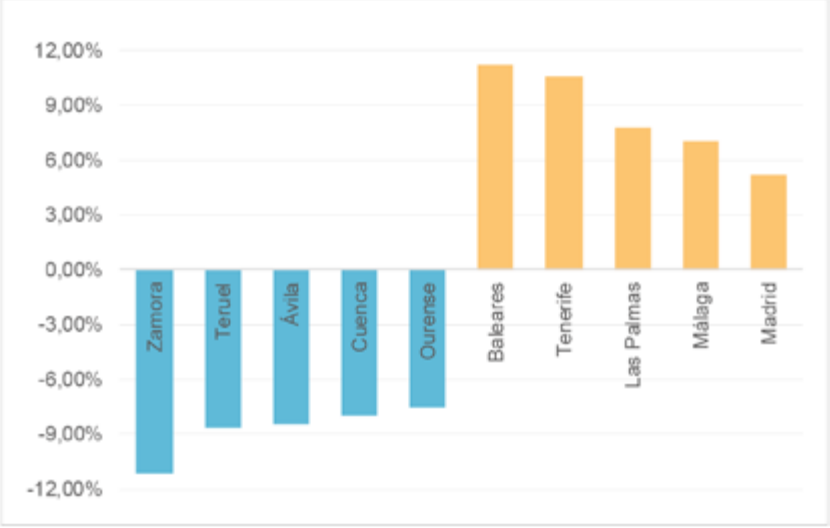
La digitalización y las nuevas tecnologías son pilares para luchar contra la despoblación y hacer atractiva la vida en el medio rural, a la vez que se contribuye a que este sea más vivo, dinámico y económicamente viable. La *Estrategia de digitalización del sector agroalimentario, forestal y del medio rural* recoge actuaciones para abordar el uso de datos, la brecha digital y el desarrollo de nuevos modelos de negocio y emprendimiento en estos territorios, estrategia que se llevará a cabo mediante el primer plan de acción bienal que se ha elaborado.

En cuanto a los *Programas de Desarrollo Rural* -dotados con un presupuesto de 848 millones de euros en el actual periodo de programación 2014-2020- tienen por objetivo potenciar, en colaboración con las Comunidades Autónomas, las medidas para fomentar el relevo generacional, a través de las ayudas a la creación de empresas agrarias para conseguir la incorporación de más de 21.300 jóvenes. Estos programas contemplan, a su vez, el desarrollo de un instrumento financiero de gestión centralizada que permitirá el acceso al crédito a los beneficiarios de las ayudas de los programas de desarrollo rural de las Comunidades Autónomas en unas condiciones económicas más favorables.

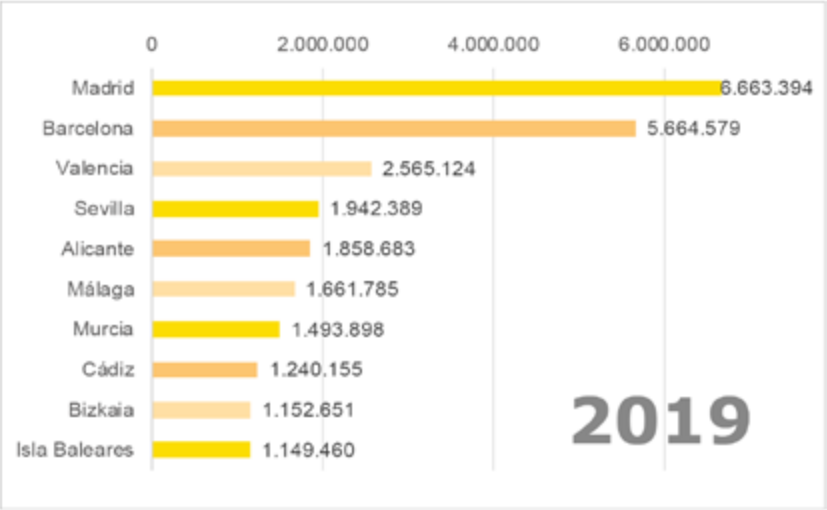
Gracias a los *Programas de Desarrollo Rural*, hasta 2019 se han instalado más de 12.500 jóvenes agricultores. Por otro lado, el pago complementario a jóvenes del primer pilar de la Política Agraria Común destinó casi 53 millones de euros, triplicando la cantidad del ejercicio anterior.

Mediante el impulso del sector agroalimentario y pesquero, como fuente de riqueza y empleo, se conseguirá revitalizar el medio rural y romper la espiral de despoblación y abandono.

Figura 10-6
Las cinco provincias de España que más población perdieron y que más población ganaron entre 2009 y 2019

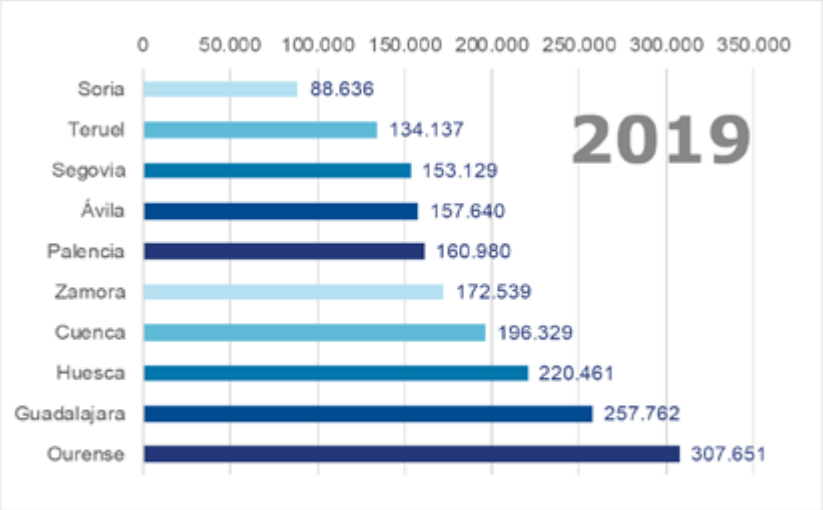


Fuente: Instituto Nacional de Estadística



Fuente: Instituto Nacional de Estadística

Figura 10-7
Las diez provincias más pobladas de España



Fuente: Instituto Nacional de Estadística

Figura 10-8
Las diez provincias menos pobladas de España

SEGURIDAD ENERGÉTICA

OBJETIVO:

Diversificar las fuentes de energía, garantizar la seguridad del transporte y abastecimiento e impulsar la sostenibilidad energética, en el marco de una transición ecológica justa.

Tendencias

La seguridad energética no es solo un suministro adecuado de energía a un precio asequible, sino que ha de consistir en un suministro de energía sostenible, que responda a las demandas de una economía descarbonizada.

España es especialmente vulnerable al cambio climático

El cambio climático es una realidad cada vez más patente y cada vez afecta de una manera más notable a la vida de las personas. En el caso de un país como España, su situación geográfica lo hace especialmente vulnerable a las consecuencias del cambio climático, tal y como indican los estudios al respecto. Es por esto, que resultan importantes tanto las políticas de mitigación del cambio climático, como las políticas de adaptación a las consecuencias del mismo.

En los últimos años el sector energético ha estado marcado por el progresivo incremento de ambición de los Estados miembros de la UE en materia de energías renovables, eficiencia energética y reducción de emisiones de gases de efecto invernadero, en consonancia con los objetivos fijados por la propia UE para los años 2020 y 2030 y, más recientemente, a 2050 como fecha para alcanzar la neutralidad climática en el marco de la UE. Todo ello dando cumplimiento a su vez a lo dispuesto en el Acuerdo de París de 2015.

Teniendo en cuenta este contexto, en el escenario energético actual confluyen tendencias procedentes del modelo energético tradicional y otras que se van conformando a medida que se avanza en la transición energética hacia un nuevo modelo. (Figura 11-1)

Respecto a estas segundas, las peculiaridades de las energías renovables deben ser consideradas como un componente importante de mejora de la seguridad energética. Las grandes instalaciones de producción de energía eléctrica alimentadas con combustibles fósiles y

los generadores síncronos están siendo reemplazados por un sistema de electricidad limpia con instalaciones conectadas a la red mediante convertidores electrónicos.

La capacidad de almacenar energía para situaciones en las que se necesite, o para reducir los vertidos que generan las energías renovables no gestionables, también es un factor importante. Las tecnologías de almacenamiento de energía, además de contribuir a que la red sea más segura, pueden proporcionar seguridad energética a instalaciones críticas. Estas dinámicas son coherentes en una sociedad en la que hay una mayor presión social para la erradicación de energías contaminantes.

En línea con las tendencias marcadas por la sostenibilidad medioambiental, cobran también importancia fenómenos como la variabilidad en las precipitaciones o las sequías, cuyo incremento reduce las reservas acuíferas para la producción de energía hidráulica. Es por esto que es tan necesario analizar las consecuencias que el cambio climático tiene sobre la cantidad de precipitaciones disponibles. Dado que, por el momento, la energía hidráulica es la más abundante y más fiable fuente de almacenamiento del sistema eléctrico español.

Por otra parte, se está introduciendo en el mercado el coche eléctrico, algo que tiene el potencial de cambiar la economía del transporte y reducir de manera significativa la dependencia de petróleo importado.

De modo paralelo a lo anterior, se observan tendencias propias del escenario energético tradicional. España continúa esforzándose para incrementar su seguridad de suministro por medio de la diversificación de fuentes y rutas, el aprovechamiento de fuentes alternativas de energía como las renovables, así como el incremento de su nivel de interconexión con países vecinos. En relación a esta última derivada, España sigue caracterizándose por su limitada interconexión energética, sobre todo de gas y electricidad con el resto de Europa, situación que aumenta la vulnerabilidad a interrupciones en el suministro.

Dado que el abastecimiento de España depende de los suministros exteriores de hidrocarburos, se sigue con especial atención el aumento de la inestabilidad geopolítica en las principales zonas productoras, puesto que podría poner en peligro el suministro de petróleo y gas de forma directa, y provocar una escalada en sus precios.

Figura 11-1
Estructura de la generación eléctrica por tecnologías

Fuente: Red Eléctrica de España

Retos

La transición energética es un desafío con oportunidades, ya que se pueden aprovechar las fortalezas que surjan en materia de inversión, financiación, tecnología, competitividad, empleo e industria, derivadas de la transformación de la economía en general y del sector energético en particular, dando cumplimiento a los objetivos que para 2030 prevé el marco normativo de la UE (reducción de emisiones de gases de efecto invernadero, incremento de aportación renovable al mix energético, incremento de la eficiencia energética e interconexiones).

Es primordial impulsar la transición energética hacia un modelo basado en la eficiencia e integración de las variables ambientales en los procesos de toma de decisión, asegurando, a la vez, una diversificación del mix energético nacional (matriz energética o combinación de fuentes de energía primaria) que proporcione una adecuada representación de fuentes energéticas y fomente el uso de fuentes autóctonas que disminuyan la dependencia exterior.

Se ha de continuar con el despliegue de las renovables autóctonas para que su producción se incremente a precios que faciliten la competitividad de la economía española, y alinear la estrategia de seguridad energética con las demás estrategias nacionales relativas a la descarbonización de la economía, como la eficiencia energética y la promoción de las energías renovables.

Para avanzar en este sentido, constituyen retos importantes conseguir la adecuada transferencia tecnológica al sector productivo de la investigación realizada con financiación pública o reducir la dependencia de minerales para la fabricación de baterías en el contexto de la transición hacia una economía electrificada y descarbonizada.

España se caracteriza por su elevada dependencia de las importaciones de gas y petróleo

Por otra parte, España sigue caracterizada por una elevada dependencia de las importaciones de gas y petróleo dado que la producción nacional es insustancial. Como medida de resiliencia, aspira a minimizar los efectos de la dependencia energética, situación que tiene un notable impacto económico en la balanza de pagos, constituyendo los productos energéticos los principales responsables del déficit de la balanza comercial. A futuro España continuará dependiendo de los precios de dichos productos en los mercados internacionales y de su volatilidad. (Figura 11-2)

La debilidad derivada de la dependencia casi absoluta de importaciones de hidrocarburos se compensa con la diversificación como elemento clave de las actuaciones de las empresas y de la Administración y la robustez y flexibilidad de las infraestructuras logísticas de gas natural y crudo y productos petrolíferos.

En 2019 España importó petróleo de más de 25 orígenes distintos repartidos entre áreas de la OPEP (60,8%) y fuera de ella (39,2%). Asimismo, el abastecimiento de gas natural sigue una estructura altamente diversificada con orígenes de 12 países diferentes. (Figura 11-3 y 11-4)

Del perfil energético español deriva el reto de diversificar los medios de transporte de recursos básicos, de forma que se garantice su complementariedad. Además, se debe mantener especial atención a la se-

guridad marítima, por su repercusión directa en el sector, al presentar España un porcentaje muy relevante de importación y exportación de gas y petróleo por esta vía. (Figura 11-5)

Constituyen, igualmente, desafíos, disponer de una mayor capacidad de intercambio eléctrico con los países vecinos, e incorporar las nuevas tecnologías de almacenamiento de energía a la red para disminuir la dependencia energética.

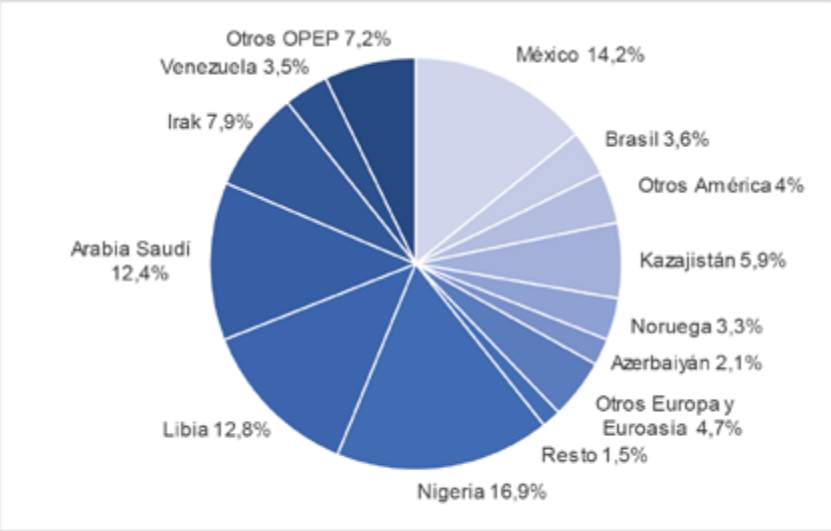
Es un reto garantizar la seguridad y protección de aquellas infraestructuras que proporcionan los servicios de distribución del suministro energético y de sus sistemas de control, con el objetivo de seguir proveyendo de energía a pesar de posibles ataques o incidentes, a la vez que se aumenta la capacidad de resiliencia, impulsando el desarrollo de herramientas que mitiguen los efectos medioambientales adversos y las acciones o ataques deliberados.

Potenciar la colaboración pública-privada con agentes del sector es necesario en aras a desarrollar y revisar protocolos de coordinación en caso de incidente en las infraestructuras estratégicas del Sector de la Energía, haciendo frente a las acciones que supongan una interrupción o disminución en la distribución de energía a los sectores productivos de la sociedad.

Igualmente, la configuración geográfica de España presenta un desafío en materia de conectividad energética en los territorios insulares, lo que, por otra parte, se ha tenido en cuenta en el borrador del Plan Nacional Integrado de Energía y Clima (PNIEC) 2021-2030, remitido a la Comisión Europea.

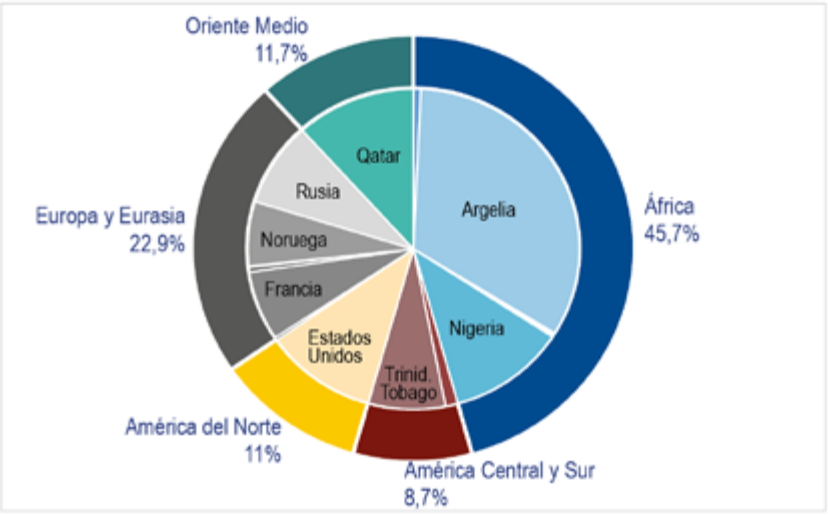
Figura 11-2
Evolución del precio del petróleo (Brent) en 2019

Fuente: Administración de Información Energética de Estados Unidos



Fuente: Cores

Figura 11-3
Importaciones de petróleo por zonas geográficas en 2019



Fuente: Cores

Figura 11-4
Importaciones de gas natural por zonas geográficas en 2019

Fuente: Elaboración del DSN

Figura 11-5
Principales rutas marítimas y estrechos internacionales

Realizaciones

El Comité de Seguridad Energética es un órgano de apoyo del Consejo de Seguridad Nacional y de especial relevancia debido a su papel en la toma de decisiones en materia de seguridad energética, mediante el análisis, estudio y propuesta de iniciativas. En 2019, destacó por su implicación en los ámbitos de tecnología e interconexiones energéticas internacionales, así como seguridad de suministro y materias primas.

Los esfuerzos realizados en este periodo se focalizaron en garantizar el suministro y abastecimiento energéticos, de una forma sostenible medioambiental y económicamente, en un contexto de transición energética hacia un modelo más seguro y eficiente.

Contribuir al fortalecimiento de la seguridad energética de la UE

El Plan Nacional Integrado de Energía y Clima 2021-2030 ha sido remitido a la Comisión Europea para su aprobación final

En 2019 se envió el borrador del PNIEC que define los objetivos de reducción de emisiones de gases de efecto invernadero, de penetración de energías renovables y de eficiencia energética a la Comisión Europea. El PNIEC contempla el almacenamiento y las interconexiones como instrumentos clave para garantizar la seguridad de suministro y la integración eficiente de las energías renovables. En particular, el Ministerio de Ciencia, Innovación y Universidades participó en su elaboración aportando su perspectiva en la dimensión de I+D+i, indicando las prioridades y oportunidades estratégicas para fortalecer la seguridad energética desde el progreso científico y tecnológico. (Figura 11-6)

En línea con lo contemplado en el PNIEC, uno de los principales logros de la implementación de las políticas y medidas incluidas en el mismo, es la reducción de la dependencia energética del exterior de la economía española. En efecto, se estima que la dependencia energética se reduciría en 12 puntos porcentuales a lo largo de la década. Es decir, gracias a la implementación de políticas de eficiencia en el consumo de la energía (renovación de equipos, cambios modales, etc.) y energías renovables (electrificación del transporte, aumento de la presencia de energías renovables en el sector eléctrico, etc.), se puede reducir notablemente la importación de combustibles fósiles. Además de los beneficios económicos derivados de esta reducción (estimados en unos 67.000 millones de euros en toda la década), también existen unos claros beneficios de seguridad.

Se llevaron a cabo múltiples iniciativas para impulsar las interconexiones, especialmente con Francia, con el fin de superar la situación de aislamiento energético que padece la península ibérica y asegurar así el cumplimiento de los objetivos de interconexión acordados por el Consejo Europeo para alcanzar el 10% de interconexión eléctrica en 2020 y el 15% en 2030. Muchas de estas iniciativas estaban incluidas en la cuarta lista de Proyectos de Interés Común, que son planes de infraestructuras transfronterizas clave que unen los sistemas energéticos de los países de la UE. Con ellos se pretenden cumplir los objetivos climáticos y energéticos, esto es, disponer de una energía sostenible, segura y asequible para todos los ciudadanos, y la descarbonización de la economía según el Acuerdo de París.

En relación a los proyectos que afectan directamente a España, la nueva lista, sometida a aprobación por el Parlamento Europeo, mantiene cuatro proyectos que ya aparecían en la lista anterior y que forman parte de los proyectos que configuran el Corredor prioritario eléctrico norte-sur de Europa occidental. Estos proyectos son:

- Interconexión entre España y Francia, que une el País Vasco y Aquitania (Francia), conocido como Proyecto Golfo de Vizcaya
- Interconexiones entre España y Francia mediante las conexiones de Aragón y los Pirineos Atlánticos, y de Navarra y Landes
- Interconexión entre España y Portugal. Incluye subestaciones en Beariz (España), Fontefría (España) y Ponte de Lima (Portugal)
- Tres estaciones de almacenamiento de electricidad con hidrobombeo

La línea eléctrica subterránea Santa Llogaia (España) - Baixas (Francia) de 320 kV de 64,5 km de longitud, en operación comercial desde el 5 de octubre de 2015, ha hecho posible duplicar la capacidad de transferencia neta (NTC) entre España y Francia, pasando de 1.400 MW a 2.800 MW de capacidad instalada. No obstante, la ratio actual de interconexión entre los dos países es de 2,8%, muy lejos aún del objetivo mínimo del 10% propuesto por el Consejo Europeo para el año 2020.

De acuerdo con los objetivos del PNIEC, la integración de una alta penetración de energías renovables supondrá un cambio de paradigma en el sistema eléctrico. La variabilidad y parcial predictibilidad de las energías renovables suponen retos orientados a los cambios de operación del sistema eléctrico, así como a la necesidad de contar con una cartera de sistemas de almacenamiento.

La integración de una alta penetración de energías renovables supondrá un cambio de paradigma en el sistema eléctrico

Por otra parte, en el primer semestre del 2019, se aprobó un nuevo paquete normativo para la regulación del mercado interior de gas y electricidad, destacando desde la perspectiva de la seguridad de suministro la aprobación del *Reglamento (UE) 2019/941 de 5 de junio de 2019 (DOUE 14 de junio de 2019) sobre la preparación frente a los riesgos en el sector de electricidad* y por el que se deroga la *Directiva 2005/89/CE* (*DOUE 14 de junio de 2019*).

Análogamente al mercado interior de gas, en este nuevo reglamento comunitario se establece un planteamiento común de la prevención y gestión de las crisis en el sector eléctrico facilitando la coordinación entre Estados miembros y la identificación de situaciones de riesgo potencial, utilizando la misma metodología, definiciones y parámetros de seguridad de suministro. Este enfoque tenía como objeto cubrir todas las crisis de electricidad en el territorio de la UE teniendo en cuenta, entre otros aspectos, las particularidades regionales y nacionales de los mercados, el *mix* de generación eléctrica y los volúmenes de producción y consumo.

Una adecuada diversificación del *mix* energético

En los últimos años España ha desarrollado una serie de actuaciones para adecuar el *mix* energético transformándolo en aras a lograr un equilibrio sostenible entre seguridad de suministro energético, competitividad y preservación del medio ambiente, aumentando el grado de autoabastecimiento y cumpliendo con las normas europeas. Así, como resultado de las diferentes coyunturas energéticas y económicas, el *mix* energético español ha sufrido una importante evolución en los últimos años. En 2018 el consumo de energía primaria alcanzó casi los 129,3 Mtep que se distribuyó entre las distintas fuentes primarias de la siguiente manera: 44,6% petróleo, 20,9% gas natural, 11,2% energía nuclear, 13,8% energías renovables, 0,2% residuos no renovables y 8,5% carbón. (Figura 11-7 y 11-8)

En 2019 el desplazamiento del carbono en el mix energético ha sido relevante por primera vez

En lo que respecta a la diversificación energética, si bien la dependencia del petróleo se ha reducido desde las crisis de 1973 y 1979, cuando este representaba más del 70% del consumo de energía primaria, los valores actuales (aproximadamente 45%) son todavía altos y superiores a los de la media europea. No obstante, las actuaciones desarrolladas para impulsar el modelo de transición energética han comenzado a mostrar resultados. En 2019, el desplazamiento del carbono en el mix energético es por primera vez relevante, incrementándose la producción fotovoltaica (1.800Mw/h) y la eólica (1.200Mw/h) respecto de la producción energética tradicional.

La seguridad y calidad del suministro a través de las redes de transporte de electricidad y gas es uno de los pilares fundamentales de la política energética de España y, por tanto, de la planificación energética, competencia de la Administración General del Estado en colaboración con las Comunidades Autónomas, los operadores y agentes del sistema y los promotores de los nuevos proyectos.

Durante 2019 comenzó la planificación de la red de transporte de energía eléctrica en el horizonte 2021-2026, proceso iniciado formalmente mediante la publicación de la Orden TEC/212/2019, de 25 de febrero. En este ejercicio de planificación se establecen nuevos principios rectores orientados hacia el desarrollo de un plan de expansión de la red de transporte que permita la integración masiva de nueva generación renovable al ritmo necesario para alcanzar los objetivos en el medio y largo plazo, garantizando la operación segura del sistema eléctrico al mínimo coste para los consumidores.

Garantizar la seguridad de abastecimiento y del suministro

Dada la alta dependencia energética del exterior, el CNI realiza un esfuerzo por analizar constantemente la evolución de los países suministradores y de tránsito más relevantes para España y hace seguimiento de los riesgos que pueden afectar a los proyectos de interconexión energética entre España y los países vecinos, así como del estado de situación y evolución previsible de las interconexiones ya existentes. Igualmente, se previenen riesgos o mitigan impactos sufridos por empresas estratégicas nacionales del sector energético en materia de seguridad física y jurídica a nivel internacional, y se analiza de las acciones

e intereses de terceros Estados en todo aquello que pueda afectar a la estabilidad del sector energético nacional.

Existe un marco internacional y nacional desarrollado que regula y gestiona la mejor aplicación de las existencias mínimas de seguridad de hidrocarburos. En caso de crisis de abastecimiento, las existencias de seguridad quedan directamente sometidas al poder de decisión de las autoridades españolas, de forma que el Consejo de Ministros, mediante acuerdo, podrá ordenar el sometimiento de las existencias mínimas de seguridad de productos petrolíferos, incluidas las estratégicas, a un régimen de intervención bajo control directo de la Administración y la Corporación de Reservas Estratégicas de Productos Petrolíferos (CORES).

Al respecto, en 2019 se iniciaron los trabajos para la actualización de la norma de referencia de seguridad de suministro en el ámbito de hidrocarburos (*Real Decreto 1716/2004, de 23 de julio, por el que se regula la obligación de mantenimiento de existencia mínimas de seguridad, la diversificación de abastecimiento de gas natural y la Corporación de reservas estratégicas de productos petrolíferos*) teniendo en cuenta, entre otros aspectos, los contenidos de la Directiva de Ejecución 2018/1581 de la Comisión, de 19 de octubre de 2018, por la que se modifica la Directiva 2009/119/CE del Consejo en lo que se refiere a los métodos de cálculo de las obligaciones de almacenamiento.

Impulsar la transición energética

El Consejo de Seguridad Nacional mediante el Acuerdo de 20 de enero de 2017, dispuso impulsar la creación del Comité Especializado de la Seguridad Energética, cuya Presidencia y Vicepresidencia son ejercidas por el Secretario de Estado de Energía y por el Director del DSN del Gabinete de la Presidencia del Gobierno. En el actual contexto energético marcado por los objetivos y contenidos de la dimensión de seguridad energética que establezca el *Plan Nacional Integrado de Energía y Clima*, el Comité Especializado de Seguridad Energética tiene como objetivo la profundización en los planes de contingencia en caso de crisis energética y sus trabajos se han articulado a través de dos grupos: "Tecnología e Interconexiones energéticas internacionales", y "Seguridad de suministro y materias primas".

El Comité Especializado de Seguridad Energética tiene como objetivo la profundización en los planes de contingencia en caso de crisis energética

Por otra parte, en los Organismos Públicos de Investigación y Universidades, se siguió realizando avances científicos y tecnológicos en el ámbito de la seguridad y soberanía energética financiados por la Agencia Estatal de Investigación. Entre estos avances se encuentran el desarrollo de metodología para evaluar y mejorar la sostenibilidad de las tecnologías energéticas, integrando el almacenamiento de energía térmica para acercarse a una economía circular y la aplicación de esta metodología en la industria y en edificios, así como el desarrollo de baterías de doble ión Na+/anión para aplicación en sistemas de almacenamiento de energía eléctrica que sustituyan al litio por estos otros materiales, y así reducir la dependencia de este mineral escaso y caro.

En materia de ahorro y eficiencia energética, el Fondo Nacional de Eficiencia Energética permite la puesta en marcha de mecanismos de

apoyo económico y financiero, asistencia técnica, formación e información u otros encaminados a aumentar la eficiencia energética en los diferentes sectores, necesarias para la consecución de los objetivos establecidos en la Directiva de Eficiencia Energética.

Promover la seguridad de las infraestructuras energéticas

Respecto a la seguridad lógica, en 2019, de los 804 incidentes registrados en operadores estratégicos, 143 (17,79% del total) fueron gestionados dentro del Sector Energético y Nuclear, colocando a este sector en el tercer puesto de los más atacados en España, después de los sectores financieros y del transporte.

En 2019 el 17,79% de los 804 incidentes registrados en operadores estratégicos fueron en el Sector Energético y Nuclear

Se potenció y reforzó la colaboración público-privada, con los distintos operadores energéticos, coordinada desde del Centro Nacional de Protección de Infraestructuras a través de la Oficina de Coordinación Cibernética, en materia de comunicación de ciberincidentes.

Se aprobaron las revisiones de cinco Planes de Seguridad del Operador, comprobando su ajuste a la situación actual de las amenazas y riesgos a los cuales se encuentran sometidas las infraestructuras críticas del sector de la energía y de la industria nuclear, actualizando la información contenida en estos planes. Se evaluaron y aprobaron, también, 122 Planes de Apoyo Operativo del Sector de la Energía, realizados por las Fuerzas y Cuerpos del Estado, dotando al Sistema PIC del apoyo inmediato de estos Cuerpos en caso de incidentes, encontrándose otros cinco pendientes de aprobación.

A lo largo de 2019 se continuó con la implantación de las Unidades de Respuesta de la Guardia Civil en el interior de las Centrales Nucleares. En concreto, en 2019 se implantó la Unidad de Respuesta en la Central Nuclear de Ascó y el proceso para finalizar el despliegue en las centrales nucleares de Vandellós, Cofrentes y Almaraz, de tal forma que las cinco centrales nucleares activas en España contarán con su respectiva Unidad de Respuesta.

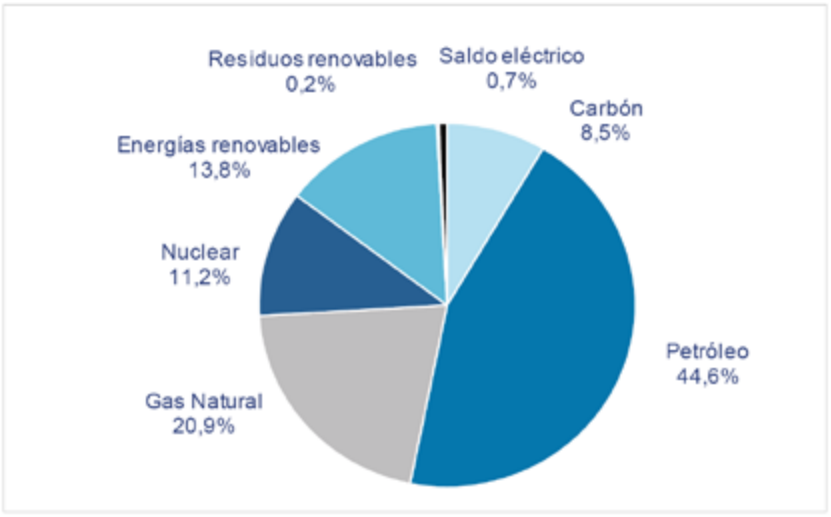
En el marco del convenio de colaboración firmado el 25 de julio de 2018 entre el Ministerio del Interior y el Consejo de Seguridad Nuclear, sobre la creación de una red de estaciones automáticas de vigilancia radiológica ambiental en instalaciones y acuartelamientos de la Guardia Civil por todo el territorio nacional, a lo largo de 2019, técnicos del Consejo de Seguridad Nuclear realizaron visitas a los acuartelamientos seleccionados para acoger dichas estaciones con el objeto de preparar la instalación de las mismas en el año 2020.

Dentro del Plan Operacional firmado en 2018 entre la OIEA y la Guardia Civil, por el que este cuerpo participa en la formación y el apoyo sobre seguridad física nuclear a diversos organismos e instituciones de países de habla hispana, en noviembre de 2019 un componente de este cuerpo participó en el programa INSSP de asesoramiento al diseño de un plan integral de seguridad nuclear en Paraguay.

Con la firma del Acuerdo de 7 de marzo de 2019, el CADEX-NRBQ de la Guardia Civil se constituyó en un referente internacional para impartir formación en seguridad física nuclear a fuerzas policiales, siendo además la primera fuerza policial a nivel mundial en tener un Centro Colaborador con la OIEA.

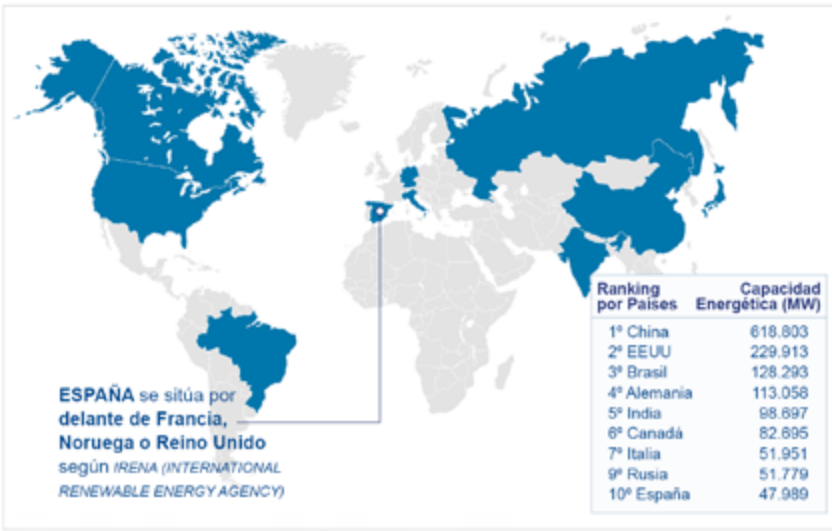
Fuente: Ministerio para la Transición Ecológica

Figura 11-6
Principales políticas y medidas del PNIEC



Fuente: Ministerio para la Transición Ecológica

Figura 11-7
Distribución del consumo energía primaria 2019



Fuente: España Global con datos procedentes de IRENA

Figura 11-8
España, décima potencia mundial en capacidad energética renovable

ORDENACIÓN DE FLUJOS MIGRATORIOS

OBJETIVO:

Prevenir, controlar y ordenar los flujos migratorios irregulares en las fronteras, así como garantizar una adecuada acogida e integración de los inmigrantes y solicitantes o beneficiarios de protección internacional.

Tendencias

Durante los últimos años el flujo de inmigración irregular hacia Europa ha variado entre las rutas del Mediterráneo occidental, central y del este. Así, mientras que en el año 2013 se registró el menor número de llegadas irregulares a España, en 2015 se produjo la llegada de 1,8 millones de inmigrantes irregulares a la UE. En el año 2018 se registró el mayor número de llegadas irregulares a España, desde que se tienen registros en 1999, situación que requirió la implementación de nuevas medidas por parte de las administraciones públicas. (Figura 12-1)

Las llegadas irregulares a España en 2019 disminuyeron en un 48,4% respecto al año anterior

El resultado se ve reflejado en la disminución del 48,4% de los llegados a España en 2019, respecto al año anterior. La reducción de las llegadas por vía marítima alcanzó el 53,4%. En sentido contrario, se han duplicado las llegadas de inmigrantes, mayoritariamente de origen subsahariano, a las islas Canarias en 2019. Se ha registrado un ligero aumento de las llegadas por vía marítima en el caso de Ceuta y por vía terrestre en Melilla. No obstante, en términos absolutos se ha producido un ligero descenso de entradas irregulares en las Ciudades Autónomas respecto al año 2018. (Figura 12-2 y 12-3)

La disminución de llegadas irregulares a España se ha logrado principalmente por el refuerzo de la coordinación a nivel interno y la potenciación del control fronterizo, así como por la utilización de la metodología de análisis de riesgos establecida, robusteciendo los sistemas de alerta temprana, y las capacidades de gestión, acogida y retorno de inmigrantes irregulares. Todo ello en estrecha colaboración con terceros países de origen y tránsito de los flujos migratorios.

La política migratoria seguida por España en los últimos años ha ayudado en gran medida a la configuración de la política europea. Una vez más, la prevención en origen, mediante la cooperación con los países

de origen y tránsito de la inmigración irregular, y una política efectiva de retornos, han demostrado su eficacia en el control y reducción de los flujos migratorios hacia la UE. En 2019, las llegadas a la UE se han reducido en torno a un 5%, siendo la ruta del Mediterráneo occidental la segunda en volumen de entradas a la UE, por detrás de la del Mediterráneo oriental. (Figura 12-4)

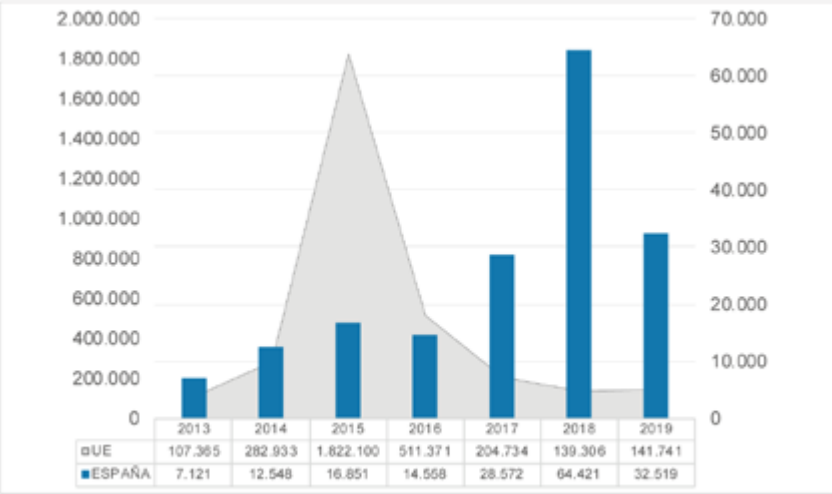
En este marco de trabajo y cooperación, hay que destacar como esencial la activa colaboración de Marruecos en la lucha contra las redes de inmigración irregular. No obstante, el refuerzo del control de fronteras por parte del país vecino está provocando un fuerte aumento de la presión migratoria en este país, siendo básicas las futuras acciones de Marruecos.

Los niveles de migración irregular en el Mediterráneo se mantendrán en los niveles actuales mientras se sostengan los esfuerzos de ciertos países ribereños del norte de África y no se produzcan inestabilidades adicionales en las zonas de origen que provoquen un aumento de desplazados. En 2020, si se mantiene la tendencia actual, se deberá prestar una especial atención a las llegadas a través de Canarias, las cuales podrían aumentar debido a la presión que tanto inmigrantes como traficantes sufren en el norte de Marruecos.

Las solicitudes de protección internacional continúan su tendencia ascendente

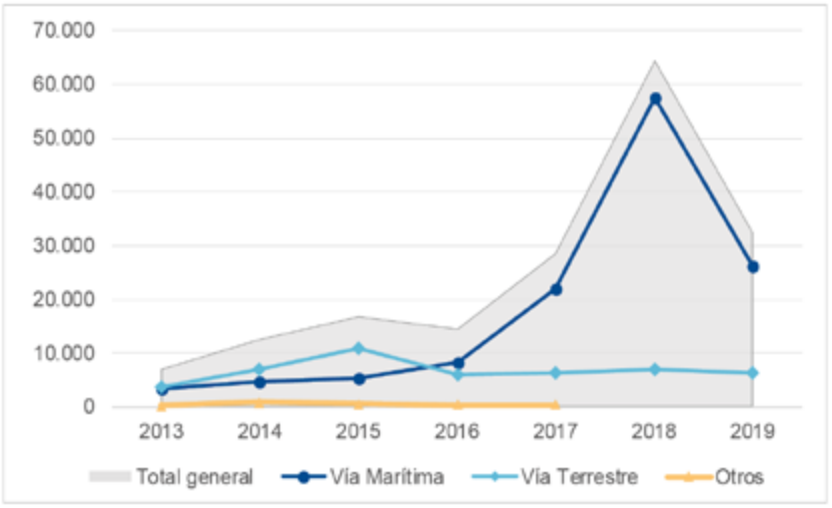
Las solicitudes de protección internacional continúan la tendencia ascendente marcada durante los años anteriores. En 2019, solicitaron protección internacional en España 118.264 personas, un aumento de más del 112% con respecto a las solicitudes presentadas en 2018. Venezuela continúa siendo el principal país de procedencia, con 40.906 solicitantes, frente a los 20.053 venezolanos que solicitaron protección internacional el año anterior. Colombia, Honduras, Nicaragua, El Salvador y Perú son los siguientes países de origen con mayor número de peticiones. (Figura 12-5)

El perfil del solicitante de protección internacional también ha variado. A partir de finales de 2016, la evolución de los conflictos geopolíticos y de la inestabilidad internacional transformaron a España en el primer destino de los flujos de América Latina, haciendo que, a día de hoy, más del 75% de los solicitantes de protección internacional provengan de esa región. (Figura 12-6)



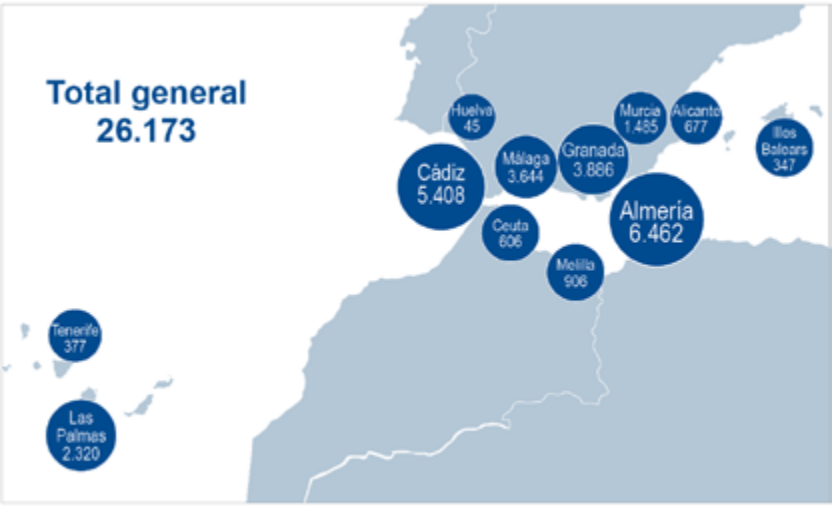
Fuente: Ministerio del Interior

Figura 12-1
Llegadas de inmigrantes irregulares a la Unión Europea y a España 2013-2019



Fuente: Ministerio del Interior

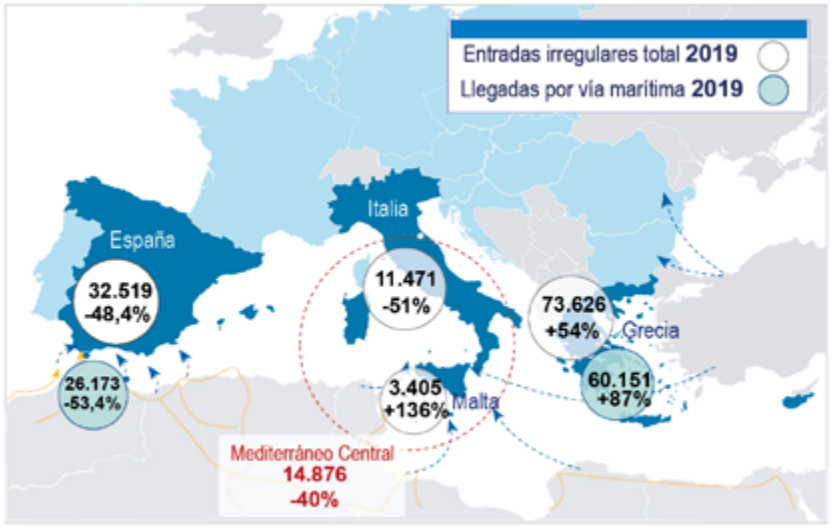
Figura 12-2
Llegadas irregulares de inmigrantes a España por vía de entrada 2013-2019



Fuente: Ministerio del Interior

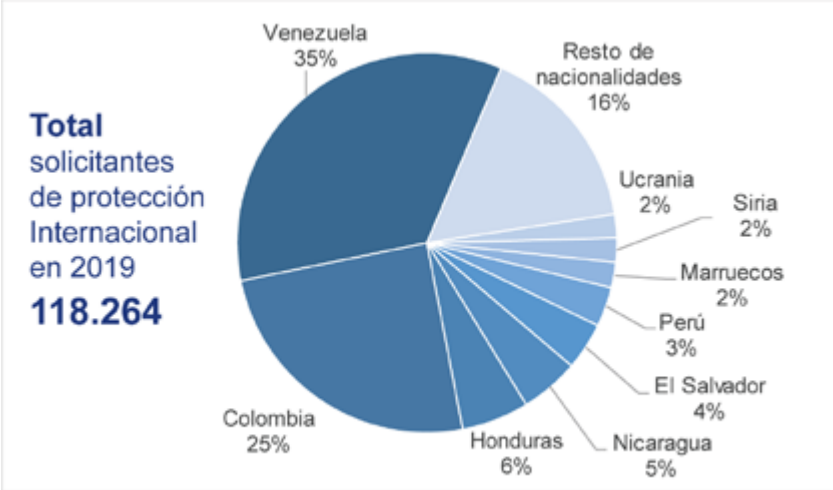
Figura 12-3
Inmigración irregular por vía marítima: provincias de desembarco en 2019

Figura 12-4
Llegadas de inmigrantes irregulares a la Unión Europea en 2019



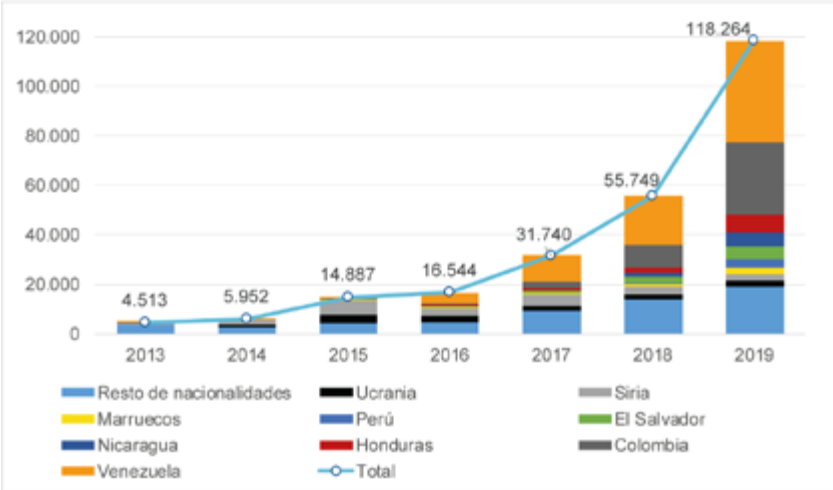
Fuente: Ministerio del Interior y Unión Europea

Figura 12-5
Solicitantes de protección internacional por nacionalidad en 2019



Fuente: Ministerio del Interior

Figura 12-6
Solicitantes de protección internacional por nacionalidad 2013-2019



Fuente: Ministerio del Interior

Retos

La colaboración con los países de origen y tránsito de la inmigración sigue siendo fundamental para reducir los flujos migratorios vía marítima hacia España. Así, se hace necesario mantener y reforzar las relaciones bilaterales con estos terceros Estados, para continuar aplicando los mecanismos de prevención de la inmigración irregular en origen, fortalecer sus capacidades operativas a través de actividades de cooperación, reducir las salidas de inmigrantes irregulares que llegan a costas españolas y favorecer el retorno. En el mismo sentido, resulta necesario liderar una mayor implicación de las instituciones europeas para multilateralizar el esfuerzo con los países de origen y tránsito de los flujos migratorios.

La colaboración integral y transversal con Marruecos es el factor principal que ha permitido reducir los flujos durante 2019, por lo que resulta conveniente mantener este nivel de compromiso para que estas cifras se consoliden y sean sostenibles. Se han de plantear acciones preventivas adicionales en otros países de salida para evitar un aumento del flujo migratorio directo, no solo en el Mediterráneo, sino también en la fachada atlántica, diseñando acciones personalizadas y orientadas a cada uno de los países y objetivos, teniendo en cuenta siempre las dinámicas regionales y las sensibilidades de cada uno.

Persiste la necesidad de potenciar los esfuerzos orientados a la identificación temprana de estos flujos migratorios, de mantener y reforzar el apoyo a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) en esta materia, así como de seguir mejorando las capacidades para la gestión de crisis humanitarias de migrantes y refugiados y de priorizar la vigilancia marítima en las áreas de presencia de estos flujos con los medios terrestres, navales y aéreos desplegados en las operaciones permanentes. En este sentido, resulta necesario garantizar una financiación adecuada para mantener las capacidades necesarias y poder llevar a cabo este tipo de misiones.

En noviembre se aprobó el nuevo Reglamento de la Guardia Europea de Fronteras y Costas, cuyo objeto es dar respuesta a los desafíos migratorios y a los posibles retos y amenazas futuros en las fronteras exteriores, con miras a gestionar esas fronteras eficientemente respetando plenamente los derechos fundamentales, y aumentar la eficiencia de la política de retorno de la Unión. Contribuye a reforzar la coordinación, la cooperación y el intercambio de información en el ámbito europeo y nacional con otras autoridades con responsabilidades en el control fronterizo, en particular la vigilancia de las fronteras exteriores, y el retorno, mejorando el uso de los recursos y la adecuada acogida de los inmigrantes y de otras personas vulnerables.

Especial atención merece el aumento de llegadas de inmigrantes desde América Latina, África y movimientos secundarios desde países del Espacio Schengen hacia España a través de aeropuertos, que hacen necesario tener en cuenta el vector aéreo como método de inmigración irregular, por medio, entre otros, de inmigrantes que exceden el tiempo legal de su visado de turista o suplantaciones de identidad.

En este sentido, la UE tiene como objetivos dos proyectos, a cargo de la Policía Nacional en España, para realizar un mejor control de estos

flujos: ENTRY-EXIT SYSTEM (Sistema de Entradas y Salidas) y ETIAS (Sistema Europeo de Información y Autorización de Viajes).

En el marco de la política migratoria europea, es conveniente incrementar el número de iniciativas comunitarias en el ámbito de la migración legal e integración. El acceso a información precisa, de manera clara, rápida y eficaz, adaptada a los perfiles concretos de cada persona inmigrante es esencial para asegurar una adecuada ordenación de los flujos migratorios que se reciben y que, sin duda, aumentarán en los próximos años.

Las migraciones pueden suponer un elemento clave para afrontar los desequilibrios de población existentes

Debe tenerse muy presente el hecho de que las migraciones pueden suponer un elemento clave para afrontar los desequilibrios de población existentes y que, según todas las previsiones, van a aumentar mucho en poco tiempo. Durante el periodo de crisis económica (desde el año 2009) al menos un millón de españoles, mayoritariamente jóvenes cualificados, se vieron obligados a abandonar España ante la falta de oportunidades.

El nuevo escenario requerirá, sin duda, tender puentes de inmigración legal de acuerdo con las necesidades del mercado laboral, preparando las vías para una inmigración ordenada, segura y regular. Esto supone una adecuada integración de la población inmigrante, algo que debe implicar una apuesta por la instauración de un marco de concertación y cooperación entre las distintas administraciones y la sociedad civil.

El desarrollo de un proyecto piloto de apoyo a la creación de una cooperativa agrícola de mujeres marroquíes y la puesta en marcha de una actuación de evaluación del programa de contratación colectiva en origen para el periodo 2019-2022 en la provincia de Huelva se presentan como proyectos piloto que pueden favorecer dinámicas de cooperación con los principales países de origen.

Se pretende la elaboración de modelos alternativos de integración profesional para los refugiados; el desarrollo de una política para favorecer y agilizar sus solicitudes de reagrupación familiar, en ejecución del Pacto Mundial de Refugiados; el diseño de un programa de becas para refugiados, en colaboración con el Alto Comisionado de Naciones Unidas para los Refugiados (ACNUR) y con la Conferencia de Rectores de Universidades Españolas; y la extensión del programa de patrocinio comunitario.

Por otro lado, los trabajos preparatorios para las reformas en la *Ley de Enjuiciamiento Criminal*, auspiciadas por la elaboración también en fase preliminar de una nueva Ley de protección de colaboradores con la Administración de Justicia (tanto testigos y peritos como investigados), que sustituirá a la actual *Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales*, abordarán el tratamiento de las personas (víctimas/testigos) implicadas en los fenómenos criminógenos unidos a los flujos migratorios para mejorar su asistencia y evitar su victimización secundaria.

La *Estrategia Integral contra el Racismo, la Discriminación Racial, la Xenofobia y otras formas conexas de Intolerancia*, aprobada por el Consejo de Ministros en noviembre de 2011, nació para dar respuesta institucional y de la sociedad civil a la necesidad de combatir la intolerancia en todas

sus formas. Sin embargo, transcurridos ocho años de su aprobación, se hace imprescindible una actualización que tenga en cuenta tanto la revisión del contexto y el diagnóstico de situación, que necesariamente ha variado en estos años, como la incorporación de las recomendaciones realizadas por los principales organismos internacionales y europeos a España. Por ello en 2019 se ha iniciado el proceso de elaboración de la *Estrategia Integral contra el Racismo, la Discriminación Racial, la Xenofobia y otras formas conexas de Intolerancia 2020-2025*, que se prevé culmine a lo largo de 2020.

En 2019 se ha iniciado el proceso de elaboración de la Estrategia Integral contra el Racismo, la Discriminación Racial, la Xenofobia y otras formas conexas de Intolerancia 2020-2025

La Estrategia, que ejemplifica el compromiso concreto de una voluntad política transformadora de una problemática que afecta a la sociedad española, prevé objetivos y medidas concretas que faciliten el desarrollo de políticas públicas para los próximos cinco años, y que den soporte a la administración y a la sociedad civil que trabaja contra el racismo, la discriminación racial, la xenofobia y otras formas conexas de intolerancia. Un elemento clave de esta Estrategia es que, pese a prestar especial atención a determinada población en situación de especial vulnerabilidad, se dirige a la población en general.

Realizaciones

El Comité Especializado de Inmigración ha impulsado la colaboración entre las Administraciones públicas

En el seno del Sistema de Seguridad Nacional, desde el Comité Especializado de Inmigración se ha impulsado la colaboración entre las Administraciones públicas con responsabilidad en materia migratoria, así como la implicación al máximo nivel de la sociedad civil y el tercer sector. En este sentido, se ha avanzado en el desarrollo de planes estratégicos destinados a la prevención de inmigración irregular en España. Además, se celebró la primera jornada de reflexión y análisis sobre el fenómeno migratorio en España desde la perspectiva de la Seguridad Nacional, en la que reconocidos expertos del mundo académico y de los medios de comunicación debatieron y expusieron propuestas para continuar avanzando en la política migratoria de España.

Fomentar la colaboración entre las Administraciones públicas, organizaciones no gubernamentales y sector privado

En esta línea de cooperación de toda la Administración española, se ha potenciado la colaboración entre los organismos involucrados en el ámbito migratorio, bien sea en el plano preventivo o de seguridad, tanto a nivel nacional como internacional. Prueba de ello son las medidas adicionales aprobadas en el mes de febrero para reforzar las capacidades operativas y garantizar la adaptación permanente de la Autoridad de Coordinación de la Inmigración en el Estrecho al que se ha dotado de un Centro de Coordinación permanente residenciado en Málaga. Además, su área de responsabilidad se ha ampliado en 2019 con el resto de la fachada mediterránea, incluyendo las Islas Baleares, y se han aprobado planes y acciones operativas destinadas a reforzar la coordinación en el traslado de inmigrantes rescatados en el mar y para hacer frente a llegadas extraordinarias de inmigración irregular.

En el ámbito del asilo, el incremento de solicitudes de protección internacional ha obligado a reforzar el sistema nacional de asilo, que ha permitido multiplicar casi por cinco el número de expedientes elevados a la Comisión Interministerial de Asilo y Refugio durante 2019 con respecto a los que se resolvieron en 2018.

Vigilar y controlar los accesos a las fronteras exteriores españolas

La vigilancia y control de las fronteras exteriores ha sido en 2019 elemento prioritario para reforzar el control de la inmigración irregular. En este sentido, se aprobó en el mes de enero un plan de medidas para el refuerzo y modernización del sistema de protección fronteriza terrestre en las Ciudades Autónomas de Ceuta y Melilla. Este plan supone la sustitución de las concertinas y la mejora de los sistemas de circuito cerrado de televisión en ambas fronteras. Está previsto que en Ceuta se implemente un nuevo sistema de circuito cerrado de televisión, mientras que en Melilla se ampliará el mismo y se mejorará la red de fibra óptica. En ambas Ciudades Autónomas se va a proceder igualmente a la modernización y refuerzo de las infraestructuras de seguridad de la frontera.

La aprobación de los Reglamentos de Interoperabilidad de los Sistemas de Información de la UE en el ámbito de justicia e interior, en cuyo

desarrollo España ha participado activamente, repercutirá en la mejora de las inspecciones en frontera de los sistemas vinculados, tanto en una gestión eficaz de la seguridad, las fronteras y la migración como en la tramitación de visados y de solicitudes de asilo en el espacio Schengen, contribuyendo así a la seguridad interior de la Unión.

En el marco de los esfuerzos de la Administración española, orientados a la reducción de los flujos migratorios procedentes de África, la actividad de Inteligencia ha estado centrada en la denominada ruta del Mediterráneo occidental.

Las actividades de vigilancia de las áreas de responsabilidad han focalizado sus esfuerzos en la coordinación de los medios que colaboran en el control y la monitorización de los flujos migratorios, principalmente en el mar de Alborán, aguas del archipiélago canario, así como a lo largo de la frontera de Ceuta y Melilla. En este mismo sentido, se ha participado en la Operación Conjunta *ÍNDALO*, en aguas de Cádiz, Málaga, Granada, Almería y Murcia, coordinada por la Agencia Europea de la Guardia de Fronteras y Costas (Frontex) y liderada por España. En el Mediterráneo central se ha participado en la operación de la UE *Eunavformed Sophia* de lucha contra las redes de tráfico ilegal de personas.

Se ha ampliado el rol del Centro Europeo de Tráfico de Inmigrantes (EMSC en sus siglas en inglés correspondientes a la denominación *European Migrant Smugling Centre*) de Europol. Es por ello que el establecimiento de la Cámara de Información (*Information Clearing House*) pretende recopilar, analizar y diseminar inteligencia y evidencias relativas a este tipo de delitos.

Por otro lado, tras la aprobación en el mes de marzo de la Estrategia operativa y técnica de Frontex, cada Estado miembro ha desarrollado su *Estrategia Nacional de Gestión de Integrada de Fronteras*. En este sentido, se ha finalizado la redacción de la Estrategia, quedando pendiente su desarrollo en los posteriores planes de acción.

En el mes de noviembre se adoptó el nuevo Reglamento de la UE sobre la Guardia Europea de Fronteras y Costas, un elemento importante del planteamiento general de la UE para la gestión de la migración y las fronteras. Este Reglamento refuerza el personal y equipamiento técnico de la Agencia y le confiere un mandato más amplio de apoyo a las actividades de los Estados miembros, especialmente en materia de control de las fronteras, retorno y cooperación con terceros países. Igualmente, incorporará el Sistema Europeo de Vigilancia de Fronteras (Eurosur) al marco de la Guardia Europea de Fronteras y Costas.

Se ha continuado con la ampliación de la capacidad de atención de los inmigrantes llegados irregularmente a España. En el mes de enero se aprobó un Plan para la mejora de las instalaciones de los Centros de Internamiento de Extranjeros y la construcción de un nuevo centro en Algeciras (Cádiz) que contará con 500 plazas.

En el mismo sentido, se ha creado un Centro de Atención Temporal de Extranjeros (CATE) en Málaga, se ha remodelado el del Puerto de Motril (Granada) y se ha ampliado el de Almería. Las capacidades de los Centros de Estancia Temporal de Inmigrantes (CETI) de las Ciudades

Autónomas se han reforzado temporalmente para asegurar el adecuado alojamiento de los inmigrantes.

Otro de los métodos por los que apuesta la UE es el retorno a sus países de origen de ciudadanos extranjeros en situación irregular en España, algunos de ellos cualificados (con antecedentes policiales). La cooperación con los países de origen resulta fundamental, principalmente a través de la red de consejeros, agregados de interior y oficiales de enlace. En la actualidad, la tendencia es la apertura de nuevas vías de diálogo, especialmente con países africanos de los que provienen mayoritariamente los flujos migratorios, para propiciar que las autoridades Consulares de dichos Estados reconozcan y documenten a sus nacionales como requisito previo necesario a la repatriación. La idea es progresar hacia un sistema de gestión conjunta y sostenible sobre la base del pleno respeto de los derechos humanos.

Lucha contra la discriminación y promoción de la integración social

En el ámbito de la protección internacional, cabe destacar la participación en diciembre de 2019 en el I Foro Global sobre los Refugiados, mecanismo de seguimiento del Pacto Global sobre los Refugiados aprobado por la Asamblea General en diciembre del 2018, en el que se presentaron los compromisos adoptados por España. Cabe señalar, entre otros, el refuerzo e impulso del sistema de protección internacional y el favorecimiento en los países de origen de condiciones que propicien un retorno en condiciones de seguridad y dignidad.

En cuanto a la acogida de beneficiarios de protección internacional, se ha desarrollado el primer programa piloto sobre patrocinio comunitario, con la participación del Ministerio de Trabajo, Migraciones y Seguridad Social, el Ministerio del Interior, el Gobierno del País Vasco y ACNUR. Dado su éxito, se pretende desarrollar nuevos programas piloto de patrocinio comunitario en otras regiones españolas.

Promover una política migratoria y de asilo común en la UE

Se ha trabajado de manera continua con las instituciones europeas y con los Estados miembros para abordar el fenómeno migratorio, animando el favorecimiento desde la UE de políticas dirigidas al desarrollo de una cooperación de carácter estratégico basada en un equilibrio entre los principios de responsabilidad y solidaridad, donde se debe abandonar este enfoque dual y sustituirlo por el de responsabilidad compartida, que se manifiesta por ejemplo en el tratamiento de las personas objeto de salvamento marítimo, cuya entrada en el territorio de la Unión no obedece a un fallo en el control de fronteras, sino al cumplimiento de las obligaciones establecidas en el derecho internacional.

España sigue defendiendo la importancia de evitar las entradas irregulares como medida preventiva frente a los problemas derivados de los movimientos secundarios entre los Estados miembros. Este empeño está dando sus frutos. En concreto, se ha logrado el reconocimiento real de Marruecos como socio estratégico de la UE en la lucha contra la inmigración irregular. Prueba de ello es un paquete de ayuda de 194 millones de euros que la UE ha destinado desde 2018 a Marruecos para la ges-

tión de sus fronteras. El nuevo Reglamento sobre la Guardia Europea de Fronteras y Costas también concede un peso creciente a la cooperación con terceros países, tanto en control fronterizo como en retorno.

Mientras que la conformación de una política de asilo común en la UE sigue siendo objeto de negociación, España apuesta rotundamente por el reasentamiento, incrementando progresivamente la dotación de sus Programas Nacionales de Reasentamiento con el objetivo de obtener una mayor optimización en la ejecución y desarrollo.

Cooperar con los países de origen y tránsito migratorio

Se ha puesto en marcha una línea de actuación para fomentar los intereses de España, incidiendo en aquellos que son comunes con otros Estados miembros de la UE y así fortalecer la presencia nacional en focos migratorios de interés. La cooperación bilateral con los países de origen y tránsito para la gestión de flujos migratorios constituye un vector fundamental de la política internacional española. Dentro de un enfoque estratégico y preventivo, se están intentando reforzar aún más las relaciones en el ámbito migratorio con varios países de origen y tránsito en la ruta del Mediterráneo occidental.

La cooperación bilateral con los países de origen y tránsito constituye un vector fundamental de la política española

El mayor protagonismo que adquirió Marruecos durante el segundo semestre de 2018 ha obligado a realizar un especial esfuerzo durante 2019 para conseguir la colaboración de este país en el control de los flujos migratorios irregulares que atraviesan y salen de su territorio. Estos esfuerzos, realizados en su conjunto por toda la Administración, han tenido como resultado un descenso visible en el número de llegadas a las costas españolas; también han evidenciado la capacidad de Marruecos para gestionar la migración irregular.

Se ha seguido trabajando intensamente con otros países vecinos, principalmente con Argelia y países del África occidental y subsahariana, lanzando nuevas líneas financieras de colaboración con diversos países africanos e intensificando las ya existentes con otros, enfocadas a favorecer la realización de actuaciones de prevención de la inmigración irregular en origen, el control fronterizo, la lucha contra las redes de inmigración irregular y trata de seres humanos y el retorno.

Igualmente, se ha colaborado en actuaciones destinadas a aliviar la presión migratoria en países de tránsito de los flujos migratorios. En este sentido, en 2019 se contribuyó con un importe de 300.000 euros al Programa de Retorno Voluntario Asistido con Reintegración de la Organización Internacional para las Migraciones en Marruecos, ayudando a retornar a sus países de origen a 474 inmigrantes.

En cuanto al establecimiento de canales legales de inmigración, se puso en marcha el proyecto *Young Generations as Change Agents* con el Reino de Marruecos, enmarcado en la convocatoria de proyectos piloto de migración legal lanzada por la Comisión Europea. El objetivo del proyecto, con una duración prevista de 20 meses, es implementar un plan de movilidad a corto plazo entre España y Marruecos con fines de estudio. Además, en este mismo ámbito, se ha desarrollado el Proyecto piloto de visados para búsqueda de empleo en España (VISAR), para la selección de profesionales cualificados, hijos y nietos de españoles de origen, procedentes de Argentina.

PROTECCIÓN ANTE EMERGENCIAS Y CATÁSTROFES

OBJETIVO:

Consolidar el Sistema Nacional de Protección Civil como instrumento integrador de todas las capacidades de España para gestionar la respuesta ante emergencias y catástrofes y asegurar su integración bajo el Sistema de Seguridad Nacional.

Tendencias

El periodo 2013-2019 se ha caracterizado por una gran variabilidad meteorológica y creciente desestacionalidad, que se ha materializado en periodos de fuerte sequía meteorológica e hidrológica (años 2017 y 2019), acompañadas de temperaturas extremas en zonas poco habituales. En 2019 hubo un aumento del número de fenómenos tormentosos durante todo el verano y un otoño con eventos de lluvias muy intensas y de corta duración que generaron desbordamientos de pequeños cauces (ramblas, torrentes y rieras) y daños puntuales en zonas con déficit de drenaje. Nuevos episodios asociados a las Depresión Aislada en Niveles Altos (DANA) produjeron pérdidas humanas y cuantiosos daños especialmente en el litoral mediterráneo.

En 2019 las inundaciones fueron el fenómeno natural que más daños causó en España

Las inundaciones se consolidaron como el fenómeno natural que más daños causó en España, con 24 fallecidos en el año 2018, el número más elevado del periodo considerado, así como numerosas pérdidas económicas. Además, se observó que en algunas regiones se repitieron con una frecuencia que, a una escala temporal de lustro, pudiera parecer mayor a las registradas en periodos anteriores. Es el caso de las inundaciones en el eje del Ebro, o del levante y en las cuencas mediterráneas andaluzas, donde se registraron episodios de graves inundaciones separadas apenas por dos años.

Aunque la incertidumbre es importante, son numerosos los trabajos y estudios científicos que apuntan cambios en los patrones de inundación como consecuencia de la influencia del cambio climático. Por lo anterior, parte esencial de los Planes de gestión del riesgo de inundación aprobados estuvieron dirigidos a mejorar el conocimiento del fenómeno de las inundaciones, a incrementar la percepción del riesgo

y proporcionar herramientas y recomendaciones para la reducción de la vulnerabilidad y la adaptación de los receptores, incluyendo la ordenación de los usos en las zonas inundables y el papel de las llanuras de inundación.

En contraste, una nueva sequía afectó a España durante 2019, después de que en febrero de 2018 se diese por finalizada la situación de sequía que había afectado a la mayor parte de las regiones desde 2017 y que, a su vez, sucedía a otro periodo seco de seis meses durante 2016.

Por otra parte, los incendios forestales continuaron con su tendencia decreciente en cuanto a número y superficie quemada, a pesar de que la variabilidad meteorológica mencionada, unida al paso de la depresión extra tropical Ophelia, provocara que ardieran cerca de 60.000 hectáreas en Galicia a mediados de octubre de 2017. Cabe mencionar la tendencia a producirse incendios en épocas no habituales, especialmente en el norte de España, con una superficie forestal ardida y número de incendios registrados durante los meses del invierno de 2018 que alcanzó un 30% de la superficie ardida durante todo el año. (Figura 13-1 y 13-2)

En cuanto a los efectos de la actividad sísmica y volcánica, España no es una zona especialmente expuesta a catástrofes producidas por terremotos, y se ha mantenido en sus niveles habituales, si bien se produjeron en el periodo considerado series o enjambres sísmicos de baja a moderada magnitud prolongados a lo largo de meses. Destacan los enjambres sísmicos de origen volcánico, caso de la isla de El Hierro en el periodo 2012-2015, La Palma en 2017 y Tenerife en 2018 y 2019. Así como los de origen tectónico en la provincia de Jaén, en Torreperogil en 2013 y Jódar y Peal de Becerro en 2016. Estos últimos volvieron a reproducirse en 2018.

El aumento del nivel del mar hace prever un incremento en los riesgos asociados a los impactos de erosión e inundación en el litoral

Por otro lado, la tendencia observada de aumento del nivel del mar, hacía prever un incremento en los riesgos asociados a los impactos de erosión e inundación en el litoral, así como en la ocurrencia de eventos extremos. Estas dinámicas y la evidencia científica indicaban que existe propensión a que se produzca un aumento en la frecuencia e intensidad de fenómenos extremos.

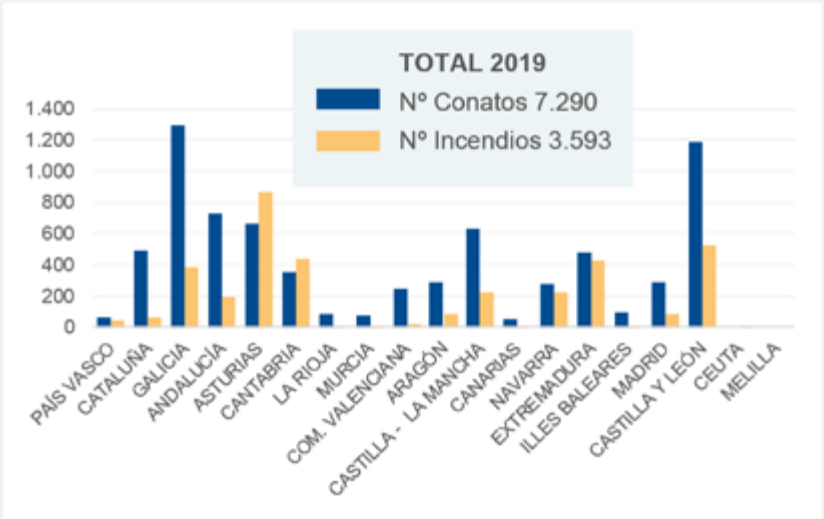
Con respecto a los riesgos tecnológicos, se mantuvieron los niveles habituales, sin ningún episodio digno de reseñar en los ámbitos nuclear, radiológico, químico, biológico y de transporte de mercancías peligrosas.

En cuanto al transporte, no ocurrieron a lo largo del año incidencias especialmente remarcables en el ámbito de emergencias y catástrofes, continuándose con la inversión necesaria para el mantenimiento y mejora de las infraestructuras, para el incremento de la seguridad operacional y en general para todo lo que suponga eliminar riesgos en la prestación de los servicios de transporte. También se mantuvo la aplicación de medidas de prevención, la realización de inspecciones o la elaboración de protocolos de actuación, tanto a nivel nacional como internacional.

El Sistema Español de Seguros Agrarios, con cuarenta años de aplicación, se ha consolidado como un instrumento eficaz para la gestión de

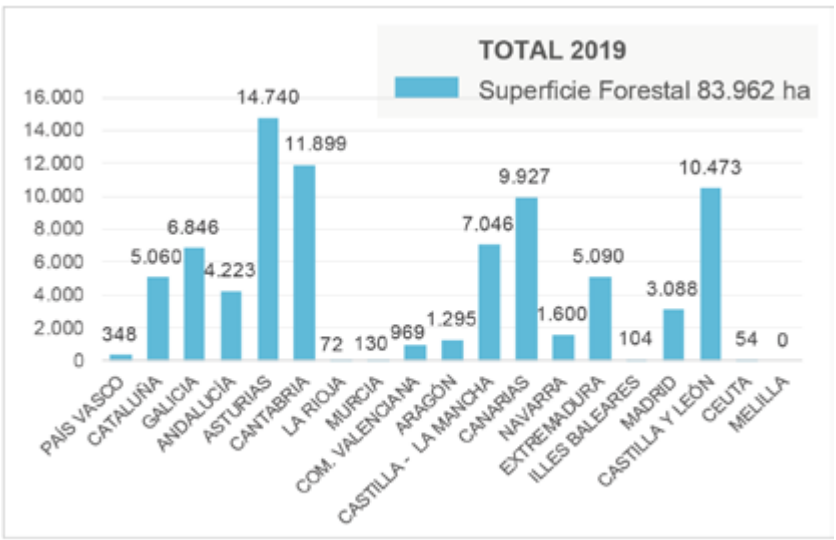
los riesgos de la naturaleza sobre la actividad agraria, contribuyendo al mantenimiento de la renta y de la producción final agraria.

En el ámbito regional, el fortalecimiento y empleo de las capacidades del Mecanismo de Protección Civil de la Unión Europea tanto dentro del entorno europeo como en el exterior, será una clara tendencia de futuro. El incremento en este tipo de misiones con personal y medios del Ministerio de Agricultura, Pesca y Alimentación, así como de la Unidad Militar de Emergencias (UME), fue una constante en el año 2019 (incendios forestales en Grecia, Amazonas Boliviano y Guatemala, e inundaciones en Mozambique).



Fuente: Ministerio de Agricultura, Pesca y Alimentación

Figura 13-1
Número de incendios forestales en España 2008-2019



Fuente: Ministerio de Agricultura, Pesca y Alimentación

Figura 13-2
Superficie Forestal quemada en 2019

Retos

Las emergencias y catástrofes por riesgos derivados del litoral y el medio marino, inundaciones o incendios constituyen retos de primer nivel

Las emergencias y catástrofes por riesgos derivados del litoral y el medio marino, inundaciones o incendios constituyen retos de primer nivel. Retos que se van a ver magnificados por el impacto del cambio climático, al que España es especialmente vulnerable, con efectos directos en la economía, productividad y sociedad. En consecuencia, es un desafío proteger y conservar el litoral y el medio marino para prevenir y responder en casos de eventos extremos. Con el objetivo de responder en casos de catástrofes o accidentes, continúa la colaboración entre los Ministerios para la Transición Ecológica, Fomento e Interior, en la aplicación del Sistema Nacional de Respuesta, especialmente en lo referente al Subsistema Costero, a través *del Plan Estatal de Protección de la Ribera del Mar contra la Contaminación (Plan Ribera)*. (Figura 13-3)

En el marco de la planificación de la gestión del riesgo de inundación, los principales retos a abordar incluyen, entre otros, el incremento de la percepción del riesgo de inundación entre la población y los sectores económicos afectados y la mejora en las estrategias de autoprotección, así como la mejora de los protocolos de comunicación y de los sistemas de información hidrológica y su coordinación con la información meteorológica, con el objetivo de generar previsiones y alertas a corto y medio plazo de crecidas e inundaciones y de sus efectos, de forma que las autoridades de Protección Civil, ciudadanos y agentes económicos puedan tener el tiempo suficiente para tomar medidas de autoprotección, aprovechando los beneficios de las redes sociales en la gestión de emergencias.

Igualmente importante es la realización de informes de evaluación de lecciones aprendidas que contemplen todos los aspectos e incluyan a todos los actores implicados; la mejora de la consideración del riesgo de inundación en la ordenación del territorio y la planificación urbana y el incremento de la colaboración con el sector científico en todo lo concerniente a la aplicación de nuevas tecnologías para la optimización de la gestión del riesgo de inundación.

Un sector relevante en este ámbito es el constituido por los medios de transporte, en el que se han de adoptar medidas que permitan aumentar la seguridad en ellos mediante, por ejemplo, del trabajo realizado por parte de organismos especializados como son las Comisiones de Investigación de Accidentes. También constituye un reto profundizar en el sistema de atención a víctimas y familiares de accidentes catastróficos en el transporte a través de la Oficina de Asistencia a Víctimas de Accidentes Aéreos y Familiares (OAV) del Ministerio de Fomento, o en los de más reciente implantación como en el caso de los accidentes ferroviarios, tendiendo a implantar un sistema multimodal.

La Comisión Técnica Nacional para Sucesos con Víctimas Múltiples, órgano colegiado dependiente del Ministerio de Justicia y adscrito a la Dirección General de Relaciones con la Administración de Justicia, previó impulsar la planificación del mecanismo de movilización, formación y coordinación de los grupos de expertos forenses creados, con el fin de mejorar las capacidades de reacción, respuesta e intervención ante sucesos con víctimas múltiples cuya atención supera los medios disponibles de una comunidad e incluso su colaboración a nivel internacional.

Para complementar la respuesta del Estado a las emergencias, es necesario mantener y fortalecer las relaciones institucionales con las autoridades competentes en su gestión, dinámica que facilita la coordinación en la respuesta y la colaboración entre instituciones, mejorando y actualizando los protocolos de actuación para mantener el nivel de excelencia en la respuesta a las emergencias que las situaciones futuras demanden. Por ejemplo, en la restauración hidrológico-forestal de terrenos afectados por grandes incendios forestales y en la reparación de otras infraestructuras rurales afectadas por desastres naturales según el *Real Decreto Ley 11/2019, de 20 de septiembre, por el que se adoptan medidas urgentes para paliar los daños causados por temporales y otras situaciones catastróficas* resulta fundamental la colaboración con las Comunidades Autónomas.

Uno de los objetivos prioritarios es continuar con el desarrollo de *la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil* en todas las actuaciones del sistema y en el aspecto normativo.

Las medidas para actuar ante estos desafíos pueden dividirse según su carácter preventivo o de respuesta. Entre las primeras se incluyen el desarrollo del proyecto de la Red de Alerta Nacional (RAN), aumentar la dotación del fondo de prevención con la finalidad de efectuar análisis de riesgos y elaborar los correspondientes mapas, desarrollar programas de sensibilización de la población y programas de educación para la prevención en centros escolares, continuar impulsando la elaboración/actualización de Planes Territoriales y Especiales en el ámbito estatal y en las Comunidades Autónomas, así como desarrollar el *Plan Estatal General.*

Por su parte, en las actuaciones para la respuesta inmediata cabe mencionar como retos potenciar las capacidades del Centro Nacional de Seguimiento y Coordinación de Emergencias (CENEM) de Protección Civil, realizar el proyecto de desarrollo de la Red Nacional de Información (RENAIN) y profundizar en la coordinación y cooperación entre todos los agentes del sistema implicados en la respuesta ante emergencias, ya sean operadores, administraciones, servicios de emergencias u otros actores, con un enfoque integrador.

La autoprotección, la cultura preventiva, la formación y la comunicación son elementos esenciales para la protección ante emergencias y catástrofes.

En relación a la autoprotección, se busca garantizar la seguridad de las personas, las instalaciones y la actividad de la empresa u organismo, mediante la gestión y el mantenimiento de un sistema de autoprotección definiendo los requerimientos de las instalaciones de protección, comprobando la disponibilidad de dichos medios, realizando tareas de prevención de riesgos y asegurando unas actuaciones coordinadas en caso de emergencia, a través de la alarma, evacuación y socorro, fomentando y desarrollando la formación en esta materia. En esta línea, también se considera la mejora de la autoprotección de los escolares mediante la realización de actividades formativas y la difusión de contenidos.

De modo paralelo, es un desafío continuo la implantación de programas de información preventiva a la población para mejorar la percepción

social del riesgo, la capacidad de respuesta ante emergencias y la resiliencia individual y social. Esta medida incluye la elaboración, el suministro y la difusión de las informaciones meteorológicas y predicciones de interés general para los ciudadanos en todo el ámbito nacional, y la emisión de avisos y predicciones de fenómenos meteorológicos que puedan afectar a la seguridad de las personas y a los bienes materiales.

Por otra parte, la formación de responsables, gestores e intervinientes del Sistema Nacional de Protección Civil, en particular la de la Policía Nacional y la Guardia Civil ha de ser una constante para garantizar una adecuada actuación en este ámbito. También ha de tenerse en cuenta la formación de profesionales para aumentar la resiliencia de los colectivos vulnerables ante emergencias y catástrofes.

Para una adecuada actuación ante las diversas catástrofes y emergencias posibles, ha de mantenerse la constante actualización de las capacidades operativas para dar respuesta a las complejas situaciones actuales y futuras con el fin de conseguir una pronta recuperación ante una situación catastrófica. En este sentido, destaca la necesidad de completar la certificación de las capacidades inscritas dentro de la Capacidad Europea de Respuesta a Emergencias Mecanismo de Protección Civil de la Unión Europea, para que los expertos y las unidades de intervención españolas continúen siendo una referencia en el ámbito de las emergencias, contribuyendo a la Acción Exterior del Estado.

Con el objetivo de impulsar propuestas que mejoren la seguridad se requiere reforzar la inversión en materia de seguridad, crear un nuevo organismo para la investigación técnica de accidentes, así como llevar a cabo mejoras en la I+D+i en el ámbito de la seguridad.

Figura 13-3
Sistema Nacional de Respuesta ante la Contaminación Marina

Fuente: Ministerio para la Transición Ecológica

Realizaciones

Respuesta ante emergencias y catástrofes

Se llevaron a cabo actuaciones ante temporales, contaminación, inundaciones e incendios.

Para responder a los temporales acaecidos en enero y febrero y la DANA de septiembre se promovieron actuaciones de emergencia para paliar los daños provocados en el litoral. Se actuó en 11 provincias (Málaga, Granada, Almería, Murcia, Alicante, Valencia, Castellón, Tarragona, Asturias, Cádiz, Guipúzcoa), por un importe total de 12,2 millones de euros.

En respuesta a los temporales en 2019 se realizaron actuaciones de emergencia por un importe total de €12,2 millones

Se realizaron dos ejercicios de lucha contra la contaminación accidental, en Pontevedra (junio 2019) y Bizkaia (noviembre de 2019), que consistieron en simulacros de actuación ante episodios ocasionales de contaminación marina con el fin de coordinar y gestionar una respuesta rápida y efectiva ante los mismos. En estos ejercicios se movilizaron los medios de los que dispone el Ministerio para la Transición Ecológica en las bases logísticas de Pontevedra y Tarragona.

Se aprobó la revisión de la evaluación preliminar del riesgo de inundación (EPRI). También, conforme a la *Directiva de Inundaciones*, se revisaron los mapas de peligrosidad y riesgo correspondientes a las Áreas de Riesgo Potencial Significativo de Inundación identificadas en la revisión de la EPRI y el 1 de agosto de 2019 se inició el proceso de consulta pública. En el ámbito de las medidas de prevención se publicaron en la página web del Ministerio para la Transición Ecológica las guías para mejorar la adaptación al riesgo de inundación. También en el ámbito de la prevención, y en cumplimiento de los *Planes de Gestión del Riesgo de Inundación*, se elaboró una guía técnica de buenas prácticas para la conservación, mantenimiento y mejora de cauces con el fin de reducir también los daños que producen las inundaciones.

Las Fuerzas Armadas (FAS) participaron en 60 intervenciones en emergencias, en los ámbitos de los incendios forestales, inundaciones, tormentas invernales y colaboraciones con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) en la búsqueda de personas desaparecidas.

Las FAS llevaron a cabo diversas actividades relacionadas con la protección ante emergencias y catástrofes, entre las que cabe citar las misiones humanitarias, las intervenciones en emergencias, las operaciones de asesoramiento o intervención en desastres en otros países a través del Mecanismo de Protección Civil de la Unión Europea o las operaciones medioambientales en curso. (Figura 13-4)

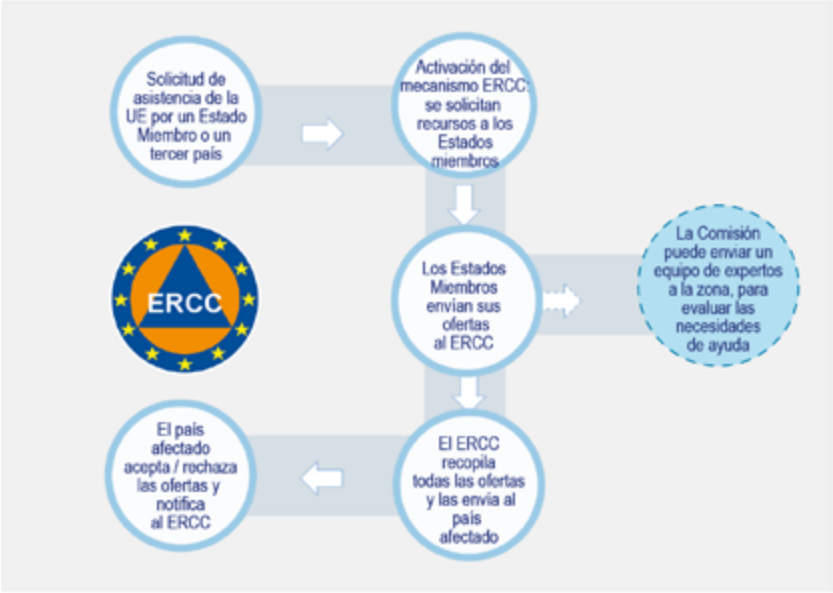
En la campaña de lucha contra incendios forestales, la UME tuvo previsto un dispositivo de 3.000 efectivos para apoyar a las autoridades competentes. En cuanto a las intervenciones con motivo de inundaciones, merecen especial atención las llevadas a cabo en Cantabria 2019(enero de 2019), así como la desarrollada en el Túnel de Barajas 2019 (mayo de 2019), por la singularidad de empleo de medios específicos de gestión de fluidos.

Las realizadas ante los efectos sin precedentes de la DANA en el levante español, centradas en la localidad de Orihuela (Alicante) y en diversas localidades de Murcia (septiembre de 2019), supusieron un esfuerzo continuado de más de 1300 efectivos de las FAS, entre miembros de la UME, los ejércitos y la Armada. En esta intervención se constituyó, por primera vez, el Mando de Emergencias de las Fuerzas Armadas creado por la *Orden DEF 160/2019 de 21 de febrero, por la que se regula la organización y funcionamiento de la Unidad Militar de Emergencias*.

El Ministerio de Cultura y Deporte, dentro de las líneas de trabajo del Plan Nacional de Emergencias y Gestión de Riesgos en el Patrimonio Cultura, ha dado un paso más en la tarea de la protección del patrimonio cultural ante situaciones de desastre con la reciente creación del Grupo de trabajo para la implantación de los Planes de Salvaguarda de Bienes en Instituciones Culturales ante emergencia. Esta iniciativa pretende ayudar a cubrir la carencia generalizada de este tipo de Planes en las instituciones de cualquier índole que custodian, exhiben obras, libros o documentos de interés cultural. Para reforzar el desarrollo de Planes de Salvaguarda en todas las instituciones culturales, se ha incorporado su obligatoriedad en el borrador de la nueva Ley de Patrimonio.

En la Reunión interministerial celebrada en abril sobre los citados Planes de Salvaguarda, se puso de relieve el consenso interministerial para reforzar la colaboración entre las unidades competentes. Además, se acordaron medidas de sensibilización, concienciación y formación a los responsables de la gestión de las emergencias y de las instituciones culturales, se estableció un programa de financiación 2019-2020 para acometer los Planes de Salvaguarda de bienes de las principales instituciones de titularidad pública, estatal y autonómica, y se propuso la creación del Centro de Atención de Emergencias en Materia de Patrimonio Cultural, en colaboración con el Ministerio del Interior, y un Programa de formación y sensibilización en el marco del Plan Nacional de Educación y Patrimonio.

Figura 13-4
Activación del Mecanismo de Protección Civil de la UE



Fuente: Elaboración del DSN

Implantación de la Estrategia del Sistema Nacional de Protección Civil

La *Estrategia Nacional de Protección Civil* fue aprobada por el Consejo de Seguridad Nacional, y constituye un nuevo e importante elemento en el desarrollo estratégico de las políticas de Seguridad Nacional. El documento fue objeto de difusión en diferentes reuniones y jornadas nacionales e internacionales a fin de profundizar en el conocimiento del Sistema Nacional de Protección Civil. (Figura 13-5)

La Estrategia Nacional de Protección Civil fue aprobada por el Consejo de Seguridad Nacional en 2019

Por otra parte, se elaboró el Análisis Nacional de Riesgos en el Ámbito de la Protección Civil como una herramienta eficaz en el conocimiento del riesgo y por tanto en las acciones preventivas.

Figura 13-5
Estructura de las capacidades del Sistema Nacional de Protección Civil

Fuente: Estrategia Nacional de Protección Civil 2019

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

La Comisión permanente del Consejo Nacional de Protección Civil informó el Plan Territorial de la Comunidad de Madrid (actualización), el Plan especial de protección civil ante el riesgo de inundaciones de la Comunidad Autónoma de Extremadura y los Planes especiales de protección civil frente a incendios forestales. Se continuó con el proceso de adaptación de los Planes especiales de ámbito autonómico a la Directriz Básica de incendios aprobada por el *Real Decreto 893/2013, de 15 de noviembre, por el que se aprueba la Directriz básica de planificación de protección civil de emergencia por incendios forestales*. Un total de 10 Comunidades Autónomas cuentan con Plan Especial informado por el Consejo Nacional de Protección Civil (Canarias, Murcia, Galicia, Asturias, Valencia, Castilla La Mancha, La Rioja, Madrid, Aragón y País Vasco). También informó los Planes de riesgo radiológico de la Comunidad de Extremadura, así como otros planes exteriores de la industria química en las Comunidades de País Vasco, Valencia y Aragón, y 10 nuevos Planes de Emergencia de Presas. El número de planes de presa informados ya asciende a 415.

En el ámbito estatal se informaron favorablemente la Directriz Básica de Planificación de Protección Civil ante Emergencias Aeronáuticas de Aviación Civil, y el Plan Estatal de Emergencia por Maremotos. Además, se está elaborando la redacción del Plan General Estatal y la Directriz Básica de Fenómenos Meteorológicos Adversos, tal como se establece en *Ley 17/2015 de 9 de julio, del Sistema Nacional de Protección Civil*.

Fomento de la colaboración público-privada

En materia de gestión de riesgos en el ámbito agrario, la colaboración público-privada ha adquirido una gran relevancia en la gestión y desarrollo de los seguros agrarios, para que los productores sean protagonistas en la protección de sus bienes y medios de producción. Como cada año, se aprobó el Plan de Seguros Agrarios Combinados para dar respuesta a las necesidades de protección de los productores, a la vez que se dota del presupuesto necesario para una más eficaz aplicación.

Por otra parte, a través del Centro Europeo de Investigación Social se están realizando campañas informativas del riesgo, así como vídeos y guías metodológicas para la prevención y conocimiento del riesgo por todas las capas de la sociedad.

Fortalecer la integración de capacidades de todo el Sistema Nacional de Protección Civil

A través de un proyecto europeo se ha estado trabajando en la plataforma de la Red de Alerta Nacional.

En el ámbito nacional, la UME desarrolló un ejercicio con un escenario de riesgo múltiple que implicó la declaración de emergencia de interés nacional (Aragón 2019) con gran participación de todos los organismos, favoreciendo la cohesión del Sistema Nacional de Protección Civil y potenciando la participación de la Administración General del Estado.

Por otra parte, se está trabajando en el Catálogo Nacional de capacidades en el ámbito de Protección Civil y en paralelo fortaleciendo las capacidades nacionales en el Mecanismo de Protección Civil de la Unión Europea.

La OAV del Ministerio de Fomento, continuó potenciando su actividad internacional en la materia, formando parte de la delegación española en la 40ª Asamblea General de la Organización Internacional de Aviación Civil (OACI) en Montreal. La OAV participó también, como ya es habitual, en los simulacros de emergencia programados con aeropuertos y aerolíneas, y con ambos se mantuvieron reuniones de coordinación para perfeccionar los mecanismos de asistencia y coordinar los planes de emergencia.

También se mantuvo la formación del personal implicado en la asistencia a las víctimas. Continuó igualmente el desarrollo de la plataforma *online* Centro de Recursos, de la que forman parte numerosos prestadores de asistencia, tanto públicos como privados, que participan en el sistema implantado por el *Real Decreto 632/2013 de asistencia a las víctimas de accidentes de la aviación civil y sus familiares y por el que se modifica el Real Decreto 389/1998, de 13 de marzo, por el que se regula la investigación de los accidentes e incidentes de aviación civil.* También se dedicaron esfuerzos y recursos al impulso de las funciones encomendadas a la Comisión Técnica Nacional para Sucesos con Víctimas Múltiples, destacando la creación de grupos de expertos forenses.

Se aprobó el *Real Decreto Ley 2/2019, de 25 de enero, por el que se adoptan medidas urgentes para paliar los daños causados por temporales y otras situaciones catastróficas*. No obstante, desde el 1 de abril se sucedieron diversos sucesos catastróficos que dieron lugar a la aprobación del *Real Decreto Ley 11/2019, de 20 de septiembre, por el que se adoptaron medidas urgentes para paliar los daños causados por temporales y otras situaciones catastróficas*.

Se actualizaron y mejoraron los protocolos de gestión y coordinación en vigor, con evidentes resultados en las campañas estacionales, entre las que cabe destacar la Operación Paso del Estrecho (OPE), que en 2019 volvió a superar los 3 millones de personas y los 700.000 vehículos, estableciendo otro record histórico.

Promover la coordinación y cooperación internacional en materia de Protección Civil

En el marco del Protocolo de Cooperación Técnica y Asistencia en materia de Protección Civil con la República Portuguesa (1992), el 2 de julio se celebró en Salamanca la XIV Comisión Mixta con representantes de la Dirección General de Protección Civil y Emergencias y de la Autoridad Nacional de Emergencias y Protección Civil de Portugal. Se trataron los temas de colaboración transfronteriza, con especial incidencia en el apoyo mutuo en la lucha contra incendios forestales.

En el marco del Mecanismo de Protección Civil de la UE España prestó apoyo a Guatemala, Bahamas, Bolivia, Mozambique y Grecia

Respecto a la coordinación de apoyo internacional en emergencias, a través del Mecanismo de Protección Civil de la UE, se prestó apoyo a Guatemala (incendios forestales), Bahamas (vertidos contaminantes) y

Bolivia (incendios forestales) en misiones de asesoramiento; se participó en misiones de asistencia del Mecanismo en Mozambique (inundaciones de marzo) con el envío de un Equipo Médico de Emergencias de la AECID y en Grecia con el envío de un avión Canadair de la reserva de capacidades rescEU. (Figura 13-6)

Por otra parte, se certificó el módulo de Lucha Contra Incendios Forestales (GFFF, *Ground Forest Firefigthing)* y la capacidad de Espeleosocorro (CAVESAR, *Cave Urban Search and Rescue*) en el Mecanismo de Protección Civil de la Unión Europea.

Con base en el Acuerdo Técnico entre el Ministerio de Defensa de Perú, y el Ministerio de Defensa de España, sobre la cooperación en el ámbito militar para la gestión del riesgo en desastres, la UME inició un programa de asesoramiento, que se enmarca como una Operación de Colaboración Militar, para la constitución de una unidad militar del Perú en la gestión del riesgo de desastres.

Continuó la participación de la UME en la Operación Libre Hidalgo, bajo mando operativo del Jefe de Estado Mayor de la Defensa con el cometido de perfeccionar la formación de los Centros de Defensa Civil del Líbano.

Por su parte, el proyecto europeo de hermanamiento con Argelia en el ámbito de la protección civil formó a 1.439 directivos argelinos. En el proyecto, desarrollado en colaboración con Francia, participaron 36 expertos del Sistema Nacional de Protección Civil, liderando cinco actividades y colaborando con expertos franceses en otras dos actividades.

En el ámbito internacional se impulsó la participación de los integrantes del Sistema Nacional en diversos ejercicios de la UE como EUCASCADE 19 y varios ejercicios MODEX de capacidades registradas en el Mecanismo de Protección Civil de la UE. En relación al Ejercicio EUCASCADE Portugal 2019, la Dirección General de Protección Civil y Emergencias participó como socio en este proyecto que lideró la Autoridad Nacional de Emergencias y Protección Civil de Portugal (ANEPC), consistente en la realización de un ejercicio internacional a gran escala, en el que también participaron Alemania, Bélgica, Francia y Croacia. Este simulacro permitió la interacción de los órganos de mando y control de emergencias y de los operativos en la gestión y respuesta a una emergencia compleja, en el ámbito tanto del Sistema Nacional Español como del Mecanismo Europeo de Protección Civil.

En el primer semestre de 2019 se aprobó la constitución del Grupo de Trabajo "Implementación del Sistema de Indicadores para seguimiento del Marco de Sendai", para reducir el riesgo de desastres Reunión del Consejo Nacional de Protección Civil de 22 de enero de 2019.

Fuente: Elaboración del DSN con datos de la Dirección General de Protección Civil y Emergencias

Figura 13-6
Participación española en acciones en el exterior en 2019

Red de Infraestructuras

Por parte del Ministerio de Fomento se elaboró el Informe sobre la seguridad en los transportes y las infraestructuras cuyo objeto es realizar un diagnóstico de los actuales sistemas, procesos y órganos que garantizan la seguridad del transporte y las infraestructuras, además de detectar posibles áreas de mejora.

Por parte de Adif se realizaron 140 simulacros, 86 en Adif y 54 en Adif-AV, en el fomento de una cultura de prevención entre los ciudadanos, que incluye conocimientos y actitudes de autoprotección, reforzando las capacidades de resiliencia ante emergencias súbitas e inesperadas. Renfe participó en un simulacro en el túnel internacional ferroviario del Pertus, otro en materia de climatología adversa con la UME y un accidente Nuclear, Biológico y Químico (NBQ) con el Ejercito. Asimismo, se actualizó el Sistema de Gestión de Autoprotección y el Plan de Asistencia a Víctimas de Accidentes Ferroviarios y sus Familiares.

Aena mejoró las condiciones de operación en caso de contingencia grave en diversos aeropuertos que obligase al abandono inmediato de la Torre de Control, dotándose de un nuevo equipamiento alternativo de contingencia. Además, se realizaron un total de 18 simulacros aeronáuticos. En cuanto a simulacros parciales de activación de sala con ensayo del protocolo de asistencia a víctimas se llevaron a cabo un total de 13 simulacros.

En lo relativo a las normas o regulaciones relacionadas con el transporte de mercancías peligrosas, en 2019 entró en vigor tanto el RID 2019 (convenio internacional para el transporte de mercancías peligrosas por ferrocarril) como el ADR 2019 (convenio internacional para el transporte de mercancías peligrosas por carretera).

La Comisión de Investigación de Accidentes e Incidentes de Aviación Civil (CIAIAC) abrió en 2019 un total de 82 investigaciones de accidentes e incidentes graves de aviación civil, emitiendo un total de 54 recomendaciones de seguridad operacional.

La Comisión de Investigación de Accidentes Ferroviarios (CIAF) decidió investigar técnicamente dos accidentes y realizar cinco exámenes preliminares de otros tantos sucesos. Asimismo, en 2019 se cerró la investigación de ocho sucesos, uno ocurrido en el año 2016 y siete en el año 2017. En el conjunto de todos ellos se emitieron 31 recomendaciones tendentes a la mejora de la seguridad ferroviaria y por tanto de las personas que utilizan este modo de transporte.

La Comisión de Investigación de Accidentes e Incidentes Marítimos (CIAIM) abrió una investigación técnica en 31 sucesos y decidió archivar las actuaciones en 236 casos, al no encontrar lecciones para la mejora de la seguridad marítima. La CIAIM está evaluando los cuatro sucesos restantes para decidir si se realiza una investigación en detalle. Por último, los informes finales de accidentes aprobados durante 2019 contienen un total de 25 recomendaciones de seguridad, dirigidas a personas, empresas y administraciones públicas.

SEGURIDAD FRENTE A PANDEMIAS Y EPIDEMIAS

OBJETIVO:

Adoptar planes de preparación y respuesta ante riesgos sanitarios, tanto genéricos como específicos, bajo el principio de coordinación entre la Administración General de Estado y las Administraciones Autonómicas y con organismos internacionales, como la Organización Mundial de la Salud, la Organización Mundial para la Sanidad Animal o, en el seno de la UE, el Centro Europeo de Control de Enfermedades.

Tendencias

Los cambios globales marcan la creciente movilidad de microorganismos patógenos capaces de generar epidemias y pandemias

Los cambios globales en las últimas décadas, con el incremento y envejecimiento de la población; el volumen creciente de viajes internacionales y la circulación transfronteriza de mercancías; los nuevos sistemas de producción y formas de consumo; los residuos generados y el cambio climático asociado marcan la creciente movilidad de riesgos para la salud pública y, en concreto, de microorganismos patógenos capaces de generar epidemias y pandemias.

Pero en este contexto, también se ha observado una mejora importante del nivel de salud de la población y el aumento de las capacidades de respuesta de los sistemas sanitarios y de salud pública.

La entrada en vigor del Reglamento Sanitario Internacional (2005) en junio de 2007, supuso un aumento de la capacidad de detección de señales de riesgo epidémico o pandémico y de respuesta. A partir del año 2015, se impulsó la implantación de las garantías de seguridad sanitaria previstas en dicho Reglamento a través de iniciativas de seguridad sanitaria global propuestas en 2014 por Estados Unidos.

En la UE, esta actividad se desarrolla desde el año 2000 a través del Sistema de Alerta Precoz y Respuesta de la UE, al que en 2005 se unió el Centro Europeo de Control de Enfermedades (ECDC por sus siglas en inglés correspondientes a la denominación *European Centre for Disease Prevention and Control*).

En España, la formalización de las actividades de preparación y respuesta ante riesgos para la salud pública se inició con la creación en 2004 del Centro de Coordinación de Alertas y Emergencias Sanitarias (CCAES) del Ministerio de Sanidad, Consumo y Bienestar Social y posteriormente, en el año 2013 del Sistema de Alerta Precoz y Respuesta.

Los mecanismos de seguridad sanitaria puestos en marcha son capaces de detectar más riesgos epidémicos y pandémicos y de forma más rápida, y también permiten una reacción precoz reduciendo su posible impacto en la población.

Aun así, persiste la vulnerabilidad de la población ante los riesgos sanitarios actuales pese al importante desarrollo de los sistemas de detección, preparación y respuesta con los que se dispone. En ocasiones, la vulnerabilidad está asociada a los peligros derivados del movimiento transfronterizo de agentes biológicos. Estos peligros pueden, por otra parte, impactar de manera natural o intencionada, debiéndose en este último caso mitigar los riesgos derivados de una eventual amenaza bioterrorista.

La gran circulación de microorganismos patógenos sigue generando importantes riesgos para la población

La gran circulación de microorganismos patógenos sigue generando importantes riesgos para la población. En el ámbito global, la última epidemia de enfermedad por virus del Ébola que se inició en la República Democrática del Congo en 2018 y que permanecía activa en diciembre de 2019, con más de 3.300 casos y más de 2.200 defunciones registradas, se ha convertido ya en la segunda mayor epidemia registrada de esta enfermedad y constituye un reto para la seguridad sanitaria global. (Figura 14-1)

El brote de esta enfermedad está proporcionando nuevos datos sobre la susceptibilidad de pacientes recuperados. Se pensaba que no existían reinfecciones, pero la descripción de un fallecimiento en una superviviente de esta enfermedad obliga también a revisar los procedimientos para el manejo de esta enfermedad, tanto en cuidados hospitalarios como en el uso de la inmunización pasiva en cuanto método de tratamiento.

En 2019 se ha sufrido la mayor epidemia de listeriosis registrada en España, con más de 200 casos confirmados, asociada al consumo de una carne mechada contaminada con *Listeria monocytogenes* producida por una empresa de Andalucía, que además ha generado un gran impacto económico en el sector afectado. (Figura 14-2)

Por otro lado, el desarrollo tecnológico puede permitir el manejo relativamente sencillo, por personas o grupos, de agentes biológicos de forma malintencionada.

Se constata una intensificación en la circulación de los microorganismos causantes de enfermedades transmitidos por vectores, en los que se observan nuevos mecanismos de transmisión con potencial epidémico. La confirmación de la transmisión sexual del virus Dengue obliga a revisar y reforzar los procedimientos tanto de control como de vigilancia.

Se mantiene la tendencia al aumento de la circulación de cepas bacterianas con resistencia extensa a antimicrobianos, algo que repercute en

la actividad del ECDC en este campo. De especial preocupación son los altos niveles de multirresistencia a antibióticos en algunos países del entorno europeo como Italia o Grecia. En este ámbito, el Ministerio de Sanidad y el ISCIII, a través del Centro Nacional de Epidemiología y el Centro Nacional de Microbiología (CNM), colaboran en todas las iniciativas de control, mediante participación con las redes internacionales dedicadas a estos temas, como el ECDC o la Organización Mundial de la Salud (OMS).

En cuanto a otros eventos transfronterizos de importancia para la salud pública, como los producidos por otros virus hemorrágicos o patógenos bacterianos de alta consecuencia, el ISCIII participa en la nueva Acción Conjunta de la UE SHARP (*Strengthened International Health Regulations and Preparedness in the EU*).

Por otra parte, se mantienen los programas para el control y erradicación de enfermedades animales, especialmente aquellas susceptibles de transmitirse al ser humano o con elevado impacto en la economía nacional, registrándose una favorable evolución de la situación sanitaria.

La protección sanitaria en frontera se lleva a cabo por los servicios veterinarios de los Puestos de Inspección Fronterizos (PIF), que verifican el cumplimiento de los requisitos sanitarios en los productos de origen animal que entran de fuera de la UE.

En cuanto a la encefalopatía espongiforme bovina (EEB), continúa la evolución favorable de los indicadores. Desde 2016 España es reconocida oficialmente por la Organización Mundial de Sanidad Animal como país con riesgo insignificante de EEB. Durante 2019 no se han registrado casos notificables de *Influeza Aviar,* por lo que se ha mantenido el estatus de país libre. Dada la situación de la peste porcina africana en otros países de la UE, el Programa Nacional de Vigilancia Sanitaria Porcina se ha reforzado para adaptarlo al mayor riesgo, y al Plan Estratégico de Bioseguridad en Explotaciones Porcinas.

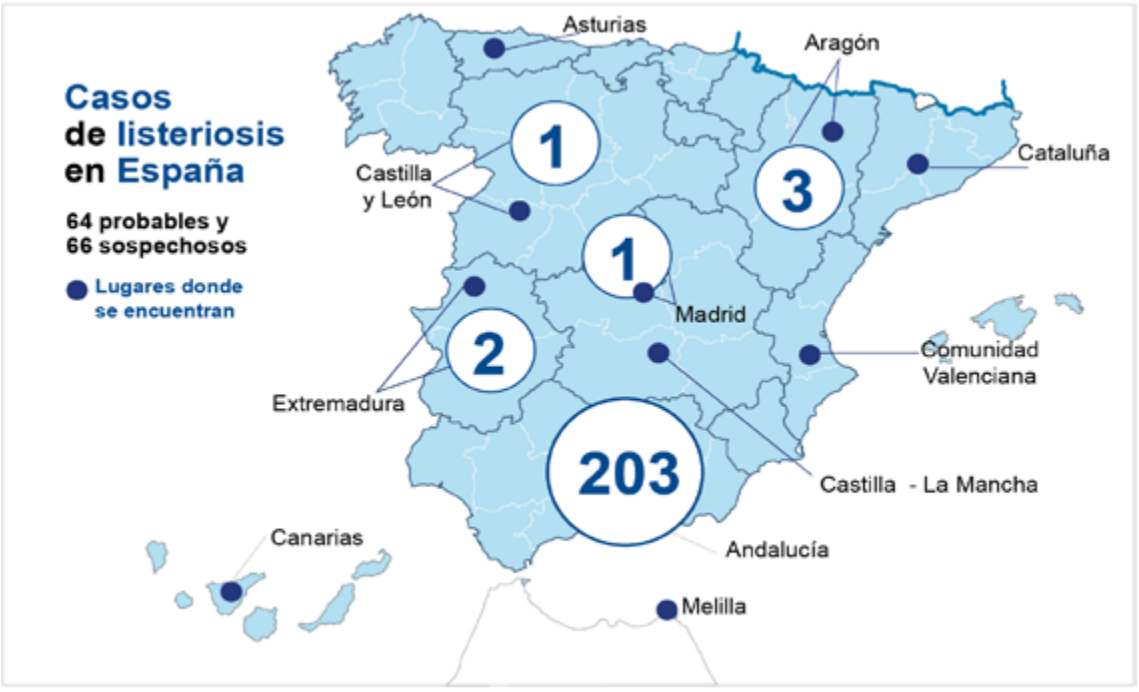
La seguridad del consumidor se refuerza con otras medidas, como el control de residuos de medicamentos veterinarios, incluido dentro del Programa Nacional de Investigación de Residuos, con 43.629 muestras y 570.567 análisis realizados en 2018.

Por otra parte, las Fuerzas Armadas (FAS) despliegan su actividad en lugares alejados del territorio nacional. Tanto la protección del personal desplegado como la necesidad de garantizar la seguridad sanitaria de España tras el repliegue de personal y material requerirán un creciente esfuerzo de gestión del riesgo de introducción de agentes, vectores y reservorios de enfermedades transmisibles.

Figura 14-1
Brote de ébola en la República Democrática del Congo: situación en 2019

Fuente: Organización Mundial de la Salud

Figura 14-2
Casos de listeriosis en España en 2019



Fuente: Ministerio de Sanidad

Retos

La aparición y diseminación de bacterias resistentes a múltiples antibióticos sigue siendo un reto clínico y de salud pública de primer nivel. Cabe destacar aquellas especies como *Acinetobacter baumannii, Pseudomonas aeruginosa* y enterobacterias multirresistentes productoras de carbapenemasas consideradas por la OMS como de "prioridad crítica" en el desarrollo de nuevos tratamientos. Se deben poner todos los medios necesarios para responder ante este reto de forma coordinada a nivel europeo e internacional.

Las bacterias resistentes a múltiples antibióticos suponen un reto clínico y de salud pública de primer nivel

La confirmación de la presencia del vector de transmisión del virus Dengue, así como de varios casos autóctonos en España, hace necesario intensificar la vigilancia y revisar los procedimientos de control para este virus, así como para otras arbovirosis, como Chikungunya, fiebre amarilla o zika, que comparten vector de transmisión.

Aunque el brote de enfermedad por el virus del Ébola en la República Democrática del Congo sigue sin control y ya ha sido declarado por la OMS como Evento de Salud Pública de Importancia Internacional, el riesgo de su reintroducción en Europa sigue siendo bajo. De cualquier manera, la descripción de un fallecimiento por reinfección en una trabajadora sanitaria, riesgo que no se contemplaba, es un factor a tener en cuenta de cara al futuro.

El Ministerio de Sanidad, Consumo y Bienestar Social impulsa la aprobación e implantación del Plan de preparación y respuesta ante una posible reintroducción de la viruela en España.

Debido a los peligros derivados del movimiento transfronterizo, es un reto de primer orden minimizar el riesgo de introducción en territorio nacional de vectores y reservorios de enfermedades humanas y animales. En este último sentido, cobra especial relevancia la necesidad de mantener la eficacia en la aplicación de las medidas de prevención destinadas a reducir el riesgo de entrada de enfermedades en las partidas de animales, material genético y productos que llegan y se incorporan a la UE a través de las aduanas españolas.

Para garantizar la seguridad frente a epidemias y pandemias, se debe observar el estado sanitario de la cabaña ganadera a través de la aplicación de medidas de prevención y con la ejecución de programas de vigilancia, control y erradicación de enfermedades.

El desafío para detectar y reaccionar ante cualquier riesgo sanitario es particularmente sensible en infraestructuras y zonas especialmente críticas como son los puertos, los aeropuertos y las fronteras terrestres. Para ello, con la intención de mejorar las capacidades, se considera esencial desarrollar protocolos de colaboración entre las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y las autoridades sanitarias para hacer frente a situaciones de crisis o emergencias derivadas de riesgos de naturaleza biológica e incrementar la vigilancia sobre aquellas prácticas ilegales que pueden favorecer la propagación de epidemias, así como impulsar la coordinación con autoridades nacionales e internacionales encargadas del control de la calidad y seguridad alimentaria.

En esta línea, se ha de dotar a las FCSE de la formación y el equipamiento necesario para hacer frente a todo tipo de riesgos biológicos a los que puedan verse sometidas durante el desarrollo de los servicios realizados en el ámbito de sus competencias, sobre todo en aquellas relacionadas con la custodia de costas, fronteras, puertos y aeropuertos y las que se desempeñan en todo el mar territorial. También es un reto la creación y dotación de una red de vigilancia epidemiológica especifica de las FAS en territorio nacional y zona de operaciones.

En España, las toxiinfecciones alimentarias han supuesto una amenaza para la salud pública durante 2019

En España, las toxiinfecciones alimentarias han supuesto una amenaza para la salud pública durante 2019. En concreto, el brote de listeriosis de Andalucía, asociado al consumo de carne mechada, ha tenido un especial impacto, tanto mediático como de salud, dada su virulencia. Este es un reto, junto con el incremento en los casos de botulismo que se han observado a lo largo del año, al que hay que prestar especial atención.

Por otra parte, conviene revisar e impulsar en los Institutos de Medicina Legal y Ciencias Forenses y el Instituto Nacional de Toxicología y Ciencias Forenses, el cumplimiento del Protocolo de intervención en relación a agentes infectocontagiosos y de medidas de seguridad para prevención de riesgos en las intervenciones médico forenses y de laboratorio.

En relación a la toxicovigilancia, los retos consisten en armonizar, de acuerdo con la normativa europea, la clasificación de mezclas y productos químicos comercializados en España, así como el procedimiento de notificación al Instituto Nacional de Toxicología y Ciencias Forenses, en calidad de organismo designado en relación al *Reglamento 1272/2008, de 16 de diciembre*, y como centro antitóxico nacional, para el cumplimiento de sus funciones de atención y prevención de intoxicaciones en la población. También se ha de impulsar el desarrollo de un programa informático para la notificación electrónica de las referidas mezclas y productos químicos peligrosos, que se realizará a través del portal europeo, desarrollado por la Agencia Europea de los Productos Químicos (ECHA, *European Chemicals Agency*). Es destacable, por otra parte, el reto de participar en el desarrollo de un sistema de toxicovigilancia armonizado en el ámbito de la UE, en relación a la exposición a sustancias y mezclas químicas peligrosas.

En coherencia con lo expuesto, es necesario modernizar los sistemas de vigilancia de la salud en España de forma que incluyan además de las enfermedades, los factores de riesgo y determinantes de enfermedad, una integración de esta información con los sistemas de alerta precoz y respuesta y una automatización de procesos que incrementen la oportunidad de las señales de riesgo y de la respuesta en caso de ser necesaria.

Este reto que se enmarca en el proceso de desarrollo de *la Ley 33/2011, de 4 de octubre, General de Salud Pública*, implica, por un lado, la adopción de un Real Decreto que establezca las bases de la Vigilancia de la Salud Pública en España y por otro, la elaboración, aprobación e implementación progresiva multianual de una estrategia que lo haga operativo. Este proceso se debe llevar a cabo de forma consensuada y coordinada con las Comunidades Autónomas.

Realizaciones

Capacidades y mecanismos de actuación

Se ha llevado a cabo la actualización de los Laboratorios Oficiales de la Dirección General de Sanidad de la Producción Agraria como centros nacionales de referencia para zoonosis y otras enfermedades animales, parte fundamental en los programas sanitarios de lucha contra las enfermedades y de garantía y seguridad para la población y la economía nacional.

También se ha realizado la primera convocatoria para la nominación de Centros, Servicios y Unidades de Referencia (CSUR) de Unidades de Aislamiento de Alto Nivel tras la aprobación el año anterior de los criterios de designación. Al margen de la Unidad que alberga el Hospital Central de la Defensa Gómez Ulla (no puede participar en convocatorias CSUR por ser de titularidad estatal), se han presentado tres de las seis Unidades de Aislamiento de Alto Nivel de las que se disponen en España. En el año 2020 se realizará una segunda convocatoria.

Por otra parte, se ha implementado el convenio entre el Ministerio de Sanidad, Consumo y Bienestar Social y el Ministerio de Defensa, firmado a final de 2018, para la vigilancia entomológica en bases aéreas y navales del Ministerio de Defensa para prevenir la importación de riesgos sanitarios transmitidos por vectores exóticos. Igualmente, se ha creado el sistema de vigilancia de las infecciones producidas por patógenos resistentes a los antibióticos y las redes de laboratorios de apoyo a dicho sistema. La resistencia a los antibióticos es considerada la mayor amenaza emergente para la salud pública de los próximos años.

Con motivo del virus del Ébola, se ha desarrollado y regulado un Protocolo de intervención forense en muertes judiciales, aplicable a otros agentes infectocontagiosos similares que causen un riesgo grave en la población, con la colaboración del Ministerio de Sanidad, Servicios Sociales e Igualdad, el Instituto Nacional de Toxicología y Ciencias Forenses y los Institutos de Medicina Legal y Ciencias Forenses, de acuerdo con las recomendaciones internacionales y europeas en estos casos. Además, se han adquirido los equipos de protección necesarios y se ha realizado formación en los Institutos del ámbito del Ministerio de Justicia en el correcto manejo y tratamiento de los equipos.

Destaca la publicación del Convenio, entre el Ministerio de Defensa y la Agencia Española del Medicamentos y Productos Sanitarios, para la custodia y gestión del depósito estatal estratégico de medicamentos y productos sanitarios para emergencias y catástrofes, el depósito estatal de antivirales, el depósito contra la viruela, el depósito de antitoxinas y medicamentos de urgencia, y la fabricación de medicamentos para situaciones especiales. Igualmente, y como medida preventiva, se almacenan y custodian vacunas contra la viruela, así como el disolvente para su reconstitución, y las agujas bifurcadas para su administración, propiedad del Ministerio de Sanidad, Consumo y Bienestar Social y del Ministerio de Defensa. Asimismo, la Farmacia del Hospital Central de la Defensa Gómez Ulla almacena y custodia antitoxinas y medicamentos de urgencia para enfermedades infecciosas de alto riesgo.

El Ministerio de Defensa lleva a cabo labores de vigilancia epidemiológica en territorio nacional y zona de operaciones de enfermedades de declaración obligatoria y brotes de interés de salud pública, en coordinación con el Centro Nacional de Epidemiologia, organismo encargado de la vigilancia a nivel nacional.

Se ha potenciado el Centro Militar de Veterinaria como laboratorio de referencia en determinadas técnicas analíticas relacionadas con la seguridad alimentaria y la higiene ambiental, mediante las correspondientes acreditaciones otorgadas por la Entidad Nacional de Acreditación. Además, se ha llevado a cabo, bajo la coordinación de la estructura de apoyo veterinario del Ministerio de Defensa, el acuerdo entre éste y el Ministerio de Sanidad, Consumo y Bienestar Social para la realización de actividades de vigilancia entomológica en instalaciones militares, bases navales y bases aéreas del Ministerio de Defensa, en colaboración con el CCAES, para contribuir a la confección del mapa entomológico nacional mediante la identificación de especies de mosquitos y otros dípteros hematófagos en instalaciones militares.

Salud Pública y Sanidad Animal

El CNM-ISCIII ha realizado el estudio comparativo molecular de todas las cepas implicadas en la alerta sanitaria debida a *Listeria monocytogenes* asociada a carne mechada, lo que ha permitido establecer las vías de transmisión y colaborar en la resolución del brote. En relación a esta alerta sanitaria, que afectó a 193 personas, los servicios de salud pública de Andalucía llevaron a cabo una investigación, con la colaboración de la Guardia Civil y del CNM del Instituto Carlos III de Majadahonda (Madrid), que permitió identificar la empresa responsable de los productos cárnicos contaminados, determinando la implicación de ocho personas e interviniendo 17 toneladas de productos potencialmente infectados, que posteriormente fueron destruidos.

El CNM-ISCIII, además, mantiene la vigilancia activa para la detección precoz de clones multirresistentes. A través de su Laboratorio de Referencia e Investigación en Resistencia a Antibióticos e Infecciones Relacionadas con Asistencia Sanitaria, participa en las diferentes redes internacionales (ECDC, OMS) de vigilancia e investigación en este tema (EARS-Net, EURGen-Net. EU-JAMRAI).

Durante 2019 han continuado los trabajos de aplicación de las medidas de prevención instauradas para reducir el riesgo de entrada de enfermedades a través de animales, materiales o productos importados. En relación a enfermedades de animales, cabe destacar: el desarrollo y la aplicación de los Programas Nacionales establecidos para la vigilancia, control y erradicación de enfermedades animales, en especial aquellas que pueden ser transmisibles a las personas y de aquellas susceptibles de ocasionar graves pérdidas en la economía del sector; el refuerzo de las actuaciones previstas en *el Plan de Acción en Materia de Bioseguridad*, con objeto de reforzar la capacidad de prevención de las explotaciones ganaderas y la reducción de su sensibilidad al contagio ante la propagación de enfermedades; o el mantenimiento de los avances de estos últimos años en la mejora de la situación sanitaria de la cabaña, para contribuir a garantizar la seguridad de los consumidores y su salud, así como para apoyar los favorables resultados económicos del sector

ganadero y la industria cárnica, fuente de exportaciones y riqueza para España.

En el marco de la lucha contra el uso irracional de medicamentos veterinarios en el ámbito de la producción animal, así como en el de los animales de compañía, con el objeto de evitar la diseminación de resistencias antimicrobianas en el medio ambiente y, por ende, en la salud humana, la Guardia Civil ha realizado atribuciones al establecimiento e impulso de las actividades contempladas en el *Plan Nacional de Resistencia a los Antibióticos 2019-2021*.

En relación a productos vegetales, en 2019 la Guardia Civil ha contribuido al mantenimiento de las medidas de restricción a los movimientos no controlados de determinados productos vegetales, para evitar la expansión de la bacteria *Xylella fastidiosa* que está afectando a multitud de especies vegetales en las islas Baleares y que se ha detectado también en algunos puntos aislados en la península. Igualmente, ha participado en la labor preventiva y la lucha contra la propagación de la plaga del Nematodo del pino, destacando la *Operación Bursátil,* llevada a cabo por el SEPRONA, mediante la cual se desarticuló una organización que estaría trasladando madera infectada con Nematodo de zonas prohibidas entre Portugal y Galicia a otras provincias del territorio nacional.

Coordinación Internacional

El Equipo Técnico Español de Ayuda y Respuesta (START), formado por profesionales del Sistema Nacional de Salud y que se integra en los Equipos Médicos Europeos de la UE y en los Equipos Médicos de Emergencias de la OMS, fue acreditado y desplegado por primera vez y con éxito, en respuesta al Ciclón IDAI que asoló Mozambique.

La Guardia Civil, a través del SEPRONA, es el cuerpo policial español en la Red Europea de Fraude Alimentario. La red canaliza las informaciones respecto a cualquier alerta alimentaria en la UE y constituye una plataforma básica para el intercambio de información y experiencias, algo que ayuda el desarrollo de investigaciones criminales en dicho ámbito. En este sentido, cabe señalar la explotación de las operaciones *Glanis, Opson* o *Txuspas* con alrededor de 100 personas detenidas o investigadas, así como destacar la operación *Monocy* realizada en coordinación con Europol y en la que se ha investigado a ocho personas.

El ISCIII, a través del CNM y del Centro Nacional de Epidemiología (CNE), forma parte de la nueva Acción Conjunta de la UE SHARP (*Strengthened International Health Regulations and Preparedness in the EU*), dedicada tanto a revisar el Reglamento Sanitario Internacional, como a la preparación ante eventos transfronterizos de origen infeccioso.

El ISCIII sigue formando parte de la estructura de vigilancia europea sustentada por el ECDC para todas las enfermedades de vigilancia en Europa.

Esta colaboración es, igualmente, constante entre los laboratorios estatales y locales y los servicios de vigilancia de vectores, para la detección temprana de mosquitos infectados por los diferentes Arbovirus.

PRESERVACIÓN DEL MEDIO AMBIENTE

OBJETIVO:

Garantizar la conservación de un medio ambiente de calidad y la protección del patrimonio natural y de la biodiversidad, como medio para mejorar la calidad de vida y contribuir a un desarrollo sostenido y sostenible, con especial incidencia en la lucha contra el cambio climático.

Tendencias

Las consecuencias cada vez más visibles del incremento de la temperatura global y su incidencia sobre otros ámbitos de la Seguridad Nacional como la seguridad energética, la ordenación de flujos migratorios o la lucha contra catástrofes y emergencias, además de su incidencia en la gestión del agua, la biodiversidad, la desertificación o la despoblación de zonas agrarias o forestales, hacen que la preservación del medio ambiente y, en particular, la lucha contra el cambio climático, cobre una particular relevancia.

El año 2019 fue el segundo año más cálido registrado después de 2016

La Organización Meteorológica Mundial ha confirmado que el año 2019 fue el segundo año más cálido registrado después de 2016. La media de la temperatura global estuvo 1,1°C por encima de la media de la era preindustrial (1850-1900). Si sigue la tendencia actual de emisiones de dióxido de carbono, a finales de siglo los incrementos de temperatura serán de entre 3-5°C.

En España, se mantiene la tendencia iniciada en 1961 de aumento de la temperatura media anual, con incrementos significativos entre 0,1 y 0,2°C por década. El año 2017 fue el año más cálido desde el comienzo de la serie en 1965, con una temperatura media de 16,2° C, valor que supera en 1,1° C al valor medio anual (periodo de referencia 1981-2010). De los diez años más cálidos en España desde 1965, siete han sido años del siglo XXI y cinco de ellos pertenecen a la actual decena que comenzó en 2011. Este aumento se traduce en una mayor frecuencia e intensidad de olas de calor con registros que llegaron a los 46,9°C en Córdoba en 2017.

En 2019 ha habido un incremento de la concienciación y presión social sobre la necesidad de hacer frente al cambio climático

En 2019 ha habido un notable incremento de la concienciación y presión social sobre la necesidad de hacer frente al cambio climático. En consecuencia, han continuado y se han acentuado los esfuerzos a nivel global por conseguir una reducción de gases de efecto invernadero (GEI) con vistas a moderar el aumento de la temperatura, aumentar las medidas de resiliencia, frenar el grave deterioro medioambiental y preservar la biodiversidad. De la misma forma, a nivel global, se hace patente la necesidad de preparar las sociedades, las economías y el medio ante los inevitables efectos de los impactos del cambio climático. (Figura 15-1)

España articula estos esfuerzos a través de acuerdos internacionales, medidas adoptadas por la UE y compromisos adquiridos en las organizaciones a las que pertenece.

En diciembre se celebró en Madrid, bajo Presidencia Chilena, la XXV Conferencia de las Partes de la Convención Marco de Naciones Unidas sobre Cambio climático (COP25) en la que, entre otras cuestiones, se adoptó el acuerdo denominado *Chile-Madrid Tiempo de Actuar*, que sienta las bases para que, en 2020, los países presenten compromisos de reducción de emisiones (NDC, por sus siglas en inglés correspondientes a la denominación *Nationaly Determined Contributions*) más ambiciosos para responder a la emergencia climática.

Durante el desarrollo de la Cumbre, la UE activó un paquete de 50 medidas para afrontar la emergencia climática. El Nuevo Pacto Verde (*European Green New Deal*) compromete a la UE a la neutralidad climática en 2050 y acuerda convertir al Banco Europeo de Inversiones (BEI) en un "Banco Climático", algo que permitirá la inversión de un billón de euros durante la próxima década. Además, el BEI ha anunciado que dejará de financiar proyectos relacionados con las energías fósiles en 2021.

El Plan Nacional de Adaptación al Cambio Climático es el marco de referencia para la coordinación entre las Administraciones públicas

En España, el *Plan Nacional de Adaptación al Cambio Climático* (PNACC) es el marco de referencia para la coordinación entre las Administraciones públicas en las actividades de evaluación de impactos, vulnerabilidad y adaptación al cambio climático. A lo largo de 2018 y 2019, se desarrolló, siguiendo los requerimientos determinados por los diferentes acuerdos internacionales de los que España forma parte, una evaluación global del Plan con el objeto de reconocer los avances logrados, los retos pendientes y las lecciones aprendidas hasta la fecha.

Se espera que los cambios normativos a favor de una economía descarbonizada, sobre los que se está trabajando a través del Marco Estratégico de Energía y Clima, aceleren la tendencia general a la disminución de las emisiones de GEI en España desde 2008. El objetivo a largo plazo, 2050, es alcanzar la neutralidad climática, para lo que se ha fijado el objetivo de lograr una reducción de emisiones de, al menos, el 90% de las emisiones brutas totales de GEI respecto al año de referencia 1990. En esa dirección, el objetivo de mitigación de emisiones para el año 2030 es, al menos, el 20% respecto a 1990. Como resultado de las medidas contempladas en el borrador del PNIEC, se pasaría de los 340,2 MtCO2-eq emitidos en 2017, a los 221,8 MtCO2eq en el año 2030, lo que implicaría retirar aproximadamente la tercera parte de las emisiones actuales en los próximos doce años. (Figura 15-2 y 15-3)

En cuanto a los espacios marinos, la actualización de la evaluación del estado del medio marino que tuvo lugar en el contexto del segundo ciclo de las estrategias marinas reveló importante información sobre las tendencias recientes y el estado de algunos de los descriptores del buen estado ambiental. En algunos casos no se ha alcanzado el buen estado ambiental (BEA) en toda la demarcación o en parte de ella. Desde el punto de vista de la gestión, se ha continuado con los trabajos de elaboración de planes de gestión de los espacios marinos protegidos de competencia estatal.

El transporte es una actividad esencial para la economía que tiene como contrapartida los efectos de sus emisiones en el medio ambiente. En este sentido, y respecto del transporte marítimo: se está limitando el contenido de azufre en los combustibles marinos; se está efectuando el seguimiento y control de las emisiones de CO2 de la flota mercante mundial con el objetivo establecido por la Organización Marítima Internacional (OMI) de reducir en un 50% en 2050 las emisiones de CO2 tomando como base las realizadas en 2018. Asimismo, a través del Convenio internacional de gestión de las aguas de lastre de los buques, que entró en vigor en 2017, se está trabajando para evitar la proliferación de especies invasoras en los ecosistemas marinos.

De la misma manera, la intensificación de la actividad agraria y pesquera favorece la competitividad y rentabilidad de la actividad agraria, el desarrollo económico y el empleo en las zonas rurales, pero, si no va acompañada de medidas para reducir su impacto ambiental, puede alterar el equilibrio entre los sistemas agrícola y ganadero y marítimo y causar impactos significativos sobre el medio ambiente. Así, es evidente la necesidad de adoptar medidas que corrijan dichos impactos y para ello desde el Ministerio de Agricultura, Pesca y Alimentación se trabaja en la elaboración de herramientas que facilitan a los productores el cumplimiento de las exigencias medioambientales.

En materia de incendios forestales, de forma general, el número de siniestros y las superficies afectadas por los mismos están íntimamente asociados a las condiciones meteorológicas. Así, en 2018, debido a la meteorología se redujeron notablemente la probabilidad de ignición y la predisposición a arder del combustible forestal, lo que supuso un descenso de más del 43% en el número de siniestros (7.143 siniestros) y de más de un 75% en la superficie forestal afectada (253162,44 ha) respecto a los valores medios del decenio 2006-2015 (13.111 siniestros y 100.796 ha). En 2019 las cifras han vuelto a acercarse más a los valores medios del decenio, con 10.883 siniestros y 83.963 ha de superficie forestal afectada.

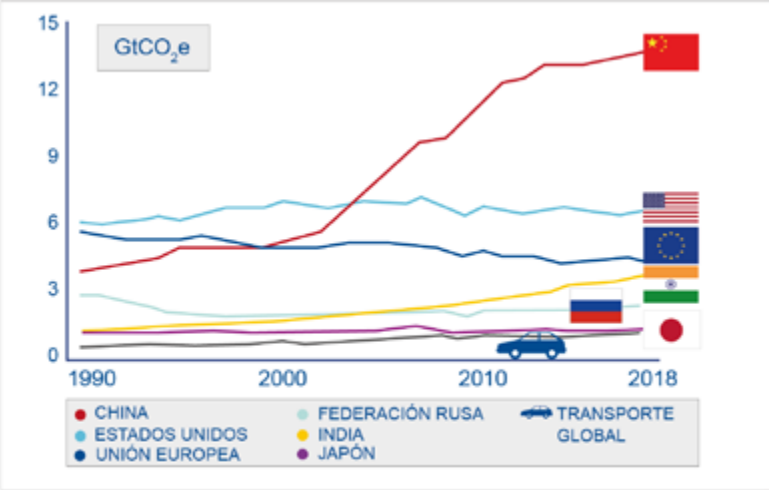
El suministro en cantidad y en calidad de un recurso esencial como el agua es fundamental para asegurar el eficaz desenvolvimiento de una sociedad y de su economía y ofrecer altos niveles de seguridad, minimizando el riesgo de fallos en cualquiera de los componentes del sistema. La disponibilidad del agua puede verse afectada por efecto de sequías y otros fenómenos en los que el calentamiento global puede tener incidencia.

En este sentido, se está promoviendo el empleo de los planes de sequía como herramienta fundamental para gestionar las situaciones en que sea necesaria su aplicación.

Por otro lado, en los últimos años se ha producido un incremento de la actividad de organizaciones criminales con carácter transnacional especializadas en delitos medioambientales. Como consecuencia de la globalización, se ha ampliado la variedad de actividades criminales cometidas gracias al aprovechamiento de vacíos legales. Dichas actividades abarcan infracciones muy diversas, entre las que destacan el tráfico ilícito de residuos, el tráfico de especies protegidas y el comercio de sustancias que afectan a la capa de ozono.

Estos grupos criminales suelen emplear estructuras empresariales para dar apariencia de legalidad a sus actividades, siendo frecuente la falsificación de documentos oficiales y privados necesarios para el comercio. Generan elevados beneficios económicos de procedencia ilícita, asumiendo un bajo riesgo sancionador. Los beneficios obtenidos ilícitamente son introducidos en el flujo legal a través del blanqueo de capitales, actuación que requiere una investigación patrimonial paralela.

Figura 15-1
Principales emisores de gases de efecto invernadero en términos absolutos



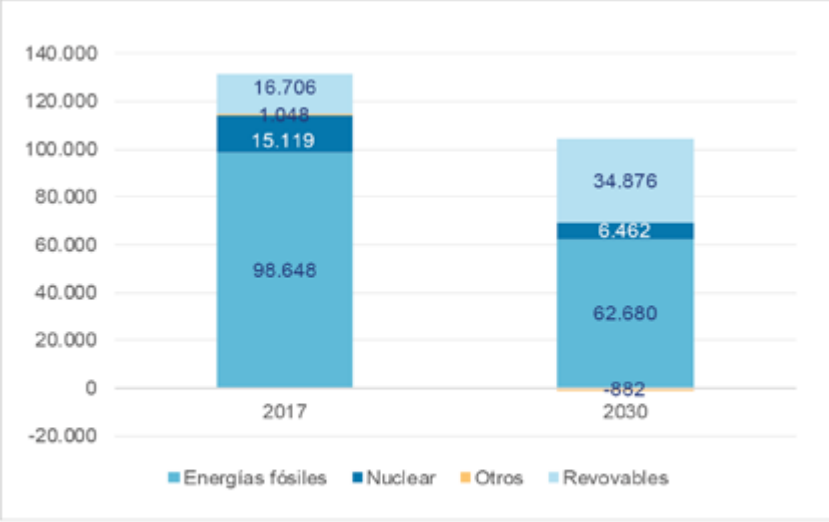
Fuente: Organización de las Naciones Unidas

Años	1990	2005	2015	2020*	2025*	2030*
Transporte	59.199	102.310	83.197	85.722	74.638	57.695
Generación de energía eléctrica	65.864	112.623	74.051	63.518	27.203	19.650
Sector industrial (procesos de combustión)	45.099	68.598	40.462	40.499	37.246	33.530
Sector industrial (emisiones de procesos)	28.559	31.992	21.036	21.509	22.026	22.429
Sectores residencial, comercial e institucional	17.571	31.124	28.135	26.558	23.300	19.432
Ganadería	21.885	25.726	22.854	23.247	21.216	19.184
Cultivos	12.275	10.868	11.679	11.382	11.086	10.791
Residuos	9.825	13.389	14.375	13.657	11.898	9.650
Industria de refino	10.878	13.078	11.560	12.247	11.607	10.968
Otras industrias energéticas	2.161	1.020	782	721	568	543
Otros sectores	9.082	11.729	11.991	14.169	13.701	13.259
Emisiones fugitivas	3.837	3.386	4.455	4.715	4.419	4.254
Uso de productos	1.358	1762	1.146	1.231	1.238	1.316
Gases fluorados	64	11.465	10.086	8.267	6.152	4.037
Total	**287.656**	**439.070**	**335.809**	**327.443**	**266.343**	**226.737**

* Los datos de 2020, 2025 y 2030 son estimativos del Escenario Objetivo de PNIEC.

Fuente: Ministerio para la Transición Ecológica

Figura 15-2
Evolución de las emisiones (miles de toneladas de CO_2 equivalente)



Fuente: Ministerio para la Transición Ecológica

Figura 15-3
Mix de energía primaria en España en 2017 y 2030 (ktep)

Retos

La producción de energía, el transporte y los procesos industriales causan gran parte de los gases de efecto invernadero

El cambio climático constituye uno de los retos actuales más significativos, con severas consecuencias ambientales, económicas y sociales, que incluyen sequías, inundaciones, calor extremo y pobreza de la población más vulnerable. Los gases de efecto invernadero que causan el incremento en temperaturas, son resultado, principalmente, de la producción de energía, el transporte, los procesos industriales e incluso factores de la alimentación. (Figura 15-4)

En este sentido, uno de los objetivos principales es ejercer un control adecuado de las actividades con alto impacto en el medio ambiente y el cambio climático, entre las que destacan aquellas relacionadas con fuentes de energía; extracción, almacenamiento y distribución de hidrocarburos; gestión de residuos y de sustancias tóxicas y peligrosas; y todas aquellas capaces de contaminar el suelo, el agua o la atmósfera.

En particular, las infraestructuras del transporte requieren medidas para prevenir, mitigar, corregir o compensar los impactos ambientales que puedan generarse en el desarrollo de su actividad, desde la fase de planificación hasta la explotación, pasando por el proyecto, su construcción y su mantenimiento.

En el transporte marítimo supone un desafío la aplicación efectiva del nuevo límite del 0,50% masa/masa de contenido de azufre de los combustibles marinos utilizados en la navegación y del 0,10% en los utilizados por los buques fondeados o en puerto, además de la reducción de las emisiones de CO2 para cumplir con los objetivos marcados por la OMI en el desarrollo de nuevos combustibles y tecnologías en el transporte marítimo. También se pretende reducir las descargas ilegales realizadas por los buques en aguas nacionales.

Respecto del sector agrario, continúa siendo esencial el reconocimiento del papel que juega en la lucha contra el cambio climático, la preservación del medio ambiente y el desarrollo sostenible, a través del desarrollo de estrategias para la mitigación y adaptación de la agricultura, la ganadería y la pesca al cambio climático, para la gestión sostenible de los recursos naturales como el agua, el suelo y el aire, para la protección de la biodiversidad y para potenciar los servicios ecosistémicos y conservar los hábitats y los paisajes.

La pérdida de suelo agrícola y la desertificación es una de las problemáticas en la que el Centro de Investigaciones Energéticas, Medioambientales y Energéticas (CIEMAT) centra su actividad, a través del desarrollo de conocimiento, tecnologías y aplicaciones en el ámbito tanto de la conservación del medio edáfico como del tratamiento de suelos contaminados, así como de técnicas de restauración ambiental de áreas afectadas antropogénicamente o el estudio de suelos agrícolas.

En cuanto a la gestión forestal, el reto es consolidar la producción de bienes, mejorando los servicios ambientales que los bosques generan, poniendo el foco en una gestión adecuada de los montes que favorezca su capacidad de absorción de CO2, su protección contra los incendios forestales y su misión protectora en zonas de especial importancia en la regulación de las aguas, mejorando así su contribución a la mitigación y adaptación al cambio climático en distintos frentes. Para ello es

importante el desarrollo de una estrategia nacional de prevención de incendios forestales y el continuo desarrollo de programas específicos de prevención de incendios forestales centrados en actuaciones directas de prevención destinadas a reducir o anular la probabilidad de que se inicie un fuego o limitar sus efectos si este se produce, así como también mediante acciones de sensibilización y concienciación o actuaciones de prevención en el marco de la gestión forestal sostenible. Asimismo, se han de desarrollar líneas de actuación para, en colaboración con las Comunidades Autónomas, proceder a restaurar zonas afectadas por grandes incendios forestales y mejorar la protección de laderas y zonas desprovistas de vegetación, para conseguir una mejor regulación de las aguas al tiempo que se incrementa la capacidad de los montes como sumideros de carbono.

En materia de protección y conservación del litoral, es importante integrar la adaptación al cambio climático en la planificación y gestión de la costa y continuar aplicando la *Estrategia de Adaptación al Cambio Climático de la Costa Española*. Así, es necesario avanzar en el diseño de metodologías para analizar las proyecciones de impactos en la costa, reduciendo la incertidumbre asociada, a fin de hacer una buena planificación de actuaciones y un uso eficiente de los recursos disponibles. También es importante incrementar la resiliencia de la costa al cambio climático y a la variabilidad climática y responder con eficacia ante los daños producidos en la costa por temporales.

Es importante integrar la adaptación al cambio climático en la planificación y gestión de la costa

En este sentido, los retos más significativos son el mantenimiento de la costa en condiciones de uso sostenible, llevando a cabo actuaciones dirigidas a su protección, la protección del medio ambiente y la recuperación del litoral. Asimismo, continúa la aplicación de las Estrategias ya aprobadas para la protección de las zonas costeras con mayores problemas erosivos (Huelva, Maresme, Castellón, Valencia y Granada) y se está avanzando en la redacción de las estrategias de Cádiz, Málaga, Almería, Baleares y de los Planes de Protección del Mar Menor en Murcia y Delta del Ebro en Tarragona.

Para la protección y conservación del medio marino, es necesario avanzar en el desarrollo del segundo ciclo de las estrategias marinas de España, cuyo objetivo es alcanzar el buen estado ambiental del medio marino en el año 2020, en la consolidación de una red de Espacios Marinos Protegidos gestionada de manera eficaz y que cumpla con los objetivos internacionales y en el desarrollo de los planes de ordenación del espacio marítimo, que deberán estar aprobados por Real Decreto no más tarde del 31 de marzo de 2021.

En casos de catástrofes o accidentes en el medio marino y costero, se requiere la colaboración entre los Ministerios para la Transición Ecológica, Fomento e Interior, en la aplicación del Sistema Nacional de Respuesta, especialmente en lo referente al Subsistema Costero, a través del *Plan Estatal de Protección de la Ribera del Mar contra la Contaminación* (Plan Ribera).

El deterioro en la calidad del aire en las ciudades y su relación con los problemas de salud continúa siendo un reto significativo que requiere investigar los procesos físicos y químicos de los contaminantes atmosféricos, determinar las emisiones de contaminantes atmosféricos, analizar los efectos sobre los ecosistemas y agrosistemas, y llevar a cabo

análisis de la interacción calidad del aire-cambio climático. CIEMAT lidera el grupo consultivo de la plataforma X Aire Limpio, que trabaja en el desarrollo de planes de calidad del aire en ciudades a nivel nacional.

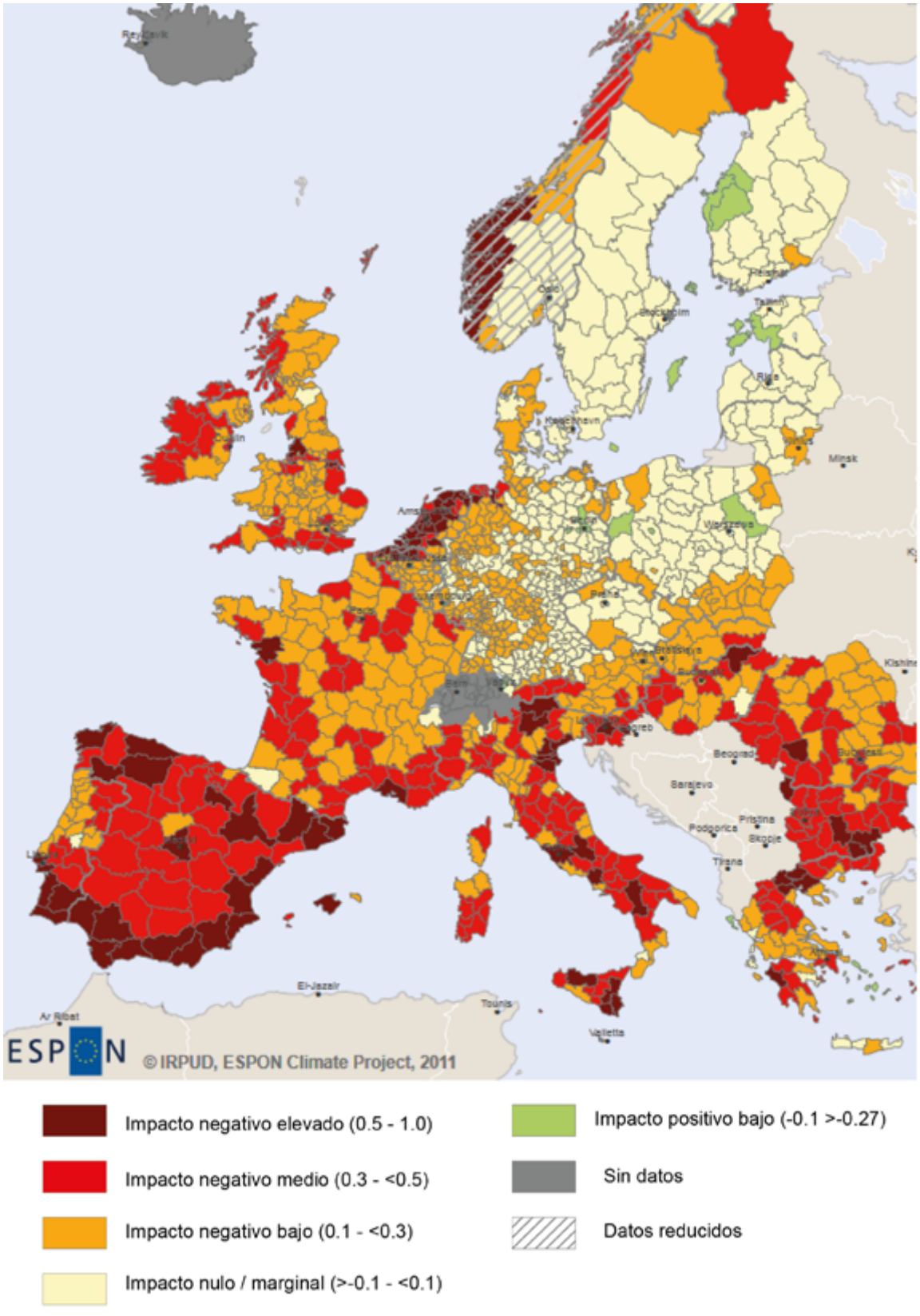
En lo relativo al traslado de residuos, el Ministerio para la Transición Ecológica continúa con el trabajo de reforzar la inspección del traslado mediante la aprobación del *Plan Estatal de Inspección en materia de Traslados Transfronterizos de Residuos 2020-2022*. Además, se ha firmado un nuevo convenio marco de colaboración entre la Agencia Tributaria (AEAT) y el Ministerio para la Transición Ecológica y ha aumentado el número de inspecciones y procedimientos sancionadores.

Por su parte, para contribuir a la preservación del medio ambiente la AEMET proporciona asesoramiento científico en asuntos relacionados con la variabilidad y el cambio climático a las Administraciones públicas, en apoyo a sus políticas medioambientales, además de elaborar y actualizar escenarios de cambio climático y de mantener una vigilancia continua, eficaz y sostenible de las condiciones meteorológicas, climáticas y de la estructura y composición física y química de la atmósfera sobre el territorio nacional.

La colaboración entre actores, tanto públicos como privados, implicados en la protección del medio ambiente y en la lucha contra el cambio climático, tanto a nivel nacional como internacional es imprescindible. A nivel nacional es preciso seguir mejorando la colaboración de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) con organismos públicos encargados de la preservación del entorno natural, así como del control administrativo ante sus posibles alteraciones, en particular con las autoridades de las Comunidades Autónomas, con el objeto de lograr una mayor eficacia en la protección de la naturaleza y contra aquellas actividades que aceleran el cambio climático.

En el ámbito internacional es clave incrementar la participación actual en Grupos de Trabajo de la Unión Europea, además de continuar cumpliendo con los compromisos de España con la UE en materias como los planes anuales de inspección de traslados transfronterizos de residuos, el tráfico ilegal de especies, el cumplimiento de la normativa sobre compuestos orgánicos volátiles, el control de la madera procedente de la tala ilegal y otros planes desarrollados por el Ministerio para la Transición Ecológica como la *Estrategia Nacional contra el uso ilegal de venenos*.

Figura 15-4
Potencial impacto agregado del cambio climático



Fuente: Red Europea de Observación para el Desarrollo Territorial y la Cohesión (Programa ESPON 2020 EU)

Realizaciones

La *Estrategia de Seguridad Nacional* 2017 incluye la "Preservación del Medio Ambiente" como uno de sus quince ámbitos y marca varias líneas de acción para conseguir ese objetivo.

En este sentido, el *Plan Nacional de Adaptación al Cambio Climático* es un elemento clave que, junto con otros planes y estrategias debe llegar a ser parte fundamental de la Seguridad Nacional y en particular de la seguridad medioambiental.

Cooperación internacional y cumplimiento de compromisos asumidos

En diciembre se celebró en Madrid bajo Presidencia Chilena la XXV Conferencia Internacional sobre el Cumbre del Clima

En diciembre se celebró en Madrid bajo Presidencia Chilena, la XXV Conferencia Internacional sobre el Cumbre del Clima (COP25). La Convención supuso un enorme esfuerzo organizativo para España, que se saldó positivamente, habiéndose recibido más de 20.000 personas de 195 países, más de 50 Jefes de Estado, Gobierno y altos mandatarios de organizaciones internacionales y dando cabida a la representación de gran número de organizaciones y asociaciones de la sociedad civil, que se involucraron enormemente y demostraron en todo momento la alta preocupación por la evolución climática, siendo muy especialmente destacable la participación de jóvenes de todo el mundo.

Si bien no se logró concluir alguno de los objetivos marcados, en particular en lo referente al Artículo 6 del Acuerdo de Paris relativo a los mercados de carbono, mecanismos que permiten el intercambio de derechos de emisiones, sí se adoptó un acuerdo que sienta las bases para que en 2020 los países presenten compromisos de reducción de emisiones más ambiciosos. También se concretaron otras importantes iniciativas, entre las que destacan un mecanismo de daños y pérdidas para destinar recursos a los países más vulnerables y afectados por fenómenos climáticos extremos y un *Plan de Acción de Género* para desarrollar medidas que den respuesta al efecto desigual del cambio climático en mujeres y niñas.

En el ámbito europeo, las líneas sobre las que se está trabajando en el actual marco de negociación para definir la PAC *post* 2020, continúan avanzando significativamente en su contribución a la atenuación del cambio climático y la adaptación a sus efectos; en la gestión eficiente de recursos naturales (agua, suelo, aire) y en la contribución a la protección de la biodiversidad. Para ello se avanza en el diseño en una arquitectura medioambiental de pagos que contemple la condicionalidad reforzada y en un nuevo incentivo para la preservación, los ecoesquemas.

En lo relacionado con la actividad ganadera, siguen los esfuerzos por reducir su impacto sobre el medio ambiente, en el marco de los compromisos internacionales relacionados con los gases de efecto invernadero. En torno al 12% del total de GEI son de origen agrícola–ganadero. El sector agrario (agricultura y ganadería) se encuentra incluido entre los sectores difusos de emisión de gases de efecto invernadero, participando en las emisiones totales de los difusos con un 12%. De acuerdo al *Plan Estratégico de Energía y Clima* presentado por España debe con-

tribuir a la mitigación del Cambio Climático con una reducción del 18% en sus emisiones en 2030 respecto de los niveles de 2005.

Por su parte, el CIEMAT ha seguido participando de forma activa en el Programa LIFE, instrumento financiero de apoyo a través de la financiación de proyectos de conservación medioambientales y el desarrollo de la política y legislación comunitaria en materia medioambiental, colaborando con otras instituciones, centros y empresas nacionales en las diferentes convocatorias que este programa ha lanzado.

Dentro del mismo programa, el Ministerio de Defensa continúa su participación en el proyecto BIOXISOIL para la recuperación de suelos afectados por hidrocarburos, mediante la combinación de procesos biológicos y de oxidación química, principalmente en terrenos del Arsenal de la Carraca (Cádiz).

CIEMAT también trabaja en la Alianza Europea sobre Cambio Climático ECRA; forma parte de la delegación española del Convenio de Minamata de contaminación de suelos por Mercurio, de la Red Ibérica de Investigación en Montaña para estudiar los efectos producidos por el cambio climático y de la delegación española del Convenio de Ginebra sobre cargas críticas de contaminantes en el aire; y participa en la misión de Horizonte Europa sobre ciudades inteligentes y neutras en carbono.

Por lo que se refiere a la lucha contra delitos medioambientales, el Consejo de la UE definió el delito medioambiental como una prioridad para el Ciclo Político 2018-2021, creando la EMPACT de Medio Ambiente en el que España desarrolla funciones de coliderazgo a través de la Guardia Civil. En 2019, de las 20 Acciones Operativas del proyecto, España lideró tres, colideró seis y participó en otras nueve.

Asimismo, en el marco del Programa de la UE EL PAcCTO, se están llevando a cabo una serie de actividades relacionadas con los delitos medioambientales dirigidas por expertos de la Guardia Civil y se está creando una red de expertos en investigación de delitos medioambientales con países latinoamericanos. Esta red (denominada Red Jaguar) ya está coordinando operaciones en el ámbito del tráfico de especies, contaminación atmosférica, minería ilegal, tráfico de mercurio, etc.

Este Cuerpo Policial también ejerce la copresidencia de la red EnviCrimeNet, red de expertos en delincuencia medioambiental, cuya presidencia es rotatoria entre España, Francia e Italia, correspondiéndole a España en 2020.

El informe SOCTA, emitido por Europol en 2017, también incluyó los delitos contra el medio ambiente como una de las ocho áreas de amenazas prioritarias en la lucha contra el crimen organizado y, ese mismo año, se creó en Europol un *Analysis Project* específico de lucha contra los delitos medioambientales, al que se incorporó un especialista de la Guardia Civil. En septiembre de 2019 se incorporó un especialista de la Guardia Civil al Programa de Seguridad Medioambiental de Interpol en Buenos Aires (Argentina).

Igualmente, en el Informe RHIPTO (2018) de Interpol (*Atlas Illicit Flows*) se ha considerado la delincuencia medioambiental como la tercera tipología delictiva más lucrativa del mundo.

En el marco del *Plan de acción de la UE contra el tráfico de especies silvestres*, articulado a nivel nacional por el *Plan TIFIES*, se han iniciado las actuaciones necesarias para materializar la creación en el seno del SEPRONA de la Oficina Central Nacional de análisis de información sobre actividades ilícitas medioambientales, con el propósito de centralizar, analizar y difundir la información referente a este tipo de actos ilícitos y de servir de punto de contacto y coordinación a nivel nacional e internacional.

En reconocimiento por diversas operaciones relacionadas con la lucha contra el comercio ilegal de gases fluorados de efecto invernadero, el SEPRONA y la Fiscalía Coordinadora de Medio Ambiente fueron distinguidas por la ONU en la ceremonia regional del Galardón Mundial del Protocolo de Montreal para agentes de aduanas y policías (*Global Montreal Protocol Award For Customs and Enforcement Officers*), evento organizado por el Programa de las Naciones Unidas para el Medio Ambiente "OzonAction", el Ministerio de Ecología y Recursos Naturales de Ucrania y el Programa de la ONU para el Desarrollo de Ucrania.

El SEPRONA también ha sido galardonado con el Premio Derechos Humanos de la Abogacía Española, categoría de "Instituciones" (XXI Edición de 2019), por su labor en la defensa de los derechos humanos a través de la protección del medio ambiente y por su compromiso con los Objetivos de Desarrollo Sostenible de la ONU.

Coordinación entre componentes del sector público y cooperación público privada

La Oficina Española de Cambio Climático lidera un grupo de adaptación al cambio climático que coordina a todas las Comunidades Autónomas en este ámbito y en el que participa, entre otros, el CIEMAT. Mediante diversas encomiendas de gestión, CIEMAT también coopera con el Ministerio para la Transición Ecológica en temas de calidad del aire, inventarios de emisiones y mapas de contaminación nacional.

La iniciativa del *Libro Verde de la Gobernanza del Agua*, impulsada desde el Ministerio para la Transición Ecológica, busca abrir espacios de debate y generar propuestas de mejora en colaboración con los actores institucionales y las partes interesadas. El objetivo es avanzar en la construcción colaborativa de un modelo de gobernanza del agua que permita hacer frente a los retos presentes y futuros a los que se enfrenta la gestión del agua.

El Ministerio de Defensa, en colaboración con la Fundación Iberdrola España, en el marco del Bosque Defensa-Iberdrola, plantó más de 70.000 árboles, creando una cubierta vegetal que servirá no solo para evitar la erosión y servir de refugio de fauna, sino que supone la creación de un sumidero de CO2 que contribuirá a compensar las emisiones de gases de efecto invernadero.

Adaptación y mitigación del cambio climático y disminución de la contaminación atmosférica y acústica

Los organismos públicos de investigación y universidades, continúan los avances científicos y tecnológicos en el ámbito de la preservación del medio ambiente financiados por la Agencia Estatal de Investigación, entre los que destacan: la obtención y producción de bioestimulantes en el marco del desarrollo de la economía circular, la formulación de propuestas financieras y tributarias dirigidas a conseguir la protección ambiental y la conservación de los recursos naturales a partir del modelo productivo circular, y la integración de las tecnologías de fitorecuperación de suelos contaminados y la producción de bioenergía (biogás) a partir de la biomasa y subproductos. CIEMAT también lleva a cabo proyectos de I+D en calidad del aire, conservación de suelos, remediación y restauración ambiental.

Por su parte, el Ministerio de Defensa ha creado un Grupo de Trabajo sobre Cambio Climático, y ha realizado un *Plan de Actuaciones en materia de cambio climático*, además de contribuir al *Plan Nacional de Adaptación al Cambio Climático*.

Asimismo, pretende completar la implementación de Sistemas de Gestión Ambiental (SGA) conforme a la Norma UNE ISO 14001 en los Recintos Militares. En la actualidad dispone de 188 Recintos Militares con certificación ambiental y se encuentra en proceso de implementación en otros 30 recintos más. Además, ha iniciado la implementación de un Sistema de Gestión Ambiental Conjunto que agrupe a todas la Yeguadas Militares.

Respecto de la contaminación atmosférica, en el marco del *Plan Aire* del Ministerio para la Transición Ecológica, AEMET ha extendido hasta dos días de alcance la predicción de concentraciones de contaminantes y de un índice global de calidad del aire de acuerdo con la normativa europea. En esta línea, AEMET ha firmado un convenio con la Comunidad Autónoma de Madrid para desarrollar un sistema de predicción de contaminantes urbanos de alta resolución.

En cuanto a la contaminación acústica, por parte de Adif se están elaborando los Mapas Estratégicos de Ruido y los Planes de Acción, con el objeto de luchar contra dicha contaminación.

Actuaciones en el marco de las aguas continentales

Están en marcha, en las 25 demarcaciones hidrográficas españolas, los trabajos de preparación de los planes hidrológicos de tercer ciclo de la Directiva Marco del Agua (2022-2027). Antes de finales de 2021 estos planes sustituirán a los de segundo ciclo, actualmente vigentes para el periodo 2016-2021.

El 1 de agosto de 2019, se anunció el inicio del proceso de consulta pública de la revisión y actualización de los mapas de peligrosidad y riesgo de inundación de las demarcaciones hidrográficas del Cantábrico occidental, Guadalquivir, Ceuta, Melilla, Segura y Júcar y de la parte española de las demarcaciones hidrográficas del Cantábrico oriental (en el ámbito de competencia de la Administración General del Estado), Miño-Sil, Duero, Tajo, Guadiana y Ebro.

Actualmente se están ejecutando diversas actuaciones dentro del Plan PIMA-Adapta-AGUA 2019. Estas actuaciones, a desarrollar entre 2017 y 2020, siguen las cuatro líneas estratégicas de PIMA-Adapta: medidas de gestión y adaptación de las reservas naturales fluviales, adaptación a los fenómenos extremos, evaluación del impacto del cambio climático en los recursos hídricos y desarrollo de estrategias de adaptación y desarrollo de proyectos de adaptación al cambio climático en el dominio público hidráulico.

Conservación, prevención y respuesta en costas y medio marino

Desde que se aprobase en 2017 la *Estrategia de Adaptación al Cambio Climático de la Costa Española*, se está trabajando en la mejora de las metodologías y de la información existente, para poder acotar la incertidumbre asociada a la predicción de los impactos de erosión e inundación costeros, considerando los efectos del cambio climático, y poder hacer un uso eficiente de los recursos disponibles.

En 2019, se presentaron las proyecciones regionales de cambio climático de variables marinas necesarias para el estudio de impactos costeros a lo largo de toda la costa española, que se encuentran disponibles para su descarga desde la página web del Ministerio para la Transición Ecológica y el Reto Demográfico.

También se avanzó en la redacción de las Estrategias para la Protección de la Costa de Cádiz, Málaga, Almería y Baleares, considerando los efectos del cambio climático, con financiación del Programa de Apoyo a las Reformas Estructurales de la Unión Europea, en la elaboración del Plan de Protección del litoral del Delta del Ebro y se encuentra en su fase final de elaboración el *Plan para la Protección del Borde Litoral de Mar Menor*.

Para la protección de la costa se llevaron a cabo diversas actuaciones con cargo al presupuesto de inversión de la Dirección General de Sostenibilidad de la Costa y del Mar, que, para 2019 ascendió a casi 61 millones de euros. Cabe destacar la redacción de varias de las actuaciones previstas en las Estrategias para la Protección de la Costa de Huelva, Maresme (Barcelona), Castellón, Valencia y Granada.

En el ámbito normativo, se aprobó *el Real Decreto 79/2019, de 22 de febrero, por el que se regula el informe de compatibilidad y se establecen los criterios de compatibilidad con las estrategias marinas*. Esta norma establece el procedimiento administrativo y los contenidos a tener en cuenta a la hora de elaborar el informe de compatibilidad establecido en el artículo 3.3 de la *Ley 41/2010, de 29 de diciembre, de protección del medio marino*.

Se han publicado los documentos de las tres primeras fases del segundo ciclo de las estrategias marinas de España (2018-2024). Estos documentos consisten en una actualización de la evaluación del estado ambiental del medio marino, de la definición del buen estado ambiental, y de los objetivos ambientales de las estrategias marinas, que fueron aprobados por Acuerdo de Consejo de Ministros (BOE nº 142, de 14 de junio de 2019).

Igualmente, se ha continuado con la elaboración de planes de gestión de los espacios marinos protegidos de competencia estatal. En concreto se ha sometido a consulta pública el Proyecto de Real Decreto por el que se amplía el Área Marina Protegida "El Cachucho" y se aprueba la actualización de su plan de gestión. También se han realizado múltiples talleres participativos para la actualización de los planes de gestión de las 24 Zonas Especiales de Canarias.

En 2019, han continuado los ejercicios y operaciones relacionados con la contaminación marina. SASEMAR ha liderado el ejercicio nacional de lucha contra la contaminación marítima en Málaga y se han realizado ejercicios provinciales de lucha contra la contaminación en Huelva, en los que ha participado la UME. Junto a las autoridades francesas se ha llevado a cabo un ejercicio de lucha contra la contaminación en aguas francesas dentro del *Plan Golfo de León de cooperación entre Francia y España para lucha contra la contaminación marina.*

Por su parte, durante el mes de octubre, la Guardia Civil ha desarrollado una vez más la operación *30 días en el mar*, coordinada por Interpol y Europol, y destinada a detectar posibles vertidos en el mar y emisiones contaminantes a la atmósfera procedentes de buques. La operación se desarrolla en los puertos y aguas territoriales de las provincias costeras españolas.

En este sentido, los servicios de inspección de las Capitanías Marinas continúan realizando inspecciones del contenido de azufre de los combustibles marinos, habiendo realizado inspecciones a 1065 buques y análisis del contenido de azufre a 212 muestras de combustibles marinos.

Por otro lado, en cumplimiento del convenio internacional para el control y la gestión del agua de lastre y los sedimentos de los buques, se han emitido los certificados exigidos para la flota española.

Asimismo, se ha realizado el control de la emisión de los Documentos de Cumplimiento exigidos por el Reglamento de la Unión Europea sobre el control de las emisiones de CO2 tanto de buques españoles como extranjeros que arriban a puertos españoles y se han comunicado a la OMI los datos anuales de consumo de combustible de toda la flota española.

Iniciativas de carácter preventivo, de respuesta y de recuperación en materia de incendios forestales

El Ministerio de Agricultura, Pesca y Alimentación despliega anualmente un amplio número de medios de extinción, entre aeronaves de gran capacidad, Brigadas de Refuerzo contra Incendios Forestales (BRIF), unidades móviles de análisis y planificación, aeronaves de coordinación y observación y aeronaves pilotadas por control remoto, que se distribuyen por todo el territorio nacional para prestar apoyo a las Comunidades Autónomas.

Durante 2019, en la extinción de incendios forestales, los medios aéreos del Ministerio de Agricultura, Pesca y Alimentación realizaron un total de 1.464 intervenciones (715 en 2018), volando un total de 4.178 horas en incendio (1.842 para 2018) y realizando 17.044 descargas so-

bre las llamas (8.786 en 2018). En cuanto a la intervención de las BRIF en la campaña 2019 trabajaron 2.147 horas en incendios (774 horas en 2018), en 287 intervenciones (149 en 2018) y realizando un total de 213.582 metros de línea combatida (101.958 metros en 2018).

Por su parte, el Ministerio de Defensa dispone de 38 Planes Técnicos de Defensa contra Incendios aprobados por el Ministerio de Agricultura, Pesca y Alimentación que dan cobertura a unas 100.000 ha. También ha firmado con las Comunidades Autónomas nueve Procedimientos Operativos de Actuación para la lucha contra incendios forestales.

Gestión adecuada de residuos

Durante 2019 ha incrementado el número de inspecciones realizadas en la gestión de residuos, iniciándose procedimientos sancionadores a los notificantes que se ha podido comprobar que estaban llevando a cabo traslados ilícitos.

En este sentido, el Ministerio para la Transición Ecológica ha llevado a cabo colaboraciones con el SEPRONA en la acción operativa sobre el tráfico de residuos derivados de las baterías al final de su vida útil del proyecto EMPACT, y con el Departamento de Aduanas e Impuestos Especiales de la Agencia Tributaria en el marco de la operación DEMETER V, para el seguimiento y control de los movimientos transfronterizos de residuos, con especial énfasis en los residuos plásticos, con el fin de identificar países o regiones exportadoras e importadoras emergentes a nivel mundial, todo ello según lo dispuesto en el Convenio de Basilea.

Asimismo, se han firmado dos Convenios para la Encomienda de Gestión del Ministerio para la Transición Ecológica a las Comunidades Autónomas de cara a la realización en el territorio de la comunidad autónoma de las inspecciones de traslado de residuos desde o hacia terceros países no pertenecientes a la UE, en concreto con el Principado de Asturias y la Junta de Extremadura, uniéndose al convenio firmado en 2018 con la Comunidad Autónoma de Castilla y León.

Por su parte, Adif ha llevado a cabo la gestión de los residuos generados en el mantenimiento y conservación de cualquier tipo de infraestructuras ferroviarias y ha realizado el control ambiental de los procesos de desherbado químico de la plataforma ferroviaria y de sus márgenes de influencia. Adicionalmente, se ha hecho cargo de la gestión ambiental de los suelos contaminados en las infraestructuras ferroviarias tanto en lo relativo a los derivados de procesos de contaminación histórica (anteriores a la constitución de Adif en 2005), como a los originados en accidentes e incidencias en la circulación o en las instalaciones ferroviarias. Todo ello en estrecha coordinación con Renfe y el resto de operadores ferroviarios.

GLOSARIO

A

ACNUR	Alto Comisionado de Naciones Unidas para los Refugiados
ACT	Action counterterrorism for Lebanon
Adif	Administrador de Infraestructuras Ferroviarias
AEA	Sistema Aéreo de Protección Electrónica Activa
AEAT	Agencia Estatal de Administración Tributaria
AECID	Agencia Española de Cooperación Internacional para el Desarrollo
AEMET	Agencia Estatal de Meteorología
AENA	Aeropuertos Españoles y Navegación Aérea
AESA	Agencia Estatal de Seguridad Aérea
AOC	Centro de Operaciones Aéreas
API	Advanced Passenger Information
AVSEC	Aviation Security Committee

B

BEA	Buen Estado Ambiental
BMD	Defensa Contra Misil Balístico
BOE	Boletín Oficial del Estado
BRIF	Brigadas de Refuerzo contra Incendios Forestales

C

CATE	Centro de Atención Temporal de Extranjeros
CCAES	Centro de Coordinación de Alertas y Emergencias Sanitarias
CCN	Centro Criptológico Nacional
CDCT	Comité del Consejo de Europa contra el Terrorismo
CDTI	Centro de Desarrollo Tecnológico e Industrial

CEAC	Conferencia Europea de Aviación Civil
CECOA	Centro de Coordinación y Alerta
CENEM	Centro Nacional de Seguimiento y Coordinación de Emergencias
CERT	Computer Emergency Response Team
CETI	Centros de Estancia Temporal de Inmigrantes
CIAF	Comisión de Investigación de Accidentes Ferroviarios
CIAIAC	Comisión de Investigación de Accidentes e Incidentes de Aviación Civil
CIEMAT	Centro de Investigaciones Energéticas, Medioambientales y Energéticas
CIFAS	Centro de Inteligencia de las Fuerzas Armadas
CITCO	Centro de Inteligencia contra el Terrorismo y el Crimen Organizado
CNE	Centro Nacional de Epidemiología
CNEC	Centro Nacional de Excelencia en Ciberseguridad
CNI	Centro Nacional de Inteligencia
CNM	Centro Nacional de Microbiología
CNPIC	Centro Nacional de Protección de Infraestructuras y Ciberseguridad
CORES	Corporación de Reservas Estratégicas de Productos Petrolíferos
COSI	Cooperación Operativa en materia de Seguridad Interior
COVE	Centro de Operaciones de Vigilancia Espacial
CSIC	Consejo Superior de Investigaciones Científicas
CSIRT	Computer Security Incident Response Team
CSUR	Centros, Servicios y Unidades de Referencia
CTBTO	Comprehensive Nuclear Test Ban Treaty Organization

D

DSN	Departamento de Seguridad Nacional
DAESH	Al Dawa al Islamyia fil Iraq wal'Sham
DDoS	Distributed Denial of Service

E

ECDC	Centro Europeo de Control de Enfermedades
ECHA	European Chemicals Agency
ECSO	Organización Europea de Ciberseguridad

EEB	Encefalopatía Espongiforme Bovina
EMASoH	European Maritime Surveillance Mission in the Strait of Hormuz
EMPACT	Plataforma Europea Multidisciplinar contra las Amenazas Criminales
ENAIRE	Gestor de la navegación Aérea en España y el Sáhara Occidental
ENISA	Agencia Europea para la Seguridad de las Redes y de la Información
ENL	Ejército Nacional de Libia
ETA	Euskadi Ta Askatasuna
EUBG	European Union Battle Group
EUNAVFOR	European Union Naval Forces
Europol	Oficina Europea de Policía
EUTM	EU Traning Mission
EL-PAcCTO	Europa Latinoamérica - Programa de Asistencia contra el Crimen Transnacional Organizado

F

FACE	Fuerzas Armadas Convencionales en Europa
FAS	Fuerzas Armadas
FATCA	Foreign Account Tax Compliance Act
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
FEINDEF	Feria Internacional de Defensa y Seguridad
FIIAPP	Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas
Frontex	Agencia Europea de la Guardia de Fronteras y Costas

G

GAFI	Grupo de Acción Financiera Internacional
GAR-SI	Groupes d'Action Rapides – Surveillance et Intervention
GEI	Gases de Efecto Invernadero
GOIF	Grupo Operativo de Inteligencia Financiera
GSN	Grupo de Suministradores Nucleares

H

HOIS	Hostile Intelligence Services
HRA	High Risk Area

I

I+D+i	Investigación, Desarrollo e Innovación
ICEX	Instituto de Comercio Exterior

INCIBE	Instituto Nacional de Ciberseguridad
INDNR	Pesca Ilegal, No Documentada y No Reglamentada
INTA	Instituto Nacional de Técnica Aeroespacial
Interpol	Organización Internacional de Policía Criminal
IoT	Internet de las cosas
ISCIII	Instituto de Salud Carlos III

J

JIMDDU	Junta Interministerial reguladora del comercio exterior de Material de Defensa de Doble Uso
JPCOA	Joint Comprehensive Plan of Action

L

LABIR	Laboratorio de Verificación Rápida
LANDSEC	Expert Group on Land Transport Security

M

MCCD	Mando Conjunto de Ciberdefensa
MENA	Middle East and North Africa
MINUSTAH	Misión de Estabilización de las Naciones Unidas en Haití
MTCR	Régimen de Control de Tecnología de Misiles

N

NAFO	North Atlantic Fishing Organization
NASA	National Aeronautics and Space Administration
NBQ	Nuclear, Biológico y Químico
NEAFC	North East Atlantic Fisheries Commission
NMI	NATO Mission Iraq
NRBQ	Nuclear, Radiológico, Biológico y Químico
NRF	NATO Response Force
NRI	NATO Readiness Initiative

O

OACI	Organización Internacional de Aviación Civil
OAV	Oficina de Asistencia a Víctimas de Accidentes Aéreos y Familiares
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OIEA	Organismo Internacional de Energía Atómica
OMI	Organización Marítima Internacional
OMS	Organización Mundial de la Salud

ONU	Organización de las Naciones Unidas
ONS	Oficina Nacional de Seguridad
OPAQ	Organización para la Prohibición de las Armas Químicas
OPE	Operación Paso del Estrecho
OPEP	Organización de Países Exportadores de Petróleo
OMI	Organización Marítima Internacional
ORGA	Oficina de Recuperación y Gestión de Activos
OSCE	Organización para la Seguridad y Cooperación en Europa
OTAN	Organización del Tratado del Atlántico Norte

P

PAC	Política Agrícola Común
PACIAP	Programa Anual de Control Integral de la Actividad Pesquera
PARP	Planning and Review Process
PCSD	Política Común de Seguridad y Defensa
PNIEC	Plan Nacional Integrado de Energía y Clima
PESCO	Permanent Structured Cooperation
PIB	Producto Interior Bruto
PIC	Protección de Infraestructuras Críticas
PIF	Puestos de Inspección Fronterizos
PLACI	Pre-loading Advance Cargo Information
PNACC	Plan Nacional de Adaptación al Cambio Climático
PNR	Passenger Name Record
PPE	Planes de Protección Específicos
PSI	Proliferation Security Initiative
PSO	Planes de Seguridad del Operador

R

RDT	Remote Data Transmission
RE-LAB	Red de Laboratorios de Alerta Biológica
RENAIN	Red Nacional de Información
RPAS	Remotely Piloted Aircraft

S

S3T	Spanish Space Surveillance & Tracking
SASEMAR	Sociedad Española de Salvamento Marítimo

SEPBLAC	Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias
SEPRONA	Servicio de Protección de la Naturaleza
SGA	Sistemas de Gestión Ambiental
SGSI	Sistema de Gestión de Seguridad de la Información
SHARP	Strengthened International Health Regulations and Preparedness
SIPE	Sistema de Información Pesquero Español
SIVE	Sistema Integrado de Vigilancia Exterior
SOCTA	Serious and Organized Crime Threat Assessment
SST	Space Surveillance and Tracking
START	Strategic Arms Reduction Treaty

T

TESSCO	Terrorismo, Espionaje, Sabotaje, Subversión y Crimen Organizado
TIC	Tecnologías de la Información y la Comunicación
TNP	Tratado de No Proliferación de armas nucleares

U

UAS	Unmanned Aircraft Systems
UE	Unión Europea
UNAMA	United Nations Assistance Mission in Afghanistan
UME	Unidad Militar de Emergencias
UNIFIL	United Nations Interim Force in Lebanon
UNSMIL	Misión de Apoyo de las Naciones Unidas en Libia
UNODC	United Nations Office on Drugs and Crime

V

VCR	Vehículo de Combate sobre Ruedas
VJTF	Very High Readiness Joint Task Force

ANEXO:

ANÁLISIS DE RIESGOS PARA LA SEGURIDAD NACIONAL 2019/2022

DSN

ÍNDICE

PRESENTACIÓN

El análisis de riesgos es una iniciativa novedosa en España, por cuanto es la primera vez que se elabora una evaluación multidimensional de las amenazas y desafíos a la Seguridad Nacional en el plano político-estratégico de forma integral. Este estudio ofrece una visión conjunta de cuáles son los riesgos que se perciben con una mayor intensidad en función de su nivel de impacto y grado de probabilidad.

El análisis toma como referencia las amenazas y los desafíos establecidos en la Estrategia de Seguridad Nacional 2017. Lejos de tratarse de un conjunto estático de quince elementos que transcurren en paralelo, su concepción se basa en una fuerte interrelación y dinamismo entre los mismos. De esta forma, uno de los propósitos de este estudio metodológico es ofrecer un punto de reflexión estratégica, dirigido a la sociedad en su conjunto, y en particular, a través de sus representantes en las Cortes, en cumplimiento al artículo 5 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, y promover la cultura de Seguridad Nacional.

La elaboración de la primera edición del análisis de riesgos a la Seguridad Nacional en España ha sido posible gracias a la participación de una red de expertos -ciento dieciséis personas procedentes de la Administración Pública, del sector privado y del ámbito de la ciencia y la investigación- que han contribuido a la elaboración de este documento con su conocimiento y experiencia.

De alguna forma, este propio informe es la mejor muestra de agradecimiento a su valiosa y desinteresada colaboración.

INTRODUCCIÓN

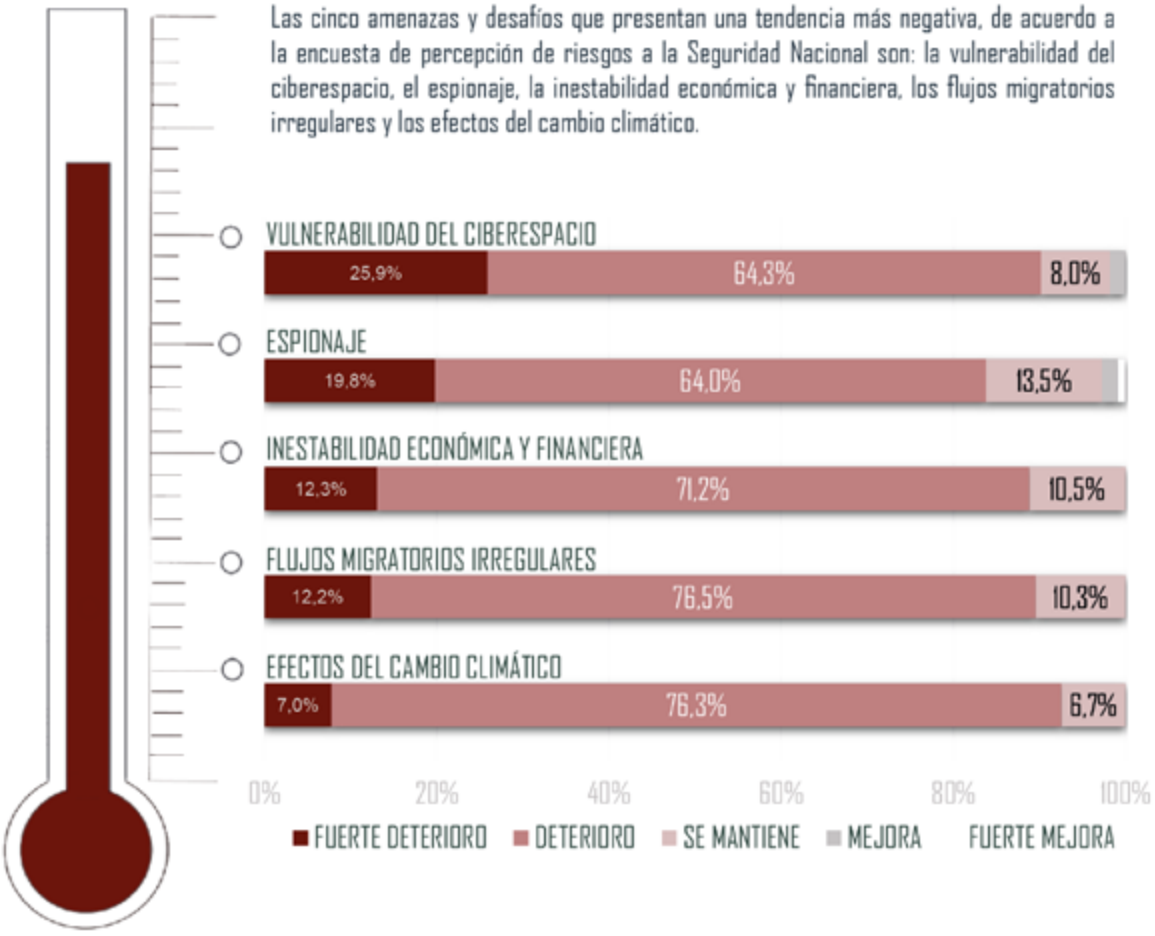


Figura 1
Barómetro de riesgos

INTRODUCCIÓN

El proceso de análisis de riesgos es un elemento central en el planeamiento estratégico de la Seguridad Nacional. La valoración de las amenazas y los desafíos, su evolución y la identificación de otros nuevos, forman parte del necesario análisis de contexto para articular el marco político-estratégico de la Seguridad Nacional. En este marco, se presenta, en el seno del Consejo de Seguridad Nacional, el primer informe de análisis de riesgos.

La información ofrecida en este estudio es el resultado del análisis de los datos recogidos en una encuesta de percepción de los riesgos para la Seguridad Nacional. En el proceso han participado personas de la Administración Pública, del sector privado y de los ámbitos del conocimiento y la investigación. En esta primera edición, la red de expertos ha estado conformada por un total de 116 personas.

El documento, que toma como referencia el conjunto de las quince amenazas y desafíos establecidos en la Estrategia de 2017, realiza una valoración de los mismos con base en dos dimensiones: el nivel de impacto y el grado de probabilidad. La parametrización permite obtener un diagnóstico integral y normalizado, al considerar todos y cada uno de los diferentes ámbitos que componen la Seguridad Nacional con una misma regla de medición y de una forma conjunta y coherente con uno de los rasgos más notables del esquema estratégico: su alto grado de interrelación.

El primer elemento del informe es un análisis a corto plazo, una imagen de la situación actual, titulada "Situación 2020". Su representación gráfica, denominada "mapa de riesgos", es uno de los productos destacados. Este gráfico ordena visualmente las quince amenazas y desafíos de la Estrategia de Seguridad Nacional 2017 según su grado de peligrosidad. Aquellas percibidos con un mayor impacto y probabilidad de que eventualmente ocurran, ocupan la denominada "zona de peligro". Es el caso de la vulnerabilidad del ciberespacio, elemento identificado en el análisis 2019-2020 como el de mayor relevancia.

Otro producto analítico incorporado en el documento de este año es el apartado titulado "Horizonte 2022". Se trata de una proyección a tres años de la posible evolución (mejora o deterioro) de los cuarenta y tres factores analizados. Ejemplos son la fragmentación del multilateralismo, las amenazas híbridas o la desinformación. Una selección de los factores permite el diseño de un escenario central, aquel que se estima como de mayor probabilidad, y un escenario alternativo, denominado "adverso" que podría eventualmente darse en caso de deterioro de los factores determinantes.

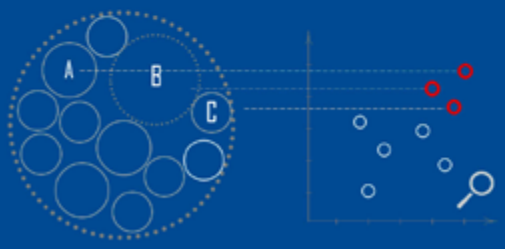
El análisis de riesgos se configura como elemento de referencia para una reflexión amplia sobre el estado de la Seguridad Nacional. Su contenido, con proyección temporal máxima a un plazo de tres años, contribuirá a valorar la evolución del entorno de seguridad de una forma metodológica y basada en parámetros cuantificables sobre el que articular la Política de Seguridad Nacional.

Además, este proceso, de carácter abierto y no clasificado, está orientado a contribuir al mandato de la Ley relacionado con la cultura de Seguridad Nacional, mediante la transmisión al ciudadano de una información transparente de los fenómenos que afectan directamente a su seguridad.

METODOLOGÍA

METODOLOGÍA: PASO A PASO

1 Situación 2020: mapa de riesgos



2 Horizonte 2022: tendencias a 3 años

3 Generación de escenarios

Figura 2
Metodología: paso a paso

METODOLOGÍA

Marco doctrinal estratégico

En el contexto temporal de la realización de la Estrategia de Seguridad Nacional se recogieron varios factores de peso que ofrecían una actualización al análisis geopolítico en 2017. La rápida transformación del contexo de seguridad obliga a una constante evaluación de las tendencias, los desafíos y las amenazas. Las nuevas realidades dibujan un escenario de doble cara: la tecnología, motor de avance y progreso, es empleada como vector desafiante. El cambio climático ya es concebido ampliamente como una amenaza a la seguridad. La capacidad de metamorfósis de las redes terroristas y del crimen organizado añade complejidad en un escenario donde la mayor competencia geopolítica traslada fragilidad a la arquitectura global y a la defensa del orden internacional basado en normas.

La visión multidimensional de la Seguridad Nacional se presenta en la Estrategia a través de un conjunto de quince amenazas y desafíos que, lejos de tratarse de un planeamiento lineal y paralelo, se muestran altamente interrelacionados y dibujan un escenario complejo y volátil.

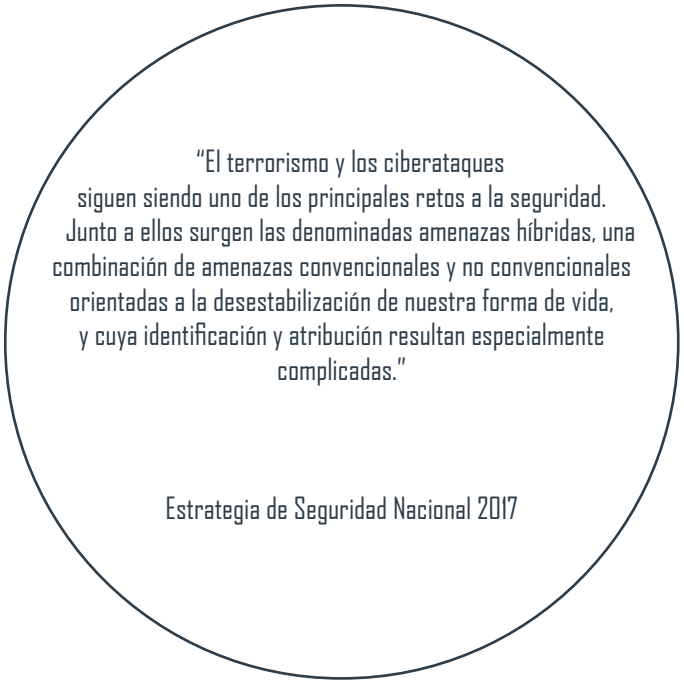


Figura 3
Texto de la introducción de la Estrategia de Seguridad Nacional 2017

Su capítulo cuarto describe los principales factores que afectan a la Seguridad Nacional y los agrupa en cuatro bloques: amenazas, amenazas y desafíos en los espacios comunes globales, amenazas sobre las infraestructuras críticas y desafíos.

De acuerdo a la Estrategia de Seguridad Nacional 2017, se entiende por "amenaza" aquel factor que compromete o puede socavar la Seguridad Nacional. Por otro lado, se considera un "desafío" aquel que, sin tener de por sí entidad de amenaza, incrementa la vulnerabilidad, provoca situaciones de inestabilidad o puede propiciar el surgimiento de otras amenazas, agravarlas o acelerar su materialización.

Proyección temporal

El análisis de los riesgos a la Seguridad Nacional es un ejercicio de corto y medio plazo, y no de prospectiva a largo plazo.

Son dos los motivos.

En primer lugar, el ciclo estratégico en España es de cinco años. De acuerdo al artículo 4 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, la Estrategia "se elabora a iniciativa del Presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico".

Consecuentemente, y dado que la actual Estrategia de Seguridad Nacional fue promulgada el 1 de diciembre de 2017, el proceso de revisión estratégica, donde el análisis de riesgos forma parte fundamental para la articulación de la Política de Seguridad Nacional, la nueva estrategia deberá ver la luz en 2022.

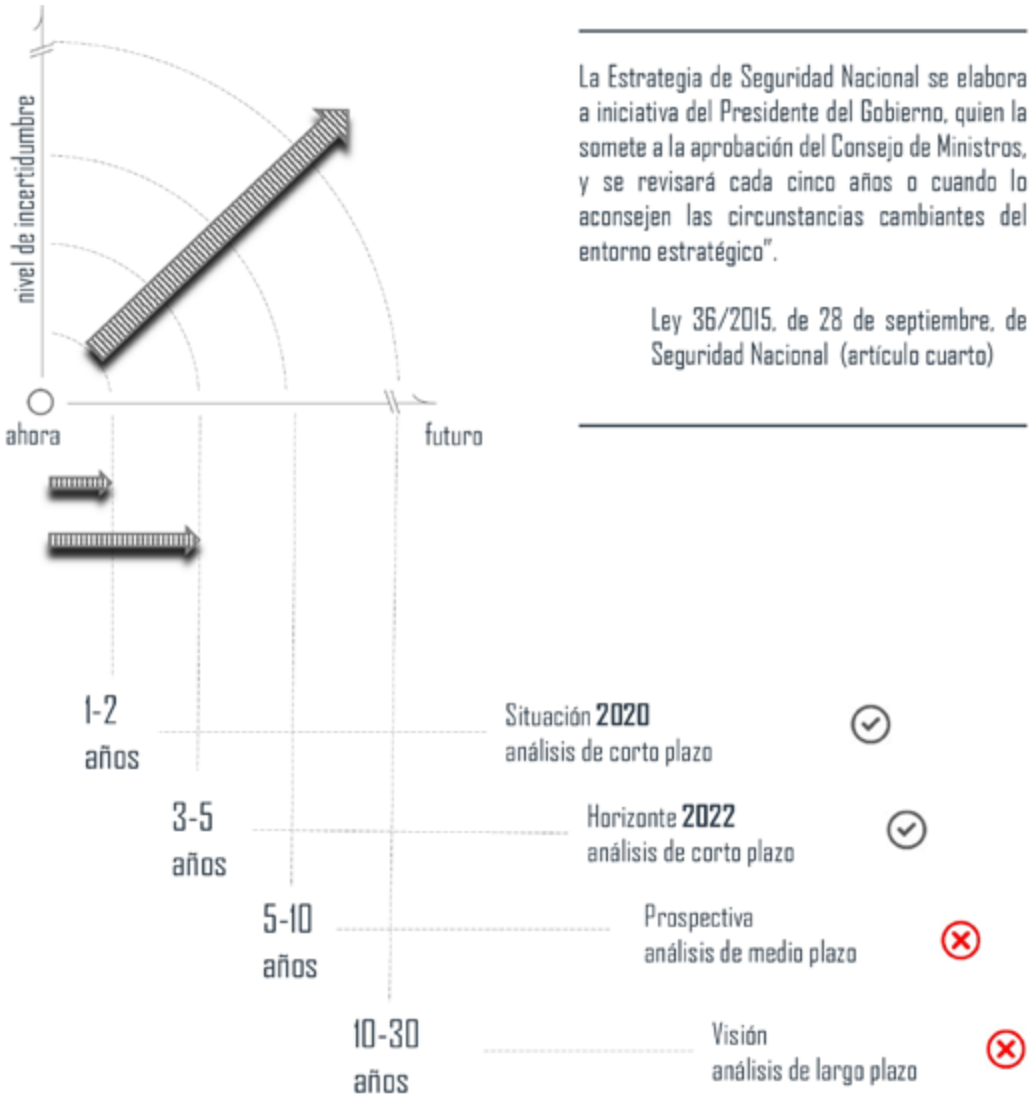
La razón para adoptar este criterio es la sincronización del análisis de riesgos dentro del proceso general de revisión estratégica.

En segundo lugar, a medida que se extiende el periodo de tiempo cubierto, aumenta el grado de incertidumbre del análisis efectuado. El análisis está concebido con una proyección temporal de corto y medio plazo.

Desde esta perspectiva de corto y medio plazo, el método empleado desarrolla dos bloques principales:

"Situación 2020", de cobertura temporal de doce meses, y cuya representación gráfica, el mapa de riesgos, ofrece una fotografía del paisaje de los riesgos a la Seguridad Nacional de carácter actual;

"Horizonte 2022", análisis de tendencias a tres años vista. Su propósito es ofrecer una percepción de la mejora o el deterioro de la situación de seguridad en el plazo de tres años. En este apartado se genera un escenario central de riesgo, basado en la selección de aquellos factores que se consideran determinantes, y un escenario alternativo, denominado "escenario adverso", de menor probabilidad de que tenga lugar, y con base en un hipotético deterioro de la evolución.



La Estrategia de Seguridad Nacional se elabora a iniciativa del Presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico".

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional (artículo cuarto)

Figura 4
Metodología: proyección temporal

De las amenazas y desafíos al concepto de riesgo: cuantificación de las variables "impacto", "probabilidad" y "tendencia"

La parametrización permite disponer de un criterio objetivo basado en indicadores sobre el que acometer una ordenación. El diagnóstico de la situación de la Seguridad Nacional se lleva a cabo mediante la cuantificación, de acuerdo a un marco metodológico estandarizado, de las quince amenazas y desafíos a la Seguridad Nacional previamente identificados en la Estrategia de 2017.

Las dos variables objeto de análisis son el nivel de impacto y el grado de probabilidad.

La escala empleada es la siguiente:

GRADO DE PROBABILIDAD		NIVEL DE IMPACTO	
1.	Muy improbable	1.	Mínimo
2.	Poco probable	2.	Menor
3.	Probable	3.	Moderado
4.	Posible	4.	Severo
5.	Muy posible	5.	Catastrófico

Figura 5
Escalas para el grado de probabilidad y el nivel de impacto

Formalmente, para cada uno de los desafíos o amenazas (denominados con las siglas "da", su grado de impacto y su probabilidad son calculados matemáticamente según la fórmula del promedio, esto es:

Nivel de Probabilidad(da) = 1/N Σ_1^n(PROBABILIDAD(da,N))

Grado de Impacto(da) = 1/N Σ_1^n(IMPACTO(da,N))

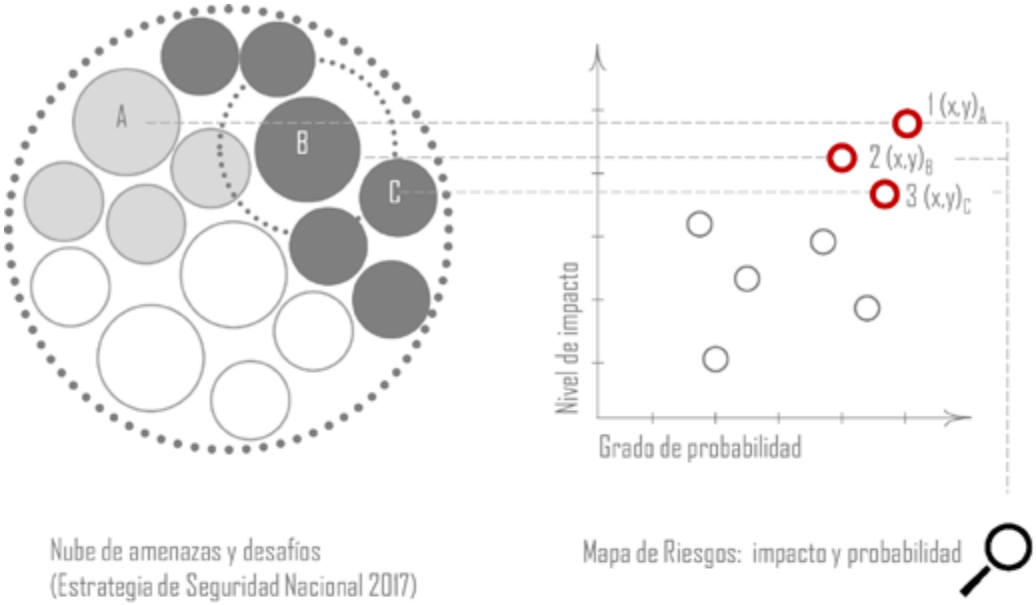
Donde "N" es el número de respuestas para un determinado desafío o amenaza.

Además, el proceso incorpora un estudio de tendencias (tercera variable del análisis) que toma como referencia la evolución de cuarenta y tres factores seleccionados en el plazo de tres años, que permite diseñar escenarios de riesgo con proyección a 2022.

La valoración de la variable "tendencia" se realiza mediante la selección de una opción (notable deterioro, deterioro, mantenimiento de la situación, mejora, notable mejora) en una escala de valores comprendidos del "1" a "5", donde la valoración más baja se corresponde con la opción de notable deterioro. La valoración de la variable tendencia (t) se obtiene mediante la aplicación de la siguiente fórmula:

Tendencia(t) = 1/N Σ_1^n(TENDENCIA(t,N))

Donde "N" es el número de respuestas para un determinado desafío o amenaza.



Nube de amenazas y desafíos
(Estrategia de Seguridad Nacional 2017)

Mapa de Riesgos: impacto y probabilidad

Horizonte 2022: tendencia

Figura 6
Metodología: conceptualización del riesgo

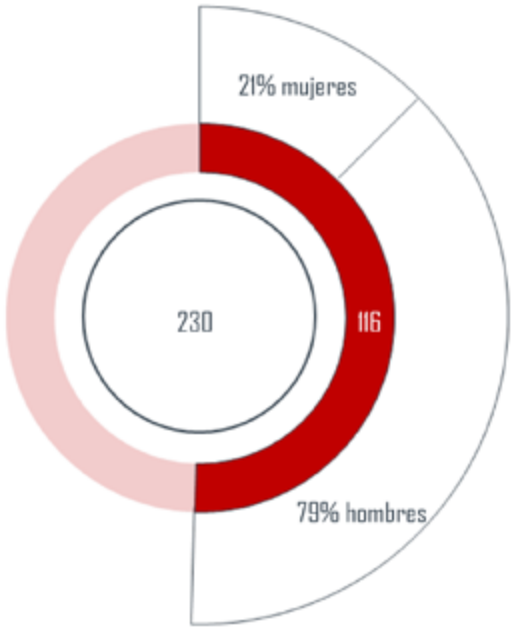
Método de obtención: la encuesta de percepción de riesgos para la Seguridad Nacional

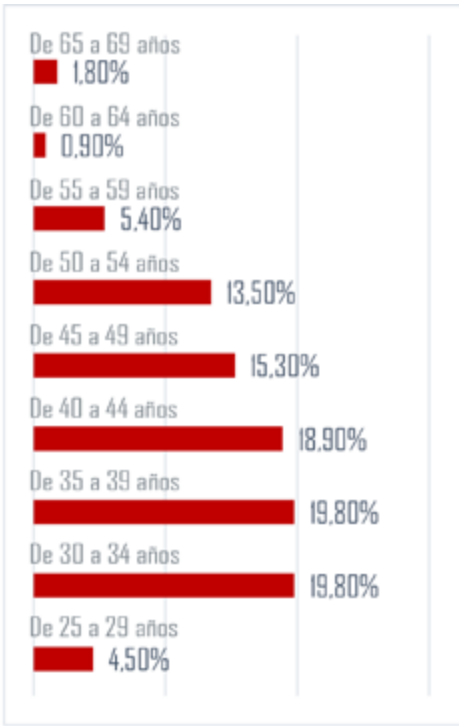
Se adopta como método de obtención de datos la "Encuesta de Percepción de Riesgos para la Seguridad Nacional".

El diseño de la encuesta, que incorpora un total de 43 preguntas, ha sido elaborado con la información incorporada en el capítulo cuarto de la Estrategia de Seguridad Nacional 2017 (Amenazas y Desafíos).

Para cada una de las preguntas, la encuesta solicita la selección de una opción de las tres variables de estudio: el nivel de impacto, el grado de probabilidad y la posible evolución de un determinado factor de acuerdo a las escalas señaladas en el apartado anterior.

El análisis de los resultados se complementa con un análisis contextual basado en informes de referencia emitidos por organismos oficiales a nivel nacional, europeo internacional, y con el proceso interno de generación de conocimiento a través de la organización por ámbitos del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno.





Figuras 7 y 8
Radiografía de la masa crítica: distribución por sexo y edad

Red de expertos

La red de expertos funcionales está formada por los siguientes:

- Vocales de todos los Comités Especializados de Apoyo al Consejo de Seguridad Nacional. Estos órganos son el Comité de Situación, el Consejo Nacional de Seguridad Marítima, el Consejo Nacional de Ciberseguridad, el Comité Especializado de Seguridad Energética, el Comité Especializado de Inmigración y el Comité Especializado de no Proliferación de Armas de Destrucción Masiva.

  De acuerdo a sus respectivas normas de funcionamiento y composición, establecidas mediante acuerdos del Consejo Nacional de Seguridad, los vocales de los comités son personas procedentes de los diferentes departamentos ministeriales y organismos con competencias relacionadas con la Seguridad Nacional y con rango asimilado a subdirector general o superior.

- Organización por ámbitos de la Seguridad Nacional, formada actualmente por treinta y dos analistas del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno.

- Todos aquellos expertos procedentes de la Administración o de la sociedad civil (universidad, centros de pensamiento, organizaciones o empresas) que el Director del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno ha estimado oportuno incorporar a la red por su amplio conocimiento, experiencia acreditada o prestigio reconocido.

A todas estas personas se les ha solicitado su participación en el proceso de análisis y evaluación de las amenazas y los desafíos a la Seguridad Nacional mediante la cumplimentación de una encuesta. De esta forma, se disponía de una masa crítica inicial de 230 personas. El número de encuestas recibidas finalmente en el proceso 2019/2020 ha sido de 116.

Figura 9
Distribución por ámbitos funcionales

SITUACIÓN 2020

SITUACIÓN 2020

SITUACIÓN 2020

El entorno de seguridad cambiante configura un paisaje de riesgos a la Seguridad Nacional en continua transformación. La evolución del terrorismo internacional en estos últimos años, el aumento de la competencia geopolítica o el impacto de la ciberseguridad y la disrupción tecnológica son tendencias que nos dibujan un contexto que, lejos de ser una foto fija, se asemeja más a un mapa dinámico y móvil.

"Situación 2020" ofrece dos elementos: el mapa de riesgos y el apartado "Seguimiento", donde se analiza con un mayor grado de profundidad la dimensión tecnológica y, en concreto, las implicaciones para la seguridad derivadas de la implantación de las redes 5G.

El primer apartado es el mapa de riesgos, un gráfico de análisis integral para el conjunto de las quince amenazas y desafíos identificados en la Estrategia de 2017. El mapa de riesgos a la Seguridad Nacional es una representación gráfica lineal de doble dimensión, donde el eje de las abscisas está conformado por los valores del parámetro "probabilidad" y el eje de las ordenadas lo forman los valores del parámetro "impacto".

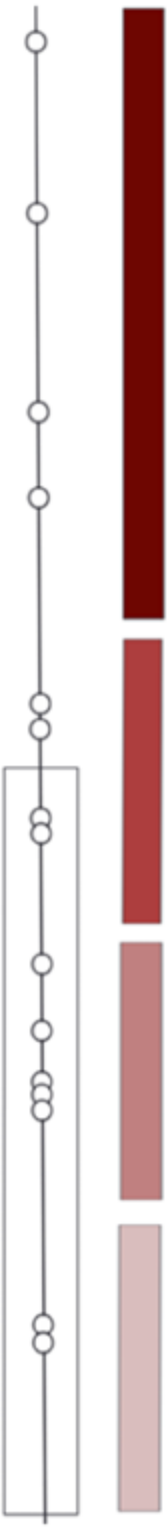
En la superficie gráfica delimitada por los dos ejes, "X" e "Y" estarán representados los quince desafíos y amenazas a la Seguridad Nacional de acuerdo a los valores asignados para cada uno de ellos.

El mapa de riesgos se complementa con un apartado donde se evalúa con mayor grado de profundidad aquel riesgo clasificado con una mayor peligrosidad. Este apartado de detalle lleva por título "Seguimiento: vulnerabilidad del ciberespacio".

Este segundo apartado es un análisis de cinco factores de carácter predominantemente tecnológico y asociados a la vulnerabilidad del ciberespacio: el acceso a la información y los datos sensibles, los ciberataques, el uso ilegítimo del ciberespacio para llevar a cabo actividades ilícitas, como por ejemplo acciones de desinformación, propaganda o financiación del terrorismo, los ciberataques específicamente dirigidos contra las infraestructuras críticas, y las amenazas para la seguridad y la competitividad económica derivadas de las tecnologías disruptivas.

El apartado "Seguimiento" se complementa con un apartado específico, denominado "Foco 5G", apoyado en el análisis de riesgos elaborado por la Comisión Europea el 9 de octubre de 2019 titulado "EU Coordinated risk assessment of the cybersecurity of 5G networks".

Análisis a corto plazo



El análisis de los resultados obtenidos ofrece un mapa donde la valoración conjunta de los riesgos a la Seguridad Nacional se encuentra en el rango alto de la escala de riesgos. Los valores obtenidos son de 3,4 para la variable "impacto" (moderado-severo) y de 3,6 para el "grado de probabilidad" (probable-posible) en una escala de 0 a 5.

Los tres factores que ocupan de forma destacada la parte alta de la tabla son la vulnerabilidad del ciberespacio, el espionaje y la inestabilidad económica y financiera.

Los flujos migratorios irregulares, pese a la fuerte disminución del número de llegadas de inmigrantes irregulares a las costas españolas en 2019, del 55% con respecto al año anterior, y los efectos del cambio climático ocupan la cuarta y quinta posición, respectivamente.

La vulnerabilidad energética, las emergencias y catástrofes y las amenazas a las infraestructuras críticas ocupan las posicions intermedias en la tabla, junto a aquellas amenazas que tradicionalmente se asocian de una forma más estrecha con los actos ilícitos y la violencia física, como son el crimen organizado, el terrorismo y los conflictos armados. La vulnerabilidad de dos espacios comunes globales, el mar y el espacio aéreo y ultraterrestre, se encuentran asimismo es este grupo intermedio.

Finalmente, los dos últimos factores son la proliferación de armas de destrucción masiva y las epidemias y pandemias. Si bien los resultados del análisis les asignan los dos últimos puestos en el ranking, su nivel de impacto es de "moderado-severo", y se encuentran en la zona comprendida entre los niveles "probable" y "poco probable".

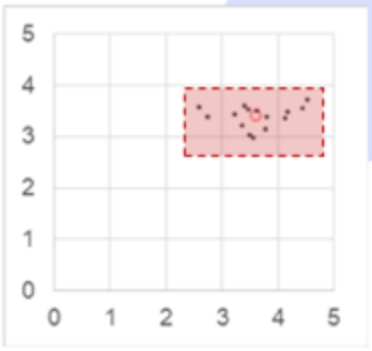
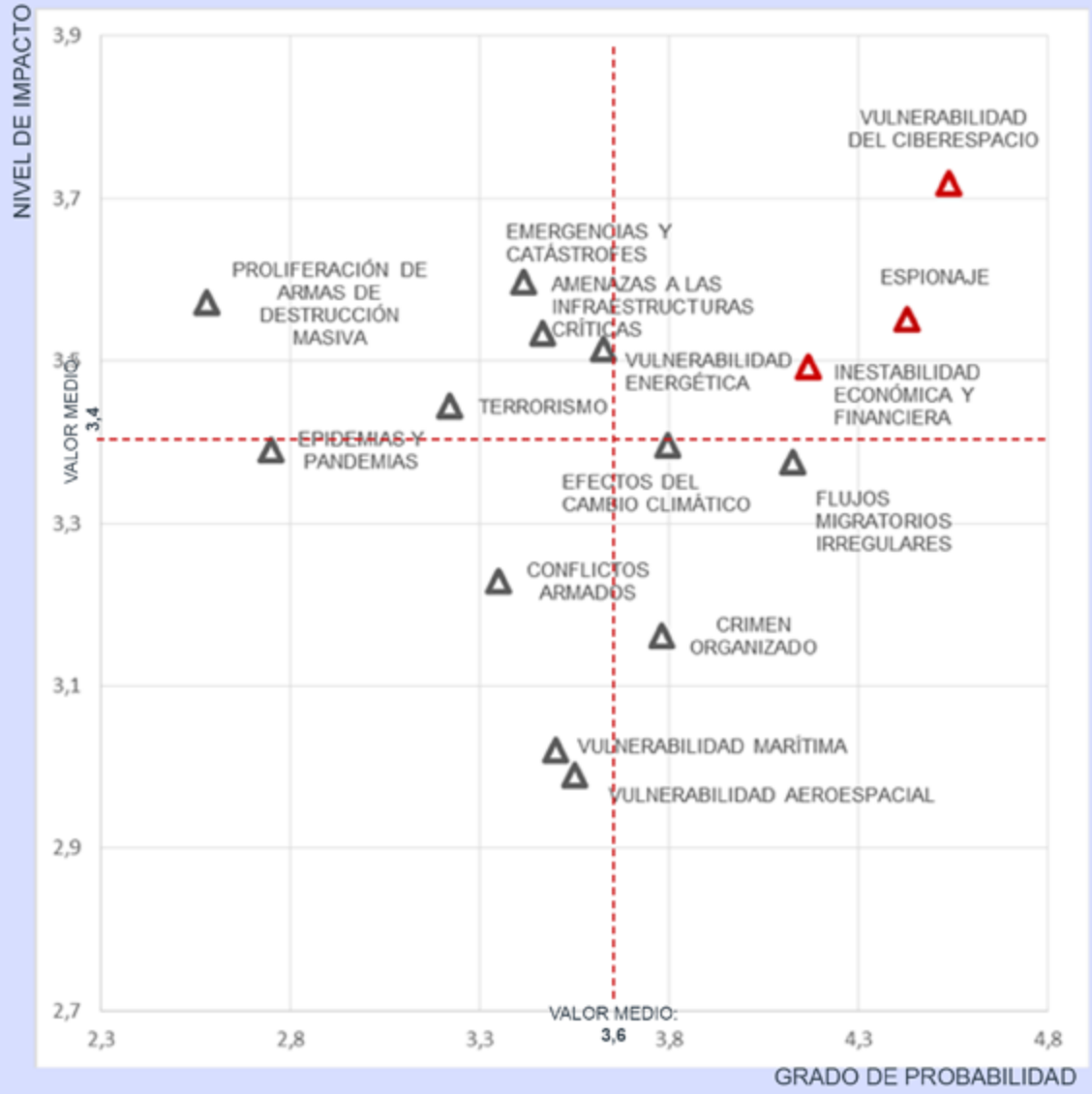


Figura 10
Mapa de riesgos

Mapa de Riesgos



LOS 5 RIESGOS DE MAYOR IMPACTO

1. VULNERABILIDAD DEL CIBERESPACIO
2. EMERGENCIAS Y CATÁSTROFES
3. PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA
4. ESPIONAJE
5. AMENAZAS A LAS INFRAESTRUCTURAS CRÍTICAS

LOS 5 RIESGOS DE MAYOR PROBABILIDAD

1. VULNERABILIDAD DEL CIBERESPACIO
2. ESPIONAJE
3. INESTABILIDAD ECONÓMICA Y FINANCIERA
4. FLUJOS MIGRATORIOS IRREGULARES
5. EFECTOS DEL CAMBIO CLIMÁTICO

Seguimiento: vulnerabilidad del ciberespacio

La ciberseguridad es uno de los ámbitos de la Seguridad Nacional que está experimentando una mayor transformación y a una mayor velocidad de cambio.

La Estrategia de Ciberseguridad Nacional, aprobada en 2019, describe el ciberespacio como "un vector de comunicación estratégico, 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 amenazas híbridas". Este concepto de ciberespacio 2.0. amplía el espectro de la concepción más tradicional de la ciberseguridad hacia la protección de la información y los datos personales.

De especial atención en 2019 ha sido la seguridad de los procesos electorales, con la celebración de las elecciones europeas, generales y autonómicas en el mes de mayo. Según datos de la Unión Europea, el 83% de las personas encuestadas considera que las noticias falsas son una amenaza para la democracia. Asimismo, el estudio, realizado en diciembre de 2018, muestra que el 73% de los usuarios de internet están preocupados por la desinformación on-line en los periodos pre-electorales.

La nube de dispersión muestra como la práctica totalidad de datos recogidos en la encuesta de análisis de riesgos se encuentran en el cuadrante superior derecho (zona de riesgo) de forma muy destacada.

En términos de nivel de impacto y probabilidad, el uso ilegítimo del ciberespacio, la desinformación y el acceso indebido a la información y datos sensibles son los factores que ha obtenido los resultados más elevados del escalafón en ambas dimensiones.

Las implicaciones para la seguridad de nuevas tecnologías, como la Inteligencia Artificial, el Internet de las Cosas, el almacenamiento en la nube, se muestran al alza. Se trata de un sector en continuo crecimiento y con un grado de penetración alto en la actividad socioeconómica, con repercusiones para el ciudadano, el sector privado y las Administraciones Públicas.

Figura 11
Riesgos de ciberseguridad

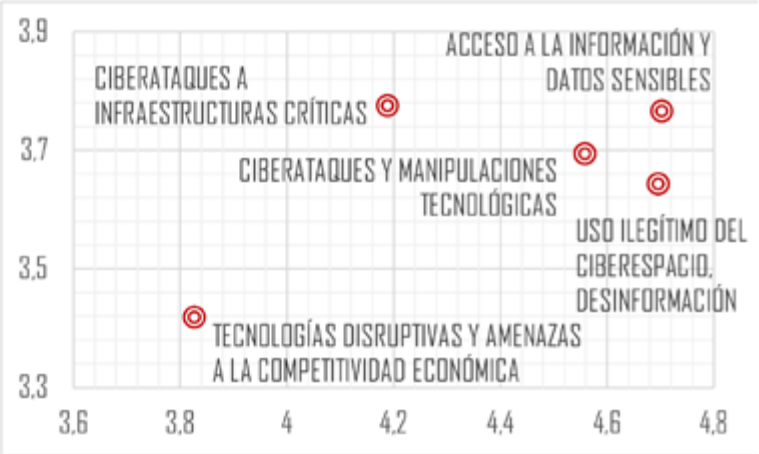


Figura 12
Nube de dispersión

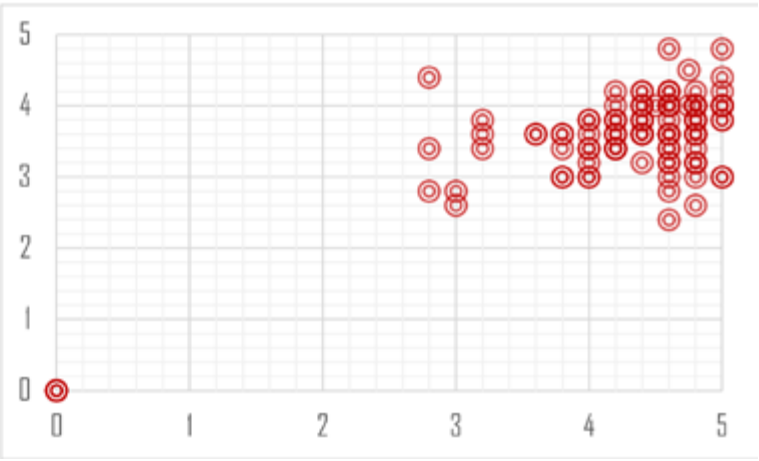
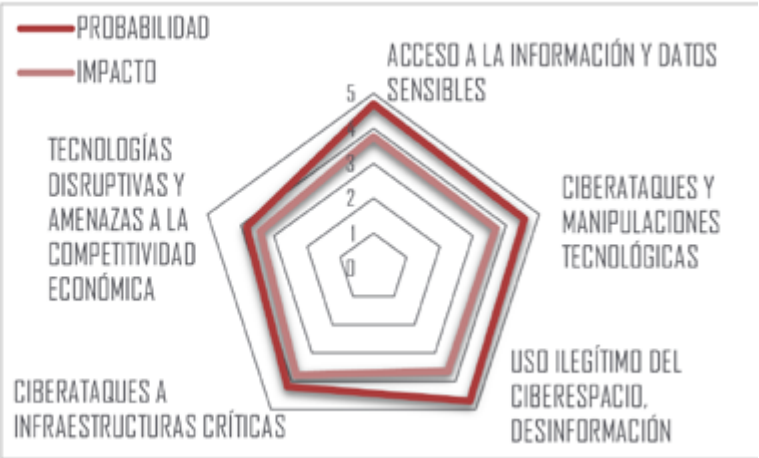


Figura 13
Gráfico dimensional



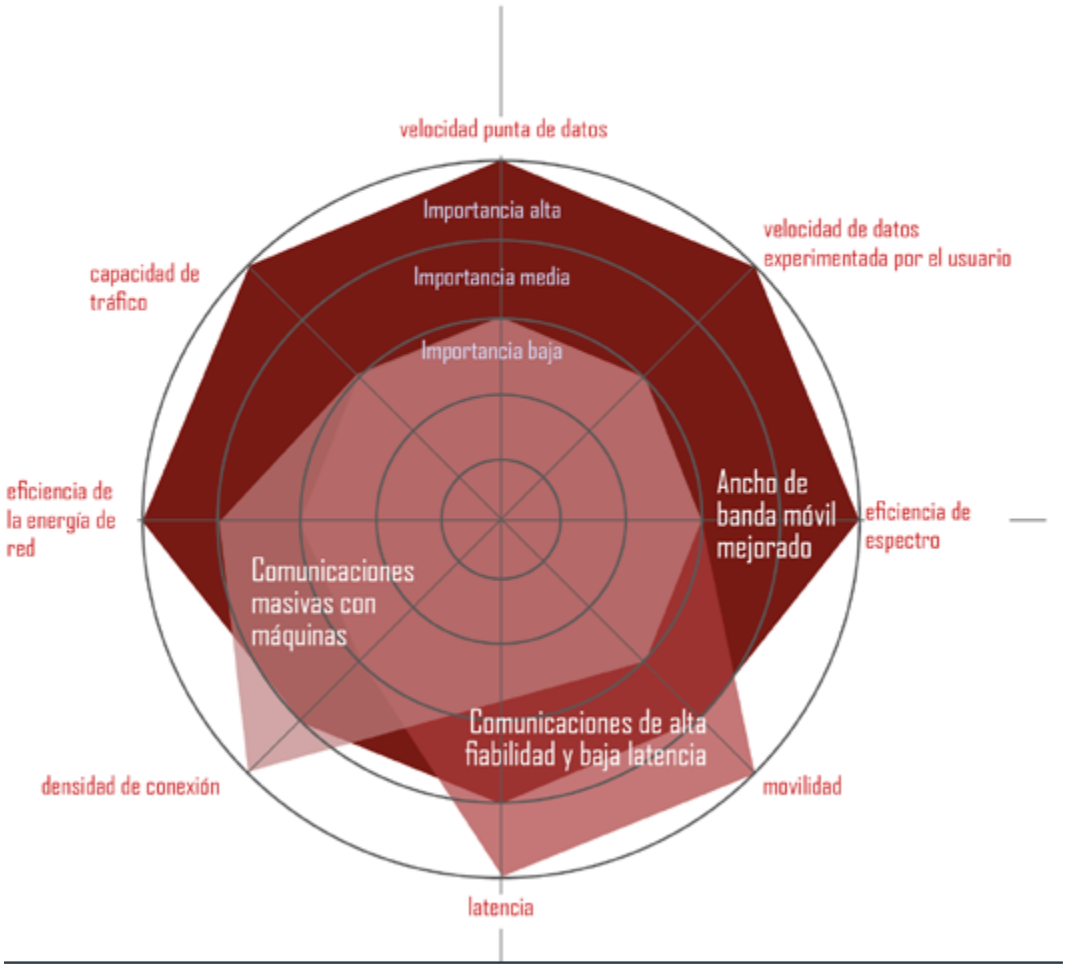
Foco 5G

5G es una tecnología de telecomunicaciones inalámbricas de gran ancho de banda, baja latencia y alta fiabilidad. Su gran velocidad (veinte veces más rápida que el Internet actual) permite el desarrollo de servicios avanzados que incluyen el Internet de las Cosas, la robótica a gran escala, o soluciones de realidad virtual, entre otros.

La implantación de las redes 5G tiene implicaciones para la Seguridad Nacional. Más allá del desarrollo tecnológico y su gran relevancia económica (algunas proyecciones económicas cifran la cantidad de 225 billones de euros en 2025 a nivel mundial), el equilibrio de intereses acapara el debate en el plano geopolítico, donde el tejido de elementos a tener en cuenta incorpora a países, organizaciones internacionales, compañías de servicios y fabricantes a nivel mundial

En 2019, la Unión Europea publicó su análisis de riesgos 5G. El informe, elaborado con las aportaciones de sus Estados miembro, ofrece una evaluación de los principales riesgos asociados al desarrollo de la tecnología e infraestructura de red con base en el estudio de tres elementos: actores, amenazas y siuaciones de riesgo.

Figura 14
Características de las redes 5G y nivel de importancia desde una perspectiva de usuario



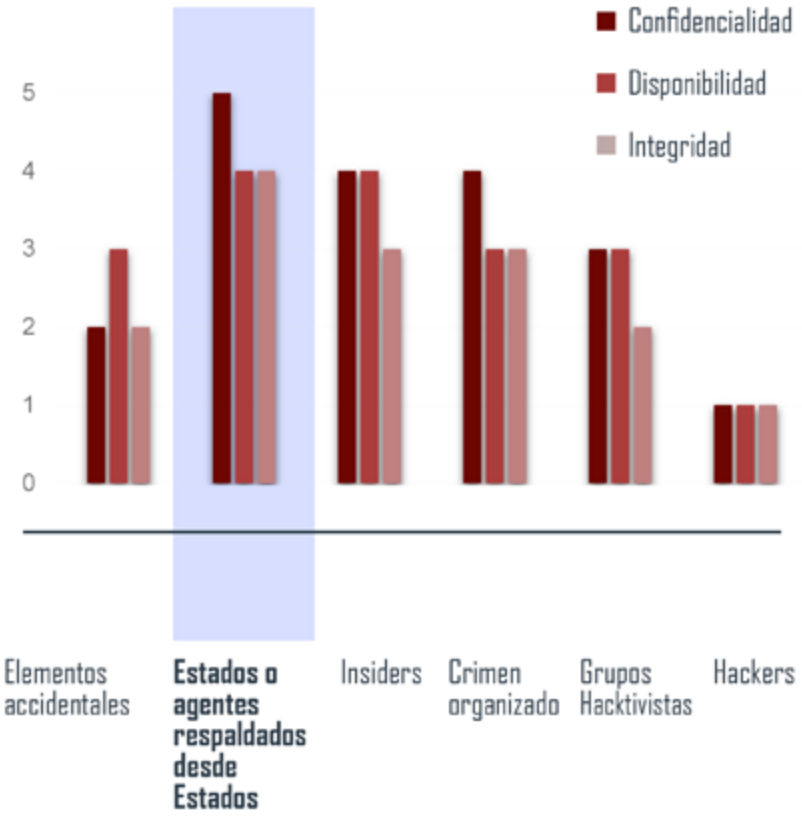
Amenazas

Con carácter general, la cadena de suministro tecnológico 5G puede verse comprometida desde tres categorías: la confidencialidad, la disponibilidad y la integridad.

De forma más concreta, la tecnología 5G se puede ver afectada por actividades como la disrupción de los servicios de red por acciones intencionadas o por accidentes, el espionaje o el robo de información a través de "puertas traseras", más conocidas por su expresión equivalente en inglés backdoors, o la destrucción o alteración de la infraestructura de red y la información digital.

Un factor diferenciador del 5G con respecto a otras tecnologías existentes es la mayor amplificación de las consecuencias en caso de producirse una disrupción del flujo de información. Estos efectos negativos pueden afectar a un mayor número de usuarios, períodos de recuperación más extendidos, pérdidas económicas más cuantiosas, un mayor número de servicios afectados, entre los que se incluyen el sector de la seguridad, y al tipo de información que circula por la red.

Figura 15
Análisis de riesgos 5G



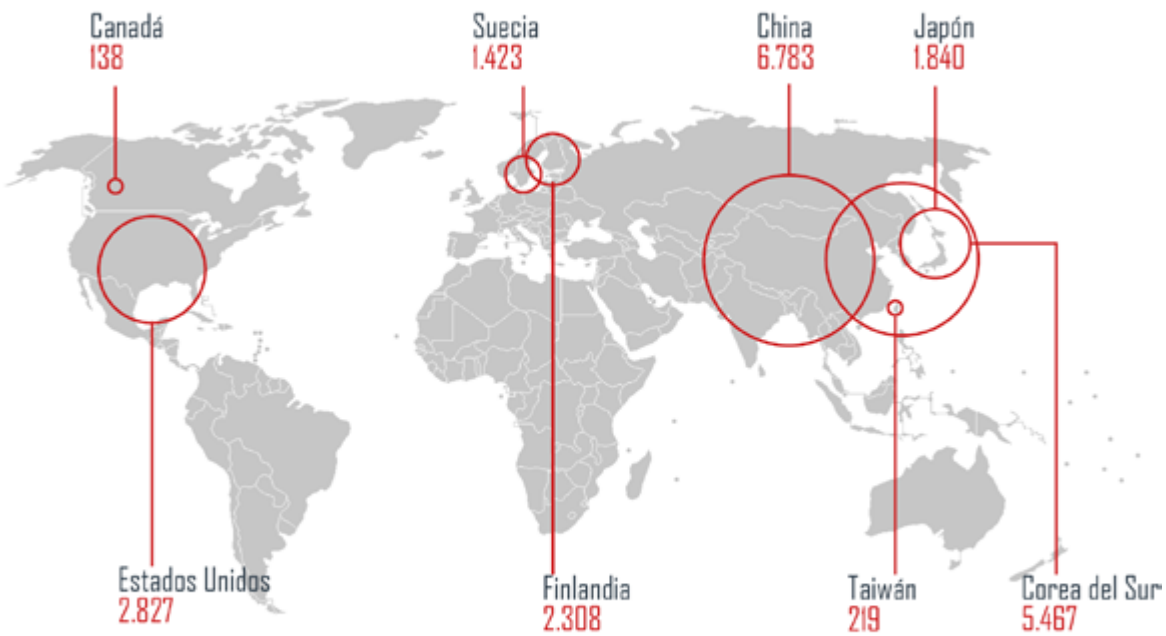
Actores

Una de las vulnerabilidades más notables de la tecnología 5G es la alta dependencia de los operadores de redes móviles, las empresas proveedoras de servicios y software, y las empresas fabricantes de elementos de infraestructura de red.

Los Estados, o los agentes respaldados desde Estados, son percibidos en el análisis de la Unión Europea como los actores que representan la amenaza más alta en función de dos variables: su capacidad y la eventual motivación para acometer acciones complejas sobre las redes 5G que pudieran acarrear consecuencias con un alto impacto negativo, por ejemplo, los ataques contra los sistemas de control de determinadas infraestructuras críticas.

Otros elementos tenidos en cuenta son el terrorismo, grupos hactivistas, insiders (empleados de compañías que trabaja para grupos de crimen organizado, terceros Estados u organizaciones hacktivistas), o las redes de crimen organizado, motivadas estas últimas por intereses económicos.

Figura 16
Número de familias de patentes 5G



DATOS: Plataforma inteligente IPlytics (actualizados a noviembre de 2019)

Situaciones de riesgo

El tercer parámetro analizado en el análisis de riesgos 5G de la Unión Europea es el relacionado con las situaciones de riesgo. Las clasifica en cinco categorías:

Los escenarios relacionados con insuficientes medidas de seguridad son aquellos derivados de un diseño deficiente que pudiera tener como consecuencias disfunciones derivadas de una configuración de seguridad deficiente de la arquitectura de red o unos controles de acceso a la red insuficientes, con efectos adversos como por ejemplo brechas de seguridad, acceso a datos sensibles, o disrupción intencionada de servicios distribuidos.

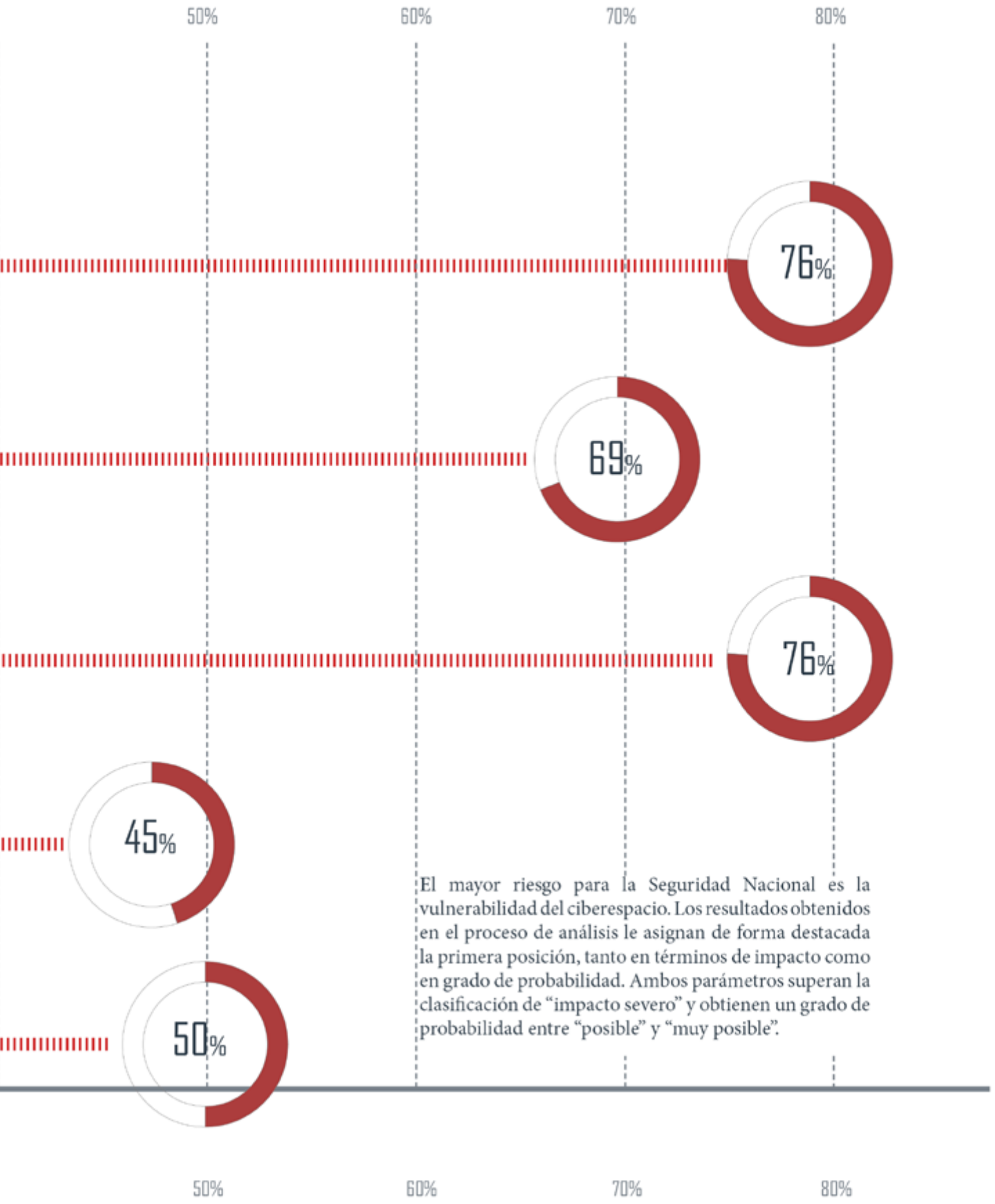
En segundo lugar, se consideran escenarios derivados de la cadena de suministro 5G. Se trata, en concreto de situaciones de vulnerabilidad debido a una excesiva dependencia de un único proveedor, tanto a nivel individual como con respecto a terceros Estados, o a deficiencias en el suministro de equipos y servicios asociados.

En tercer lugar, determinados escenarios de riesgo están directamente asociados con el propósito de causar daño de forma intencionada. En particular, ciertos Estados pueden ejercer presión sobre proveedores de servicios y equipos 5G para acometer ciberataques de acuerdo a sus intereses nacionales. Las redes de crimen organizado, o grupos hacktivistas también son tenidos en cuenta en el análisis de vulnerabilidades, donde un factor clave es el acceso a elementos de red asociadas con la seguridad, como puede ser el caso de instalaciones militares, localizaciones próximas a zonas de seguridad o infraestructuras críticas.

El cuarto caso que contempla el informe es precisamente el ataque a los sistemas de control de una infraestructura crítica, como por ejemplo una planta de generación eléctrica. Este escenario se caracteriza por su eventual alto impacto.

Finalmente, el último supuesto está asociado al fuerte incremento del Internet de las Cosas a través de redes 5G en actividades económicas que guardan relación con la seguridad. Ejemplos de estos escenarios son los sistemas automáticos de producción industrial, de control del tráfico de mercancías vía contenedores marítimos o los sensores de control medioambiental.

Figura 17
Seguimiento: vulnerabilidad del ciberespacio



El mayor riesgo para la Seguridad Nacional es la vulnerabilidad del ciberespacio. Los resultados obtenidos en el proceso de análisis le asignan de forma destacada la primera posición, tanto en términos de impacto como en grado de probabilidad. Ambos parámetros superan la clasificación de "impacto severo" y obtienen un grado de probabilidad entre "posible" y "muy posible".

HORIZONTE 2022

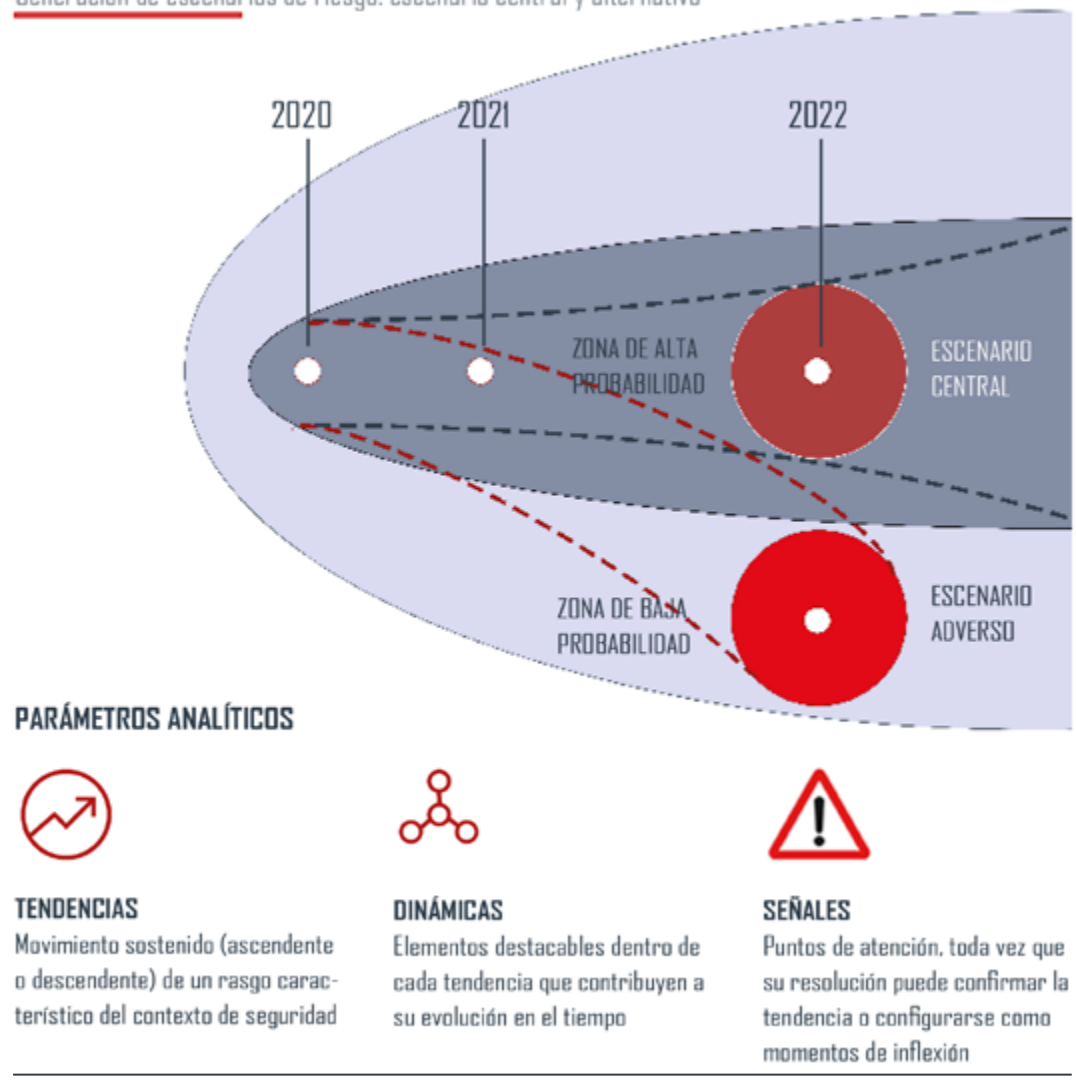
Figura 18
Perspectivas a tres años

HORIZONTE 2022: PERSPECTIVAS A TRES AÑOS

El objetivo de este apartado del análisis de riesgos es diseñar un escenario central que proyecte a 2022 un dibujo de la situación de mayor probabilidad mediante el análisis de tendencias y las principales dinámicas asociadas. Adicionalmente, a través del análisis de contexto, se identifican las potenciales señales, puntos de inflexión, que puedan ser causa de modificaciones de las tendencias proyectadas a tres años, y trasladarnos a un contexto de mayor adversidad. Esta situación alternativa se denomina "escenario adverso".

El estudio de tendencias a 2022 parte de una selección de factores. El primero de ellos son los conflictos híbridos. Cinco se caracterizan por su carácter predominantemente tecnológico: el empleo de drones, los ciberataques a las infraestructuras críticas, las manipulaciones maliciosas que afectan a elementos tecnológicos, el uso ilícito del ciberespacio y el acceso a información y datos sensibles. En tercer lugar, las políticas proteccionistas que minan el aperturismo del comercio internacional, en un contexto global económico-financiero de crecimiento débil, aparecen como uno de los factores de mayor preocupación.

Figura 19
Generación de escenarios de riesgo: escenario central y alternativo



Escenario central

El escenario central en 2022 se caracterizará por una mayor competencia entre actores globales y un debilitamiento del multilateralismo. La inestabilidad regional será especialmente acusada en Oriente Medio, África del Norte y el Sahel.

El contexto de seguridad en 2022 tendrá un marcado carácter híbrido. Se distinguirá por un mayor protagonismo del desarrollo tecnológico y el tratamiento digital de los datos como elemento de soberanía y lucha por la competitividad económica. La implementación en las instituciones, las empresas, y en la sociedad de nuevas herramientas y productos conectados a la red se producirá a un ritmo de progresión acelerado y supondrá grandes oportunidades de progreso. Sin embargo, la dependencia de la red también generará serios desafíos a la seguridad.

El débil crecimiento económico en Europa irá acompañado de dos elementos de incertidumbre geopolítica: la evolución de la guerra comercial entre las dos principales potencias, Estados Unidos y China, y el desarrollo de la futura relación entre Reino Unido y la Unión Europea tras el fin del periodo de transición que finaliza el 31 de diciembre de 2020.

Los fenómenos meteorológicos extremos, a los que España no será ajena, protagonizarán escenarios de desastres y emergencias civiles cada vez más frecuentes y de mayor repercusión social. Entre las áreas geográficas más afectadas se encuentran precisamente aquellas donde la población es más vulnerable, como es el caso del continente africano.

Figura 20
Escenario central


Fragmentación del multilateralismo
Cambio climático
Inestabilidad económica y políticas proteccionistas
Empleo generalizado de drones en zonas en conflicto
Disrupción tecnológica y ciberseguridad
Inestabilidad, violencia y terrorismo
ESCENARIO CENTRAL 2022:
Mayor competencia entre actores globales en un entorno de inestabilidad
Conexto de seguridad hibrido: predominio de los factores tecnológicos y económicos en la geopolítica
Cambio climático y seguridad

Mayor competencia entre actores globales en un entorno de inestabilidad

Tres son las dinámicas identificadas que se analizan a continuación: la fragmentación del multilateralismo, la inestabilidad en espacios estratégicos de interés para España, como Oriente Medio, África del Norte y el Sahel, y el aumento en el empleo de vehículos aéreos tripulados de forma remota en conflictos.

Fragmentación del multilateralismo

La fragmentación del multilateralismo se observa desde una doble perspectiva: la diferencia de posturas entre países en cuestiones clave para determinadas organizaciones internacionales de las que son miembros y las diferencias en el posicionamiento ante conflictos regionales y su actuación en los teatros de operaciones.

Son varios los acontecimientos en el pasado reciente que ilustran el debilitamiento de la arquitectura del sistema internacional frente a desafíos de orden global y regional. De particular preocupación resulta el ámbito de la no proliferación de armas de destrucción masiva.

En mayo de 2018, Estados Unidos anunció su retirada del Plan de Acción Integral Conjunto. Meses después, en octubre del mismo año, hizo lo propio con el Tratado de Fuerzas Nucleares de Distancia Intermedia (de 500 a 5.000 kilómetros de alcance). El primer caso inyecta un elemento de incertidumbre adicional a la ya de por sí deteriorada relación con Irán. En el segundo caso, el anuncio de suspensión vino acompañada con acusaciones de violación por parte de Rusia.

La renovación, en 2021, del Tratado de Reducción de Armas Estratégicas (START por sus siglas en inglés correspondientes a Strategic Arms Reduction Treaty) entre Estados Unidos y Rusia será determinante en esta dinámica de disolución de los principales mecanismos de control en materia de proliferación armamentística.

Arco de Inestabilidad: Oriente Medio, Norte de África y el Sahel

Desde la perspectiva de los conflictos regionales, el escenario central para 2022 continuará siendo de alta inestabilidad en el arco geográfico Sur-Este.

En Oriente Medio, la volatilidad de la situación continuará siendo una constante en la región, con implicaciones para la seguridad internacional de primer orden. Un factor de relevancia que determinará la evolución del panorama regional es la política de presencia de tropas estadounidenses en la región. La política anunciada de retirada progresiva de tropas no se está trasladando al plano de los hechos de forma lineal. Ejemplos como el repliegue del frente norte de Siria ha tenido serias consecuencias estratégicas. Por otro lado, dos de los eventos más relevantes han provocado un refuerzo del despliegue militar. Tras el ataque a la refinería petrolífera en Abqaib, en septiembre de 2019, Estados Unidos envió efectivos adicionales, sistemas de vigilancia aérea y baterías de misiles Patriot a Arabia Saudí. En el escenario iraní, tras la operación contra el general Sulemaini del 3 de enero de 2019, el refuerzo de tropas fue de 3.500 aproximadamente.

⚠ En Libia, la conferencia de Berlín de 19 de enero de 2020, con participación de todos los actores involucrados, podría haber significado un paso adelante en un conflicto que se muestra enquistado. Sin embargo, la situación dista mucho de cumplir las necesarias condiciones para un acuerdo multilateral de paz. La misión de Naciones Unidas en Libia (UNSMIL) ha denunciado recientemente violaciones del embargo de armas impuesto por Naciones Unidas. La nueva operación PCSD (Política Común de Seguridad y Defensa) anunciada en 2020 por el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad es una iniciativa que reforzará el papel de la Unión Europea como actor involucrado en la resolución efectiva de un conflicto que afecta a los intereses europeos.

⚠ Con respecto al Sahel, el deterioro de la situación de seguridad, especialmente en la zona geográfica donde se sitúa la triple frontera Burkina Faso – Mali – Niger genera sombras sobre cualquier posibilidad de mejora. Según el informe elaborado por la Oficina de Naciones Unidas para África Occidental y el Sahel (UNOWAS, por sus siglas en inglés correspondientes a la denominación United Nations Office for West Africa and the Sahel), las cifras de ataques terroristas han experimentado un devastador incremento, con más de 4.000 fallecidos en 2019. Este número multiplica por cinco el correspondiente a los de tres años anteriores. El informe de Naciones Unidas destaca, además, una fuerte interrelación entre el terrorismo, el crimen organizado y la violencia entre comunidades, con atentados contra blancos civiles y militares casi a diario. Francia, uno de los actores más activo en la zona, ha aumentado recientemente el número de efectivos en la operación Barkhane, desplegando seiscientos militares más.

Las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado seguirán centrando su esfuerzo en la contribución a las operaciones y misiones en el exterior de las organizaciones internacionales de las que España es miembro. Con el mantenimiento de la situación actual, en 2022 se podría hablar de una "cronificación" de los conflictos, con operaciones en el exterior que se extienden, en algunos casos, en más de diez años desde su inicio.

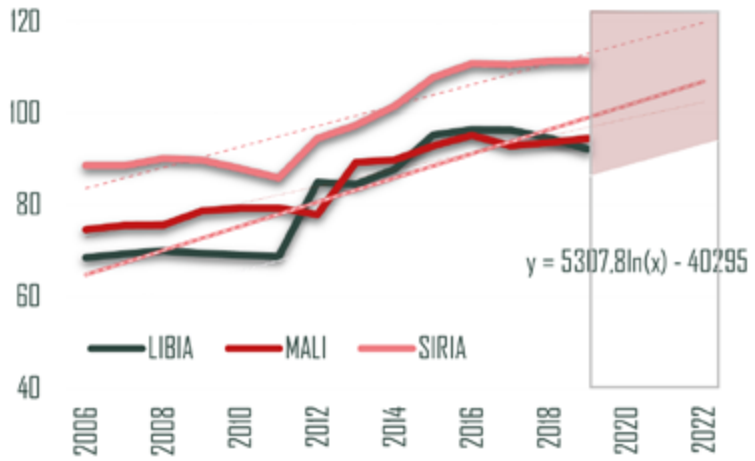


Figura 21
Evolución del índice de Estados Frágiles correspondiente a Libia, Malí y Siria

Empleo generalizado de drones en zonas en conflicto

Una de las dinámicas destacadas en el análisis, común a las zonas de conflicto, es el aumento en el empleo de vehículos aéreos tripulados de forma remota (drones).

Desde la década de los años 90, donde los drones comenzaron a ser usados para tareas de vigilancia y reconocimiento aéreo en la guerra de la exYugoslavia, o en la operación "Tormenta del Desierto" (Irak), su empleo no ha hecho sino aumentar en cantidad, en capacidad operativa y en sofisticación tecnológica. Se trata de un medio al que actores no estatales también recurren. Desde 2015 se tiene evidencia del empleo de drones por grupos terroristas en escenarios como Siria, Líbano o Yemen.

Dos de los sucesos recientes más relevantes, mencionados anteriormente, como son el asesinato del general Suleimaini y el ataque a las refinerías saudíes y han sido llevados a cabo con drones.

La guerra en Libia es también escenario de drones por los dos principales contendientes en el conflicto. Tanto el Ejército Nacional Libio como las fuerzas del Gobierno de Acuerdo Nacional emplean estos vehículos aéreos para misiones de vigilancia, reconocimiento, inteligencia y ataque, proporcionados por actores internacionales en apoyo de una u otra facción.

El rápido desarrollo tecnológico nos transporta a un escenario a corto plazo de mayor sofisticación tecnológica de estos vehículos aéreos, cada vez de menor tamaño y mayor capacidad. De especial preocupación es el desarrollo de los denominados "sistemas de armas letales autónomas", o LAWS (por sus siglas en inglés correspondientes a la expresión "Lethal Autonomous Weapon Systems". La posibilidad de empleo operacional, haciendo uso de procedimientos de ataque en enjambre, con procesos de toma de decisión distribuidos y automáticos basados en inteligencia artificial plantea cuestiones éticas, derivadas de la no intervención humana para determinadas funciones donde la decisión final puede implicar misiones letales.

Figura 22
Tendencia "mayor competencia entre actores globales en un entorno de inestabilidad": Dinámicas y señales

Un contexto de seguridad más híbrido: geotecnología y economía

El análisis de tendencias proyecta un escenario en 2022 de predominio de los vectores tecnológicos y económicos. Es el caso de la tecnología 5G y sus implicaciones en el ámbito de la seguridad.

Disrupción tecnológica y ciberseguridad

El desarrollo del 5G a nivel global es fuente, en gran medida, de tensiones geopolíticas entre los dos grandes polos de poder a nivel global: Estados Unidos y China. La Unión Europea y sus Estados miembro se ve afectada, asímismo, por esta dinámica de fricción tecnológica, económica y geopolítica. La seguridad de la conectividad se verá desafiada por la generación de asimetrías y la competitividad en determinados sectores industriales entre los que se encuentran el tecnológico, el energético y el de la seguridad del tejido empresarial europeo.

En este esquema bipolar, la Unión Europea buscará un posicionamiento orientado hacia la autonomía estratégica a través del desarrollo y fortalecimiento de su potencial tecnológico para estrechar la brecha actualmente existente con las macro-compañías de bandera estadounidense y asiáticas. El nuevo marco normativo europeo de control de las inversiones extranjeras se orienta a la protección de sectores estratégicos, como pueden ser las telecomunicaciones o el energético, frente a eventuales amenazas a la seguridad o el orden público. Los mecanismos de actuación europeos nacen partiendo de la premisas del aperturismo del comercio internacional, la no discriminación a ningún país, la transparencia y la coordinación entre los Estados miembro de la Unión.

En España, las cifras de ciberataques muestran una tendencia al alza. Las proyecciones trasladan un escenario a tres años donde el número de incidentes en 2022 relacionados con el intento de acceso a la información, el robo de datos, o el daño a los mismos será de aproximadamente 50.000 si se mantiene el ritmo experimentado en años anteriores. De particular atención resultan las cifras de ciberataques a infraestructuras críticas. Si continúa la tendencia al alza a este ritmo, al final de 2022 podría verse incluso duplicado el número de ataques sufridos en 2019.

Indicadores prospectivos

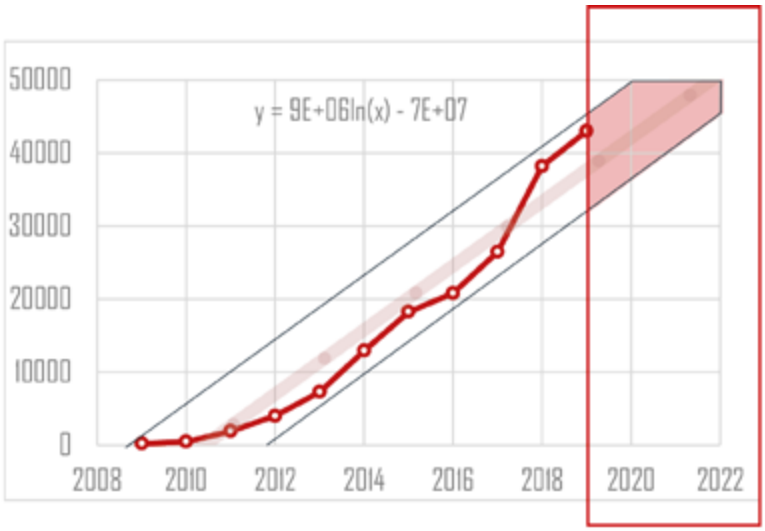


Figura 23
Proyección logarítmica a tres años (2022) del número de ciberincidentes gestionados por el CCN relacionados con el acceso a información o el daño a datos digitales

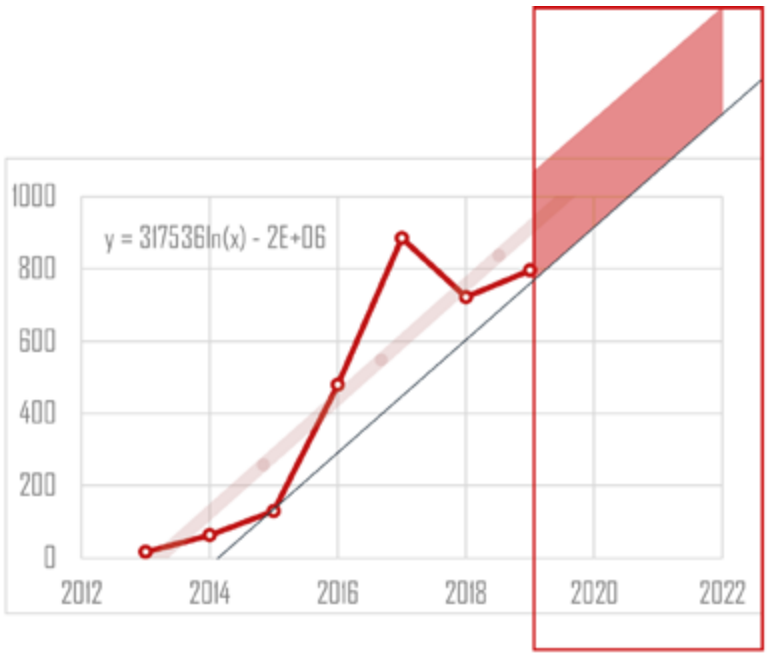


Figura 24
Proyección logarítmica a tres años (2022) del número de ciberataques a infraestructuras críticas

Inestabilidad económica y políticas proteccionistas

Los estudios prospectivos elaborados por las principales organizaciones a nivel internacional y las instituciones nacionales de referencia en materia económica y financiera muestran un escenario hasta 2022 de crecimiento económico positivo, pero a un ritmo menor que en años anteriores. Además de la ralentización económica, las políticas proteccionistas se identifican como el principal elemento de preocupación. La salida de Reino Unido de la Unión Europea (Brexit) y la guerra comercial son dos factores que trascienden más allá de su dimensión económica y tienen implicaciones para la seguridad.

El 31 de enero de 2020, Reino Unido dejó de ser formalmente un Estado miembro de la Unión Europea. El acuerdo de retirada contempla un periodo de transición hasta el 31 de diciembre de 2020 donde se deberán establecer los términos de la relación entre ambas partes. En materia de seguridad se prevé firmar un partenariado de cooperación. Las fórmulas de participación de Reino Unido en la Política Común de Seguridad y Defensa y en aquellas iniciativas europeas surgidas en 2016 tras la presentación de la Estrategia Global de Política Exterior y de Seguridad de la Unión Europea, como por ejemplo la Cooperación Estructurada Permanente (PESCO, por sus siglas en inglés) parten de la premisa de que Reino Unido es un actor estratégico principal para la seguridad de Europa y, por tanto, los modelos de cooperación se basarán en una relación de muy estrecha confianza.

La guerra comercial entre Estados Unidos y China es uno de los factores a los que se atribuye el debilitamiento en el crecimiento económico global. El 15 de enero de 2020 se firmaba un pacto entre ambos que daba fin a la denominada "Fase 1", a modo de tregua en la imposición de aranceles y de intercambio comercial. Con este acuerdo, Estados Unidos suspende la imposición de nuevas tarifas (estaba previsto aumentar un 15% los aranceles a productos chinos por valor superior a 165.000 millones de dólares) y accede a una retirada progresiva de los aranceles impuestos durante los últimos dieciocho meses. China se compromete a aumentar las importaciones de bienes y servicios en más de 200.000 millones de dólares en un plazo de dos años, hasta 2022.

Europa no ha sido inmune a estas dinámicas proteccionistas. Alemania, España, Francia y Reino Unido se encuentran entre los países más afectados. La desaceleración de la economía global también afecta de forma más acusada a las economías débiles, cuestión que produce tensiones en el proyecto de integración europea.

Para España, la imposición de aranceles en octubre de 2019 a productos agrícolas por valor de 9.600 millones de euros tras la resolución de la Organización Mundial del Comercio en contra de los subsidios a empresas europeas del sector aeronáutico implicará un descenso en las exportaciones agrícolas del 12%, según estimaciones oficiales.

Indicadores prospectivos

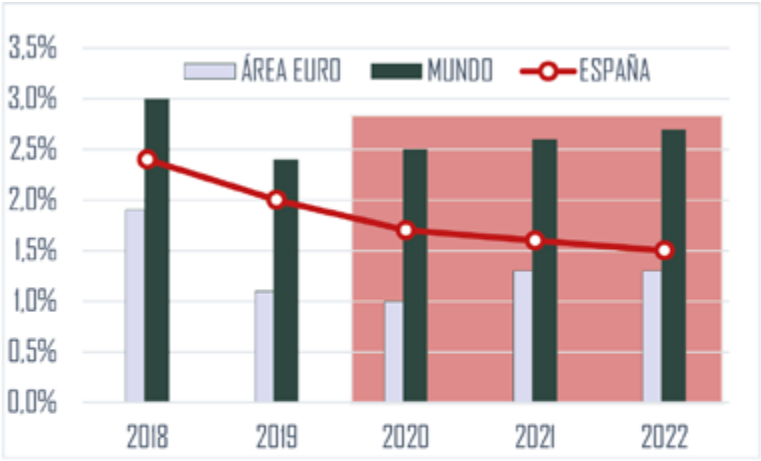


Figura 25
Proyección a tres años (2022) de la evolución del Producto Interior Bruto en España, el área Euro y el mundo, según datos del Banco de España

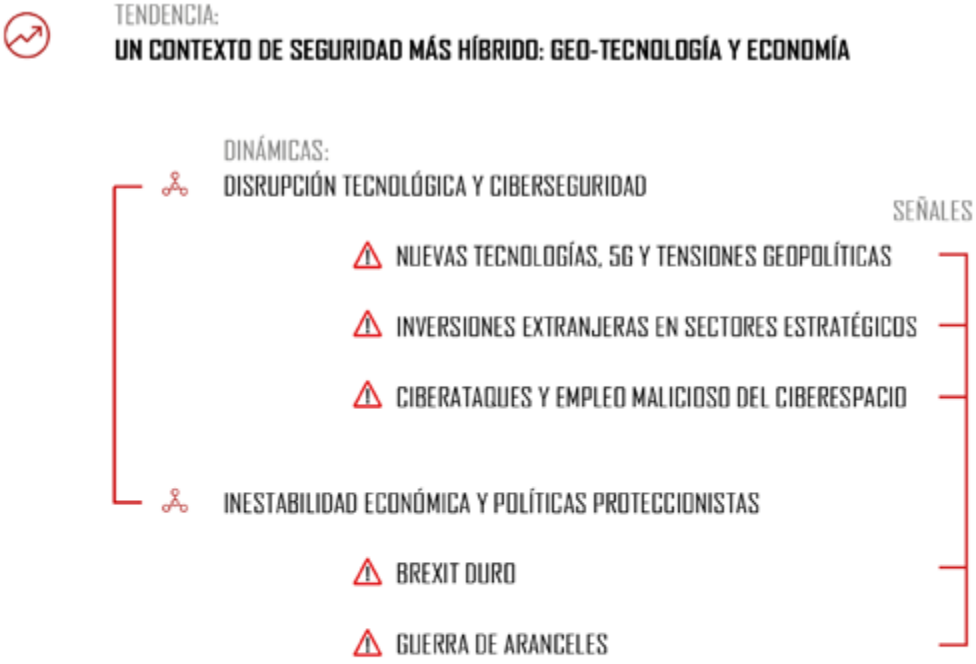


Figura 26
Tendencia "un contexto de seguridad más híbrido: geotecnología y economía": Dinámicas y señales

Cambio climático y seguridad

Una de las mayores preocupaciones a nivel global es el cambio climático. Más allá del calentamiento global y del deterioro ecosistémico, los efectos del cambio climático tienen serias repercusiones para la seguridad. La primera y más importante es el riesgo para la propia vida humana.

El cambio climático tene un significativo impacto económico. Algunas compañías aseguradoras cifran en 165.000 millones de euros los daños causados por desastres naturales a nivel global en 2018, según datos del Foro Económico Mundial.

Además, la dificultad de acceso a recursos vitales, como son el agua o los alimentos básicos puede ser fuente de tensiones geopolíticas. África es uno de los continentes donde los efectos del cambio climático tienen una mayor repercusión para la población. Las fuertes sequías o los episodios de meteorología extrema, como por ejemplo las inundaciones, arruinan cosechas y ahogan al ganado, sectores socio-económicos clave para una población que se caracteriza por su joven perfil demográfico y la dificultad de prosperar en un entorno de inestabilidad política y violencia.

En estas condiciones, un gran número de personas encuentran la migración forzosa como única vía de prosperidad, arriesgando sus vidas y poniéndolas a disposición de redes criminales.

El índice de adaptación global de la Universidad de Notre Dame es una de las referencias empleadas por Naciones Unidas para el análisis de los efectos del cambio climático y la capacidad de respuesta frente a la degradación medioambiental y los desastres y emergencias civiles derivados de episodios meteorológicos extremos. En el ranking, de los diez países más vulnerables, ocho se encuentran en África.

España ocupa el puesto 24 de un total de 181 países. Entre los múltiples parámetros analizados destaca, por mostrar una acusada tendencia negativa, el descenso de la población rural. Se trata de una vulnerabilidad con implicaciones para la seguridad. Entre los motivos se encuentra la falta de atención sobre una considerable extensión territorial, el deterioro del medio natural y el incremento de la probabilidad de desastres naturales.

Figura 27
Tendencia "cambio climático y seguridad":
Dinámicas y señales

Indicadores prospectivos

Figura 28
Los diez países más vulnerables al cambio climático, de acuerdo al Índice de Adaptación Global de la Universidad de Notre Dame

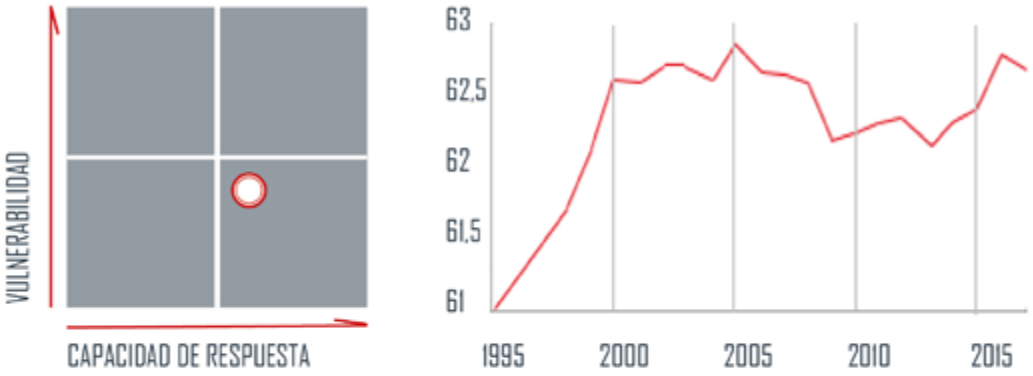


Figura 29
España ocupa el puesto número 24 en el índice, de un total de 181 países analizados

Escenario adverso

El escenario adverso plantea una situación de seguridad deteriorada en 2022 como consecuencia de la confirmación de determinados sucesos determinantes para la evolución del contexto estratégico. Los factores identificados en el análisis de riesgos, denominados en este informe como "señales", son de orden geopolítico, tecnológico, económico y medioambiental.

El equilibrio geopolítico en Oriente Medio, África del Norte y el Sahel es frágil, tres áreas geográficas que han experimentado en 2019 episodios de aumento notable de la tensión y de los niveles de violencia. Las divisiones en acuerdos internacionales que hasta ahora suponían elementos de solidez, plantean dudas para el futuro. La no renovación del tratado START, en 2021, supondría un retroceso frente a la lucha contra la no proliferación de armas de destrucción masiva en particular, y en general, desde un punto de vista ámplio, al orden internacional en su conjunto.

En el plano geo-tecnológico, además de la preocupante tendencia al alza del número de ciberincidentes y del progresivo empleo de los medios digitales para fines ilícitos, el diferente posicionamiento de cada país respecto a las redes 5G puede ahondar brechas en la esfera de las relaciones internacionales.

En la dimensión económica, se identifican dos señales: la posibilidad de un Brexit duro y un deterioro de las tensiones comerciales.

Con respecto al Brexit, el principal desafío viene derivado de la posibilidad de no alcanzar un acuerdo en los términos de la futura relación de Reino Unido con la Unión Europea antes de que finalice el periodo de transición el 31 de diciembre de 2020. No es descartable la posibilidad de que el plazo temporal de once meses no sea suficiente para dar solución a múltiples aspectos clave en múltiples ámbitos y se produzca una situación no deseada de ruptura, o "Brexit duro". Este factor, de producirse, causaría un impacto negativo a nivel internacional, con especial intensidad para España.

Con respecto a la guerra comercial, el 15 de enero de 2020 entró en vigor la denominada "fase 2" del acuerdo entre Estados Unidos y China . Esta fórmula de entendimiento y acercamiento de posiciones entre las dos mayores potencias a nivel mundial favorece un escenario de confianza económica. La celebración de las elecciones presidenciales en Estados Unidos, el 3 de noviembre, dibujan a lo largo de 2020 un año de transición en materia de política exterior. Sin embargo, otros factores geopolíticos, como la pugna por la supremacía tecnológica, o los litigios marítimos en el mar del Sur de China, podrían afectar a la situación actual, deteriorando posibles dinámicas de recuperación económica.

Finalmente, y en lo que respecta a las implicaciones para la seguridad derivada de los efectos del cambio climático, el último informe del Grupo Intergubernamental de Expertos sobre el Cambio Climático estima un modelo climático donde el nivel de confianza sobre el aumento de las temperaturas medias en la mayoría de las regiones terrestres y oceánicas y los episodios de calor extremo es alto. Un aumento de las temperaturas medias superior a 1,5º supondrá un incremento en número, frecuencia e intensidad de los fenómenos meteorológicos adversos.

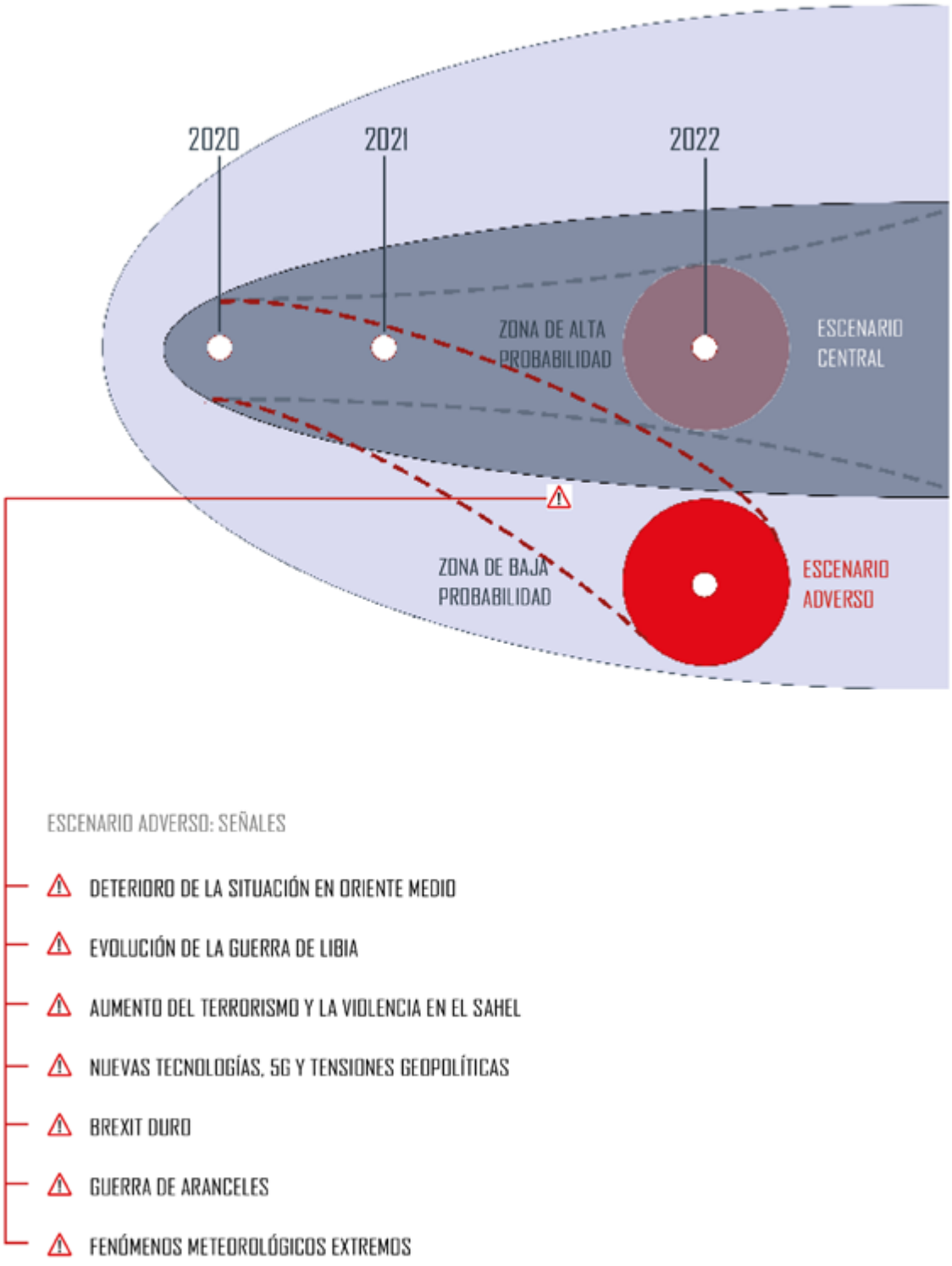
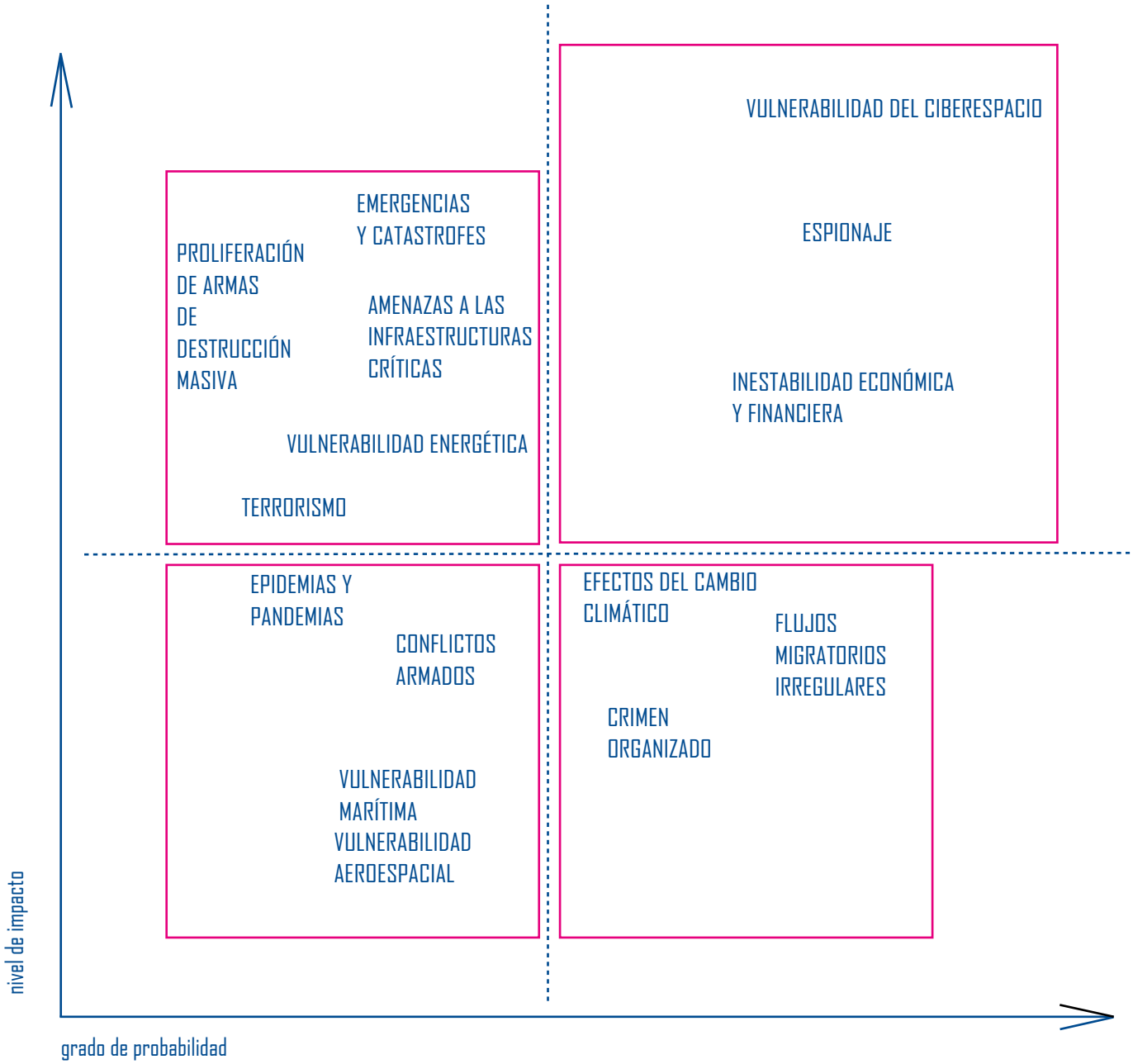


Figura 30
Escenario adverso

CONCLUSIONES



CONCLUSIONES

CONCLUSIONES

Este informe se perfila como el primer paso hacia la elaboración de la próxima Estrategia de Seguridad Nacional, toda vez que ofrece un punto de referencia inicial en el proceso de revisión del entorno estratégico mediante el estudio de los desafíos y las amenazas.

El análisis dibuja un contexto de seguridad híbrido, donde la topografía de los riesgos se muestra en contínua transformación y las conexiones son igual o más relevantes que los elementos analizados.

La principal conclusión del análisis es la constatación del predominio de los riesgos de carácter tecnológico para la Seguridad Nacional, con afección al ciberespacio como dominio funcional, el espionaje y la inestabilidad económica y financiera.

Los factores de mayor preocupación son aquellos derivados del uso malintencionado del ciberespacio. El robo de datos o el acceso a información sensible, los ciberataques a infraestructuras críticas o la desinformación son percibidos como riesgos de fuerte impacto y alta probabilidad de que afecten a la sociedad, las empresas y la Administración Pública.

La implantación de nuevas tecnologías, como el 5G, plantea diferencias entre diferentes actores que trascienden al terreno geopolítico. Además, si se tienen en cuenta las implicaciones para la economía y la competitividad, este panorama genera un modelo delimitado por tres dimensiones, la tecnológica, la económica y la geopolítica, en cuya intersección se encuentran elementos de atención para la Seguridad Nacional.

El sentimiento generalizado sobre la futura evolución de los riesgos tiene signo pesimista. Las proyecciones a tres años muestran un deterioro en la práctica totalidad de los factores analizados.

Con estos elementos, el escenario de mayor probabilidad para 2022 se configura con tres tendencias: mayor competencia entre actores globales en un entorno de inestabilidad, un contexto más híbrido, de predominio de las amenazas de signo geo-tecnológico y económico, y una mayor preocupación por los efectos del cambio climático y las implicaciones para la seguridad.

ANEXOS

ANEXOS

ANEXO I

Tabla-resumen de gráficos

ANEXO II

Factores analizados

Tensión Geopolítica, competición interestatal y fragmentación del orden internacional debido, entre otras causas, al aumento de capacidades de proyección militar de diversos Estados

Conflictos híbridos (definidos en la Estrategia de Seguridad Nacional 2017 como aquellos que incorporan operaciones de información, subversión, presión económica y financiera junto a acciones militares)

Persistencia de graves focos de inestabilidad y de Estados fallidos o de débil gobernanza, en particular en zonas próximas a territorio español

Pérdida de confianza en las organizaciones de seguridad colectiva

Terrorismo yihadista: atentados indiscriminados en lugares de concentración de personas, medios de transporte o infraestructuras críticas

Retorno de combatientes terroristas desde escenarios como Siria e Irak

Radicalización, extremismo violento, captación y adoctrinamiento con fines terroristas

Capacidad desestabilizadora del crimen organizado sobre el Estado y la gobernanza económica

Aprovechamiento por parte de las redes criminales de la crisis migratoria y de refugiados

1 Vinculación del crimen organizado con redes terroristas

Empleo de armas de destrucción masiva (nuclear, química, bacteriológica o radiológica) por parte de Estados en zonas de conflicto

Empleo de armas de destrucción masiva por actores no estatales, en particular, por grupos terroristas

Deterioro de los mecanismos internacionales de cooperación y colaboración en materia de la lucha contra la proliferación de armas de destrucción masiva

Empleo del ciberespacio por parte de Estados, grupos o individuos para llevar a cabo tareas de espionaje (acceso a información y datos sensibles)

Espionaje industrial, cuyo objetivo es acceder al conocimiento tecnológico y estratégico que permite adoptar una posición diferencial con respecto a la competencia

Agresiones procedentes de servicios de inteligencia extranjeros contra intereses nacionales, tanto por procedimientos clásicos como a través del ciberespacio

Disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos, tales como el robo de datos, ramsomware, ataques de denegación de servicios, hacking de dispositivos móviles o ciberataques a infraestructuras críticas

Uso ilegítimo del ciberespacio para llevar a cabo actividades ilícitas como por ejemplo acciones de desinformación, propaganda o financiación del terrorismo

Amenazas derivadas de actos intencionados y de naturaleza delictiva (piratería, terrorismo, tráficos ilícitos, actos contra la conservación del patrimonio cultural subacuático, redes de inmigración irregular por vía marítima o explotación incontrolada de recursos, como por ejemplo la pesca

Accidentes marítimos y catástrofes naturales en el espacio marítimo

Competencia interestatal por ampliar el acceso y control sobre los espacios marítimos

Violaciones a la seguridad y al orden internacional en el espacio aéreo por parte de actores estatales y no estatales

Uso de aeronaves pilotadas de forma remota (drones) par acciones de naturaleza agresiva o ilícita por parte de Estados u organizaciones no estatales

Competición entre Estados por el acceso, uso y control del espacio ultraterrestre

Interrupciones a los servicios proporcionados por las infraestructuras de los sectores estratégicos que tienen su origen en causas no deliberadas

Amenazas de carácter físico a las infraestructuras críticas con origen intencionado

Amenazas a las infraestructuras críticas a través de ciberataques

Debilitamiento del crecimiento económico

Políticas proteccionistas que minan el aperturismo del comercio internacional

Tecnologías disruptivas y amenazas a la competitividad económica

Inestabilidad geopolítica en las principales zonas productoras de recursos energéticos

Aumento del precio de los recursos energéticos

Vulnerabilidad de la red de suministro energético y las infraestructuras asociadas

Inmigración irregular

Falta de integración social

Emergencias a consecuencia de episodios de meteorología adversa o fenómenos naturales como erupciones volcánicas o maremotos

Accidentes deliberados contra el medio ambiente, como por ejemplo los incendios forestales

Riesgo nuclear o radiológico

Alertas sanitarias con impacto a nivel nacional

Empleo intencionado de sustancias contagiosas con fines dañinos

Aumento de la competencia por el acceso a los recursos naturales en zonas de interés para la Seguridad Nacional

Degradación medioambiental en diversas manifestaciones (desertificación del territorio, degradación de los recursos hídricos, acidificación del océano y aumento del nivel del mar)

Aumento de los movimientos migratorios forzosos a causa de la degradación medioambiental

DSN

www.dsn.gob.es