

Informe Anual de Seguridad Nacional

2025

Catálogo de publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



© Autor y editor,

NIPO (edición impresa): 143-24-008-0

NIPO (edición on-line): 143-24-009-6

DL M 17825-2014

Fecha de edición: abril de 2026

Imprime: MASQUELIBROS, SOCIEDAD LIMITADA

Informe Anual de Seguridad Nacional 2025

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 Presidencia, Justicia y Relaciones con las Cortes; el Ministerio de Defensa; el Ministerio de Hacienda; el Ministerio del Interior; el Ministerio de Transportes y Movilidad Sostenible; el Ministerio de Trabajo y Economía Social; el Ministerio de Industria y Turismo; el Ministerio de Agricultura, Pesca y Alimentación; el Ministerio de Política Territorial y Memoria Democrática; el Ministerio para la Transición Ecológica y el Reto Demográfico; el Ministerio de Cultura; el Ministerio de Economía, Comercio y Empresa; el Ministerio de Sanidad; el Ministerio de Ciencia, Innovación y Universidades; el Ministerio de Inclusión, Seguridad Social y Migraciones; el Ministerio para la Transformación Digital y de la Función Pública y el Centro Nacional de Inteligencia.

El informe fue aprobado por el Consejo de Seguridad Nacional en su reunión de 21 de abril de 2026.

SUMARIO

INTRODUCCIÓN	7
RIESGOS Y AMENAZAS A LA SEGURIDAD NACIONAL.....	11
TENSIÓN ESTRATÉGICA Y REGIONAL	12
TERRORISMO Y RADICALIZACIÓN VIOLENTA	42
EPIDEMIAS Y PANDEMIAS.....	58
AMENAZAS A LAS INFRAESTRUCTURAS CRÍTICAS.....	72
EMERGENCIAS Y CATÁSTROFES	80
ESPIONAJE E INJERENCIAS DESDE EL EXTERIOR	100
CAMPAÑAS DE DESINFORMACIÓN	106
VULNERABILIDAD DEL CIBERESPACIO	114
VULNERABILIDAD DEL ESPACIO MARÍTIMO.....	140
VULNERABILIDAD AEROESPACIAL	158
INESTABILIDAD ECONÓMICA Y FINANCIERA.....	174
CRIMEN ORGANIZADO Y DELINCUENCIA GRAVE	190
FLUJOS MIGRATORIOS IRREGULARES.....	210
VULNERABILIDAD ENERGÉTICA	226
PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA.....	238
EFECTOS DEL CAMBIO CLIMÁTICO Y DE LA DEGRADACIÓN DEL MEDIO NATURAL	248
ANÁLISIS DE RIESGOS 2025/26.....	273
CULTURA DE SEGURIDAD NACIONAL.....	286
GLOSARIO	296

INTRODUCCIÓN

El Informe de Seguridad Nacional es un instrumento al servicio de la política pública de Seguridad Nacional. Así, este decimotercero Informe Anual de Seguridad Nacional recorre los dieciséis ámbitos de la Seguridad Nacional identificados en la Estrategia de Seguridad Nacional de 2021, y subraya las realizaciones y los retos más significativos de cada uno de ellos. Su propósito es ofrecer una visión integral de los retos de seguridad presentes a los que nos enfrentamos y hacerlo con ambición constante de mejora.

Asimismo, este informe está ligado de forma estrecha con el fomento y la difusión de la cultura de Seguridad Nacional, cuyo objetivo es acercar al ciudadano a los retos de seguridad presentes y futuros, especialmente en estos momentos de constantes desafíos y amenazas.

En el transcurso de 2025, la tensión geopolítica ha seguido marcando el escenario internacional. La guerra de Ucrania continúa como un eje central de inestabilidad en Europa, así como el conflicto regional entre Israel y Hamás se ha mantenido como el principal punto de fricción en todo Oriente próximo con un aumento de la tensión regional. En el continente africano, la situación de seguridad en el Sahel central se ha deteriorado gravemente en los últimos años, hasta convertirse en el centro de gravedad del terrorismo mundial.

Este contexto de inestabilidad se ha reflejado en el deterioro del sistema de control de armamentos, lo que, unido al cuestionamiento por diversos actores de las bases del sistema de no proliferación, ha acelerado la necesidad de una respuesta coordinada del Estado, resultando en la aprobación por el Consejo de Seguridad Nacional el 16 de diciembre de 2025 de la primera Estrategia Nacional contra la Proliferación de Armas de Destrucción Masiva. De igual forma, este tenso escenario geopolítico ha tenido su impacto en el plano económico, con un incremento de la importancia de comercio del material de defensa y de doble uso. Igualmente, la rivalidad sistémica entre grandes potencias ha derivado en políticas comerciales coercitivas y un proteccionismo tecnológico.

Paralelamente, la aceleración tecnológica en 2025 en el plano de la ciberseguridad ha precipitado un cambio de escala y de naturaleza, con un panorama de ciberamenazas cada vez más complejo. Del mismo modo, la desinformación se ha consolidado como vector de inestabilidad y la Inteligencia Artificial ha dejado de ser únicamente una herramienta de producción para convertirse en un soporte integral de campañas de desinformación a nivel estratégico, táctico y operativo.

A su vez, en el ámbito del crimen organizado y la delincuencia grave, destaca la evolución hacia nuevas operativas ilícitas apoyadas en innovaciones tecnológicas. Para avanzar en la prevención y lucha contra los fenómenos criminales, el Consejo de Seguridad Nacional aprobó el 14 de julio la Estrategia contra el Crimen Organizado y la Delincuencia grave 2025, adaptada a la evolución de la amenaza.

Las infraestructuras marítimas se consolidan como un ámbito de atención prioritaria, especialmente, la protección de los cables submarinos, que ha pasado a ser una de las principales preocupaciones en lo que respecta a las amenazas híbridas y su proyección en espacios marítimos.

Por su parte, el ámbito aeroespacial se presenta como un escenario estratégico altamente codiciado, lo que ha motivado que el Consejo de Seguridad Nacional aprobara el 14 de julio de 2025 la Estrategia de Seguridad Aeroespacial Nacional. Un documento que busca dar respuesta a los profundos cambios que han alterado el equilibrio en el espacio aéreo y ultraterrestre en los últimos años. De forma particular, el uso indebido de drones adquiere una relevancia creciente como vector de riesgo en el entorno europeo, debido a su accesibilidad, su dificultad de detección y su potencial para usos ilícitos.

Por otra parte, la vulnerabilidad energética ha sido protagonista del panorama de Seguridad Nacional con la caída del sistema eléctrico en la península el 28 de abril de 2025, dando lugar a la adopción de numerosas medidas para mejorar la resiliencia de la red eléctrica.

Respecto a la migración irregular, el aspecto más destacable de 2025 ha sido la reducción de las llegadas (entradas por vía marítima y las terrestres por Ceuta y Melilla) a nuestro país cerca de un 43% respecto del año 2024, alcanzando las cifras más bajas desde el año 2022.

Para terminar, completan el cuadro de la Situación de Seguridad Nacional los fenómenos meteorológicos extremos derivados del cambio climático, que cada vez se producen con mayor frecuencia e intensidad en todo el mundo. En nuestro país, el calor registrado en la época estival ha situado el verano de 2025 como el más cálido desde 1961, lo que ha tenido un impacto en el desarrollo de la campaña de prevención y lucha contra incendios forestales. Así, se han registrado 63 grandes incendios forestales (con una superficie afectada superior a las 500 hectáreas), una cifra muy superior a los 23 de la media del decenio precedente.

Por su parte, el Sistema de Seguridad Nacional ha continuado avanzado en su desarrollo orgánico y planeamiento estratégico a lo largo de 2025. El Consejo de Seguridad Nacional se ha reunido en 10 ocasiones durante el año, especialmente, seis de ellas tuvieron lugar entre los días 28 y 30 de abril para el seguimiento de la situación y la coordinación de las posibles consecuencias del cero energético. Además, 2025 ha sido un año de revisión estratégica para la Seguridad Nacional. Así, en su sesión de 24 de abril, el Consejo aprobó la revisión de la Estrategia de Seguridad Nacional de 2021, dado el profundo cambio del contexto geopolítico global desde la aprobación de la anterior estrategia. Igualmente, está en curso la revisión de la Estrategia nacional de Ciberseguridad de 2019 y la elaboración de una nueva Estrategia Nacional contra las Campañas de Desinformación.

Finalmente, como en ediciones anteriores, este informe incorpora el Análisis de Riesgos para la Seguridad Nacional, que presenta los resultados de la encuesta de percepción realizada a una red de 806 expertos, en distintos ámbitos de la seguridad.

En cuanto a los resultados obtenidos, el informe ofrece tres elementos analíticos.

El primero es el mapa de riesgos, gráfico que ofrece una representación visual de los dieciséis riesgos y amenazas en función del grado de probabilidad y del nivel de impacto en una escala de 0 a 5. Los resultados de este año vuelven a situar a la vulnerabilidad del ciberespacio y las campañas de desinformación en posición destacada en el área correspondiente a valoraciones en cuanto a nivel de impacto superior a 4 y grado de probabilidad cercana a 4. Una mirada retrospectiva cinco años atrás permite afirmar el predominio de la preocupación para la sociedad del empleo del ciberespacio para fines irregulares y las campañas de desinformación. Son dos amenazas para la seguridad nacional que, al margen de la situación coyuntural de cada año, siempre han ocupado los puestos más altos en el *ranking* del mapa de riesgos. Como rasgo más distintivo de lo acontecido a lo largo de 2025, cabría identificar la crisis de suministro eléctrico del 28 de abril, evento que ha vuelto a poner de manifiesto la importancia de la seguridad energética, que ocupa el tercer puesto.

El segundo elemento es un estudio de las tendencias a cinco años. Al igual que sucede en el caso anterior, los resultados de la encuesta sitúan a la vulnerabilidad del ciberespacio y las campañas de desinformación como las dos amenazas que se perciben con mayor deterioro.

En tercer lugar, el estudio acomete unos escenarios prospectivos proyectados con un horizonte temporal de 10 años en función de las cuatro dimensiones analíticas de la Estrategia de Seguridad Nacional 2021: geopolítica, económica-social, tecnológica y medioambiental. El panorama que resulta es pesimista. En particular, en clave geopolítica, el 77% de los encuestados consideran que el contexto geopolítico en 2035 se caracterizará por ser un escenario de mayor fragmentación y complejidad.

Por último, cierran este informe los avances realizados en 2025 en materia de cultura de Seguridad Nacional, destacando la importancia de fortalecer una sociedad concienciada, preparada y resiliente ante un entorno de riesgos complejos y cambiantes, a través del Plan Integral de Cultura de Seguridad Nacional. Durante este ejercicio, se registró un notable incremento de las actividades impulsadas por las administraciones públicas, con especial énfasis en la formación y la comunicación pública, así como en la colaboración público privada y la participación ciudadana, reforzando la corresponsabilidad del conjunto de la sociedad en la prevención y respuesta ante amenazas. El balance refleja resultados positivos tras cuatro años de aplicación del Plan, consolidándolo como un marco de referencia esencial para seguir promoviendo la seguridad, la cohesión social y la protección del bienestar y los derechos de la ciudadanía.

RIESGOS Y AMENAZAS A LA SEGURIDAD NACIONAL



TENSIÓN ESTRATÉGICA Y REGIONAL

- La guerra en Ucrania sigue siendo un eje central de inestabilidad en Europa, aunque el foco estratégico se ha desplazado hacia un escenario más amplio en el que confluyen otros conflictos regionales, la competencia tecnológica y la seguridad energética.
- El Consejo de Seguridad Nacional, en su sesión del 24 de abril, acordó aprobar la revisión de la Estrategia de Seguridad Nacional, motivado por el cambio geopolítico desde 2021 y el vencimiento de los plazos legales de vigencia.
- España ha reforzado su proyección hacia Asia-Pacífico mediante la Estrategia española para Asia-Pacífico 2026-2029 aprobada por el Consejo de Ministros el 9 de diciembre de 2025. Una hoja de ruta que orienta una acción exterior más activa hacia esta región.

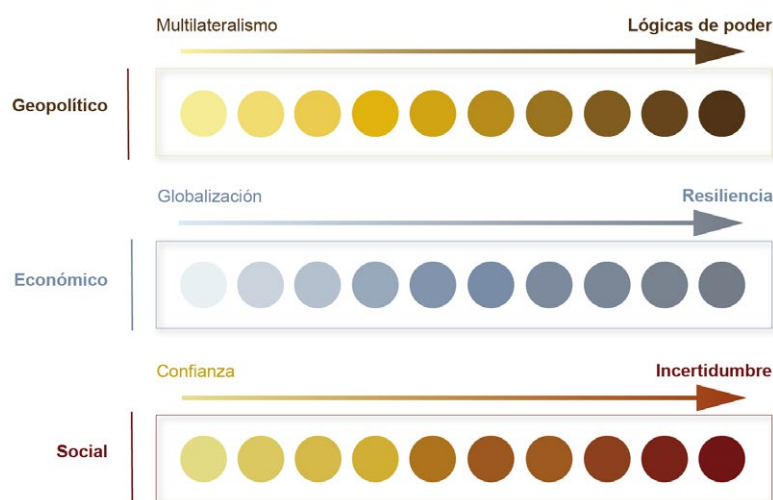
TENSIÓN ESTRATÉGICA Y REGIONAL

El contexto geopolítico internacional se caracteriza por una creciente complejidad e interconexión de los conflictos, que combinan guerras convencionales, tensiones regionales y amenazas transnacionales como la ciberdelincuencia y el crimen organizado. La proliferación de actores no estatales, a menudo vinculados o instrumentalizados por Estados, y la expansión de la desinformación contribuye a un entorno de seguridad más volátil e incierto.

La guerra en Ucrania sigue siendo un eje central de inestabilidad en Europa, pero el foco estratégico se ha desplazado hacia un escenario más amplio en el que confluyen otros conflictos regionales, la competencia tecnológica y la seguridad energética.

En el entorno estratégico de España, en la confluencia de los espacios atlántico, mediterráneo, europeo y africano, se sitúan varios conflictos y focos de inestabilidad como la agresión rusa contra Ucrania, la inestabilidad en el Sahel o los conflictos de Oriente Próximo. La Estrategia de Acción Exterior (EAE), en vigor desde 2025, señala tres desplazamientos del orden internacional: a) de un mundo con reglas hacia otro en el que priman lógicas de poder, b) de la eficiencia económica de la globalización hacia la búsqueda de resiliencia, c) y de la confianza en el progreso a la incertidumbre. (Figura 1.1)

UN MUNDO EN TRANSICIÓN: TRES DESPLAZAMIENTOS DEL ORDEN INTERNACIONAL



Fuente: Elaboración propia DSN de acuerdo con la Estrategia de Acción Exterior del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación

Figura 1.1: Un mundo en transición: tres desplazamientos del orden internacional

Europa. Invasión rusa de Ucrania. Evolución del conflicto

Desde su inicio en febrero de 2022, la invasión rusa de Ucrania ha evolucionado desde un intento de toma rápida de Kiev hacia un conflicto prolongado de desgaste. Después de casi cuatro años desde el inicio de la invasión rusa de Ucrania, Moscú no ha renunciado a ninguno de sus objetivos y mantiene una posición maximalista ante una posible negociación que ponga fin, al menos, a los combates en el frente. Además, mantiene su presión en el campo de batalla como forma de mejorar su posición en una futura mesa de diálogo.

En 2025, la guerra en Ucrania continuó, con una situación en el campo de batalla marcada por la superioridad numérica del bando ruso que, sin embargo, no se tradujo en un logro de avances decisivos. Durante la primera mitad del año ninguno de los dos bandos alcanzó un punto de ruptura. Los frentes se mantuvieron relativamente estables, aunque Rusia consiguió ocupar algunas plazas de cierta importancia. En la segunda mitad del año, Rusia avanzó lenta pero firmemente en el este de Ucrania, con unas bajas de personal y material muy desproporcionadas en relación con los beneficios obtenidos. Al cierre de este informe, se mantiene el ritmo de avance, a fin de capturar todo el terreno posible antes del deterioro meteorológico debido a la estación lluviosa y el invierno. Tras la recuperación del terreno perdido en el Óblast de Kursk, se han desplazado gran número de unidades en el Donbás, que sigue siendo su objetivo operacional.

De esta forma, el conflicto ruso-ucraniano se caracteriza por fases de ofensivas limitadas y contraofensivas condicionadas por las capacidades logísticas y el apoyo externo, sin que ninguna de las partes pueda permitirse una derrota, y sin que exista, por el momento, una vía clara de terminación. Rusia proyecta una imagen de voluntad negociadora mientras consolida posiciones sobre el terreno y desarrolla una estrategia de intervención indirecta e híbrida orientada a desestabilizar a Occidente y minar el apoyo a Ucrania.

El último esfuerzo negociador del año 2025 ha sido el Plan de paz de los 20 puntos desvelado por Zelenski el 24 de diciembre y objeto de la negociación entre los presidentes Trump y Zelenski el 28 de diciembre en Mar-a-Lago. Por otra parte, la Coalición de Voluntarios ha sido el foro donde se han reunido 35 países afines, entre ellos España, para discutir fundamentalmente un esquema de garantías de seguridad a Ucrania con una fuerte implicación de países europeos.

En este contexto, el conflicto ha evolucionado hacia una “cristalización” en la que el frente tiende a estabilizarse, pero se intensifica el uso de drones, guerra electrónica, interferencias GPS, inteligencia satelital y ciberataques, con especial foco en infraestructuras energéticas ucranianas y en nodos industriales petroleros en Rusia, así como en sabotajes y acciones híbridas en territorio europeo. Estas actividades, que incluyen ataques a cables submarinos, redes eléctricas, instalaciones militares y puertos, se apoyan a menudo en redes criminales y se acompañan de campañas de desinformación y acciones en el dominio cognitivo que también tienen a España como objetivo, lo que incrementa la preocupación de la OTAN, la UE y las autoridades nacionales sobre la posible extensión de estos métodos a la infraestructura crítica europea. Por otra parte, la agresión de Rusia a Ucrania ha provocado uno de los mayores desplazamientos en Europa desde la Segunda Guerra Mundial, con más de 7 millones de ucranianos buscando refugio en la UE.

Aunque España se considera un objetivo secundario de la actividad híbrida rusa, la creciente acción de la llamada “flota fantasma” de petroleros rusos en el Mediterráneo, que eluden sanciones y operan cerca de las costas españolas, añade riesgos de accidentes, contaminación, daños a infraestructuras submarinas y un eventual, pero a la vez muy poco probable, uso como plataforma para el lanzamiento de drones, obligando a reforzar la vigilancia naval, el control portuario y la inteligencia marítima.

Paralelamente, la prolongación del conflicto ha impulsado una profunda reconfiguración de la arquitectura de seguridad europea y global, con un incremento sostenido del gasto militar, inversiones en defensa y ciberseguridad y una revisión de las doctrinas de disuasión y resiliencia estratégica de Occidente.

Así, el conflicto en Ucrania ha actuado como catalizador de un aumento significativo de la inversión en defensa en toda Europa, redefiniendo las prioridades de seguridad de la UE y la OTAN. La principal implicación ha sido un cambio de mentalidad, que ha llevado a los países europeos a reconocer la necesidad de fortalecer su autonomía estratégica y capacidades de defensa ante la “amenaza existencial” que representa la agresión rusa.

La actual postura estratégica de la Alianza se centra, principalmente, en reforzar la disuasión y defensa. En los últimos años, debido a la guerra de agresión de Rusia contra Ucrania, la OTAN ha reforzado su presencia avanzada en el flanco este, estableciendo agrupaciones de combate multinacionales en Bulgaria, Estonia, Hungría, Letonia, Lituania, Polonia, Rumanía y Eslovaquia, misiones de policía aérea en diversos países, y la iniciativa Centinela Oriental (*Eastern Sentry*), para reforzar la defensa y la disuasión en los espacios aéreos aliados. (Figura 1.2)



Fuente: Elaboración del DSN con datos del Ministerio de Defensa

Figura 1.2: Presencia reforzada de la OTAN en el Flanco Este

La OTAN presta especial atención a las agresiones híbridas que están sufriendo los aliados con más frecuencia, abogando porque estos incrementen su preparación para hacerles frente, en particular, reforzando la resiliencia contra esta amenaza.

Ucrania ha aumentado la disponibilidad de recursos, y ha aumentado la capacidad de producción propia, en munición de artillería y, especialmente, en Vehículos Aéreos no Tripulados (UAV, por sus siglas en inglés). Esto ha permitido reducir el desequilibrio entre ambos bandos, aunque no en la medida necesaria para Ucrania. Particularmente, Ucrania se encuentra necesitada de unidades de defensa aérea, pues los ataques en profundidad de Rusia están dañando severamente su infraestructura crítica.

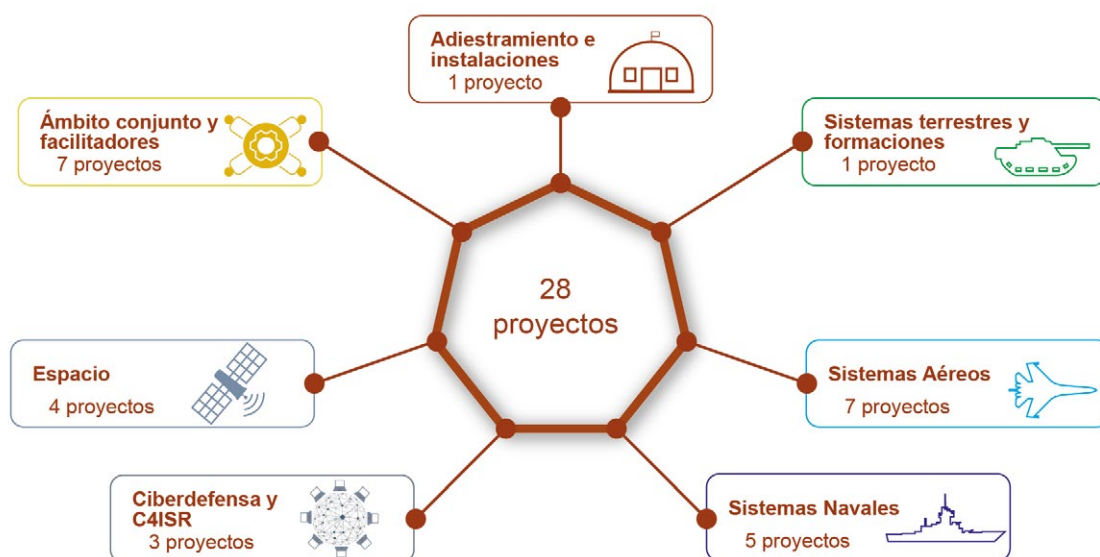
Por ello, a pesar de los grandes avances ucranianos para desarrollar su propia industria de defensa, el país sigue dependiendo del apoyo occidental, tanto de su ayuda militar como de la económica, ambas siendo un factor decisivo para determinar el futuro del conflicto.

Mientras, en el lado ruso, el presupuesto de defensa para 2025 ha sido de 140.000 millones de dólares, y el Gobierno ha manifestado que los rusos deben prepararse para un gran esfuerzo en defensa hasta 2028.

La OTAN, que no participa en el suministro directo de apoyo, continúa su implicación con Ucrania, a través de apoyo militar y financiero a las Fuerzas Armadas de Ucrania, desde la financiación de forma directa o a través de mecanismos como el *Prioritised Ukraine Requirements List* (PURL).

La Unión Europea es el mayor apoyo de Ucrania tanto en volumen de ayuda total como en ayuda militar y mantiene un marco sostenido y de largo plazo, combinando presión económica sobre Rusia; financiación específica para Ucrania; y, adaptación de instrumentos de la Política Común de Seguridad y Defensa. Además, se han consolidado y ampliado instrumentos clave como la Misión de Asistencia Militar a Ucrania (EUMAM-UA), el Fondo Europeo de Apoyo a la Paz (EPF), el mecanismo de entrega conjunta de munición, el uso de beneficios extraordinarios (*windfall profits*) y la puesta en marcha del instrumento “*Acción de Seguridad para Europa*” (*Security Action for Europe, SAFE*) dentro del Plan *ReArm Europe*. Paralelamente, la UE ha desarrollado nuevas líneas estratégicas como la Hoja de Ruta de Preparación para la Defensa, la Alianza de Drones y el nuevo *Ukraine Support Instrument* (USI).

En marzo de 2025, la Comisión Europea y la Alta Representante de la Unión Europea presentaron el “Libro Blanco sobre la Defensa Europea y el Plan *ReArm Europe 2030*”. Este documento recoge una serie de medidas ambiciosas destinadas a garantizar la autonomía estratégica de la Unión, reforzando las capacidades militares, impulsando a la industria de defensa europea, simplificando el marco regulatorio y mejorando significativamente la financiación del sector.



Fuente: Ministerio de Defensa

Igualmente, España no es ajena al esfuerzo colectivo para contener los efectos del conflicto y mitigar sus riesgos y colabora a través de diferentes líneas de acción:

Por un lado, en el ámbito bilateral, España ha ampliado de manera significativa la asistencia militar, humanitaria, sanitaria y logística, situando el acuerdo de seguridad firmado el 27 de mayo de 2024 como eje estructural del compromiso nacional que reafirma el apoyo a largo plazo a la defensa, soberanía e integridad territorial de Ucrania. En particular, en cuanto a la asistencia militar, España ha realizado una contribución muy significativa en apoyo a las fuerzas armadas ucranianas, que asciende a un total de 2.795 millones de euros, desde el inicio de la invasión a gran escala en febrero de 2022, lo que la sitúa en 2025 como el octavo Aliado de la OTAN por valor del apoyo militar a Ucrania.

Por otro, en el marco de la UE, España es uno de los principales financiadores del mecanismo EPF (cuota en función de la renta nacional) y va a dedicar a Ucrania 215,7 M € de los 1000 M € en préstamos asignados a nuestro país a través del mecanismo SAFE de la Unión Europea para refuerzo de las industrias de defensa. España apoya la integración del sector ucraniano en el europeo. España viene siendo el cuarto contribuyente de los Estados Miembros de la UE a la misión EU EUMAM Ucrania por número de militares entrenados. España participa asimismo en la misión civil de la UE en Ucrania EUAM y apoyamos el actual proceso de refuerzo de los mandatos de ambas misiones de la UE como parte del conjunto de las garantías de seguridad para Ucrania que se basan en apoyar unas Fuerzas Armadas ucranianas capaces de disuadir y defender ante potenciales futuras agresiones. Además de las aportaciones al EPF, su asistencia se concreta, entre otros instrumentos, en la Misión de Asesoramiento de la Unión Europea en Ucrania (*EUAM Ukraine*), que apoya la reforma del sector de la seguridad y, como medida principal, el adiestramiento a personal ucraniano en dentro de la mencionada EUMAM UA, Hasta el año 2025 incluido, España ha adiestrado a 8.699 ucranianos en 218 módulos. Igualmente, la Guardia Civil participa mediante la Unidad de Acción Rural, que ha impartido formación en tácticas especiales contraterroristas a oficiales de la Guardia Nacional y del Servicio Estatal de Guardia de Fronteras ucranianos.

A su vez, dentro del marco de la OTAN, España participa en diversos mecanismos e iniciativas, tales como el *Pledge of Long-Term Security Assistance*, la “Iniciativa de Apoyo en materia de Seguridad y Entrenamiento a Ucrania” (*NATO Security Assistance and Training for Ukraine*, NSATU), o la reciente adhesión al mencionado mecanismo PURL, en el que España participó con una contribución voluntaria de 100 M € en 2025. Además, el Ministerio de Asuntos Exteriores y Cooperación contribuyó con 1 millón de euros al Paquete de Asistencia Integral de la OTAN (CAP) a Ucrania en 2024 y, de nuevo, otro millón en 2025.

Además, España forma parte del Grupo de Contacto para la Defensa de Ucrania (*Ukraine Defense Contact Group*, UDCG) junto a otras 56 naciones; entre ellas, los 32 miembros de la OTAN.

Finalmente, en coordinación con otros órganos de la administración, el Ministerio de Defensa apoya los traslados y el tratamiento de personal militar ucraniano en hospitales militares y civiles españoles, y otras actividades humanitarias en apoyo a las personas y familias especialmente vulnerables. Además, desde la Red Europea de Institutos Forenses (ENFSI), las Fuerzas y Cuerpos de Seguridad del Estado contribuyen a la acreditación de crímenes de guerra en Ucrania. Además, la Guardia Civil consolida un papel activo como proveedor de asesoramiento policial y de un modelo de seguridad eficiente para el postconflicto, reforzando la interoperabilidad con fuerzas ucranianas y europeas y la resiliencia frente a amenazas transnacionales.

En este sentido, España, a través de la Guardia Civil, ha participado en el taller internacional organizado en Kiev para apoyar la elaboración de la Estrategia y Plan de Acción Nacional de Ucrania contra el tráfico ilícito de armas, municiones y explosivos.

Paralelamente, en la periferia rusa, se ha producido la firma de un preacuerdo entre Armenia y Azerbaiyán para poner fin al conflicto. Dicho documento, firmado en la Casa Blanca, presupone un cierto aumento de la estabilidad en la zona, en la que no se han registrado incidentes armados de importancia.

Por su parte, España, a través, de la Policía Nacional, ha apoyado la celebración de la reunión anual de los órganos ejecutivos y de gestión de ENFSI (Red Europea de Institutos Forenses) en Yereván (Armenia), participando activamente en la misma, promoviendo así el acercamiento y la cooperación entre el *National Bureau of Expertises* (NBE-SNPO) y la comunidad ENFSI.

Oriente Próximo

Los ataques terroristas de Hamás el 7 de octubre de 2023 y la respuesta israelí han desencadenado una guerra en la Franja que dura ya dos años. Este conflicto ha provocado la muerte de más de 68.700 palestinos y más de 170.700 heridos. A raíz de la ofensiva terrestre y aérea israelí, según la Oficina de las Naciones Unidas para la Coordinación de Asuntos Humanitarios (OCHA), más del 92% de los edificios del enclave han sido destruidos o dañados y los dos millones de palestinos que viven en la Franja han sufrido sistemáticamente desplazamientos forzosos.

Durante 2025, el conflicto Israel-Hamás se ha mantenido como el principal punto de fricción en todo Oriente Próximo, que, a su vez, ha provocado un aumento de las tensiones en toda la región, entre las que destaca la guerra de los Doce Días en junio de dicho año, durante la cual Israel y Estados Unidos bombardearon instalaciones nucleares iraníes. Además, el 9 de septiembre, Israel ejecutó un ataque a la cúpula de Hamás en Doha, tras el cual se ejerció la presión diplomática necesaria para lograr un acuerdo de alto el fuego en Gaza.

A mediados de septiembre, en el marco de la Conferencia Internacional de Alto Nivel para la Solución Pacífica de la Cuestión de Palestina y la Implementación de la Solución de los Dos Estados, impulsada por España y copresidida por Francia y Arabia Saudí, se produjo el reconocimiento del Estado de Palestina por parte de Francia, Reino Unido, Canadá, Australia, Portugal, Bélgica, Luxemburgo, San Marino, Andorra y Malta. Asimismo, la Asamblea General adoptó una resolución que endosa la Declaración de Nueva York para la Implementación de la Solución de los Dos Estados, declaración que fija los objetivos para alcanzar una solución justa y duradera al conflicto.

Tras más de dos años de conflicto, a finales de septiembre, el presidente Donald Trump presentó un plan de paz de 20 puntos para poner fin a la guerra. El 9 de octubre, Israel y Hamás alcanzaron un acuerdo de alto el fuego, anunciado por Trump y celebrado por líderes internacionales. El pacto contemplaba la liberación de todos los rehenes a cambio de la excarcelación de presos palestinos, el cese de hostilidades, la entrada de ayuda humanitaria y el inicio de un proceso de repliegue parcial del Ejército israelí a una “línea amarilla” bajo supervisión internacional. Se dejarían para las siguientes fases negociadoras los asuntos de mayor complejidad como el futuro de Gaza y Hamás, una vez la organización terrorista haya entregado las armas.

El Plan de Paz estadounidense incluye, entre otras cuestiones: la liberación de los rehenes y entrega de los cuerpos de los fallecidos; el desarme de Hamás y el reconocimiento de amnistía a aquellos que depongan las armas; la entrada inmediata de la ayuda a través de organismos internacionales; la administración de Gaza por un gobierno transitorio tecnocrático supervisado por una Junta de Paz; un plan económico internacional de reconstrucción y la creación de una zona económica especial; el despliegue de una Fuerza Internacional de Estabilización (FIES) con participación de Estados regionales, entre otras medidas. El Plan de Paz también recoge una mención al establecimiento de

un futuro Estado palestino, condicionado a la reconstrucción de Gaza y las reformas de la Autoridad Palestina. No obstante, dicho plan ha omitido toda referencia a Cisjordania, donde Israel ha ido dando pasos hacia una anexión *de facto* que perjudica directamente a la causa palestina.

En una primera fase, este Plan de Paz facilitó que Hamás devolviera a todos los rehenes vivos e Israel liberara cerca de 2.000 presos palestinos y aceptase retirarse hasta la primera línea acordada. Aunque durante la tregua se han intercambiado ataques, las negociaciones de la segunda fase continúan, pero existen puntos críticos de difícil consenso, en particular respecto del futuro órgano de gobierno de la Franja, el desarme de Hamás y el despliegue de una fuerza internacional de estabilización, en la que queda por ver qué países participarán y qué misiones le son atribuidas. Asimismo, hay preocupación por el papel de la Autoridad Palestina, que debe tener un papel central en todos los órganos de transición, y su participación en todas las fases representa una condición indispensable para avanzar hacia la estabilización efectiva y la reconstrucción.

Finalmente, el 13 de octubre se celebró en Sharm el Sheikh la firma del Acuerdo de Paz, a la que acudió también el Presidente de Gobierno, Pedro Sánchez. Por su parte, el Consejo de Seguridad de Naciones Unidas (CSNU) aprobó el 17 de noviembre la Resolución 2803, basada en el plan de paz estadounidense, que autoriza la creación de una Junta de Paz y el despliegue de una fuerza internacional de estabilización en Gaza.

Actualmente está en marcha el proceso de generación de esta fuerza internacional, teniendo en cuenta las ofertas de diversos países. Por su parte, EEUU ha establecido el Centro de Coordinación Cívico Militar (CMCC) en localidad de Kiryat Gat (Israel), con representantes de varios Estados, para coordinar y supervisar la aplicación del alto el fuego y facilitar el flujo de ayuda humanitaria, logística y seguridad a Gaza. No obstante, el desarme de Hamás será el principal desafío de los países que aporten tropas para esta nueva misión internacional, que operará en un escenario altamente inestable, donde las amenazas para las fuerzas participantes serán muy altas.

En un primer momento, la respuesta militar de Israel a los ataques del 7 de octubre de 2023, la violencia, violaciones del derecho internacional y catástrofe humanitaria sobre el terreno, generaron fuertes críticas por parte del mundo árabe, como reflejan las resoluciones de la Liga de Estados Árabes y de la Organización de Cooperación Islámica. Sin embargo, el Plan de Paz cuenta con el apoyo de los vecinos regionales, al considerarlo una oportunidad para poner fin, sobre todo, a la crisis humanitaria vivida en Gaza.

Asimismo, todos los actores implicados están muy pendientes de los términos en los que se desarrolle la resolución de la segunda fase, para la que consideran imprescindible el amparo de la ONU y la inclusión de una solución política dirigida al establecimiento del Estado palestino, principal demanda de los países árabes. Además, mucho de ellos también han mostrado su disposición al envío de tropas para integrar la fuerza multinacional que se integraría en Gaza, en sustitución del Ejército israelí y las fuerzas de seguridad de Hamás.

No obstante, existe actualmente incertidumbre sobre varias cuestiones del plan, incluido el desarme de Hamás, la composición y funciones de la Junta de Paz, el mandato concreto de la fuerza de estabilización o el papel de la ONU, cuestiones todas ellas que no han quedado definidas en la Resolución CSNU 2803.

A su vez, en el seno de la Unión Europea, los Estados Miembros debaten sobre su implicación activa en la definición de las siguientes fases y la estabilización de la Franja. Se está estudiando las alternativas para reforzar y relanzar las misiones europeas de apoyo a la Autoridad Palestina: EUBAM Rafah y EUPOL COPPS. Por su parte, España contribuye a EUBAM Rafah con el mayor contingente (10 efectivos) junto con Italia.

La política exterior de España ha sido firme respecto del conflicto en Gaza. El Gobierno de España ha ejercido un firme liderazgo por la paz y la justicia, que refleja el sentir mayoritario de la opinión pública española. La posición española es reconocida por los principales actores regionales, y es en muchos casos pionera, señaladamente en lo relativo al reconocimiento del Estado de Palestina, que España llevó a cabo en mayo de 2024.

Ante las sistemáticas violaciones de derechos humanos y del derecho internacional, y la crítica situación humanitaria sobre el terreno, España ha trabajado intensamente para poner fin al conflicto sobre la base de un compromiso con el sistema multilateral, el derecho internacional y el derecho humanitario. En este sentido, a nivel nacional, el Gobierno ha adoptado medidas firmes con objeto de aumentar la presión sobre las partes y lograr el cese de hostilidades. En el marco de la Unión Europea, también ha abogado por la necesidad de adoptar sanciones comunitarias para garantizar el cumplimiento del derecho internacional y avanzar hacia una paz justa y duradera.

En foros internacionales, como la Alianza Global, el liderazgo de España ha sido determinante para movilizar a la comunidad internacional. En junio de 2025, España y Palestina impulsaron una Resolución de la Asamblea General de las Naciones Unidas sobre protección de la población civil y cumplimiento de las obligaciones jurídicas y humanitarias en relación con el conflicto en Gaza. Asimismo, la celebración de la Conferencia de Naciones Unidas para el Arreglo Pacífico de la Cuestión de Palestina y la Implementación de la Solución de Dos Estados (28-30 de julio y 11 de septiembre) también es muestra de ello, y permitió la de la Declaración de Nueva York, endosada posteriormente como Resolución de la Asamblea General.

Por su parte, las Fuerzas Armadas españolas, a través del mecanismo de Protección Civil de la Unión Europea, han llevado a cabo en 2025 dos operaciones de aerotransporte médico de personal civil enfermo procedente de Gaza, que, junto con sus familiares, se han trasladado desde Jordania para su tratamiento en hospitales españoles.

Hasta el momento, aunque la situación de seguridad en la región de Oriente Próximo sigue siendo incierta, con la caída del régimen anterior, se observa una mejoría en la situación en Siria, si bien la amenaza del Dáesh y de otros grupos insurgentes sigue siendo importante. Además, durante 2025, tuvieron lugar episodios de violencia entre Irán e Israel y la continuación del conflicto Israel-Hamás, que ha mantenido durante el año un ciclo de violencia con treguas. Israel ha logrado avances militares significativos contra el Eje de Resistencia proiraní, incluyendo golpes severos a Hamás, Hezbolá, Yihad Islámica Palestina en Gaza, Cisjordania, Líbano y Siria, la contribución a la caída del régimen sirio, la invasión del sur de Siria durante la caída de Damasco, la creación de una zona de seguridad en el sur del Líbano, bombardeos a objetivos hutíes en Yemen y ataques directos a Irán, junto con EEUU, que han destruido su defensa antiaérea así como su capacidad de misiles y afectado gravemente su programa nuclear.

No obstante, aunque el cumplimiento parcial del Plan de Paz sugiere avances diplomáticos y la tregua ha logrado reducir significativamente la tensión en Oriente Medio, la viabilidad del Plan de Paz es compleja y a corto plazo la coexistencia no parece posible, tan sólo avanzar en el plan y que el paso del tiempo consolide la reconciliación estructural. Igualmente, la crisis humanitaria, los ataques aislados y la posible reorganización de Hamás durante la tregua cuestionan la estabilidad a corto plazo.

Por su parte, España mantiene una presencia activa en la región para proteger sus intereses y contribuir a la estabilidad, participando en misiones de seguridad y protección diplomática, donde la Guardia Civil ha desplegado capacidades.

Adicionalmente, la Guardia Civil ha venido participando en 2025 en misiones europeas clave, como la EUPOL COPPS Palestina (hasta el 28 de noviembre de 2025), operando en relativa normalidad pese

al conflicto y sin presencia en Gaza; y en EUBAM Rafah, con dos equipos especializados en control policial de fronteras y en seguridad.

Mientras, en el Líbano, tras años de estancamiento político, Beirut ha logrado formar un nuevo Gobierno, caracterizado por una agenda reformista y su intención de lograr el monopolio estatal del armamento, que implica el desarme de Hezbolá.

En enero de 2025, Líbano puso fin al bloqueo institucional con el nombramiento como presidente del país del General Joseph Aoun, hasta entonces Jefe de las Fuerzas Armadas. La formación de un gobierno, dirigido por el Primer Ministro Nawaf Salam, ha permitido iniciar las reformas políticas y económicas necesarias para resolver las múltiples crisis a las que se enfrenta el Líbano en los últimos años, con el apoyo de la comunidad internacional.

Líbano se encuentra en una situación compleja tras el conflicto abierto con Israel y la presión para desarmar a Hezbolá. Israel mantiene su presencia en cinco posiciones y dos zonas de amortiguamiento en territorio libanés desde la operación terrestre lanzada en octubre de 2024, a pesar de llegar a un acuerdo de alto el fuego entre Israel y Hezbolá el 27 de noviembre de 2024 que preveía su retirada y el despliegue de las Fuerzas Armadas libanesas. El gobierno libanés ha aprobado un plan de desarme de las milicias, que incluye a Hezbolá, y ha aumentado su presencia militar en el sur, con el objetivo de alcanzar 10.000 efectivos desplegados. La fragilidad de dicho alto el fuego con Israel, marcado por incursiones israelíes en el sur para eliminar elementos de Hezbolá, ha elevado la tensión, con el presidente libanés ordenando respuestas del ejército que amenazan escalada bélica.

Por otra parte, el conflicto ha puesto en una posición muy complicada a la Fuerza Interina de Naciones Unidas en Líbano (UNIFIL), liderada por el General español Aroldo Lázaro hasta junio de 2025. España participa de manera ininterrumpida en UNIFIL desde 2006, como muestra de su compromiso con la estabilidad y seguridad del Líbano y de Israel, y con la paz en toda la región y con la plena implementación de la Resolución 1701 del CSNU. En este contexto de enfrentamientos, UNIFIL mantuvo sus posiciones sobre el terreno liderando España el sector Este, a pesar de las exigencias israelíes de retirada tras el inicio de su operación terrestre, y sigue desempeñando su mandato de verificación de alto el fuego y acompañamiento a las Fuerzas Armadas libanesas. El despliegue español en el Líbano continúa siendo, junto con Italia y Francia, uno de los más importantes de la UE.

En este contexto, marcado por la incertidumbre, el Consejo de Seguridad de Naciones Unidas aprobó la extensión por última vez del mandato de UNIFIL, que finalizará el próximo 31 de diciembre de 2026, con un calendario de retirada y repliegue a partir de esa fecha en un período no superior a un año. Esta decisión abre un nuevo escenario en Líbano, situando al país en una delicada encrucijada -con tensiones internas y presiones externas- para lograr la estabilización del país, y para lo que tendrá que contar con el firme respaldo de la comunidad internacional.

La prevista finalización de la misión de UNIFIL a finales de 2026, tras más de cuatro décadas plantea un escenario de incertidumbre y en un escenario de amenaza alta, dado que las Fuerzas Armadas libanesas no tienen los medios para desplegarse y controlar todo el sur del Líbano, e Israel mantiene sus ataques contra personal e infraestructura de Hezbolá. Está en proceso de definición el escenario post-UNIFIL, bien sea mediante una nueva misión de ONU, de la Política Común de Seguridad y Defensa o por acuerdos bilaterales.

España contribuye a la estabilización mediante UNIFIL, con un despliegue de 664 españoles, para verificar el cese de hostilidades y apoyar a la autoridad gubernamental sur del Litani. La Guardia Civil participa desde 2006 aportando un Provost Marshal y, desde 2007, con varios componentes para la Unidad de Policía Militar.

África

África Occidental, incluido el Sahel, es una de las prioridades de la estrategia España África 2025-2028.

Los países del Sahel Occidental continúan afectados por un elevado grado de inestabilidad a nivel político, de seguridad y económico, que constituye un foco de amenaza significativo para el vecindario sur de la OTAN, la UE y España. Especialmente, la situación en el Sahel central (Mali, Níger y Burkina Faso) se ha deteriorado dramáticamente en los últimos años, hasta convertirse en el centro de gravedad del terrorismo mundial. Las operaciones cada vez más complejas y coordinadas y el uso de armamento avanzado ponen de manifiesto la mejora de las capacidades de los grupos terroristas.

En 2025, los actuales gobiernos de transición de estos países, dirigidos por Juntas Militares que han alcanzado el poder a través de distintos golpes de Estado y que continúan fragmentadas, no han logrado revertir las situaciones de crisis crecientes, ni materializar sus planes de transición hacia gobiernos democráticos.

Por otro lado, la incapacidad de respuesta estatal para desarrollar estructuras de seguridad y consolidar la presencia de las fuerzas armadas y de seguridad en amplias zonas de sus territorios continúa generando un vacío que facilita la actividad de los grupos terroristas, de criminalidad organizada y de las redes de inmigración irregular. Así, a una situación política y de seguridad de por sí deteriorada, se suman el decrecimiento económico, la lucha endémica de las comunidades por el control de unos recursos naturales cada vez más escasos y las rivalidades intercomunitarias, que en su conjunto conforman un ecosistema de crisis complejas, de muy difícil solución a corto y medio plazo.

Al tiempo, el vacío de poder y de ausencia de estructuras de seguridad sólidas ha sido ocupado por otros países en competencia geopolítica en la región y que desarrollan unas agendas locales y regionales, en el marco de una estrategia global, frecuentemente divergentes con los intereses españoles.

En Mali, el número de ataques y muertes se ha reducido en los últimos años, pero se ha producido una expansión sin precedentes del Grupo de Apoyo al Islam y los Musulmanes (JNIM) que ha extendido su influencia hacia el oeste y el sur del país, llegando a cortar intermitentemente las principales vías de aprovisionamiento. En Burkina Faso las autoridades apenas controlan la mitad de territorio. En Níger el número de ataques ha aumentado y la cifra de víctimas terroristas ha incrementado notablemente.

El riesgo de extensión del conflicto a los países costeros del Golfo de Guinea es ya una realidad, sobre todo en Benín y Togo, donde en los primeros seis meses de 2025 se han producido más muertes relacionadas con ataques terroristas en el norte de ambos países que en todo 2024.

La estabilidad en los países de la banda del Sahel resulta clave para la seguridad de España y Europa debido a la permeabilidad fronteriza ante amenazas africanas, los recursos energéticos y mineros que atraen a diversos competidores. Por su parte, Rusia despliega una amplia variedad de instrumentos, tanto militares (*África Corps*), como híbridos y diplomáticos para influir en la región.

La mayor amenaza para la seguridad en la región continúa siendo la actividad terrorista, en especial la de JNIM, filial de Al Qaeda en el Magreb Islámico (AQMI), y también, aunque en menor medida, Dáesh en la Provincia del Sahel (ISSP), filial del Dáesh en la región. Durante el último año la actividad de estos grupos ha persistido e incluso se puede decir que ha aumentado, aun a pesar de los esfuerzos de las Juntas Militares de Burkina Faso, Mali y Níger, países que conforman la confederación de la Alianza de Estados del Sahel (AES).

Los países de la AES continúan con su fortalecimiento de relaciones con socios no occidentales y con el desarrollo de una política común en materia económica, diplomática y de seguridad. En este último punto destaca la puesta en funcionamiento de la Fuerza Unificada de la AES (FUAES), que ha llevado a cabo operaciones contraterroristas y, aunque de manera limitada, ha ido cosechando algún éxito con la neutralización de líderes terroristas.

Perseverar en la atención a la seguridad en África es necesario, tanto de forma bilateral como en el ámbito de la UE, la OTAN y de organizaciones regionales. Así, el compromiso de España incluye escenarios de cooperación terrestre, marítima (con especial proyección al Golfo de Guinea), y aérea, con un enfoque basado en el respeto y la comprensión de las necesidades específicas de asistencia de los países apoyados para reforzarse ante sus respectivos desafíos de seguridad.

La Unión Europea ha iniciado un proceso de reflexión para responder a la nueva situación política y de seguridad en el Sahel (*Renewed Approach*), en el que España ha tenido un papel activo. En abril (2025), España presentó un documento de reflexión a favor de una posición pragmática que permita a la UE estar presente en la región. En estos momentos, el estado de situación en la UE reside en una voluntad general de no abandonar el Sahel y de reanudar la cooperación a nivel técnico en sectores estratégicos, como la lucha contra el terrorismo y los tráfico ilícitos, incluida la migración ilegal. Actualmente se debate en el ámbito de la UE la articulación concreta de la Política Común de Seguridad y Defensa en la región en el marco de este enfoque renovado.

Desde hace varios años la UE ha movilizado más de 8.000 millones de euros en la región del Sahel, desplegando proyectos de buena gobernanza, gestión de fronteras, resolución de conflictos y lucha contra el terrorismo, entre otros. No obstante, en la actualidad, la UE se enfrenta a grandes desafíos geopolíticos en la región.

Tras el cierre en 2024 de la misión militar de entrenamiento de la UE en Mali (EUTM) y de la misión civil para el fortalecimiento de las capacidades de las fuerzas de seguridad interior en Níger (EUCAP Sahel Níger), tan solo continúa operando EUCAP Sahel Mali, cuyo mandato se ha extendido hasta el 31 de enero de 2027 y donde España participa con varios expertos. Por su parte, la EUCAP Sahel Mali tiene mecanismos para fortalecer la cooperación entre las fuerzas de seguridad malienses y las homólogas en otros países del arco saheliano como Chad, Burkina Faso, Níger y Mauritania.

Por su parte, España mantiene su colaboración, a través de la Policía Nacional, que continúa liderando la formación forense en Misión Multidimensional Integrada de Estabilización de las Naciones Unidas en la República Centroafricana (MINUSCA RCA), con profesionales de Policía Científica, así como de la Guardia Civil, que participa activamente mediante misiones y proyectos en EUCAP Sahel Mali y en la Misión Consultiva de la UE en la República Africana (EUAM RCA). Adicionalmente, el Ministerio del Interior apoya a través de sus Agregados en Marruecos, Mauritania, Senegal y Túnez, más un Oficial de Enlace con la Gendarmería marroquí. Igualmente, destaca la participación española en distintos proyectos como OTAN “Frontera Sur”, *CT-Public Spaces* o SEACOP V; así como en ejercicios, como el Flintlock 2025 en Costa de Marfil en el que participaron Guardia Civil y Fuerzas Armadas españolas.

España concede una especial atención al Golfo de Guinea. El 20% de los aprovisionamientos de petróleo de España proceden de esta región (solamente Nigeria aporta el 18% del petróleo y el 14% del gas natural que consume España). La disrupción del aprovisionamiento de los países enclavados del Sahel (casi el 100% del petróleo que consume Mali entra por los puertos de Abidjan, Dakar y Conakry) puede tener efectos negativos directos para España. España despliega buques de la Armada semestralmente en el marco de las Presencias Marítimas Coordinadas de la UE y apoya las iniciativas de la UE en materia de Seguridad Marítima. La Iniciativa de Seguridad y Defensa en el Golfo de Guinea (EU SDI GoG) se encuentra operativa en Costa de Marfil, Ghana, Benín y Togo, centrada en asistir en reforzar

las capacidades locales en la protección de rutas marítimas y la cooperación con fuerzas locales frente a amenazas de grupos armados no estatales. La piratería se mantiene latente en el golfo de Guinea, contenida, pero no erradicada. Se tiene constancia de la existencia de grupos activos piratas con capacidad para actuar en el golfo de Guinea y, por lo tanto, no se puede descartar que puedan llevar a cabo ataques a buques en aguas internacionales y secuestrar a sus tripulaciones.

Por otra parte, en el golfo de Adén, sur del mar Rojo y el estrecho de Bab El-Mandeb, la mayor amenaza a la seguridad marítima han sido los ataques al tráfico marítimo por parte de las milicias hutíes, que en 2025 hundieron dos mercantes en el mar Rojo, encuadrados dentro del apoyo de estas milicias a la causa palestina.

No obstante, con el alto el fuego acordado en Gaza, la tensión en el mar Rojo y golfo de Adén ha disminuido notablemente. Así, en el marco de la Operación EUNAVFOR Atalanta que se desarrolla en este área, destaca el descenso del número de acciones de piratería y la mejora de seguridad en la zona. Sin embargo, la persistencia de la piratería como amenaza evidencia la necesidad de mantener la operación Atalanta en la zona para contribuir a la seguridad marítima en el área. España es la nación líder de la operación y la única que ha aportado unidades de manera ininterrumpida desde el comienzo de la operación en 2008.

La Operación EUNAVFOR Atalanta ha continuado en 2025 desempeñando su mandato con eficacia, destacando la lucha contra la piratería en su área de operaciones, el fomento de redes de cooperación con actores regionales, con actividades conjuntas y la llamada “diplomacia naval” y las actividades de inteligencia marítima. España, que aloja su cuartel general operacional en Rota, continuará apoyando en 2026 la operación. La labor de la misión se ha visto ampliada con tareas de inteligencia para el seguimiento de la conocida como “Flota Fantasma” rusa.

Mientras, en Somalia, continúa la Misión de Entrenamiento de la UE en (EUTM-Somalia), donde el principal reto que afronta el país continúa siendo la seguridad frente a la amenaza yihadista.

Por otra parte, en Mozambique, la crisis sociopolítica derivada de las elecciones presidenciales de OCT24 se encuentra relativamente estabilizada. Esta crisis impactó de manera muy superficial a la misión de asistencia militar de la UE (EUMAM Mozambique) en la que participa España con dos observadores.

A su vez, el Magreb, continúa siendo una zona clave para la seguridad y defensa de nuestro país.

En 2025, las relaciones bilaterales con los países del Magreb continuaron reforzándose, con ocasiones de consolidación institucional de la relación y visitas de alto nivel. España celebró su I Reunión de Alto Nivel con Mauritania, el 16 de julio en Nuakchot, precedida de un encuentro empresarial; y la XIII RAN con Marruecos, que tuvo lugar en Madrid el 4 de diciembre de 2025. Asimismo, la IV Conferencia Internacional sobre Financiación al Desarrollo, celebrada en Sevilla entre el 30 de junio y el 3 de julio, contó con una amplia participación de líderes de los países del Magreb. Asistió el primer ministro marroquí, Aziz Akhannouch, el primer ministro argelino, Nadir Larbaoui, el presidente de la República de Mauritania, Mohamed Ould Cheikh Ghazouani, la primera ministra de Túnez, Sara Zaafrani Zenzri, y el presidente del Consejo Presidencial libio, Mohamed Yunus Al-Menfi.

Las relaciones económicas continúan siendo excelentes. En 2025, España fue el primer socio comercial para Marruecos (de manera ininterrumpida desde 2012); en relación con Argelia, las exportaciones españolas se incrementaron más de un 168%, siendo Argelia el principal suministrador de gas natural de nuestro país. Todo ello en el contexto más amplio de las relaciones de la UE-Magreb, salvo en el caso de Mauritania, la UE sigue siendo con diferencia el principal socio comercial de todos los países de la región.

En el ámbito de la seguridad, sigue destacando el impacto en la región de la inestabilidad en el Sahel, causa de movimientos de población que están en el origen de una parte de los flujos migratorios irregulares hacia Europa. La cooperación para afrontar este fenómeno, tanto en clave europea como bilateral, ha resultado esencial y fructífera. En 2025, fruto de esta colaboración, se redujeron ostensiblemente las llegadas irregulares a Canarias, con una disminución del 62% respecto del año anterior.

También en el ámbito de seguridad de la OTAN, se ha continuado trabajando en el marco del Diálogo Mediterráneo, reforzado en 2024 con el lanzamiento en la cumbre de Washington del Plan de Acción para la Vecindad sur que propone bases concretas para hacer frente a los desafíos en la región a través de un enfoque más estratégico y orientado a los resultados y en el que España desempeña un importante papel impulsor.

Mención específica merece la evolución de Libia y el refuerzo del papel de España en apoyo de los esfuerzos de Naciones Unidas, a través de UNSMIL y la Representante Especial del Secretario General de la ONU para Libia, Hannah Tetteh, en el actual conflicto interno libio. En 2025 Naciones Unidas ha establecido una hoja de ruta para lograr la celebración de elecciones presidenciales y parlamentarias que conduzcan a la reunificación institucional y a la reconciliación nacional, y se ha reactivado el proceso de Berlín al que España se ha incorporado, participando en la reunión del Comité de Seguimiento Internacional para Libia.

Finalmente, en línea con la apuesta de España por mantener el Mediterráneo como una prioridad estratégica de su acción exterior, en el marco de la celebración del 30 aniversario del Proceso de Barcelona en 2025 se ha lanzado el Nuevo Pacto del Mediterráneo y la Nueva Visión Estratégica de la Unión por el Mediterráneo, reforzando el nuevo paradigma en la relación de la UE con su Vecindad Sur y los instrumentos de la política euromediterránea.

A este respecto, la Iniciativa “5+5 Defensa” se ha mantenido como un foro de diálogo privilegiado que reúne a los diez países del Mediterráneo occidental: Portugal, España, Francia, Italia y Malta del lado europeo, y Mauritania, Marruecos, Argelia, Túnez y Libia por el lado de la ribera africana.

Finalmente, en el marco de las misiones de Diplomacia de Defensa en África, se llevan a cabo actividades de seguridad cooperativa, en particular en el ámbito de la seguridad marítima y la enseñanza. En este sentido, se continúan impulsando estas actividades de cooperación para mejorar la preparación de las Fuerzas Armadas de los países socios en el Norte de África con la finalidad de fortalecer sus capacidades y la formación de sus mandos fundamentalmente a través del Programa de Cooperación Internacional en Materia de Enseñanza Militar.

Asia-Pacífico y Central

La región de Asia-Pacífico se ha consolidado como uno de los principales centros de gravedad de la geopolítica y la geoeconomía mundial, donde confluyen los intereses estratégicos de las grandes potencias y se intensifica la competencia sistémica, en particular entre Estados Unidos y China. En este contexto, Estados Unidos continúa reforzando su red de alianzas y partenariados de seguridad, como AUKUS con Reino Unido y Australia, el Quad con Australia, India y Japón, o diversas iniciativas trilaterales con Japón, Corea o Filipinas, y la Unión Europea despliega su Estrategia de cooperación para el Indo-Pacífico y potencia la agencia estratégica con socios como la India. La región concentra aproximadamente el 60 % de la población mundial, el 45% del PIB global y cerca del 45% de la producción industrial, lo que explica su creciente centralidad en las relaciones internacionales.

España ha reforzado su proyección hacia Asia-Pacífico mediante la Estrategia española para Asia-Pacífico 2026-2029 aprobada por el Consejo de Ministros el 9 de diciembre de 2025, hoja de ruta que orienta una acción exterior más activa hacia esta región. España apuesta por profundizar sus relaciones políticas, económicas y de cooperación con los países asiáticos, como reflejan el viaje de Sus Majestades los Reyes a China en 2025, las visitas del Presidente del Gobierno a China, Corea, India, Japón y Vietnam, y el apoyo a la conclusión de acuerdos de libre comercio de la UE con socios como India, Indonesia y Nueva Zelanda. Aumenta asimismo la cooperación científica, tecnológica, educativa y cultural, apoyándose en el sistema universitario español, en redes europeas como Horizonte Europa y en instrumentos como Casa Asia y las Fundaciones Consejo con Australia, China, India y Japón.

EEUU y China siguen compitiendo por la influencia en diversas regiones del mundo. A la rivalidad político-diplomática, se une la tendencia a un mayor desacoplamiento económico y a la instrumentalización política de las cadenas de suministro, en particular, la competencia por recursos energéticos y minerales críticos como el litio, el cobalto y las tierras raras.

La reconfiguración de las cadenas de suministro tras la pandemia, por la guerra de Ucrania, y en el mencionado contexto de la creciente rivalidad entre EEUU y China, es una realidad con profundas implicaciones económicas, geopolíticas y, sobre todo, de seguridad.

Este contexto convive con varios focos de tensión que continúan condicionando la seguridad regional, entre ellos la crisis en Myanmar, la evolución de la situación en la península de Corea, marcada por el fortalecimiento de los vínculos entre Corea del Norte y Rusia, y las tensiones en el estrecho de Taiwán y en el mar de China Meridional.

Respecto a Afganistán, es reseñable como el Movimiento Talibán busca activamente el reconocimiento internacional, aunque el país no da ninguna muestra de integración internacional y, en la actualidad, continúan las tensiones entre Afganistán y Pakistán en la frontera de ambos países. Además, persisten numerosos desafíos debido al incremento del terrorismo, principalmente del Movimiento de los Talibanes Pakistaníes (Tehrik-i-Taliban Pakistan, TTP), que encuentra su refugio en Afganistán DIH. (Figura 1.4)



Fuente: Jefatura de Información de la Guardia Civil

Figura 1.4: Mapa de localización de grupos terroristas en Afganistán (frontera con Pakistán)

América Latina y el Caribe

La implementación del Acuerdo de Paz entre el Gobierno colombiano y las FARC, firmado en 2016, ha sido un proceso complejo y lleno de desafíos. Si bien se han logrado avances importantes, como la desmovilización de 13.000 guerrilleros, la reincorporación de los excombatientes a la vida civil y el establecimiento de políticas de reparación para las víctimas, persisten varios obstáculos.

Las disidencias de las FARC y otros grupos armados han mantenido una presencia activa, lo que ha empeorado la seguridad de varias regiones del país. Además, la implementación de reformas estructurales en áreas como la reforma rural y la justicia transicional ha avanzado a un ritmo más lento de lo esperado, y el contexto político interno en Colombia ha generado desacuerdos sobre la profundidad y la efectividad de la implementación.

El 31 de octubre de 2025, el Consejo de Seguridad de Naciones Unidas adoptó la Resolución 2798 (2025), por la que se prorroga, con algunos ajustes, el mandato de la Misión de Verificación en Colombia. El mandato renovado se centrará en tres aspectos fundamentales del Acuerdo de Paz: la reincorporación política, económica y social de los excombatientes de las FARC-EP; las garantías de seguridad para firmantes de paz, sus familias, líderes y comunidades afectados por el conflicto y la reforma rural.

Por su parte, España mantiene su firme compromiso con la implementación del mencionado Acuerdo de 2016, tanto a través del apoyo de la Cooperación Española como mediante el despliegue de observadores militares en la Misión de Verificación. Además, apoya la política de Paz Total y mantiene su implicación, como país acompañante, en el proceso de negociación con el ELN, pese a su estancamiento. El Gobierno colombiano ha reconocido en múltiples ocasiones el apoyo activo de España, como aliado clave cuya constancia y credibilidad refuerzan la legitimidad de los distintos procesos en un contexto de crecientes desafíos de seguridad y polarización interna. En noviembre 2025, España se incorporó como mediadora al proceso negociador entre el Gobierno de Colombia y el autodenominado “ejército gaitanista” de Colombia.

Así, España ha sido un aliado estratégico en la implementación del Acuerdo, tanto en términos de respaldo diplomático como a través de programas de cooperación para la reintegración de excombatientes y para el fortalecimiento de la justicia transicional. Igualmente, a nivel europeo, España ha sido una voz influyente en la UE, instando a una mayor colaboración internacional para garantizar que se logren los objetivos del Acuerdo. Asimismo, ha expresado sus preocupaciones respecto a la persistencia de la violencia en ciertas zonas del país y ha enfatizado la necesidad de que el proceso de paz sea inclusivo, no solo para los excombatientes de las FARC sino para todas las víctimas del conflicto colombiano, incluidas las comunidades más vulnerables y los líderes sociales.

Por otra parte, respecto a Haití, la Misión Multinacional de Apoyo a la Seguridad (MSS, por sus siglas en inglés) en Haití, fue establecida en octubre de 2023 en virtud de la Resolución 2699 del Consejo de Seguridad de Naciones Unidas, tras la solicitud del Gobierno de Haití de asistencia internacional urgente ante el grave deterioro de la situación de seguridad. La Misión se concibió como un esfuerzo multinacional de carácter no perteneciente a Naciones Unidas, con el mandato de apoyar a la Policía Nacional de Haití (HNP) en la restauración de la seguridad, la estabilización de infraestructuras críticas y la creación de condiciones necesarias para el acceso de la ayuda humanitaria y la reanudación de los procesos políticos e institucionales.

Ante el interés del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación en contribuir a la misión, la Guardia Civil puso a disposición a un Oficial en la Oficina de Apoyo a la Misión de Apoyo a la Seguridad en Haití, en Washington (EEUU). La oficina coordina los esfuerzos diplomáticos, logísticos y de comunicación estratégica y actúa como principal punto de enlace entre la Misión sobre el terreno, Naciones Unidas, la OEA, los países donantes y las organizaciones regionales.

Por otra parte, el Proyecto EU-OMA-COLIBRI se encuentra en su segunda fase, con el objetivo de intensificar la coordinación y los esfuerzos internacionales con el fin de luchar contra la delincuencia organizada y hacer frente a los retos que plantea el tráfico de cocaína en América Latina y el Caribe, así como en África Occidental y Central. Está orientado principalmente al control y la vigilancia de la aviación general, y es coordinado por las Fuerzas y Cuerpos de Seguridad del Estado.

A su vez, la Guardia Civil ha participado en otros proyectos de lucha contra el tráfico ilícito de drogas y el crimen organizado, con la aportación de expertos a corto plazo, como son el desarrollado a apoyar a la Policía Nacional del Perú o a la Policía de Bolivia (UE-FIAP).

Por último, cabe señalar la participación de Fuerzas y Cuerpos de Seguridad del Estado en el Programa El PACCTO (Europa Latinoamérica Programa de Asistencia contra el Crimen Transnacional Organizado), iniciativa de cooperación internacional impulsada por la Unión Europea para fortalecer las capacidades institucionales en América Latina en la lucha contra el crimen organizado, el narcotráfico, la corrupción y otras amenazas transnacionales. La participación ha consistido en asistencia técnica para formación y asesoramiento, capacitación especializada sobre metodologías de investigación, inteligencia operativa y cooperación internacional, y sobre fortalecimiento institucional.

Finalmente, en cuanto a Venezuela, a cierre de 2025, la crisis se ha visto acompañada por un incremento significativo de la tensión en el Caribe, con el despliegue estadounidense “*Southern Spear*”, que ha incluido ataques e interceptaciones a embarcaciones vinculadas a redes de contrabando y narcotráfico.

Diplomacia humanitaria

La diplomacia humanitaria de España es componente clave de la seguridad nacional. Su aplicación contribuye a crear y preservar espacios de paz, reducir los riesgos derivados de los conflictos armados, proteger a las poblaciones más vulnerables frente a los efectos del cambio climático y favorecer la estabilidad regional y global.

Con la Estrategia de Diplomacia Humanitaria (2023-2026), España ha definido un marco sólido para orientar su acción exterior, promoviendo el respeto del Derecho Internacional Humanitario, la protección de las personas más vulnerables y el acceso humanitario seguro y eficaz a la ayuda en contextos de crisis, mediante liderazgo diplomático y respaldo operativo.

En el ámbito de Naciones Unidas, España está dando seguimiento e impulsando el “Reset Humanitario”, para reformar la arquitectura humanitaria global y adaptarla al nuevo contexto internacional, marcado por la multiplicación de conflictos y la creciente crisis de financiación, fomentando la eficiencia, la diversificación de fuentes de financiación y el refuerzo de actores locales en la respuesta humanitaria. España también ha reforzado su cooperación con agencias humanitarias clave como el Programa Mundial de Alimentos, la Agencia de la ONU para los Refugiados (ACNUR) o Agencia de Naciones Unidas para la población refugiada de Palestina (UNRWA), contribuyendo a garantizar la asistencia vital, la protección de las personas refugiadas y desplazadas, y la respuesta a necesidades humanitarias en contextos de alta complejidad.

En un escenario de hiper priorización de las necesidades y de drástica caída del apoyo financiero al ecosistema humanitario, España reforzó su presencia en contextos prioritarios, con un esfuerzo presupuestario de 181 millones de euros en 2024, de los cuales 133 millones correspondieron a la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), destinados a responder a crisis en América Latina, el Sahel, Sudán, Ucrania, Afganistán y Oriente Medio, especialmente Palestina. Según cifras aún provisionales, el presupuesto humanitario de la Dirección de Acción Humanitaria de la AECID en 2025 fue de 123,9 millones de euros.

De este modo España sigue avanzando en el cumplimiento de sus compromisos de financiación internacional, hacia el cumplimiento del compromiso legal de alcanzar el 0,7% de la Renta Nacional Bruta (RNB) para Ayuda Oficial al Desarrollo (AOD) en 2030 y el 10% de la AOD para acción humanitaria.

En Gaza y Ucrania, España ha mantenido una posición coherente de diplomacia humanitaria como la mejor vía para generar confianza en el sistema multilateral, defendiendo la aplicación universal del Derecho Internacional Humanitario y de los principios humanitarios de neutralidad, imparcialidad e independencia, la protección de civiles y de bienes indispensables para la supervivencia, y el acceso humanitario seguro y entrada sostenida y sin trabas de ayuda humanitaria. En el caso de Gaza, España ha intensificado la entrega de ayuda humanitaria a través de la Dirección de Acción Humanitaria, destinando 24 millones de euros en 2025 y superando los 50 millones acumulados desde el 7 de octubre de 2023, para asistir a millones de personas desplazadas o afectadas tanto en Gaza, como en Cisjordania.

En el seno del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, España ha respaldado la Iniciativa Global del Comité Internacional de la Cruz Roja sobre Derecho Internacional Humanitario, asumiendo liderazgo y participación en la protección de la misión médica y los hospitales, un pilar fundamental del Derecho Internacional Humanitario que obliga a salvaguardar al personal, instalaciones y transportes sanitarios, prohibiendo los ataques contra los mismos.

Por último, en el ámbito de la Unión Europea, España ha reforzado la coordinación con las instituciones y Estados miembros para alinear posiciones, movilizar recursos y mejorar la interoperabilidad en la preparación y respuesta humanitaria, contribuyendo a una acción europea más coherente y eficaz ante crisis internacionales.

España en la OTAN

La actual postura estratégica de la OTAN viene definida por el Concepto Estratégico aprobado en la Cumbre de Madrid de 2022, que reafirma como propósito principal de la Alianza garantizar la defensa colectiva de sus miembros sobre la base de un enfoque de 360 grados.

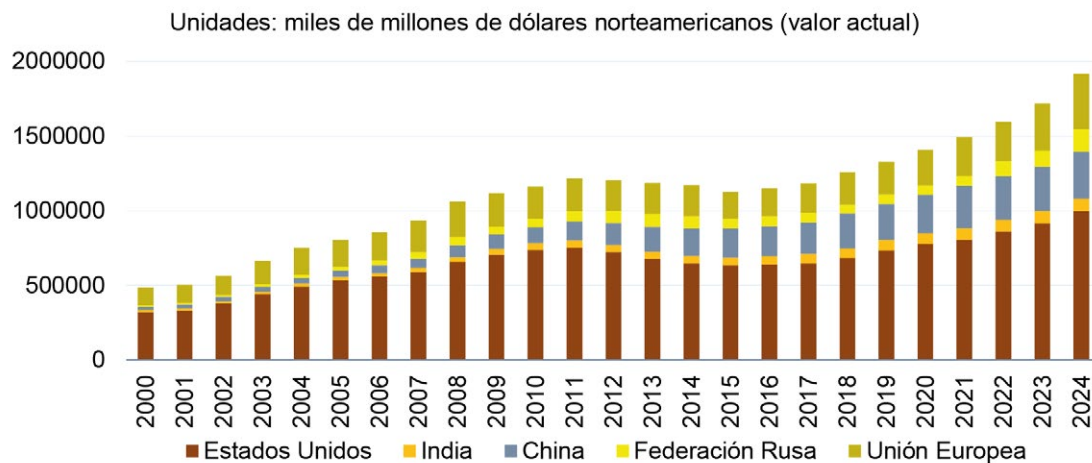
España, aliada desde 1982, desempeña un papel activo y reconocido en la OTAN, proyectándose como proveedor de seguridad para sus aliados y socios y basando su actuación en el compromiso y la solidaridad como principio esencial de la cohesión de la Alianza. Su contribución es sostenida y se materializa en la participación muy significativa en uno de los elementos clave como son los despliegues de la OTAN tanto en el flanco Este como en la Vecindad Sur, en la aportación de capacidades terrestres, navales y aéreas altamente interoperables, y en la puesta a disposición de infraestructuras estratégicas en su territorio, incluidos los importantes nodos de proyección y apoyo logístico que suponen las bases de Rota y Morón y los distintos cuarteles generales de la OTAN en territorio español. España ha sido además uno de los impulsores de la atención reforzada al flanco sur, subrayando la interrelación entre la seguridad del vecindario meridional, y en particular el Sahel,

el Norte de África y Oriente Próximo, y la seguridad del conjunto de la Alianza, y apoyando una acción coherente en el seno de la OTAN entre la Alianza y las prioridades de la política de seguridad y defensa de la Unión Europea.

Gasto e inversión en Defensa y participación industrial

El aumento del gasto en Europa, impulsado en gran medida por la guerra en curso entre Rusia y Ucrania, y en Oriente Medio, a raíz de la guerra en Gaza y los conflictos regionales más amplios ha llevado a un aumento por segundo año consecutivo del gasto militar en las cinco regiones geográficas del mundo (África, Oriente Medio, Asia y Oceanía, Europa y América).

Así, durante 2024, tal y como recogen los datos del Instituto Internacional de investigación para la Paz de Estocolmo, el gasto militar mundial aumentó hasta 2.718.000 millones de dólares, con un aumento del 9,4%, lo que constituye el incremento interanual más pronunciado desde al menos 1988. (Figura 1.5)



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

Figura 1.5: Evolución del gasto en defensa a nivel mundial

Entre 2021 y 2025, los cinco mayores proveedores de armamento principal fueron Estados Unidos, Francia, Rusia, Alemania y China, mientras que los principales importadores de armamento en dicho período fueron Ucrania, India, Arabia Saudí, Qatar y Pakistán. (Figura 1.6)

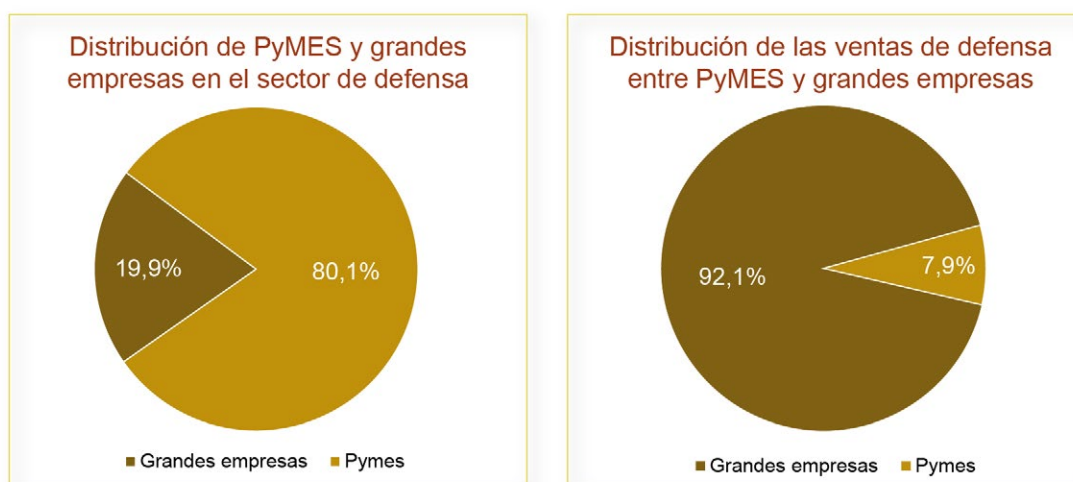
Figura 1.6: Principales exportadores e importadores de armamento en 2021-2025

EXPORTADORES	Porcentaje global (%)	IMPORTADORES	Porcentaje global (%)
1. Estados Unidos	42	1. Ucrania	9,7
2. Francia	9,8	2. India	8,2
3. Rusia	6,8	3. Arabia Saudí	6,8
4. Alemania	5,7	4. Qatar	6,4
5. China	5,6	5. Pakistán	6,4
6. Italia	5,1	6. Japón	3,9
7. Israel	4,4	7. Polonia	3,6
8. Reino Unido	3,4	8. Estados Unidos	2,9
9. Corea del Sur	3,0	9. Kuwait	2,8
10. España	2,3	10. Australia	2,9

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

En cuanto a la participación de la industria española de Defensa, cabe destacar que, en el año 2024 la distribución del tamaño de las empresas en el conjunto de la industria nacional (sectores defensa y civil) está dominada por la presencia de un 99,8% de PyMES y el 0,2% de grandes empresas. Sin embargo, el perfil de la base industrial de defensa es diferente: está igualmente dominado por las pequeñas y medianas empresas, pero en menor medida, ya que su participación sobre el conjunto de la industria de defensa es del 80,1%, mientras que las grandes empresas representan el 19,9%.

El dato anterior contrasta con otra realidad: Cuando se analiza la distribución de las ventas según el tamaño empresarial, aunque las PyMES representen el 80,1% del total de empresas, su participación en las ventas de defensa es del 7,9%. (Figura 1.7)

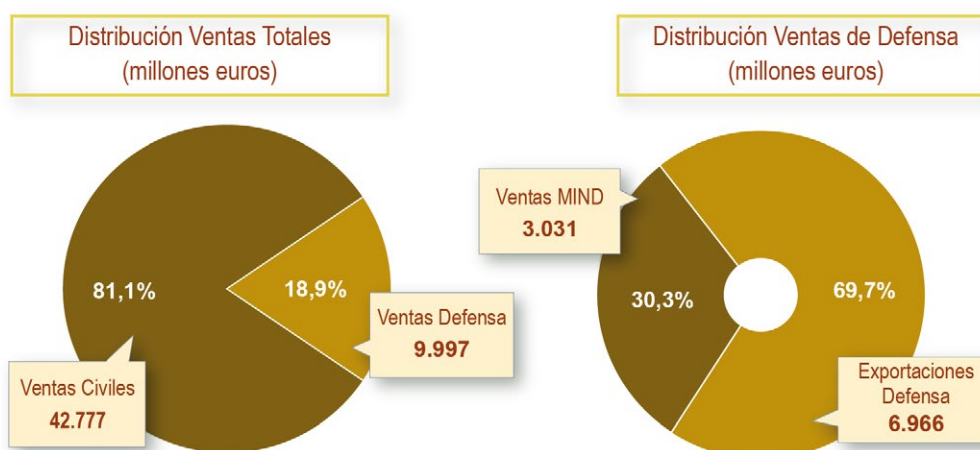


Fuente: Ministerio de Defensa

Figura 1.7: Distribución de las empresas en el sector de defensa y sus ventas

Las grandes empresas continúan acumulando la mayor parte del negocio en el sector defensa, especialmente en el ámbito internacional, donde su capacidad operativa y redes comerciales les otorgan una posición dominante. Sin embargo, la intervención del Ministerio de Defensa en el mercado interno contribuye a mitigar esta concentración, facilitando el acceso de las PyMES al ecosistema de defensa, y su participación en la cadena de valor del sector, ya sea por contratación directa, y especialmente a través de las subcontrataciones, cuyas cifras no deben incluirse en el análisis macroeconómico principal para evitar duplicar las cifras de ventas generales. No obstante, si analizamos las cifras de estas ventas indirectas, observamos que el alcance de las PyMES es significativamente mayor en esta parcela del mercado de defensa. Estas operaciones alcanzan un total de 2.625 millones de euros, siendo la participación de las PyMES en esta ocasión del 15,1% sobre ese total.

Las ventas de defensa directas (al Ministerio de Defensa y exportaciones) declaradas por la industria en el año 2024 son de 9.997 millones de euros, un 17,1% más que el año anterior. Estas ventas se reparten entre 3.031 millones de euros de ventas al Ministerio de Defensa (un aumento del 35,2% con respecto al 2023), y 6.966 millones de euros de exportaciones de defensa (un aumento del 10,6% con respecto al 2023). (Figura 1.8)



Fuente: Ministerio de Defensa

Figura 1.8: Ventas de defensa por subsectores

Bajo la denominación de industria de defensa se engloba a numerosas compañías suministradoras de equipos, sistemas o servicios de armamento y material, infraestructura, sistemas de información y telecomunicaciones de aplicación militar. Debido a esta diversidad, se hace indispensable encuadrarlas en subsectores, sistemas y subsistemas que permitan la clasificación del tejido industrial. La industria de defensa en España dispone de un sólido y diverso conjunto de capacidades industriales, respaldado por empresas con experiencia en el diseño, desarrollo e integración de sistemas complejos en los ámbitos naval, terrestre y aéreo.

En el año 2024 las ventas de defensa por subsector destacan, como es costumbre, las del subsector aeronáutico, especialmente por sus exportaciones, si bien resultan muy relevantes este año las asociadas a sistemas de munición y a plataformas navales. (Figura 1.9)



Fuente: Ministerio de Defensa

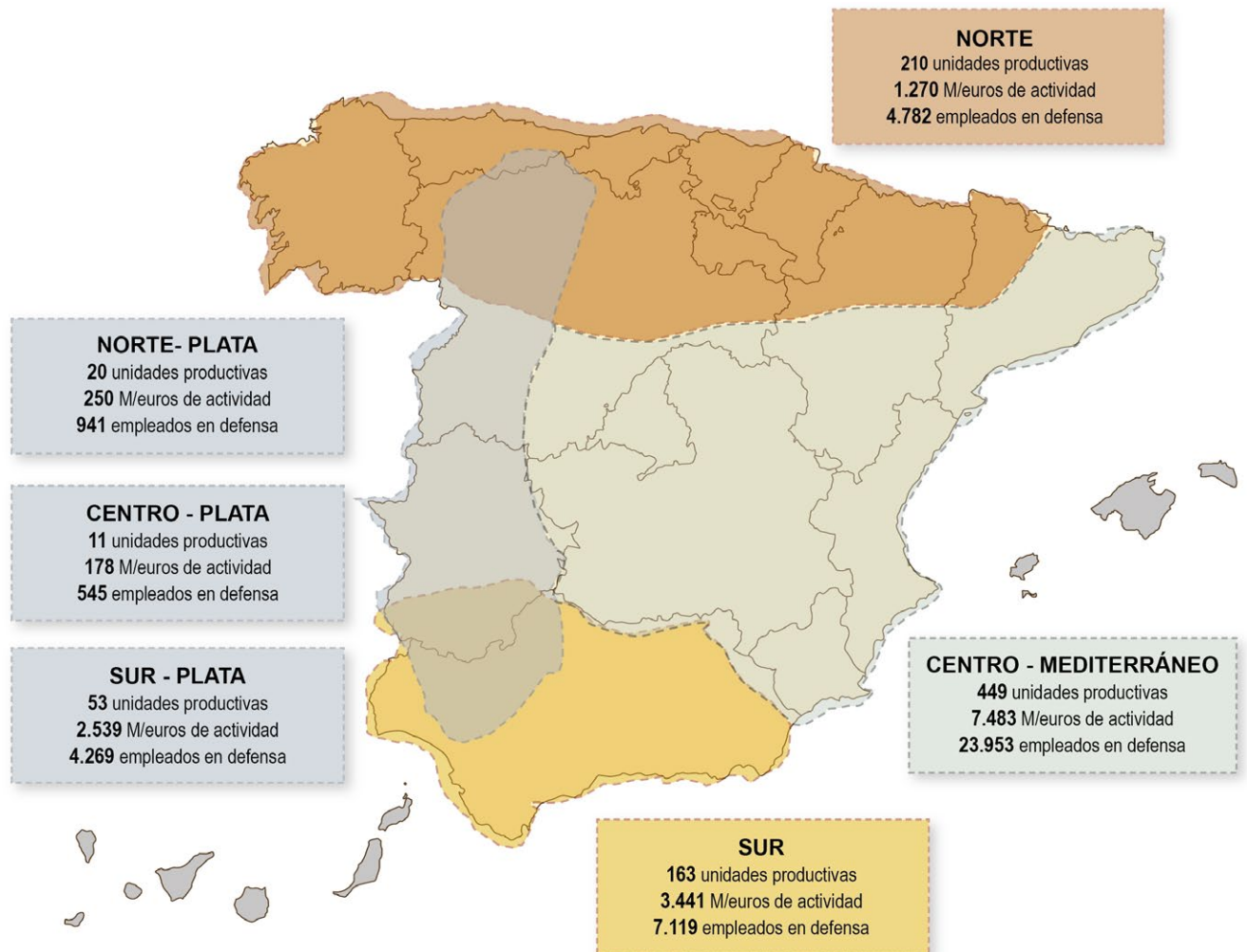
Figura 1.9: Ventas de defensa por subsector y tipología

Según la Estrategia Industrial de Defensa 2023, la industria de defensa está llamada a ser un motor de distribución de riqueza a través de inversiones públicas y privadas, promoviendo que la financiación alcance los niveles más bajos de la cadena de suministro y se extienda lo máximo posible por todo el territorio nacional.

La Base Industrial y Tecnológica de Defensa (BITD) se organiza en tres grandes corredores industriales: el Corredor Norte, el Corredor Centro Mediterráneo y el Corredor Sur. Estos corredores actúan como redes capilares que extienden los beneficios de las inversiones en defensa a lo largo del territorio nacional, permitiendo que empresas de distintas regiones se integren en la cadena de suministro del sector. Esto contribuye a la generación de empleo altamente cualificado y al fortalecimiento de las economías regionales.

Con el objetivo de ampliar esta capacidad de impacto territorial, se plantea no solo la expansión de los tres corredores existentes, sino también la creación de nuevos ejes industriales. Esta estrategia busca impulsar el desarrollo del sector industrial y tecnológico, así como fomentar la creación de empleo especializado. En este marco, se propone el impulso de un cuarto corredor: el Corredor de La Plata.

La imagen (Figura 1.10) presenta un resumen de los principales indicadores de los cuatro corredores industriales de la BITD: número de unidades productivas o centros de actividad, volumen de actividad en defensa, medido en ventas, y empleo directo generado en el sector. Dado que el Corredor de La Plata se solapa parcialmente con los corredores Sur y Norte, los datos correspondientes a las zonas de confluencia se han desglosado por separado. Esta diferenciación permite una lectura más precisa del impacto territorial y económico de cada corredor, evitando duplicidades y facilitando el análisis comparativo.



Fuente: Ministerio de Defensa

Figura 1.10: Corredores industriales

Por otra parte, la Comisión Europea ha estado promoviendo el gasto en defensa, las compras conjuntas y, sobre todo, la consecución europea de una autonomía estratégica. Se espera que la tendencia continúe durante los próximos años, independientemente de los desarrollos que se produzcan en el conflicto de Ucrania. Sin embargo, podrían surgir diferencias entre los Estados miembros que pretendan mantener o aumentar su industria de defensa frente al resto de países de la UE.

Finalmente, en lo relativo a la inversión en I+D en Defensa, la inversión declarada por las empresas que integran la base de datos del Registro de la Industria de Defensa ha sido en el año 2024 de 953 millones de euros. Este escenario de tensión geopolítica y creciente inestabilidad global ha puesto de manifiesto la urgente necesidad de invertir en defensa para garantizar la seguridad y la autonomía estratégica europeas. En este contexto, el Plan Industrial y Tecnológico para la Seguridad y la Defensa ha asignado al Centro para el Desarrollo Tecnológico y la Innovación (CDTI) del Ministerio de Ciencia, Innovación y Universidades, para el ejercicio 2025, un total de 500 millones de euros.

De esta cantidad, 300 millones de euros se han destinado a inversiones en fondos de capital riesgo especializados que ayuden a fomentar un ecosistema de defensa; otros 100 millones se han consignado a líneas de subvenciones para consorcios empresariales y empresas de base tecnológica en el ámbito de seguridad y defensa; 50 millones se han orientado expresamente al fortalecimiento y la mejora de las capacidades de centros tecnológicos y centros de excelencia en cuanto a proyectos transversales; y otros 50 millones a actividades de compra pública precomercial de prototipos y demostradores y/o convenios estratégicos en el ámbito de la seguridad y la defensa.

En cuanto a las líneas de subvenciones, destaca la orientada a la capacitación para la autonomía estratégica en seguridad y defensa que, dotada con 80 millones de euros, persigue contribuir a dotar a España, por medio de la I+D empresarial, de una mayor soberanía estratégica en determinados ámbitos de actividad relativos a seguridad y protección de la información, sistemas automatizados y de gestión remota, plataformas aéreas, terrestres o navales, protección y seguridad de infraestructuras críticas y protección frente a riesgos NRBQ.

Adicionalmente, y en base al Protocolo General de Actuación entre el Ministerio de Defensa y el Ministerio de Ciencia, Innovación y Universidades, firmado en 2019, el CDTI financia proyectos de tecnologías duales de interés para el Ministerio de Defensa. Desde su entrada en vigor hasta la fecha se han presentado un total de 147 proyectos, siendo aprobados 98 (a los que cabría sumar otros 16 proyectos, actualmente en proceso de evaluación). El presupuesto aprobado total para estas actuaciones es de 157 millones de euros, de los cuales la aportación CDTI asciende a 114 millones de euros.

Concretamente, en 2025 se han presentado, hasta el momento, 25 proyectos de estas características, con un presupuesto asociado próximo a los 33 millones de euros. De estos, hasta la fecha se han aprobado un total de 8, con un presupuesto de 8,5 millones de euros y una aportación CDTI próxima a los 6,5 millones de euros.

La Agencia Estatal de Investigación ha financiado dos proyectos de investigación relacionados con la tensión estratégica por importe de 118.750,00 €.

Todas estas iniciativas se alinean con la nueva Estrategia de Tecnología e Innovación para la Defensa (ETID 2026), cuya publicación está prevista en el primer trimestre de 2026, que establece el marco de referencia para orientar la I+D+i en el conjunto del sector de la defensa y define las capacidades tecnológicas prioritarias que España debe desarrollar para reforzar su autonomía estratégica. La ETID impulsa una colaboración más estrecha entre administraciones, industria y centros de investigación, y refuerza la participación de nuestro país en programas europeos e internacionales de innovación en defensa. Con ello, se articula un marco de actuación coherente que integra inversiones, cooperación en I+D+i y proyectos de alto impacto tecnológico, asegurando que los esfuerzos nacionales de innovación contribuyan de manera efectiva al fortalecimiento de las capacidades militares y a la competitividad de la base industrial y tecnológica de la defensa.

Las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad en el Exterior

En el año 2025, las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y las Fuerzas Armadas han desplegado más de 19.601 componentes en el exterior durante 2025 para apoyar en la promoción del sector seguridad de países amigos, facilitar la proyección de la estabilidad internacional o atender a la disuasión frente a amenazas externas, siempre dentro del marco establecido por las líneas estratégicas fundamentales en el ámbito de la Defensa y enmarcadas dentro de operaciones de Organismos Internacionales (ONU, OTAN y UE), de actividades bilaterales o de Coaliciones que atienden las peticiones de aquellos países donde se actúa.

Así, han tenido presencia en 8 misiones civiles de la Política Común de Seguridad y Defensa (PCSD) de la Unión Europea: EUBAM Rafah y EUPOL COPPS, en Palestina, EUAM Ucrania, EUCAP Sahel Malí, EUAM Irak, EUBAM Libia, EUAM RCA y EUSDI Golfo de Guinea, con un total de 47 funcionarios desplegados, superando los datos de años anteriores; lo cual pone de manifiesto el compromiso del Ministerio del Interior para con la consecución de los objetivos establecidos en el Pacto para la PCSD Civil de la Unión Europea, en materia de personal cedido en misiones.

En el ámbito de las Naciones Unidas, además de la contribución de las Fuerzas Armadas a UNIFIL anteriormente citada, las FCSE han tenido efectivos desplegados en MINUSCA, en la República Centroafricana y en la Misión de Verificación de las Naciones Unidas en Colombia para la implementación del Acuerdo Final firmado entre el Gobierno de Colombia y las FARC-EP, con un total de 13 funcionarios desplegados. Igualmente, 2 miembros de las FCSE han estado desplegados en la Oficina de Apoyo de la Misión de apoyo a la seguridad de Haití (MSSO-Haití), actual Oficina de apoyo de las Naciones Unidas en Haití (UNSOH).

Además, las FCSE han participado en misiones de gestión civil de crisis, un total de 62 miembros de en 2025, la cifra más alta de los últimos años. Los despliegues de las FCSE se han concentrado especialmente en los Equipos Especializados en la misión EUBAM Rafah, en la Misión de Verificación de las Naciones Unidas en Colombia y en las misiones EUAM Ucrania y EUCAP Sahel Mali.

En el ámbito de las misiones OTAN la participación española incluye: “NATO Mission Iraq”, para fortalecer las fuerzas de seguridad iraquíes para la lucha contra el terrorismo, entre otras funcionales; y en la Coalición contra Dáesh (*Inherent Resolve*), España despliega en Bagdad un contingente para apoyo y entrenamiento a fuerzas iraquíes. Además, España presta apoyo a Turquía en Incirlik para defensa antiaérea y en la operación “*Persistent Effort*”.

Las Fuerzas y Cuerpos de Seguridad del Estado participan en CT-JUST (UE) para fortalecer capacidades contraterroristas en la región MENA, Sahel, Cuerno de África y Oriente Medio. Bajo este marco, la Policía Nacional ha organizado cuatro semanas presenciales de formación forense a FCS iraquíes en 2024, actividades en 2025, visita de estudios a la Comisaría General de Policía Científica y visitas de altos mandos iraquíes (noviembre 2024, julio 2025).

En el ámbito de las misiones militares, en el año 2025 la Guardia Civil ha participado en la Misión militar UNIFIL en el Líbano, en la Misión de la OTAN en Irak, así como en la Operación F-E SVK en Eslovaquia. La Guardia Civil contribuye activamente en la Misión OTAN en Irak (NMI), aportando un puesto de asesor senior en formación policial, en la línea de apoyar el desarrollo de unas fuerzas armadas e instituciones de seguridad sostenibles y eficaces, capaces de combatir el terrorismo e impedir el resurgimiento del Dáesh. También lo hace en UNIFIL, y en los Destacamentos de Seguridad en las representaciones diplomáticas en Jerusalén y Beirut. A su vez, en lo que respecta a la participación en la misión de la OTAN en Eslovaquia, el Ministerio del Interior contribuye a la brigada multinacional, ya que mantiene en 2025 la presencia de Oficiales de la Guardia Civil como Provost Marshal (Asesor Policial) del elemento avanzado, con cometidos de enlace con las autoridades policiales de la nación anfitriona. Además, ha contribuido durante 2025 con un total de ocho (8) componentes desplegados como Expertos Nacionales en cuatro (4) de las Misiones Civiles y de Gestión de Crisis de la PCSD de la UE: EUAM Ucrania (3), EUPOL COPPS Palestina (1), EUAM RCA (3) y EUCAP SAHEL Mali (1).

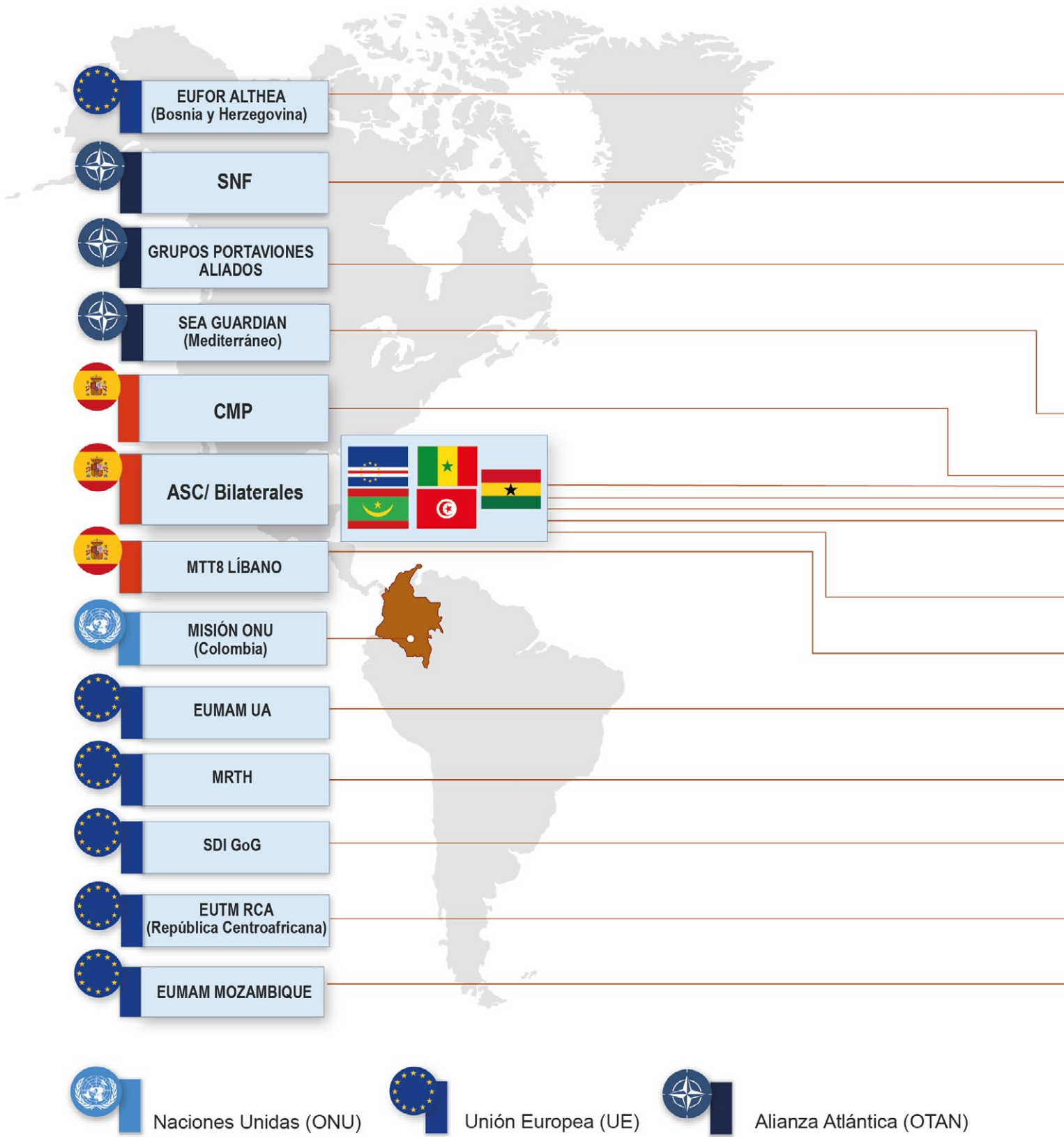
Asimismo, también se ha participado en la Iniciativa de la Unión Europea en Defensa y Seguridad en el Golfo de Guinea (EU-SDI-GoG), establecida en diciembre de 2023 en colaboración con Costa de Marfil, Ghana, Togo y Benín, proporcionando apoyo dirigido tanto desde la perspectiva civil y militar, cuyo mandato reside en fortalecer las capacidades de defensa y seguridad de esos países. La contribución en 2025 ha consistido en prestar capacidades sobre fotografía aérea y análisis de imágenes, en la formación en el manejo de drones de los integrantes del Grupo de Operaciones Especiales (GPOS) y el Grupo Especial Multipropósito de Intervención (GSPI), ambos de la Policía de la República de Benín.

Figura 1.11: Efectivos participantes en despliegues de misiones y ejercicios internacionales en 2025

EFECTIVOS PARTICIPANTES EN DESPLIEGUES DE MISIONES Y EJERCICIOS INTERNACIONALES EN 2025		NÚMERO DE EFECTIVOS 2025
APOYO A MALI-211G0017	MISIONES NACIONALES	62
MARES AZULES-211G0062	MISIONES NACIONALES	79
APOYO A MAURITANIA-211G0033	DIPLOMACIA DE DEFENSA ESPAÑA	6
ACTIVIDADES DIPLOMACIA DE DEFENSA-211G0060	DIPLOMACIA DE DEFENSA ESPAÑA	100
PRESENCIAS MARÍTIMAS COORDINADAS (CMP)-211G0048	DIPLOMACIA DE DEFENSA ESPAÑA	158
SEGURIDAD COOPERATIVA TÚNEZ-211G0038	DIPLOMACIA DE DEFENSA ESPAÑA	8
COALICIÓN INTERNACIONAL CONTRA DÁESH Y NATO MISIÓN IRAK-211G0029	OTAN	618
DEPLIEGUE DE FUERZAS TERRESTRES EN EL FLANCO ESTE-211G0053	OTAN	2.555
DESPLIEGUE EN LOS FLANCOS ORIENTAL Y MERIDIONAL.ARF.-211G0056	OTAN	1.334
ENRF (FUERZAS DE RESPUESTA REFORZADA DE LA OTAN) 211G0049	OTAN	687
NATO READINESS INITIATIVE (NRI)-211G0047	OTAN	5.038
PERSISTENT EFFORT-IAMD-211G0052	OTAN	1.568
PRESENCIA AVANZADA REFORZADA (E-FP)-211G0039	OTAN	1.929
SEA GUARDIAN-211G0036	OTAN	316
ASISTENCIA EN SEGURIDAD Y ADIESTRAMIENTO A UCRANIA DE OTAN-211G0058	OTAN	5
EU BATTLE GROUP PACKAGE-211G0044	UE	350
EUFOR ALTHEA-211G0007	UE	6
EUNAVFOR ATALANTA-211G0004	UE	1.525
EUTM RCA-211G0035	UE	14
EUTM SOMALIA-211G0013	UE	47
GOLFO DE GUINEA (EU SDI GOG)-211G0057	UE	20
OBSERVADORES EUTM MOZAMBIQUE-211G0045	UE	4
OBSERVADORES Y OFEMS DE LA UE EN EL MEDITERRÁNEO 211G0043	UE	17
ASISTENCIA MILITAR DE LA UE A UCRANIA (EUMAN UA)-211G0050	UE	1.576
MONITORIZACIÓN DEL ACUERDO DE PAZ COLOMBIA-211G0034	ONU	5
UNIFIL-211G0009	ONU	1.572
ASISTENCIA EN EL REFUERZO DE LAS CAPACIDADES MARÍTIMAS UCRANIA-211G0059	MARITIME CAPABILITY COALITION	2
TOTAL PERSONAL EN OPERACIONES		19.601

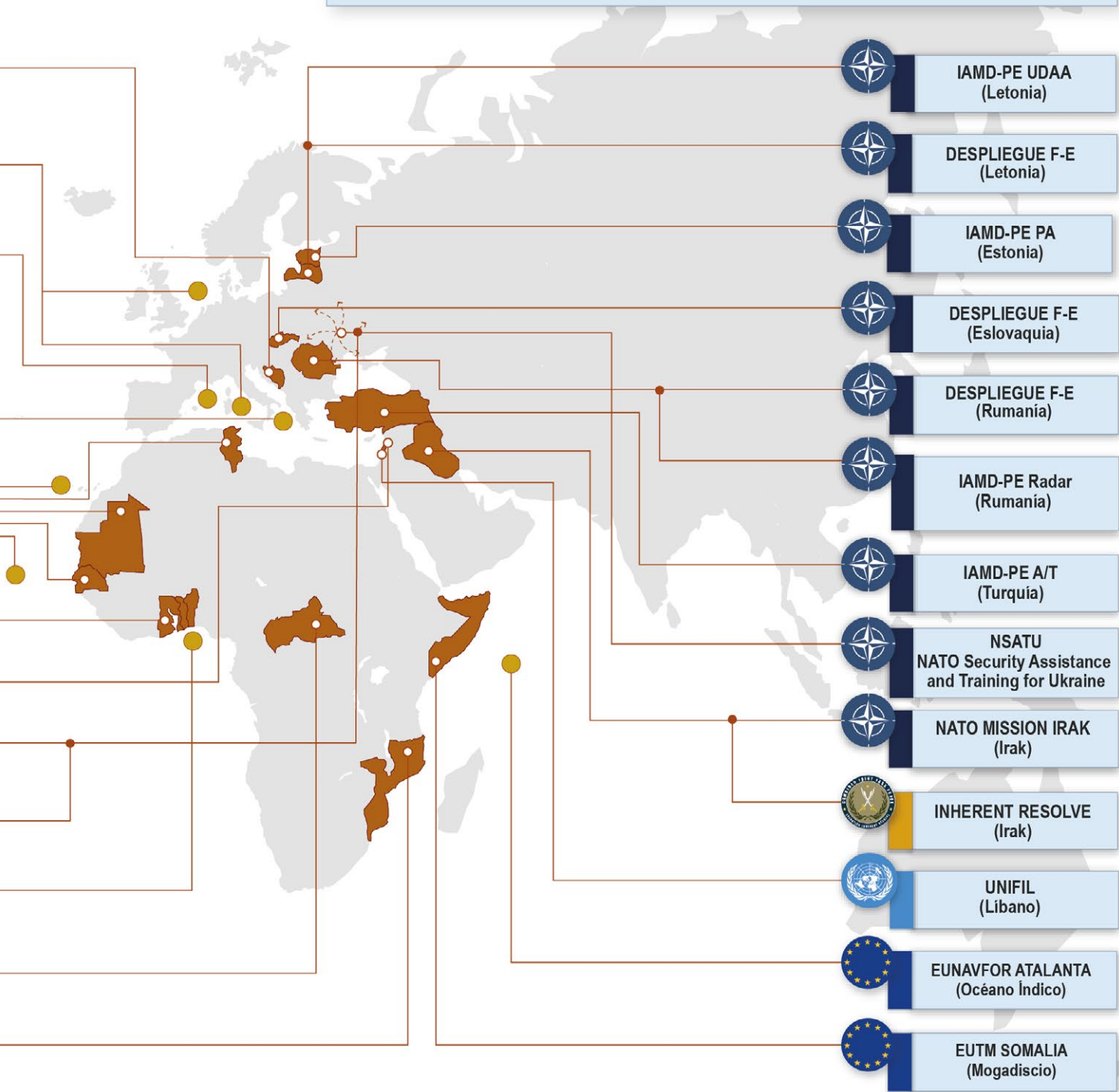
Fuente: Ministerio de Defensa

Figura 1.12: Misiones y operaciones de las FAS y FCSE en el exterior en 2025



Fuente: Elaboración del DSN con información del Ministerio de Defensa

ASC: Actividades de Seguridad Cooperativa
CMP: Presencias Marítimas Coordinadas
SNF: (Standing Naval Forces) Agrupaciones Navales Permanentes de la OTAN
Despliegue F-E: Despliegue de Fuerzas Terrestres en el flanco este
IAMD-PE: Integrated Air and Missile Defense System-Persistent Effort
PA: Policía Aérea



Coalición Global



Diplomacia de Defensa España

TERRORISMO Y RADICALIZACIÓN VIOLENTA

- El terrorismo yihadista en África, y en particular en el Sahel, se ha consolidado como el principal núcleo de actividad de esta ideología radical.
- El uso de la inteligencia artificial para crear contenido propagandístico y desinformativo por parte de grupos extremistas añade complejidad a la lucha contra la radicalización en el entorno digital.
- En abril de 2025 tuvo lugar el lanzamiento de la Red Global de Asociaciones de Víctimas de Terrorismo (VoTAN), un proyecto impulsado con el apoyo financiero de España y gestionado por la Oficina de Naciones Unidas Contra Terrorismo.

TERRORISMO Y RADICALIZACIÓN VIOLENTA

El terrorismo continúa siendo una de las principales amenazas para la seguridad global debido a la capacidad de adaptación tanto de sus estructuras como de sus instrumentos de actuación. Durante 2025, el terrorismo yihadista se ha mantenido como amenaza significativa incorporando una creciente regionalización en África y, en especial, en el área del Sahel, que se ha consolidado como su principal área territorial. Por otra parte, la persistencia de conflictos armados y el debilitamiento de las capacidades estatales en determinadas regiones han favorecido la resiliencia de las organizaciones vinculadas a Al Qaeda y a Dáesh, además del impulso de herramientas digitales para la propaganda, la radicalización y la financiación, que acentúa su dimensión transnacional. Europa se mantiene como uno de los principales objetivos, debido a la repercusión e impacto que tendría la comisión de una acción violenta en su territorio.

En este contexto, España continúa enfrentándose a la amenaza terrorista de ideología yihadista, marcada principalmente por la potencial actuación de actores solitarios autorradicalizados que, según las detenciones practicadas en el último año presentan un perfil progresivamente más joven, incluyendo individuos menores de edad. Igualmente, contribuyen a la amenaza la influencia de dinámicas externas de los principales grupos terroristas, especialmente procedentes del Sahel, Oriente Medio y Asia Central, así como el riesgo asociado al retorno o desplazamiento de Combatientes Terroristas Extranjeros. La cooperación internacional, la prevención de la radicalización y el fortalecimiento de las capacidades de detección y respuesta siguen siendo los pilares para su prevención. España, durante el 2025, ha mantenido su Nivel de Amenaza Antiterrorista en un grado 4 de 5.

África Sahel

El terrorismo yihadista en África, y en particular en el Sahel, se ha consolidado como el núcleo principal de la actividad global de esta ideología radical. En esta región, la presencia de grupos vinculados a Al Qaeda y al Dáesh se ha extendido con especial intensidad en Mali, Burkina Faso, Níger y Nigeria. La dinámica regional que se observa en la denominada “triple frontera” se caracteriza por la búsqueda de control territorial y por la implantación de estructuras de influencia sobre comunidades locales, lo que facilita la proyección de la amenaza hacia otros países limítrofes. En conjunto, se muestra una continuidad en la tendencia a una mayor presencia del yihadismo en África al producirse un desplazamiento progresivo desde Irak y Siria hacia el continente y con un fortalecimiento de la actividad en el Sahel que incide directamente en la estabilidad regional.

En este entorno, las filiales de Al Qaeda y del Dáesh han desarrollado capacidades operativas que les permiten incrementar su actividad. Al Qaeda actúa fundamentalmente a través de la coalición JNIM que está desarrollando en Mali una estrategia estructurada en fases en la que se establece, en primer término, la expulsión de actores extranjeros; seguido por el control de zonas rurales; una tercera fase se centraría en provocar el aislamiento de las grandes ciudades; y, finalmente, culminaría con el intento de, o bien controlar al gobierno actual o bien instaurar otro alineado con sus intereses. Según esta planificación, JNIM se situaría durante el 2025 entre la segunda y la tercera fase, en un contexto en el que mantiene acciones destinadas a interrumpir los flujos energéticos y comerciales hacia Bamako.

Por su parte, Dáesh opera mediante la Wilaya del Sahel, que ha ampliado su margen de actuación en Mali, Níger y Burkina Faso. La consolidación de estos espacios de actividad plantea escenarios en los que los gobiernos locales, especialmente aquellos surgidos de procesos de ruptura institucional, podrían tener dificultades para mantener su control territorial y podrían facilitar la consolidación de dichos grupos hacia el Golfo de Guinea y su extensión hacia el norte de África. (Figura 2.1)

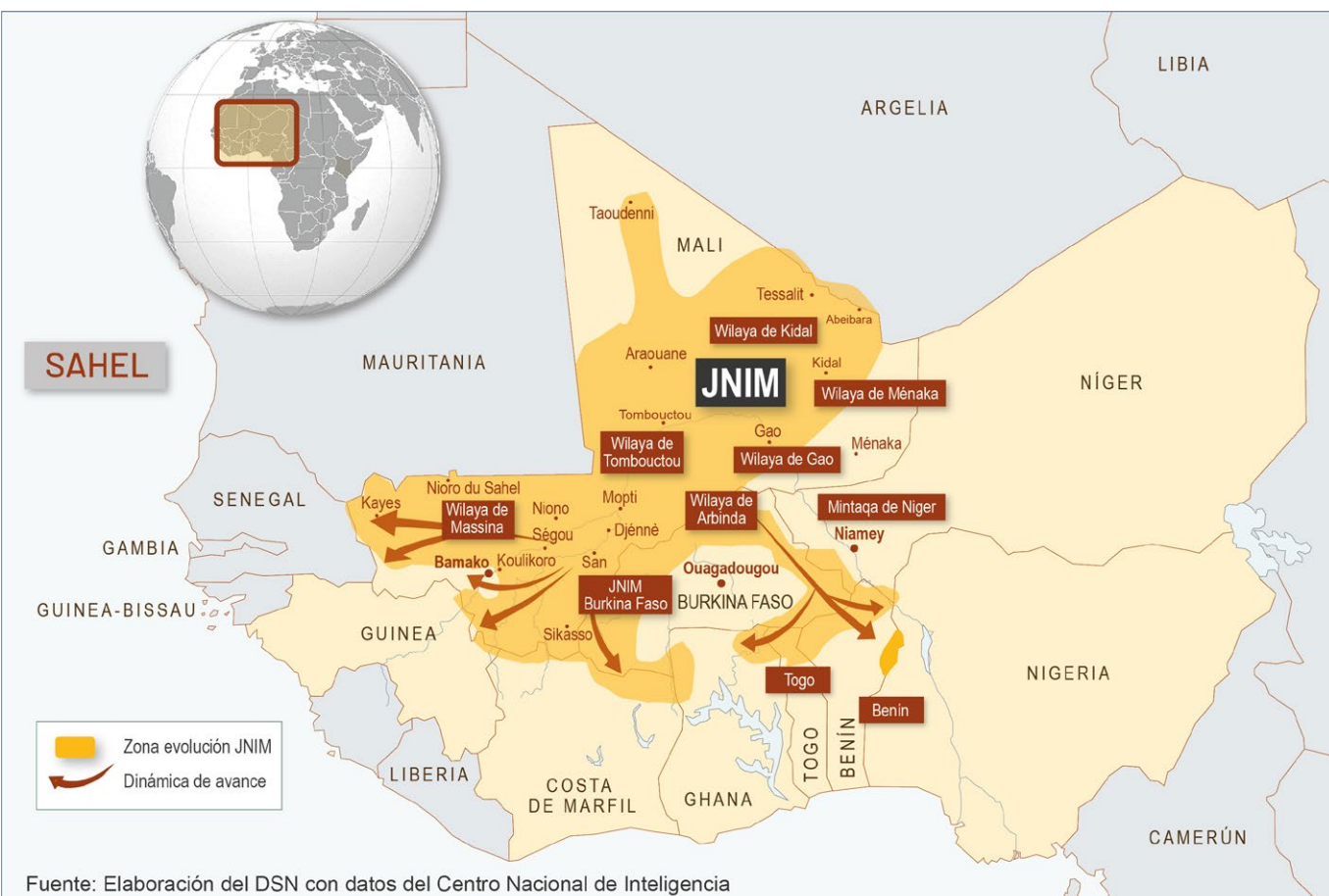
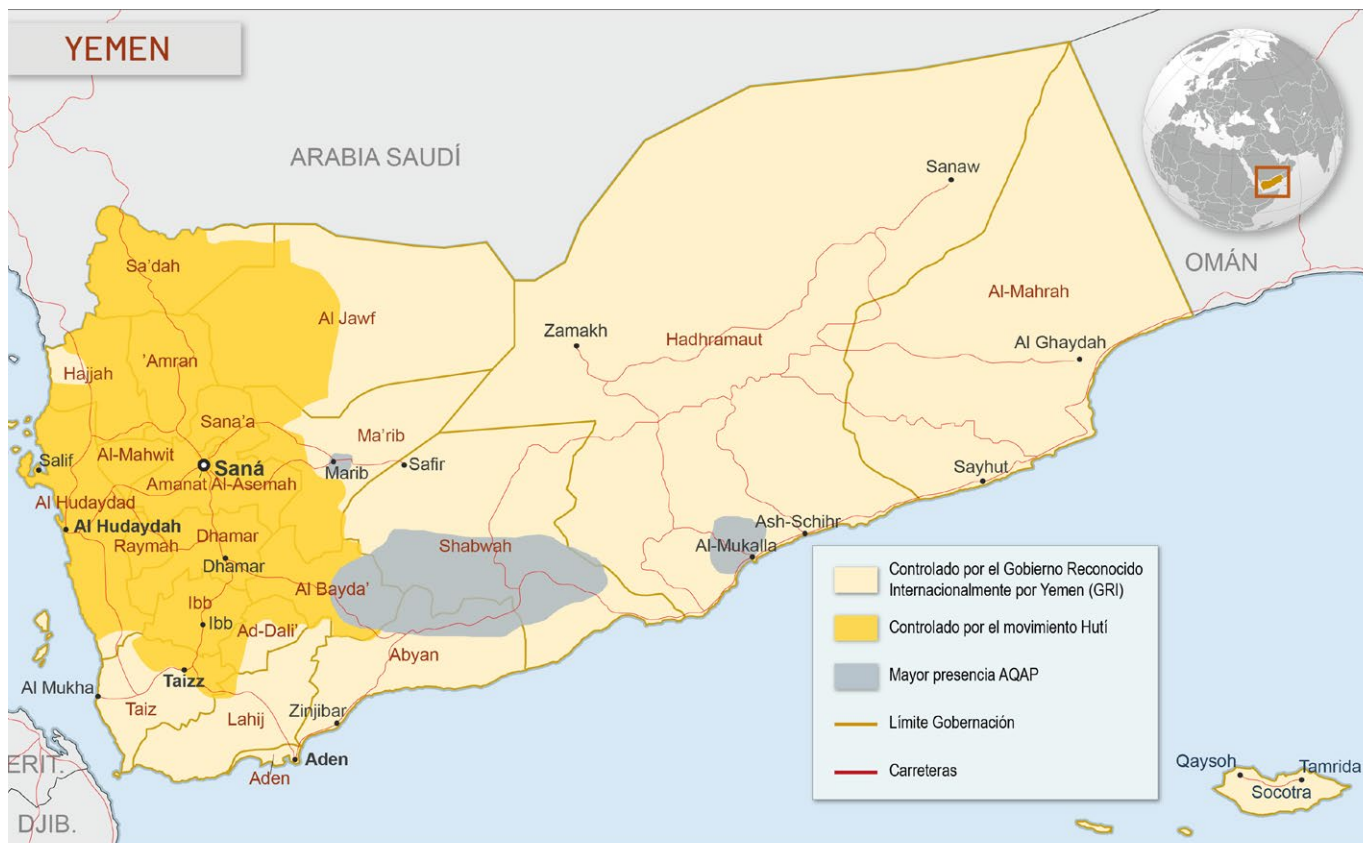


Figura 2.1: Presencia de las filiales de AQ (JNIM) y del Dáesh en el Sahel

La eventual proyección hacia el Magreb forma parte de las directrices emitidas por la dirección de Dáesh a su filial en el Sahel, con el objetivo de recuperar capacidades y redes en Argelia, Túnez, Libia y Marruecos. Esta orientación se justifica por el origen norteafricano de buena parte del yihadismo que opera actualmente en el Sahel y por el interés declarado de reactivar estructuras previas en ese espacio.

Resto de África

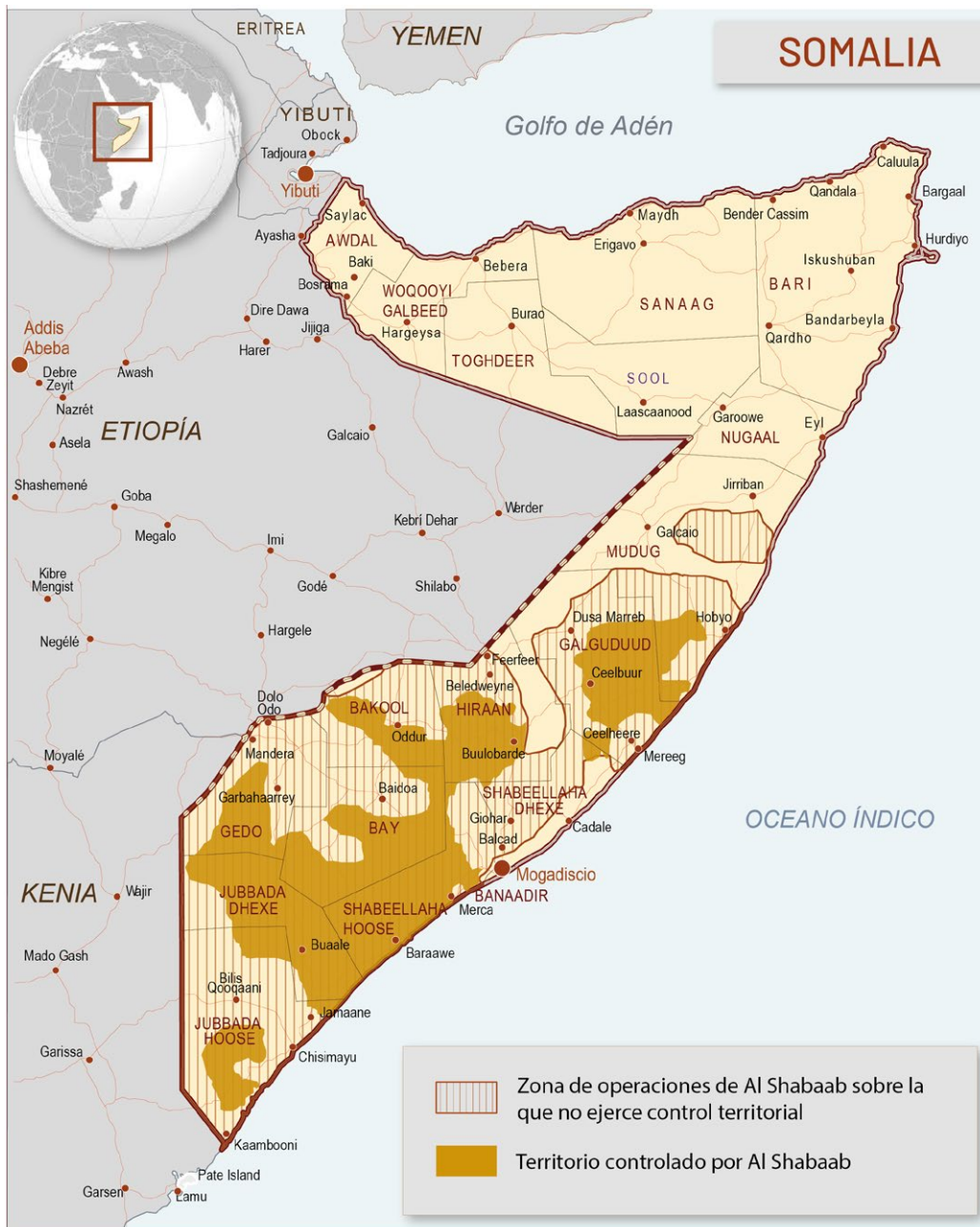
En África oriental y en el Cuerno de África se observa un estancamiento y descenso operativo de los grupos vinculados a Al Qaeda y Dáesh respectivamente en Somalia, debido a la campaña militar por parte de las fuerzas contrainsurgentes. Al Shabaab, afiliada a Al Qaeda, mantiene el control de amplias zonas del centro y sur del país, lo que le permite generar recursos económicos y desarrollar estructuras para ampliar el control del territorio más allá de Somalia. Por otra parte, su relación con los hutíes en Yemen presenta un vector transnacional con impacto en el golfo de Adén y potencial extensión al mar Rojo, el canal de Suez y el océano Índico. (Figuras 2.2. y 2.3)



Fuente: Centro Nacional de Inteligencia

Figura 2.2: Grupos presentes en Yemen

Por su parte, la filial de Dáesh en el norte de Somalia desarrolla enfrentamientos continuos con las fuerzas locales y ha integrado a varios cientos de Combatientes Terroristas Extranjeros (CTE), varios de ellos con vínculos estrechos con España, al ser antiguos residentes o tener familia en nuestro país. Además, ha desarrollado una importante estructura de financiación y facilitación de movimientos, entre sus integrantes. En este marco, el gobierno somalí, apoyado por socios internacionales, ha puesto en marcha desde finales de 2024 y durante 2025, la operación Hilaac, orientada a reducir las capacidades del Dáesh en áreas concretas, lo que ha reorientado parte de la actividad de este grupo a Sudán, aprovechando la inestabilidad derivada del conflicto armado y la crisis humanitaria que vive el país.



Fuente: Centro Nacional de Inteligencia

Figura 2.3: Somalia. Presencia de Al-Shabaab

Oriente Medio y Asia

El conflicto en Gaza ha tenido un impacto significativo en la narrativa yihadista regional. Aunque Al Qaeda y Dáesh no han intervenido operativamente en el escenario entre Israel y Hamás, sí lo han explotado en el plano propagandístico. Por otra parte, la destrucción de estructuras clave de Hamás ha eliminado un factor de contención frente a individuos afines que podría propiciar en el medio plazo la aparición de células yihadistas en la zona.

En paralelo, algunas organizaciones islamistas han difundido mensajes que justifican el recurso a la violencia. Destacan dos fetuas de la Unión Internacional de Eruditos Musulmanes, vinculada a los Hermanos Musulmanes. La primera, en octubre de 2023, instando a apoyar militarmente a Hamás y calificando la yihad en Palestina como obligación religiosa; la segunda, en marzo de 2025 alentando el apoyo armado, operativo e informativo contra la “entidad sionista”.

El conflicto, en su proyección regional ha generado efectos en otros escenarios, especialmente en Irak y Yemen, donde las milicias proiraníes y los hutíes han intensificado ataques contra buques vinculados a Israel o a sus aliados, hasta el acuerdo alcanzado entre los EE.UU. y los hutíes en octubre de 2025, con impacto directo en la seguridad de la navegación en el mar Rojo y en el comercio internacional.

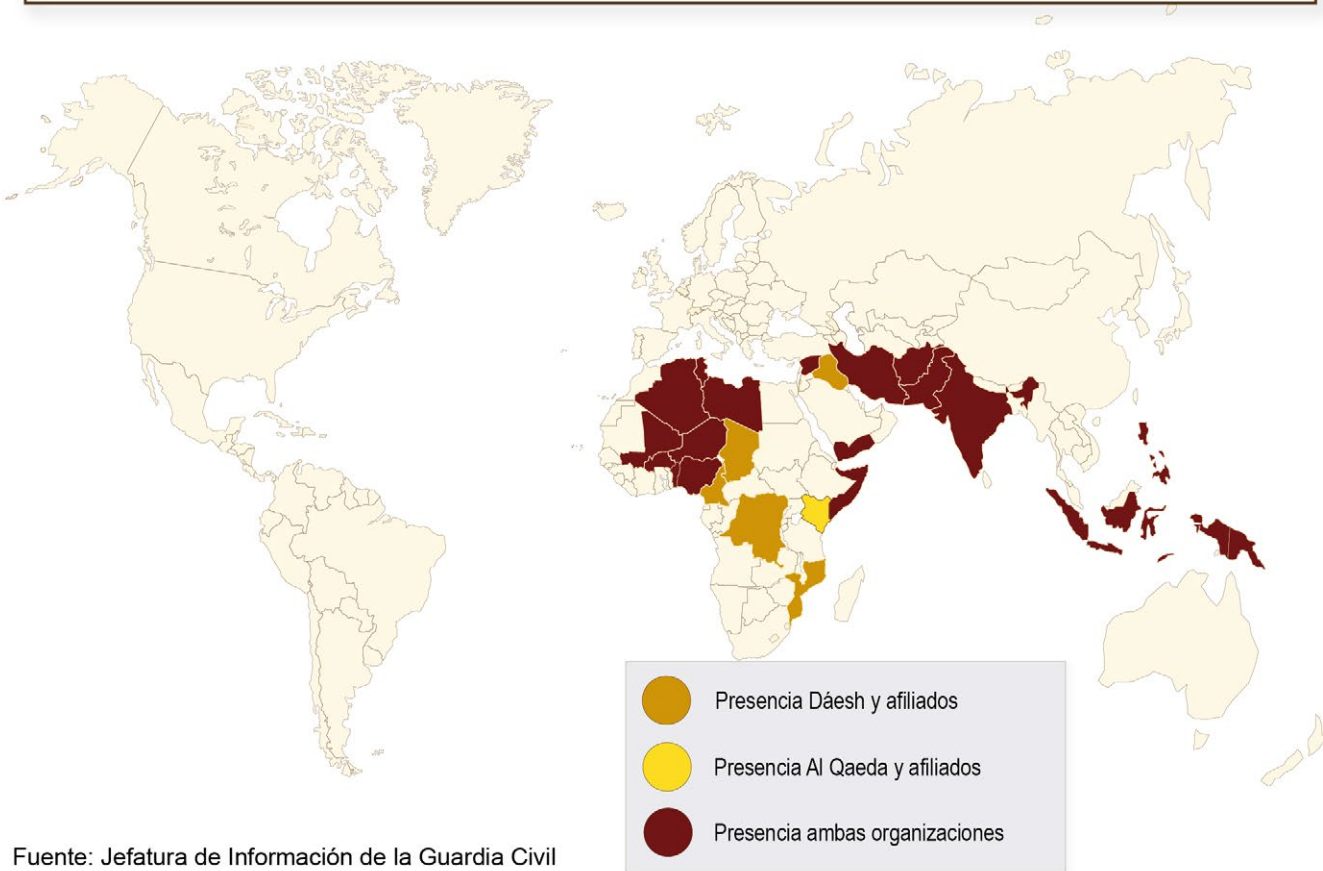
En Siria, el cambio político tras la caída del régimen de Al Assad y la llegada de Hayat Tahrir alSham (HTS) mantiene una estabilidad débil debido a las tensiones sectarias y al incremento de la actividad de Dáesh, que en muchas áreas recupera capacidades. El acercamiento del nuevo Gobierno a Estados Unidos y su incorporación a la Coalición Global contra Dáesh limitan la influencia iraní, sin embargo, este hecho plantea el riesgo de una posible atracción de actores yihadistas hacia territorio sirio. En este marco, el Dáesh ataca a las Fuerzas Democráticas Sirias y controla los campos de refugiados.

En Irak, la relativa estabilidad del Gobierno y de las fuerzas de seguridad dificulta la recuperación operativa de Dáesh, si bien la tensión sectaria entre sunitas y chiítas y la liberación gradual de detenidos podrían propiciar una recuperación del grupo terrorista.

En Asia Central y el entorno afgano-paquistaní, Dáesh, a través su filial en la Provincia del Jorasán (ISKP), mantiene un papel central para la amenaza yihadista. En el momento actual, el ISKP tiene mermadas sus capacidades debido a la pérdida de líderes y recursos, lo que ha reducido temporalmente la operatividad de su aparato exterior, sin embargo, continúa reforzando su red de apoyo mediante estructuras logísticas, de reclutamiento y de propaganda. Este hecho ha concentrado su actividad en los entornos afgano y paquistaní, desde los que mantiene vínculos transfronterizos orientados a asegurar su continuidad.

En el ámbito europeo, ISKP conserva su voluntad de actuar y dispone de contactos a través de redes de origen centroasiático y norcaucásico. Estas células, presentes en varios países europeos, recurren a actividades ilícitas dirigidas a su financiación, como la facilitación de movimientos irregulares, la falsificación documental o la comercialización de vehículos sustraídos, lo que les permite mantener capacidades de movilidad y sostenimiento. (Figura 2.4)

MAPA PRESENCIA DÁESH, AL QAEDA Y AFILIADOS



Fuente: Jefatura de Información de la Guardia Civil

Figura 2.4: Mapa presencia Dáesh, Al Qaeda y afiliados

Terrorismo en Europa

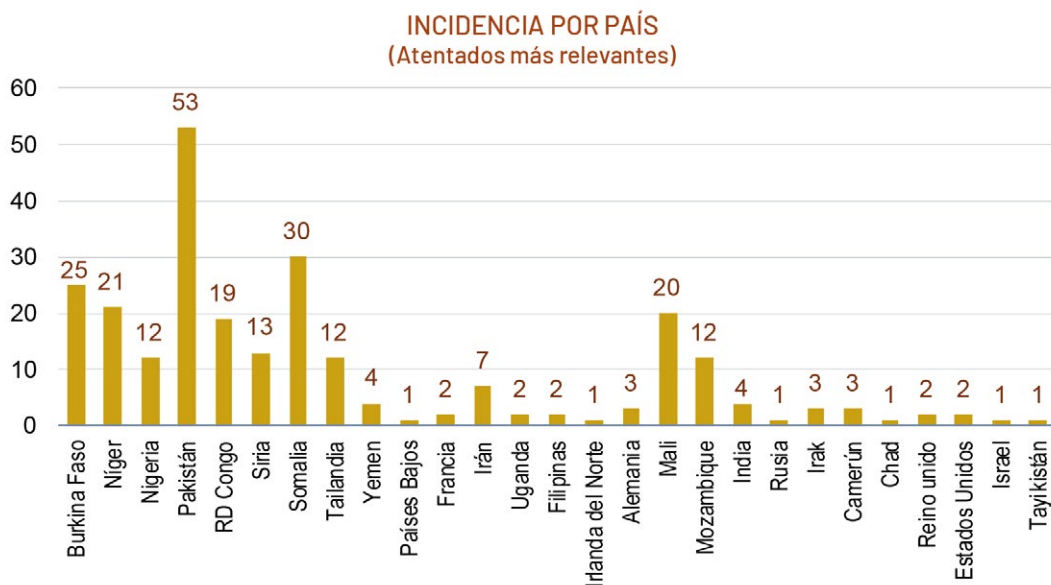
En Europa, el terrorismo yihadista continúa representando una de las principales amenazas para la seguridad. El fenómeno del terrorista autóctono, el conocido como *Homegrown Terrorist Fighter* (HTF) se ha consolidado como uno de los factores más relevantes en la configuración de esta amenaza. Este perfil afecta especialmente a jóvenes y menores de edad que son cada vez más representativos entre los grupos radicalizados y que, actualmente, son los que alcanzan el mayor protagonismo, atendiendo al número de detenidos por actividades terroristas. Estos detenidos comparten un perfil caracterizado por una limitada formación religiosa, escaso o nulo vínculo previo con organizaciones terroristas y una alta exposición a contenidos violentos en internet, lo que incrementa su vulnerabilidad a procesos de radicalización digital.

El conflicto en Oriente Medio actúa como elemento que alimenta dinámicas de radicalización en Europa, favoreciendo acciones individuales justificadas como defensa de la comunidad islámica y, por otra parte, un incremento del señalamiento de intereses israelíes. Esta situación ha propiciado un aumento de incidentes antisemitas y amenazas dirigidas contra ciudadanos e infraestructuras vinculadas a Israel. La presencia de integrantes o simpatizantes de Hamás en algunos países europeos es un factor para considerar en la evaluación del riesgo.

Aunque Europa no ha registrado recientemente ataques de alto impacto, el continente continúa afectado por acciones protagonizadas mayoritariamente por actores solitarios auto-radicalizados. Los atentados de baja sofisticación llevados a cabo por actores solitarios continúan siendo una de las principales preocupaciones en la lucha contra el terrorismo en Europa y España. Estos ataques, de “modus operandi” sencillo y que emplean medios simples y asequibles, tales como armas blancas o vehículos, reflejan un cambio en las tácticas terroristas, que han evolucionado hacia métodos más accesibles, menos complejos y más difíciles de prevenir. Los individuos que cometen estos actos suelen estar radicalizados previamente, influidos por la propaganda de grupos como Dáesh o Al Qaeda a través de internet, que incitan a la acción sin la necesidad de pertenecer a estructuras terroristas formales. Los ataques, al ser realizados sin coordinación entre uno o varios actores y sin infraestructura compleja o muy sencilla, representan un desafío para las autoridades, ya que resulta más difícil su anticipación y detección. Paralelamente, las investigaciones y operaciones contraterroristas mantienen un ritmo elevado, con un incremento respecto al año anterior. En 2025 se llevaron a cabo 113 detenciones, 100 en España y 13 en el extranjero, la mayoría vinculadas a individuos con un perfil recurrente: actores solitarios, mayoritariamente de nacionalidad española, entre los que figuran individuos de ascendencia magrebí, con acceso continuado a repositorios de propaganda yihadista y tendencia a consumir, almacenar o redistribuir estos materiales.

Por otra parte, la presión contraterrorista ha condicionado la evolución de las estrategias de Dáesh, que prioriza los ataques guiados como vía operativa más eficaz y de menor coste. Este modelo se basa en la participación de sujetos europeos radicalizados que se encuentran sobre el terreno en distintas provincias de la organización y que actúan como enlaces con sus redes en Europa. Desde estos escenarios facilitan procesos de radicalización y orientan la preparación de ataques por parte de personas que permanecen en territorio europeo, reforzando la capacidad de acción de la organización sin necesidad de desplazamientos físicos.

Además de estos perfiles, algunos individuos de origen sirio, afgano o centroasiático vinculados al ISKP representan un potencial riesgo para la seguridad en Europa, debido a su experiencia previa en zonas de conflicto y a su conexión con redes transnacionales. En este contexto, el ISKP se mantiene como la filial de referencia en la proyección exterior del yihadismo, con intención acreditada de actuar en Europa y Occidente. Por su parte, el aparato mediático del ISKP continúa difundiendo contenidos en múltiples idiomas y alentando acciones en territorio occidental, lo que mantiene la relevancia del grupo como actor a considerar en el escenario europeo. (Figura 2.5)



Fuente: Jefatura de Información de la Guardia Civil

Figura 2.5: Número de atentados más relevantes por país

Situación en España

A continuación, se expone la situación de seguridad en España en relación con cuestiones clave de la amenaza terrorista, como los Combatientes Terroristas Extranjeros (CTE), la financiación, la radicalización, lo concerniente al ámbito penitenciario y el terrorismo autóctono.

La principal amenaza en España continúa vinculada al yihadismo transnacional y, en particular, a los combatientes terroristas extranjeros, debido al retorno de individuos con experiencia en zonas de conflicto y capacitación en técnicas y procedimientos paramilitares, así como al fenómeno del terrorista autóctono (HTF).

Combatientes Terroristas Extranjeros

En relación con los combatientes terroristas extranjeros cabe reseñar que la inseguridad en Siria, tras la fuga de numerosos detenidos, eleva el riesgo de reorganización de células y retorno de individuos con experiencia de combate

Para mitigar el riesgo, España refuerza la cooperación internacional y la interoperabilidad de sistemas de información de la UE, y lidera y participa en grupos de trabajo orientados a la identificación, detección y prohibición de entrada de estos CTE en suelo Schengen.

España mantiene en seguimiento a los CTE que se habrían desplazado desde España a la zona en conflicto, cuyo total asciende a 288, de los cuales 111 aún permanecerían en el área, 72 habrían retornado y 105 habrían fallecido. Por otra parte, el retorno de nacionales europeos y magrebíes se considera uno de los vectores más determinantes del nivel de amenaza en el continente, junto a la posible desestabilización en el noreste de Siria y la aparición de nuevos focos de atracción en África.

En el plano interno, durante 2025, se ha registrado en España una acción violenta asociada al fenómeno del HTF que está siendo investigada como delito de terrorismo asociado al ideario yihadista. Las operaciones policiales muestran un perfil dominante de este tipo de actores autoradicalizados, mayoritariamente en el entorno digital, que operan con recursos limitados, tácticas de bajo coste y alto impacto, y aprovechamiento de oportunidades inmediatas.

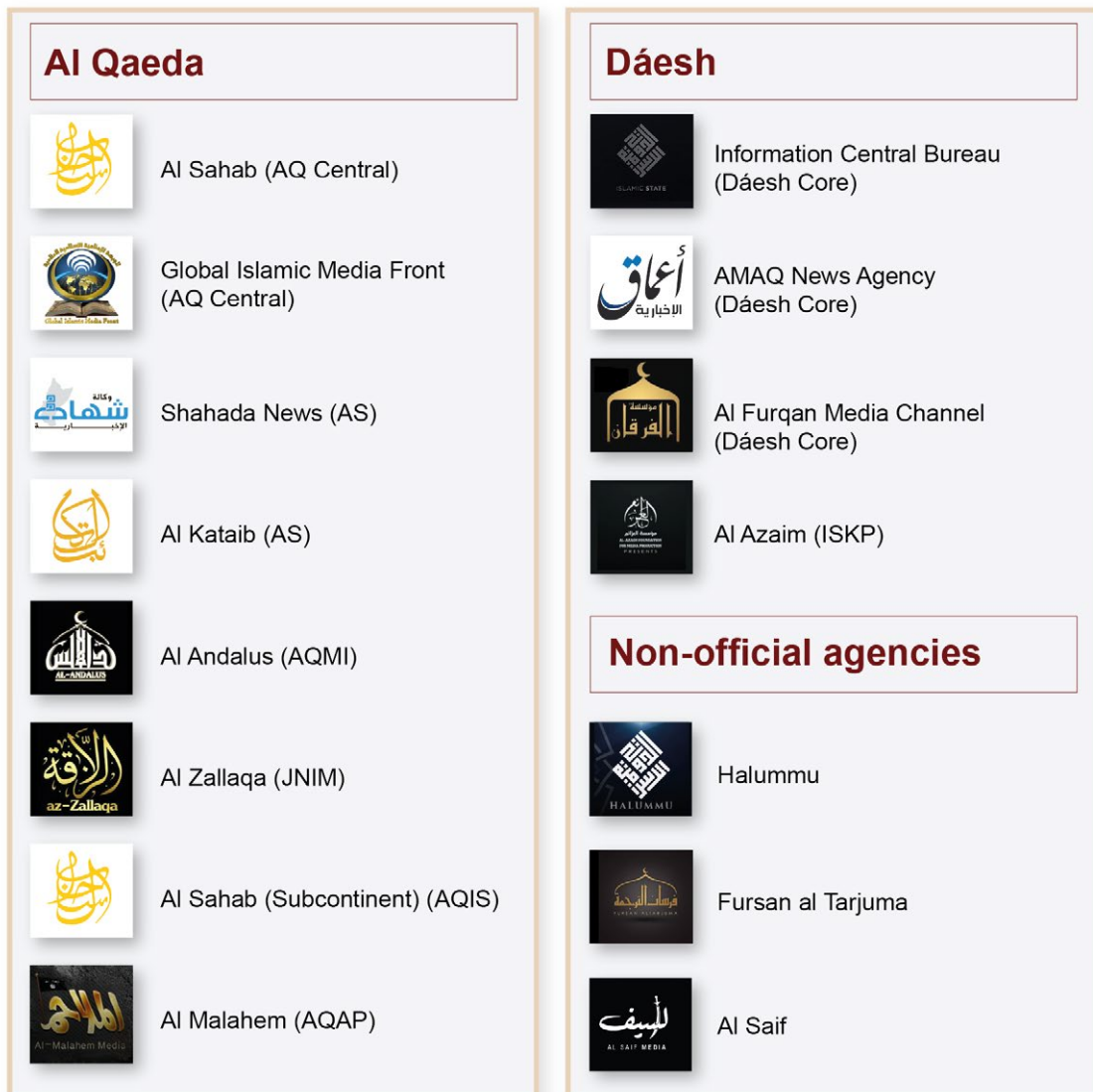
Esta imprevisibilidad obliga a combinar monitoreo de espacios online con detección temprana.

Nuevas tendencias

Además, destacan nuevas tendencias, como el uso intensivo de Internet, redes sociales y tecnologías emergentes (incluida la IA generativa) para propaganda, instrucción operativa y desinformación, con especial incidencia en jóvenes y menores. Se observa la traslación de comunidades a espacios descentralizados, su presencia en ecosistemas de *gaming*, y métodos aparentemente inocuos (p. ej., entrenamientos de calistenia) para adoctrinamiento continuo y acortamiento de tiempos de radicalización.

En este contexto se observa cómo la evolución tecnológica ha reforzado la resiliencia y la capacidad de difusión del yihadismo, que explota redes sociales, servicios de mensajería y la *dark Web* para mantener la cohesión ideológica y asegurar la persistencia de contenidos. La presión sobre las estructuras centrales de Al Qaeda y Dáesh ha impulsado una mayor producción de materiales dirigidos a individuos radicados en Europa y otros países occidentales a los que se insta a actuar en sus lugares de residencia, además de facilitar la difusión de manuales operativos y de técnicas, tácticas y procedimientos operativos a través de plataformas utilizadas por simpatizantes.

Así, en este escenario, la propaganda se mantiene como un elemento clave de captación y radicalización. Destaca el aparato mediático del ISKP, con productos como *Voice of Khorasan*, que incorpora diseños inspirados en videojuegos para atraer a audiencias jóvenes. Su difusión se apoya en redes de reclutadores multilingües que operan en plataformas como *Telegram*, *RocketChat* o *Session*, que alcanza una especial incidencia en los países occidentales. (Figura 2.6)



Fuente: Ministerio de Defensa

Figura 2.6: Aparato mediático de Al Qaeda y Dáesh

Financiación

En materia de lucha contra el terrorismo, la actuación en el ámbito financiero se erige como un elemento de primer orden. Así, la cooperación entre los servicios de inteligencia, las fuerzas de seguridad, las unidades de inteligencia financiera y el sector privado continúa siendo esencial para detectar y neutralizar las redes de financiación del terrorismo.

Las organizaciones terroristas financian su actividad mediante la explotación de recursos naturales, secuestros, extorsiones y cobros ilícitos en áreas bajo su control. En el ámbito transnacional, continúan empleando canales alternativos como *hawala* y las criptomonedas, especialmente Bitcoin y USDT, con un aumento de flujos entre filiales de Dáesh y un uso intensivo de criptoactivos difíciles de rastrear, como Monero en el caso del ISKP.

Paralelamente, estas redes amplían mecanismos que incrementan la opacidad financiera, plataformas DeFi, servicios anidados, *brokers* y servidores en terceros países, junto con un uso creciente de *stablecoins* como *Tether*. Del mismo modo, utilizan fondos obtenidos por actividades, tanto legales como ilícitas, procedentes de ingresos de baja cuantía enviados a través de empresas de remesas reguladas hacia jurisdicciones próximas a los escenarios de conflicto. También se ha detectado el uso de algunas ONG y campañas colectivas para enviar fondos hacia campamentos de refugiados vinculados a estructuras yihadistas, utilizando recursos bajo apariencia de ayuda humanitaria. Los actores solitarios recurren principalmente a medios propios o a un *crowdfunding* limitado.

En España, la financiación del terrorismo yihadista se articula principalmente a partir de fuentes legales, salarios, ahorros, donaciones y actividades comerciales, complementadas por envíos en efectivo, servicios de transferencia de dinero, criptomonedas y transferencias con datos falseados, incluida la apertura de cuentas mediante técnicas de inteligencia artificial. Igualmente, se han utilizados ONGs y campañas humanitarias para canalizar fondos hacia campamentos vinculados a estructuras yihadistas, especialmente en Siria a través de Turquía.

La evolución del terrorismo yihadista, dado su alcance transnacional y la conexión de diferentes escenarios geográficos, hace que la cooperación internacional siga siendo un elemento imprescindible, tanto dentro de la UE como a través de la colaboración con otros socios internacionales.

Radicalización violenta

Con relación al marco vinculado a los extremismos violentos, éstos continúan mostrando capacidad de crecimiento y adaptación en un contexto marcado por el aumento del fanatismo y la polarización social. Este escenario ha favorecido la aparición de grupos que, con una base de militantes cada vez más jóvenes, articulan llamamientos a la acción violenta en torno a campañas vinculadas a acontecimientos políticos, sociales o económicos. Su actividad se concentra en movilizaciones puntuales que buscan amplificar posiciones ideológicas y proyectar capacidad de influencia en el espacio público.

En España, la polarización y la sensibilidad creciente de estos movimientos a eventos nacionales e internacionales sitúan la evolución de esta amenaza en una tendencia ascendente en el ámbito nacional, aunque alejada del marco de muchos países europeos. Este escenario refuerza la necesidad de monitorizar dinámicas de movilización ligadas a contextos geopolíticos que puedan actuar como catalizadores de comportamientos violentos.

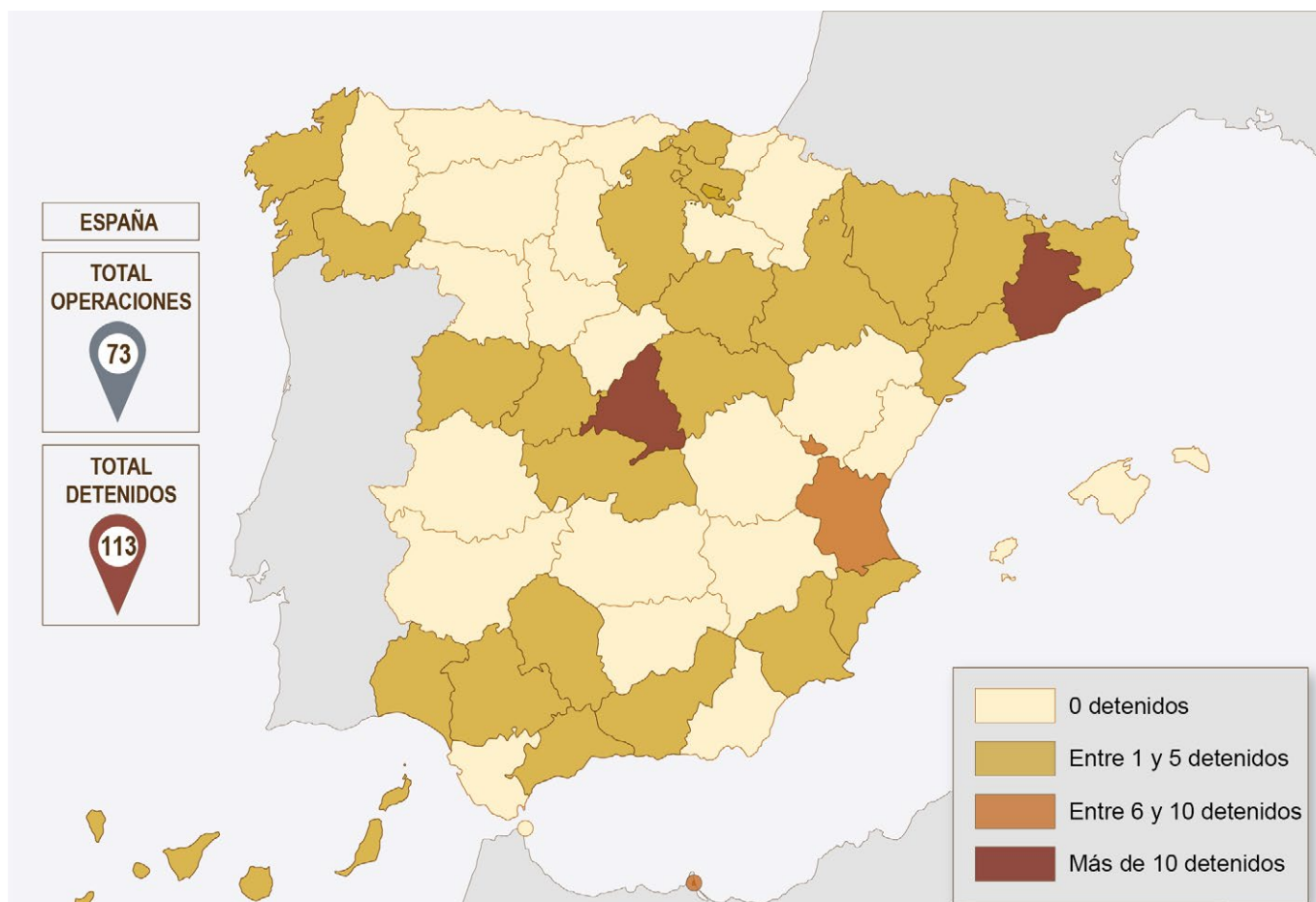
El incremento del fanatismo y la polarización ideológica tiene como consecuencia más inmediata el afloramiento de grupos o colectivos extremistas que, nutriéndose de militancia cada vez más joven, centran su actividad en el llamamiento a cometer acciones violentas en torno a campañas puntuales

que aprovechan las circunstancias políticas, sociales y económicas del momento para dar visibilidad a su posición ideológica respecto de situaciones y eventos de diferente naturaleza.

Cabe destacar la primera operación policial contra la célula terrorista aceleracionista internacional de etiología de extrema derecha, conocida como “The Base”, explotada el 11 de noviembre, que concluyó con la detención de tres personas que estaban gestando en España una célula operativa con conexiones directas con el fundador de esta organización, el cual ha estado realizando llamamientos a sus células internacionales para la comisión de ataques con el fin de colapsar las instituciones democráticas occidentales.

El auge de la tecnología y las redes sociales ha facilitado la difusión de ideologías extremas, especialmente entre los jóvenes, lo que ha impulsado a las autoridades a reforzar la monitorización en estos espacios. En 2025, la inteligencia artificial se ha convertido en una herramienta poderosa para extremistas que buscan crear contenido de desinformación y propaganda, intensificando los retos en la lucha contra la radicalización digital. Además, la invasión de Ucrania o el conflicto en Oriente Medio han influido en el crecimiento de discursos extremistas en España

Los videojuegos constituyen también una vía de radicalización y de captación de jóvenes, y permiten la confluencia de ecosistemas *online*, en donde se interactúa y se generan vínculos de confianza, con ecosistemas *off line*, a través de contactos en persona en centro de juego.



Fuente: Elaboración del DSN con datos del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado

Figura 2.7: Mapa con número de detenidos en España por su vinculación con el terrorismo

En 2025, el marco del Reglamento TCO, la Unidad Nacional de Retirada de Contenidos Ilícitos (UNEI), integrada en la División Antiterrorista del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), cuya principal función es la monitorización de fuentes abiertas (OSINT) para detectar, analizar y actuar frente a amenazas relacionadas con el terrorismo y el extremismo violento en el entorno digital, ha llevado a cabo 14.330 notificaciones de retirada y 48 órdenes de retirada.

Por otra parte, el desarrollo tecnológico facilita las capacidades de un terrorismo no convencional, mediante acciones orientadas a generar desestabilización o afectar servicios esenciales. En 2025 se observó una reducción de los sabotajes, pero aumentaron los incidentes relacionados con drones en instalaciones civiles y militares, así como la persistencia de actividades vinculadas al ciberterrorismo y al *hacktivismo* de inspiración extremista.

Ámbito penitenciario

La radicalización en el entorno penitenciario continúa constituyendo un ámbito de atención prioritaria, al representar un vector de amenaza significativo tanto por la posible formación de grupos organizados con capacidad operativa dentro de los centros, como por el riesgo que suponen aquellos internos que, una vez cumplida su condena, mantienen vínculos o convicciones extremistas susceptibles de propiciar su reincidencia. Preocupa especialmente el volumen de internos con ideología yihadista firme excarcelados en 2025 o próximos a ser liberados.

En España, 85 personas cumplen condena por terrorismo yihadista y 152 presos comunes están investigados por islamismo extremista. Desde 2022, 176 internos vinculados al terrorismo o al radicalismo yihadista han sido excarcelados por cumplimiento de condena o por agotamiento del periodo máximo de prisión preventiva.

Los perfiles son diversos y abarcan desde condenados por auto-adoctrinamiento hasta internos con trayectorias consolidadas en delitos de pertenencia o captación. En cuanto a la radicalización dentro de las propias prisiones responde a varios factores, como el aislamiento social, el contacto con internos radicalizados, la influencia de líderes con capacidad de influencia o la fragmentación étnica o religiosa. Tras la excarcelación, se ha constatado que una parte significativa de estos individuos mantiene su ideología. En los casos en los que no procede la expulsión del país, se establecen medidas de control en el marco de la libertad vigilada para reducir el riesgo de reincidencia y limitar su capacidad de influencia.

Terrorismo autóctono

La actividad terrorista de origen autóctono mantiene un nivel de amenaza residual tras la desactivación de las organizaciones que operaban en España, como ETA, GRAPO o Resistencia Galega.

En este escenario, las dinámicas asociadas al antiguo entorno de ETA se centran en la disputa por el relato y en acciones de movilización orientadas a proyectar reivindicaciones vinculadas a la situación de los presos, el retorno de los huidos y la reivindicación política de independencia, sin manifestar capacidad operativa organizada. En este contexto, también se registran actuaciones individuales de naturaleza delictiva relacionadas con la apología del terrorismo. Así, en el mes de febrero, un varón fue detenido en Zaragoza por enaltecimiento del terrorismo, humillación a las víctimas y amenazas a diversas personalidades a través de internet, reflejando la persistencia puntual de expresiones de apoyo a la violencia por parte de individuos aislados.

Paralelamente, las Fuerzas y Cuerpos de Seguridad del Estado mantienen abiertas investigaciones sobre atentados cometidos por ETA que permanecen sin esclarecer. Estas actuaciones se apoyan

en el análisis de documentación y material informático entregado por Francia en 2018, vinculado a procedimientos judiciales instruidos en ese país tras la detención de miembros de la organización. Asimismo, el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado mantiene actualizado un listado de miembros huidos de ETA con requisitorias judiciales en vigor, contabilizándose 23 individuos ubicados en distintos países, como Brasil, Cabo Verde, Cuba, Francia, México, Uruguay y Venezuela.

Proyectos de cooperación en materia de lucha contra el terrorismo

España ha mantenido durante 2025 una participación activa en los principales foros internacionales contra el terrorismo:

- participación en 2025 en las reuniones de la Coalición Contra el Dáesh, a la que se aporta un contingente militar; y celebración en Madrid el 10 de junio de la reunión de Directores Políticos,
- participación en las reuniones del Foro Global Contra Terrorismo, tanto en los Grupos de Trabajo como en el Comité de Coordinación celebrado en Doha en octubre;
- presencia mensual en los grupos de trabajo de la UE sobre terrorismo (COTER) y sanciones en el ámbito de terrorismo (COMET);
- participación en reuniones e iniciativas *ad hoc* como el Proceso de Aqaba -la dedicada a los Balcanes Occidentales en Sofía en abril y otra en Roma en octubre-;
- participación en la 11ª Conferencia de las Partes de la Convención de Naciones Unidas contra la Corrupción (Doha, diciembre).

España es uno de los países que ha firmado la Convención de NNUU sobre Cibercrimen en su ceremonia de apertura a la firma en Hanoi el 25 de octubre.

Igualmente, España participa y lidera proyectos financiados por la Unión Europea orientados al fortalecimiento institucional y a la capacitación de fuerzas de seguridad en regiones estratégicas, además de colaborar activamente con los grupos de trabajo del Consejo y de la Comisión sobre terrorismo, radicalización, extremismos violentos y fenómenos emergentes. Asimismo, el establecimiento en Europol de un grupo específico para investigar actividades de naturaleza híbrida, consideradas modalidades de terrorismo no convencional, refuerza la capacidad europea de análisis y respuesta.

En el ámbito de la cooperación internacional contra la financiación del terrorismo, España participa activamente en los trabajos del Grupo de Acción Financiera Internacional (GAFI), principal organismo internacional encargado de establecer estándares y evaluar el cumplimiento de medidas para prevenir el blanqueo de capitales y la financiación del terrorismo. Además, en junio de 2026, España afronta la Evaluación del Grupo de Acción Financiera Internacional.

De esta forma, en Oriente Medio y Norte de África, el Ministerio del Interior y el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, participan en el proyecto CTJUST, liderado por

España, cuyo objetivo es reforzar las capacidades de las autoridades desarrollando y fortaleciendo toda la cadena penal antiterrorista.

Por otra parte, miembros de las Fuerzas y Cuerpos de Seguridad del Estado están desplegados en la misión EUCAP Sahel Malí, donde desarrollan actividades de capacitación en materia de lucha contra el terrorismo.

Además, en el área del Sahel y África Central y Occidental, la Guardia Civil lidera el proyecto GARS Sahel, orientado a reforzar las capacidades operativas de las autoridades nacionales y a mejorar el control efectivo del territorio, incluida la creación de unidades “tipo GAR” (Grupos de Acción Rápida de la Guardia Civil), en Senegal y Mauritania. La Guardia Civil lidera también el proyecto *Public Spaces+*, dirigido a mejorar la protección de espacios públicos frente a amenazas terroristas, con actividades en Ghana, Kenia y Senegal. Del mismo modo, la Policía Nacional cuenta con un Equipo Especializado de Policía Científica desplegado en la misión de Naciones Unidas en la República Centroafricana (MINUSCA), contribuyendo a las capacidades de análisis y actuación en un entorno especialmente afectado por dinámicas extremistas.

En el área del Cáucaso, miembros de las Fuerzas y Cuerpos de Seguridad del Estado participan en el proyecto EU-ACT: EU – Acción contra el crimen organizado y el terrorismo, que presta apoyo y refuerzo en la lucha contra el terrorismo.

Protección y apoyo a las víctimas del terrorismo

La protección y apoyo a las víctimas del terrorismo continúa siendo un eje prioritario de la lucha contra el terrorismo. En este ámbito, se ha reforzado la prevención frente a procesos de radicalización, especialmente entre menores, un fenómeno creciente vinculado al uso intensivo de redes sociales y plataformas de juego en línea.

El 28 de abril de 2025 tuvo lugar el lanzamiento de la Red Global de Asociaciones de Víctimas de Terrorismo (VoTAN, en sus siglas en inglés). Este proyecto, impulsado con el apoyo financiero de España y gestionado por la Oficina de Naciones Unidas Contra el Terrorismo (ONUCT) fue uno de los resultados de la Conferencia Internacional de Naciones Unidas sobre Víctimas de Terrorismo, celebrada en Vitoria-Gasteiz en octubre de 2024. El Ministro de Asuntos Exteriores, Unión Europea y Cooperación volvió a copresidir la reunión ministerial del Grupo de Amigos de Víctimas de Terrorismo, celebrada en septiembre de 2025 en Nueva York. El Secretario de Estado de Asuntos Exteriores y Globales participó en el segmento de Alto Nivel de la Conferencia de Víctimas de Terrorismo africanas celebrada en Rabat en diciembre de 2025.

La Dirección General de Apoyo a Víctimas del Terrorismo (DGAVT) impulsa una estrategia integral basada en memoria, atención y coordinación institucional. En el ámbito educativo, desarrolla el programa “Memoria y prevención del terrorismo”, dirigido a 4º de ESO y Bachillerato, con materiales didácticos y la participación directa de víctimas para reforzar la contranarrativa frente al extremismo violento.

En 2025 se ha reforzado de forma significativa la atención integral a las víctimas. Se han gestionado más de 300 solicitudes de ayudas e indemnizaciones, así como 132 propuestas de condecoración de la Real Orden de Reconocimiento Civil. La DGAVT acompaña estrechamente a las familias de dos ciudadanos españoles fallecidos en atentados en Berlín y Jerusalén, mientras su equipo psicossocial ofrece apoyo continuado, visitas, atención presencial y telefónica, elaboración de informes sociales, derivación psicológica y un programa de inserción laboral que beneficia a más de 500 personas. Además, la institución mantiene un amplio marco de derechos asistenciales y concede anualmente

subvenciones a asociaciones de víctimas, destinando en 2025 un millón de euros a 16 entidades para programas de sensibilización, apoyo asociativo y atención social y jurídica.

La cooperación institucional constituye otro eje estratégico. El 20 de mayo, la DGAVT reunió a representantes de todas las comunidades y ciudades autónomas para compartir iniciativas, armonizar derechos y fortalecer la coordinación territorial. Asimismo, durante el curso académico se ha formado a las academias de la Guardia Civil en el sistema de protección a víctimas y en los protocolos de actuación en caso de atentado, incorporando el testimonio de una víctima miembro del cuerpo. Finalmente, el 17 de noviembre de 2025 se celebró una jornada específica sobre actuación operativa y atención a víctimas con la participación de Guardia Civil, Policía Nacional, policías autonómicas, Poder Judicial y Ministerio Fiscal.

Seguimiento de la Estrategia Nacional contra el Terrorismo 2023

La Estrategia Nacional contra el Terrorismo 2023 (ENCOT2023) establece el marco político-estratégico para la lucha contra este fenómeno. Al cumplirse la primera anualidad de vigencia de esta, se ha procedido a su evaluación en torno a los cuatro pilares en los que está estructurada: Prevenir, Proteger, Perseguir y Preparar la Respuesta, así como a las correspondientes líneas estratégicas y de acción, con el fin de valorar el grado de cumplimiento de los objetivos previstos y, sobre esa base, orientar la optimización de recursos y esfuerzos.

Dicho documento fue presentado en el seno del Comité Especializado contra el Terrorismo (CECT), como órgano de apoyo a la dirección y coordinación de esta política, para posteriormente ser aprobado por el Consejo de Seguridad Nacional.

La cooperación entre organizaciones ilícitas se evidencia en múltiples áreas, de ahí que la Estrategia Nacional Contra Crimen Organizado y Delincuencia Grave 2025 haga referencia a los vínculos con el terrorismo.

EPIDEMIAS Y PANDEMIAS

- Los virus de la familia Coronaviridae, siguen siendo una de las prioridades para los sistemas de inteligencia epidémica y detección precoz global, aunque desde 2023, la COVID-19 ya no constituya una Emergencia de Salud Pública de Importancia Internacional.
- Desde finales del año 2022 se ha detectado un aumento en el número de casos y brotes de sarampión a nivel mundial que se mantiene en ascenso.
- La Ley 7/2025, de 28 de julio, crea la Agencia Estatal de Salud Pública (AESAP), una entidad con personalidad jurídica propia para mejorar la preparación y respuesta ante amenazas sanitarias.

EPIDEMIAS Y PANDEMIAS

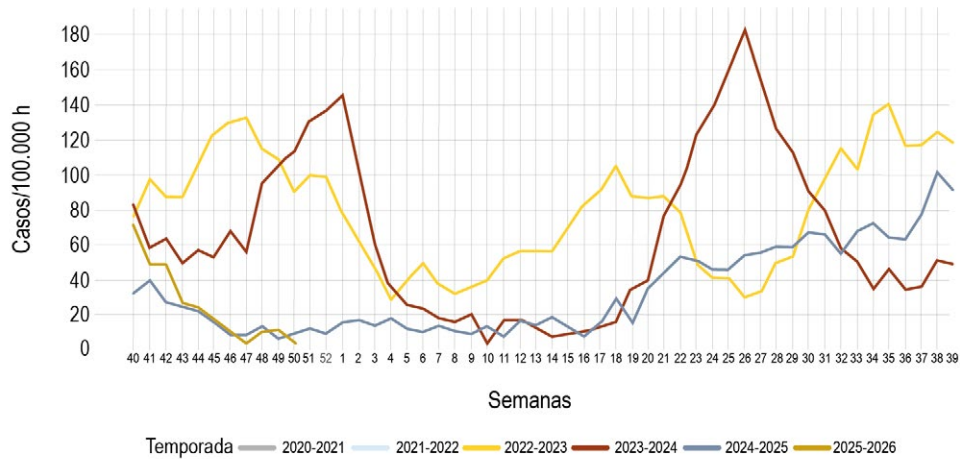
Evolución de la Pandemia de Covid-19

El 5 de mayo de 2023, el Director General de la OMS, de acuerdo con el informe del Comité de Emergencia del Reglamento Sanitario Internacional (RSI) sobre la pandemia de enfermedad por COVID-19 elaborado tras su decimoquinta reunión, concluyó que la COVID-19 ya no constituye una Emergencia de Salud Pública de Importancia Internacional (ESPII). Desde entonces, aunque se encuentran disponibles datos globales, no hay una actualización pormenorizada de los distintos países y los sistemas de detección y notificación varían entre los estados, lo que no permite una comparación directa entre ellos ni con periodos de tiempo previos con sistemas de vigilancia diferentes. La vigilancia actual se centra en la valoración de tendencias de diferentes virus respiratorios circulantes y de la parte de carga de enfermedad correspondiente al SARS-CoV-2 (virus causante de la COVID-19) y en la detección de variantes de interés. En España, el Sistema de Vigilancia de Infección Respiratoria Aguda: gripe, COVID-19 y VRS (SiVIRA), lleva la vigilancia de la COVID-19. Los datos hasta el momento muestran tendencia descendente de la COVID-19 desde 2022 con periodos de mayor actividad, pero sin un patrón estacional claro. La circulación en el inicio de la temporada 2025-2026 es baja, similar a la temporada 2024-2025.

No obstante, los virus de la familia *Coronaviridae*, siguen siendo una de las prioridades para los sistemas de inteligencia epidémica y detección precoz global al haber sido capaces en varias ocasiones de adaptarse a varias especies incluido el ser humano.

Las variantes actuales de Coronavirus SARS-CoV-2 siguen acumulando mutaciones que permiten eludir la inmunidad humoral pero no la inmunidad celular. Como consecuencia, las reinfecciones son de bajo impacto, excepto para los grupos de riesgo conocidos. La COVID persistente, o secuelas de la infección por SARS-CoV-2, es la mayor preocupación actual, por el número de personas afectadas, las características de los síntomas que en muchos casos impiden llevar una vida normal, la incertidumbre sobre sus causas y la ausencia de un tratamiento específico. Afecta preferentemente a mujeres, y afecta a todos los tramos de edad, siendo la mediana de edad de unos 44 años, la misma de la población española en su conjunto. (Figura 3.1)

Tasa estimada de COVID-19 por temporada. Vigilancia en atención primaria
Temporadas 2020-2021 a 2025-2026. SiVIRA



Fuente: Instituto de Salud Carlos III

Figura 3.1: Tasa estimada de COVID-19 por temporada, Vigilancia en atención primaria. Vigilancia de Infección Respiratoria Aguda: gripe, COVID-19 y VRS. Semana 50/2025

En España la vacuna frente a COVID-19 se ha venido recomendando junto con la vacuna de la gripe como parte de la campaña estacional de vacunación de otoño a los mayores de 60 años y personas con enfermedades de base. En 2025, para COVID-19 por primera vez esta recomendación se ha movido a las personas mayores de 70 de años.

La cobertura con estas vacunas ha venido disminuyendo a lo largo de los años. En la última temporada 2024-2025, el número y proporción de personas vacunadas con una dosis de recuerdo de vacuna adaptada por franjas de edad fue:

- Número de personas ≥ 80 años vacunadas: 1.622.285 (48% vs. 65% el año previo).
- Número de personas 70-79 años vacunadas: 1.704.653 (38% vs. 53% el año previo).
- Número de personas 60-69 años vacunadas: 1.403.248 (22% vs. 33% el año previo).

Sarampión

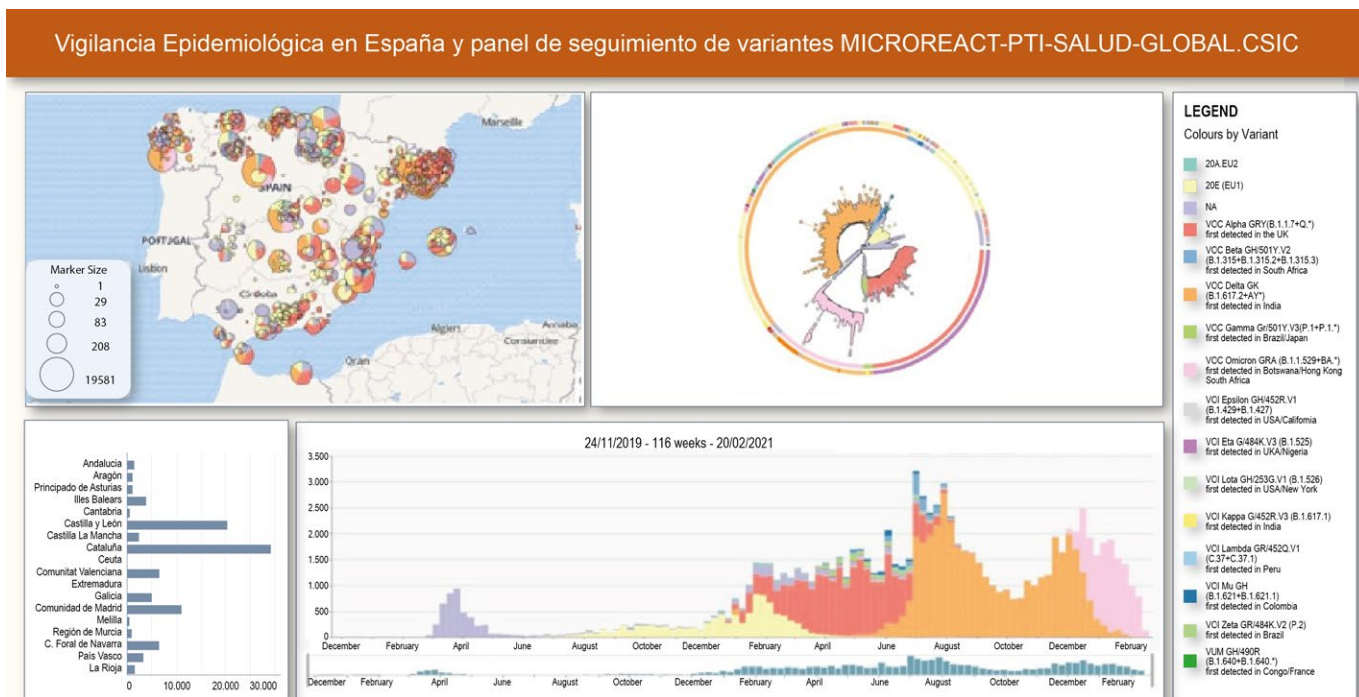
Desde finales del año 2022 se ha detectado un aumento en el número de casos y brotes de sarampión a nivel mundial que se mantiene en ascenso durante 2023, 2024 y 2025. Dicho aumento también se ha observado en los países de nuestro entorno y en España. Nuestro país cuenta con una cobertura de vacunación superior al objetivo del 95% con 1 dosis y algo por debajo de ese umbral con 2 dosis. Sin embargo, el incremento de los brotes observados en 2025 y que para algunos de ellos no se pudiera identificar el origen, supuso que, como como ha sucedido en otros países, se considere que la

transmisión del sarampión se ha restablecido, perdiendo el certificado de eliminación que se mantenía desde 2016.

Según el informe de situación de la semana 50 de la Red Nacional de Vigilancia Epidemiológica, a fecha 14 de diciembre de 2025 se han confirmado 395 casos en nuestro país, de los cuales 203 son importados o relacionados con importación del virus y el origen de 192 está en investigación o se desconoce. En el año 2024 se confirmaron 227 casos.

El principal objetivo de control, en el contexto actual, es alcanzar y mantener unas coberturas de vacunación por encima del 95% para las dos dosis en todas las comunidades autónomas, además de la detección precoz de casos y sus contactos y la caracterización genómica de los aislamientos de virus que permitan hacer el seguimiento correcto de los brotes epidémicos.

El Consejo Superior de Investigaciones Científicas (CSIC), a través de su Plataforma Salud Global, desarrolla protocolos de prevención, vigilancia y seguimiento en tiempo real, así como equipamiento de protección personal y materiales adaptables a las características de cada emergencia. La reticencia a la vacunación está en aumento en España, especialmente en el ámbito de la vacunación infantil, pese a que tradicionalmente el país ha mostrado alta confianza en las directrices de salud pública; este fenómeno, reforzado en parte por la desinformación vinculada a la pandemia de COVID-19, se refleja en el incremento de casos de enfermedades prevenibles, como los 227 casos confirmados de sarampión en 2024 frente a 14 en 2023, y 179 en el primer trimestre de 2025, que ha supuesto la pérdida del certificado de “eliminación del sarampión” alcanzada en 2016. La figura muestra los avances en vigilancia epidemiológica en España y el panel de seguimiento de variantes MICROREACT-PTI-SALUD-GLOBAL.CSIC. (Figura 3.2)



Fuente: MICROREACT-PTI-SALUD-GLOBAL.CSIC

Figura 3.2: Vigilancia epidemiológica en España

Gripe Zoonótica A(H5N1)

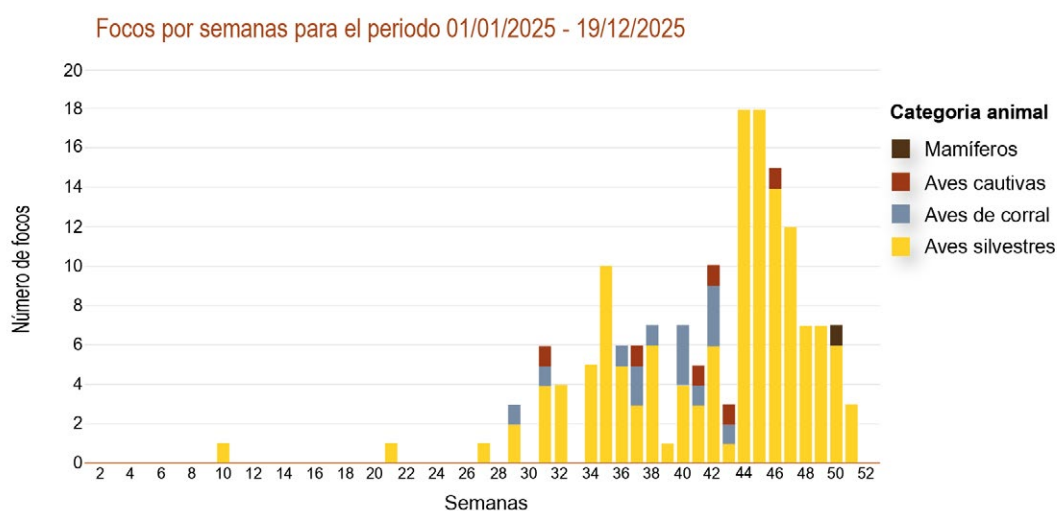
Entre el 1 de enero y el 19 de diciembre de 2025 se han notificado 30 casos humanos de gripe aviar por el virus A(H5N1). La mayoría de ellos (18 casos) han sido notificados por Camboya. La letalidad entre los casos detectados en 2025 fue del 38%, algo por debajo del casi 48% observada en el periodo 2003-2025 (476 defunciones/992 casos).

Hasta la fecha, no se ha demostrado capacidad de transmisión de este virus entre humanos. Sin embargo, la expansión del virus entre animales en Europa, principalmente aves, pero también varias especies de mamíferos incrementan el riesgo de exposición de los seres humanos y favorecen la adaptación del virus a la transmisión entre personas. En 2025 se han notificado en Europa más de 2.400 focos de diferente magnitud en animales silvestres y más de 70 en animales domésticos y un aumento significativo de detecciones con respecto a temporadas anteriores en mamíferos silvestres.

Otros virus de gripes zoonóticas de interés han tenido una diseminación limitada. Las detecciones del subtipo A(H5N5) han sido escasas, detectándose tanto en aves como en mamíferos silvestres. No obstante, en noviembre de este año Estados Unidos notificó el primer caso humano a nivel global de H5N5. En la Unión Europea no se han notificado casos humanos.

El riesgo de transmisión de gripe aviar para la población general es bajo, no obstante, la capacidad del virus para mutar y propagarse entre distintas especies, incluyendo mamíferos no se puede descartar y requiere una vigilancia constante.

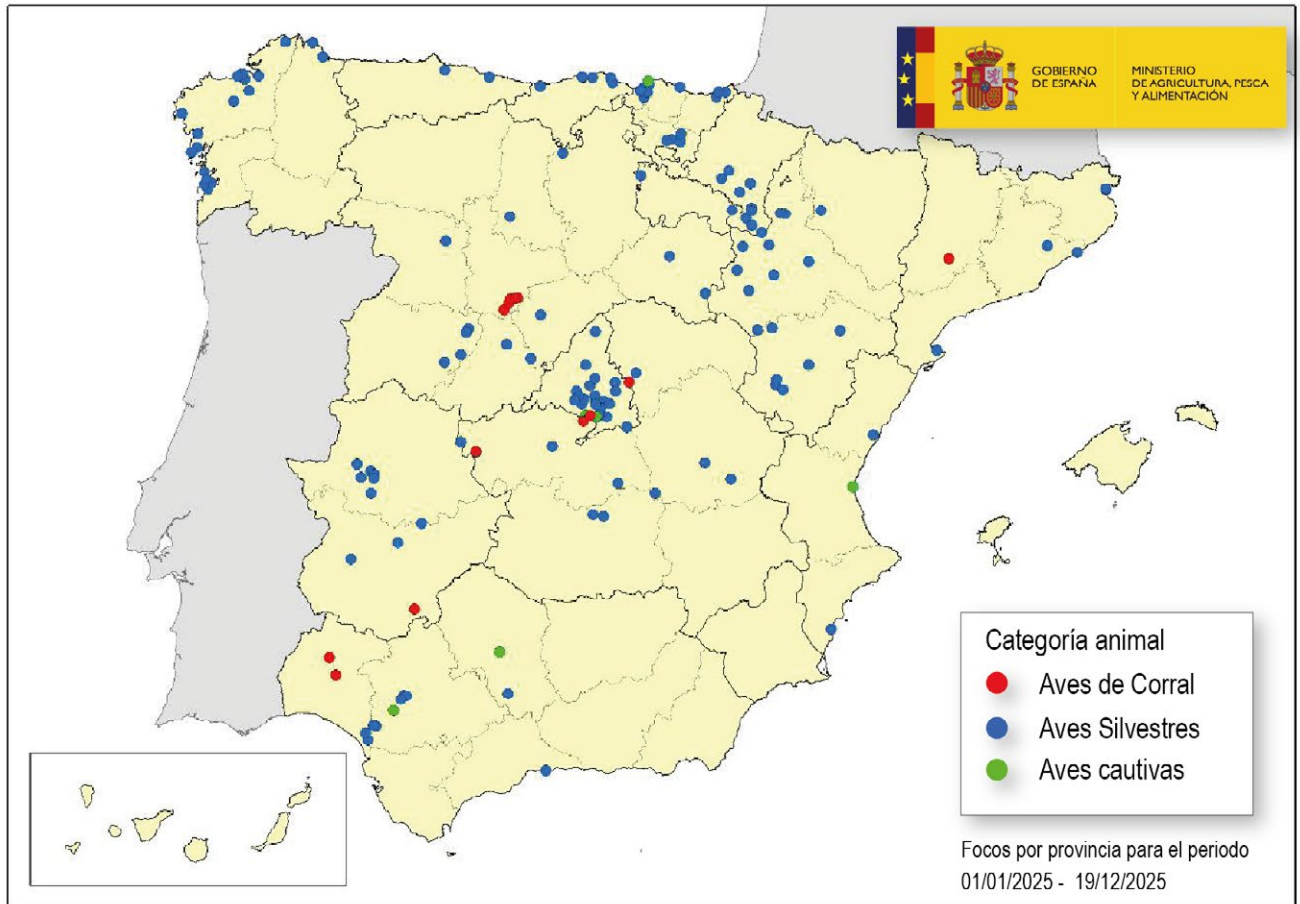
A nivel nacional, los Ministerios de Sanidad y de Agricultura, Pesca y Alimentación, hacen un seguimiento diario de la evolución de la epidemia de gripe aviar (de los diversos virus) en nuestro país en el marco de sus competencias respectivas y coordinan acciones conjuntas con las Comunidades Autónomas con una orientación de “Una Sola Salud”, entre las que se encuentra el desarrollo del Plan para la prevención, vigilancia y control de infecciones por virus influenza de origen zoonótico. (Figuras 3.3 y 3.4)



Fuente: Ministerio de Sanidad

Figura 3.3: Línea temporal de notificación de focos semanales de Influenza aviar para el año 2025

FOCOS NOTIFICADOS POR RASVE AÑO 2025



Fuente: Centro de Coordinación de Alertas y Emergencias Sanitarias

Figura 3.4: Localización por municipios para el año 2025 de los focos notificados por (Figura 16.10), del Ministerio de Agricultura, Pesca y Alimentación

La situación epidemiológica en España se configura como un escenario de riesgos multifactoriales en la interfaz: ganadería y cadena agroalimentaria. La introducción y distribución de carne y productos de origen animal al margen de los controles oficiales, incluyendo movimientos ilegales, canales no declarados o productos sin trazabilidad, debilita las barreras de bioseguridad y favorece la circulación de enfermedades zoonóticas de alto impacto económico y ambiental, como se ha puesto de manifiesto en brotes recientes de gripe aviar de alta patogenicidad o de dermatosis nodular contagiosa (DNC) en bovino.

Frente a ello, el sistema de vigilancia y control descansa en la coordinación entre autoridades veterinarias, ambientales, aduaneras y cuerpos de seguridad, donde la Guardia Civil, a través del Servicio de Protección de la Naturaleza (SEPRONA), aporta la capacidad operativa sobre el terreno en

materia de inspección, investigación e inteligencia ambiental, pero integrado en una arquitectura más amplia de prevención y respuesta.

En este contexto, reforzar la trazabilidad, el control de movimientos, la gestión segura de subproductos y la lucha contra el tráfico ilícito de carne no es sólo un objetivo sanitario, sino un vector esencial de la seguridad del Estado, especialmente frente a su explotación sistemática por grupos criminales organizados.

Las explotaciones ganaderas y mataderos clandestinos representan una amenaza directa para esta seguridad alimentaria. Al operar fuera de los sistemas de inspección sanitaria y control oficial, estos lugares pueden producir alimentos contaminados, portadores de enfermedades zoonóticas o contaminantes químicos. La falta de control veterinario, condiciones higiénicas deficientes y la ausencia de trazabilidad convierten la carne procedente de estas instalaciones en un producto potencialmente peligroso para los consumidores, al tiempo que generan una competencia desleal frente a los productores legales, afectando a las cadenas de suministro reguladas y debilitando sectores productivos estratégicos para la economía nacional.

Las actividades ilícitas vinculadas al sacrificio clandestino de animales y a la introducción de carne y productos de origen animal sin control veterinario en la cadena alimentaria responden a un modelo de delincuencia estructurada que puede encuadrarse en la delincuencia grave y el crimen organizado. Estas redes articulan un ciclo completo que abarca la captación y movimiento irregular de ganado, el sacrificio y despiece en instalaciones ocultas o no autorizadas, la falsificación o eliminación de la trazabilidad, el transporte y almacenamiento en condiciones higiénico-sanitarias deficientes y la posterior distribución de la carne de forma encubierta a establecimientos de restauración, comercios minoristas o canales de venta informal.

Para ello, se basan en un reparto estable de funciones entre sus miembros, en canales de distribución opacos y en mecanismos de ocultación de los beneficios obtenidos, combinando delitos contra la salud pública, contra la sanidad y el bienestar animal, contra la Hacienda Pública, falsedad documental y pertenencia a organización criminal. La dimensión económica, el carácter transregional o incluso transnacional de algunas redes y su capacidad para operar de forma persistente al margen de los sistemas de control sitúan estas conductas en un nivel de riesgo equiparable al de otras manifestaciones de criminalidad organizada que afectan a intereses esenciales del Estado.

España, a través del SEPRONA de la Guardia Civil, ha liderado una Acción Operativa referente a esta problemática en el EMPACT de Medio Ambiente y ha desarrollado este 2025 a nivel nacional la Orden de Servicio “GERION”, cuyos resultados a 31 de diciembre se exponen a continuación: (Figura 3.5)

Figura 3.5: Resultados de la Orden de Servicio “GERION”

RESULTADOS GLOBALES	
INSPECCIONES	1.499
CONTROLES / VERIFICACIONES	3.159
INFRACCIONES ADMINISTRATIVAS	3.316
INFRACCIONES PENALES	65
DETENIDOS / INVESTIGADOS	93
APREHENSIONES MEDICAMENTOS VETERINARIOS (Unidades)	141
ANIMALES INMOVILIZADOS / SACRIFICADOS	1.441

Fuente: Servicio de Protección de la Naturaleza de la Guardia Civil

Viruela del Mono (MPox)

Hasta 2022, la mpox era una zoonosis africana con casos humanos esporádicos, pero el brote global de ese año cambió el escenario, con más de 90.000 casos. Así, el 23 de julio de 2022, el Director General de la Organización Mundial de la Salud (OMS), declaró el brote mpox causado por el clado II (subclado IIb) una Emergencia de Salud Pública de Importancia Internacional (ESPII). Esta declaración se mantuvo vigente hasta mayo del 2023. Posteriormente, en agosto de 2024 se declaró una nueva ESPII ante la expansión del clado I de este virus en varios países africanos.

Esta segunda emergencia producida por el mpox se mantuvo activa hasta el 5 de septiembre de 2025, cuando se dio por finalizada tras un año de seguimiento y la disminución sostenida de casos y muertes en países como la República Democrática del Congo y otros países afectados como Burundi, Sierra Leona y Uganda. El Director General destacó que el levantamiento de la emergencia no implicaba el fin de la amenaza, ya que existe el riesgo de que se produzcan nuevos brotes.

En 2025, España y otros países europeos han mantenido una circulación del virus mpox clado II en niveles muy bajos, sin cambios significativos en las características clínicas y epidemiológicas de los casos observadas en años previos. Sin embargo, desde septiembre de 2025 se han notificado en países no endémicos casos de mpox clado Ib adquiridos localmente, sin relación con zonas endémicas. Estos casos se han detectado principalmente en hombres, sobre todo en hombres que tienen sexo con hombres (HSH). Hasta el momento, la detección de casos de mpox del clado Ib a nivel internacional, no se ha asociado con una mayor gravedad ni con una mayor transmisibilidad que el clado II.

A 9 de diciembre de 2025, España ha registrado 15 casos de mpox clado I sin vínculos con viajes ni personas que hubieran viajado a zonas endémicas, lo que indica una transmisión comunitaria sostenida en nuestro país.

En España, desde abril del 2022 hasta el 04 de noviembre de 2025, se han notificado 9.111 casos confirmados de mpox. El 93% del total de casos tuvieron lugar en el año 2022 (7.521 casos), el 3,6% en 2023 (325 casos), 7,6% en 2024 (695 casos) y el 6,3% restante en 2025. En España se han producido 3 fallecimientos en 2022 y uno en 2025.

El 90 % de los casos notificados no estaban vacunados contra la viruela humana o desconocía su estado vacunal. La vacuna contra la viruela humana ha mostrado su eficacia contra el mpox.

La clínica que presentan los casos suele ser leve y localizada y según la evidencia actual, el riesgo global de infección por mpox clado Ib se evalúa como moderado para los hombres que tienen sexo con hombres y bajo para la población general. (Figura 3.6)

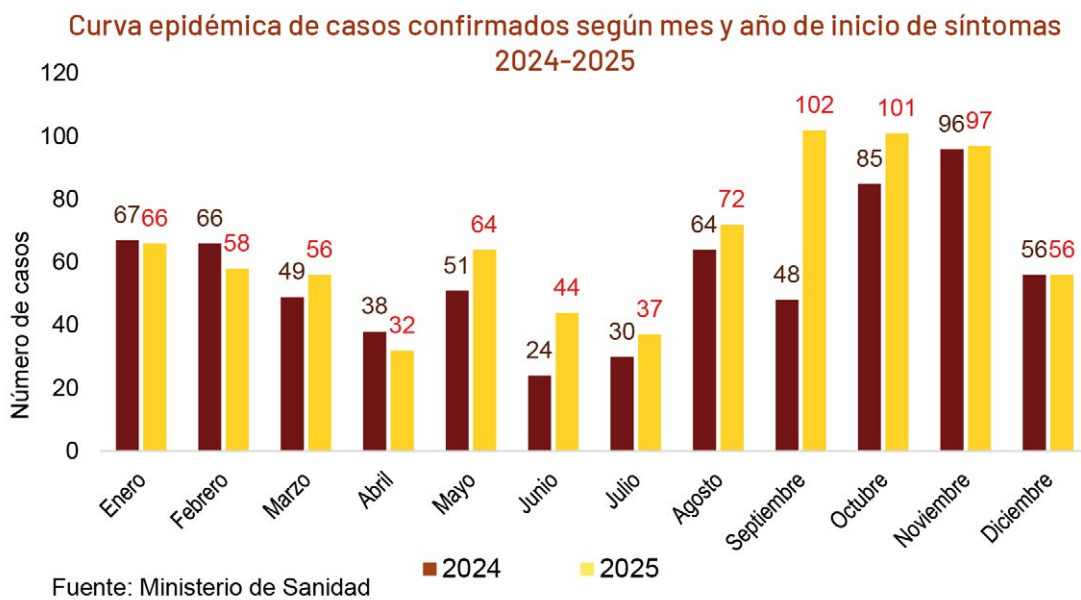


Figura 3.6: Curva epidémica de casos confirmados de mpox en España según el mes de inicio de los síntomas en 2024-2025

Fiebre del Nilo Occidental

La fiebre por el virus del Nilo occidental (FNO, o virus *West Nile*) es una enfermedad infecciosa transmitida por picadura de mosquitos. En las últimas décadas, se han detectado brotes y epidemias con una importante proporción de casos graves en regiones templadas de Europa y América, convirtiéndose en una amenaza de salud pública, humana y animal.

El virus del Nilo occidental es endémico en algunas zonas de España. Las aves son los reservorios. El ser humano y otros mamíferos, como los équidos, son huéspedes accidentales del virus. La incidencia de enfermedad en équidos y humanos varía de manera importante entre las temporadas, de acuerdo con la variabilidad de la densidad del vector y la circulación del virus. En 2020 se produjo un brote importante en España, con 77 casos graves detectados y 8 fallecidos en Andalucía y Extremadura. En 2024 tuvo lugar el mayor brote desde que hay registro, así como una expansión de las áreas geográficas y un alargamiento en la temporada, con la detección de 158 casos humanos autóctonos de FNO (142 confirmados y 16 probables), en las Comunidades Autónomas de Andalucía, Extremadura y Castilla-La Mancha.

Durante 2025, se han notificado 45 casos humanos autóctonos de FNO (36 confirmados, 9 probables y 2 casos con clasificación desconocida; datos aún no consolidados). De los casos confirmados, 32 tuvieron exposición en Extremadura (29 en Badajoz y 3 en Cáceres), 3 en Andalucía (Almería y Sevilla) y 1 en la Comunidad Valenciana (Alicante). Los casos se presentaron entre la semana epidemiológica 32 y la 44, excepto un caso en Almería en la semana 28 y afectó a ambos sexos y a todos los grupos de edad a partir de los 25 años. Cinco fueron asintomáticos, detectados en los cribados realizados entre donantes de sangre en Extremadura. De los 31 casos confirmados, 20 (64%) precisaron ingreso hospitalario y 4 (13%) fallecieron.

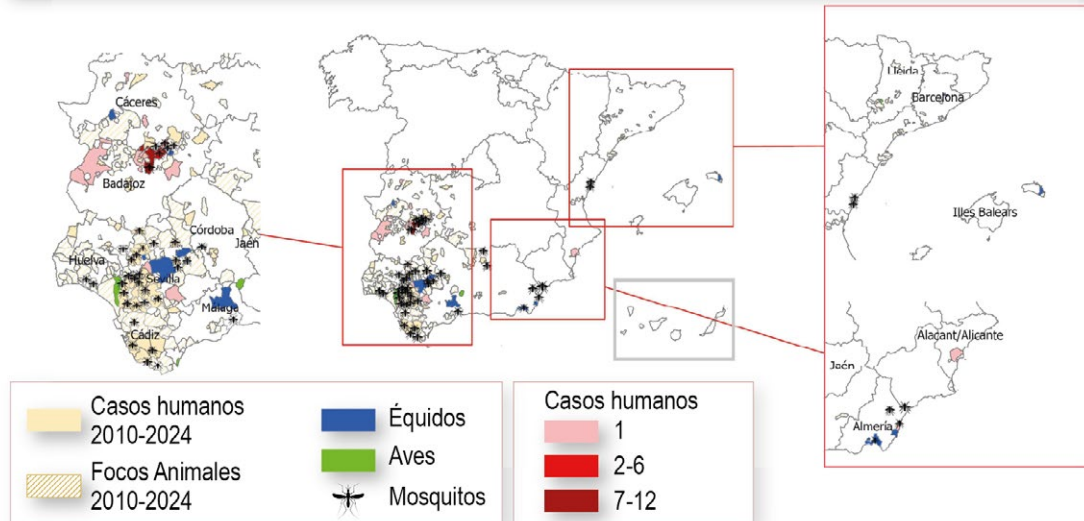
Además, de acuerdo con los datos proporcionados por el Ministerio de Agricultura, Pesca y Alimentación (MAPA) a través de la Red de Alerta Sanitaria Veterinaria (RASVE), en la temporada 2025 se detectaron 12 focos en équidos en las provincias de Almería, Sevilla, Badajoz, Barcelona, Cáceres, Málaga, Córdoba e Islas Baleares, y 4 focos en aves en las provincias de Lleida, Cádiz, Huelva y Córdoba.

En relación con la distribución territorial se constata expansión hacia el este, avalada por la detección de un caso en Comunidad Valenciana, detección de casos en Almería, así como de focos animales, por primera vez en las Islas Baleares.

Los datos tanto de casos humanos como de casos en animales muestran en la temporada 2025 una expansión territorial del virus hacia el este de la península.

En 2023 se adoptó un nuevo Plan Nacional para la detección, vigilancia y control de las enfermedades transmitidas por vectores, con la finalidad de disminuir el riesgo y reducir el impacto global de estas enfermedades emergentes desde la perspectiva de “Una Sola Salud”. El Plan, en sus partes I y II, está centrado en la prevención de los virus del Nilo occidental, Usutu, Dengue, Zika, Chikungunya, Fiebre Amarilla y Fiebre del Valle del Rift. (Figura 3.7)

VIRUS DEL NILO OCCIDENTAL EN ESPAÑA



Fuente: Centro de Coordinación de Alertas y Emergencias Sanitarias del Ministerio de Sanidad con datos de RENAVE

Figura 3.7: Relación de casos humanos, focos de équidos, aves, y detección del virus del Nilo occidental en vectores distribuidos por municipios en España en 2025 y acumulados 2010-2024

Fiebres virales hemorrágicas en países de África

Entre enero y noviembre del 2025 se han declarado cuatro brotes de fiebres virales hemorrágicas (enfermedad por virus del Ébola y virus de Marburgo) en Tanzania, Uganda, República Democrática del Congo y Etiopía. Tres de ellos se han cerrado: el de Tanzania con 10 casos, todos fallecidos, el de Uganda con 14 casos y 4 fallecimientos y el de República Democrática del Congo con 64 casos y 45 fallecimientos. El brote de Etiopía continúa activo en diciembre.

El Centro de Coordinación de Alertas y Emergencias Sanitarias (CCAES) del Ministerio de Sanidad ha realizado un seguimiento estrecho de cada brote, evaluando el riesgo para España. Se ha informado y mantenido en alerta a la Red Unidades de Aislamiento y Tratamiento de Alto Nivel, especializadas en el tratamiento y de estas enfermedades, consideradas de alto riesgo.

En caso de detectarse casos importados en España, la probabilidad de transmisión secundaria en nuestro país sería muy baja, siempre que los casos se identificaran de una manera precoz y se implementaran las medidas de control previstas de manera oportuna. El Instituto de Salud Carlos III dispone de la capacidad de laboratorio para la detección de virus de clase 4, como es el caso de estos agentes.

Cólera

En 2025, los principales puntos se localizan en la región africana (especialmente República Democrática del Congo, Sudán del Sur y Angola) y la región del Mediterráneo Oriental (en la que Afganistán, Yemen y Sudán concentran la mayor carga) con brotes activos y elevada mortalidad, especialmente en contextos de conflicto, desplazamientos, precariedad del agua y saneamiento. Así, la OMS ha advertido que la interacción entre eventos climáticos y fragilidad sociopolítica está generando brotes más complejos y persistentes. Además, también se encuentran afectadas la región del sudeste asiático (principalmente Myanmar, India y Nepal), la región de las Américas (en la que Haití se mantiene como el principal país afectado) y la región del Pacífico Occidental.

En contraste, no se han reportado casos en la Región Europea en 2025.

El último informe epidemiológico de RENAVE (Instituto de Salud Carlos III, en adelante, ISCIII) que recoge casos de cólera en España corresponde a 2024. A finales del año 2023 y durante el año 2024 se notificaron 3 casos importados de cólera en España. No hay casos autóctonos ni importados en los tres años previos. Anteriormente, desde 2015 solo se han registrado nueve casos, todos importados salvo uno detectado en 2018 cuyo origen no pudo determinarse. Los países de procedencia fueron India (4), República Dominicana (3) y Filipinas (1), y no se registró ninguna defunción.

España mantiene la vigilancia del cólera como enfermedad de declaración obligatoria, recomendándose el envío de casos sospechosos al laboratorio de referencia del ISCIII para su confirmación y caracterización mediante métodos validados, incluyendo la detección de toxina colérica o de los genes responsables de su producción.

Salud Mundial

La Organización Mundial de la Salud estima que en el año 2019 las resistencias a antibióticos contribuyeron al fallecimiento de 5 millones de personas en el mundo; este dato se puede comparar con los 7 millones fallecidos de COVID en 2020-2023, en 3 años. Es una amenaza latente pero prioritaria en España que ya se encuentra presente y que está poniendo en jaque los avances médicos como es el tratamiento del cáncer.

En España, en 2023 se estimaron 150.000 infecciones por bacterias resistentes y 23.000 fallecidos que eran portadores. El 45% de los casos infectados por bacterias resistentes notificados eran casos hospitalarios. Por otro lado, la movilidad global de personas favorece la diseminación de patógenos como la tuberculosis multirresistente. El Plan Nacional de Resistencias a los Antibióticos, que se implementa en España desde 2014 ha permitido una reducción importante en el uso inadecuado de los antibióticos. En mayo de 2025 se actualizó dicho Plan para el periodo 2025-2027 con un enfoque multisectorial que incluye la salud humana, animal y ambiental, I+D de nuevos fármacos y vacunas, y un uso más eficiente de los tratamientos actuales.

Enfermedades como la malaria, tuberculosis o VIH, si bien muestran, en general, tendencias descendentes, siguen generando una alta carga de enfermedad y mortalidad a nivel mundial. El cambio climático, la alta movilidad de personas y descenso de la percepción de riesgo para estas enfermedades a nivel global y la reducción de fondos para ayuda y desarrollo sanitario requieren incrementar su vigilancia. España, por su afectación particular por los factores mencionados debe prestar especial atención a las enfermedades importadas y a otras de baja endemicidad como la tuberculosis y el VIH. Los recientes aumentos de fondos españoles para salud global buscan prevenir enfermedades en su origen y reforzar la seguridad sanitaria nacional.

Por otra parte, destaca el impacto que la reducción en 2025 de fondos del Norte Global, como el cierre de USAID, ha generado interrupciones en programas de control de enfermedades en el Sur Global, con estimaciones de 600.000 muertes ya ocurridas y proyecciones de hasta 14 millones adicionales para 2030, acelerando un traslado desordenado de decisiones hacia estos países.

Respuesta europea a las crisis sanitarias

La globalización del transporte de materiales y la movilidad humana a escala global, junto con el cambio climático, son factores clave que subyacen a la emergencia y reemergencia de enfermedades transmitidas por mosquitos en Europa y España.

La introducción de vectores (en sus diversos estadios del ciclo vital) y patógenos está más relacionada con la globalización de los movimientos de personas, animales y mercancías, que con el cambio climático. Sin embargo, es crucial considerar el cambio climático, ya que favorece su establecimiento y modificará la exposición al riesgo de estas enfermedades en nuestro territorio, debido a cambios en los patrones estacionales de abundancias, impacto de eventos extremos (inundaciones, sequía).

La llegada de estos nuevos insectos vectores y la movilidad a escala global de las enfermedades no se va a detener, y el crecimiento del riesgo epidemiológico ya se ha hecho notar en Europa en las últimas décadas.

Es imperativo intensificar la vigilancia y el control de los mosquitos transmisores de enfermedades para contener un posible aumento de estas patologías, que incluyen el virus del Nilo occidental, la malaria, el dengue y otros.

La investigación básica sobre la ecología de estos vectores, junto con la consideración de aspectos sociológicos, es crucial para informar estrategias de vigilancia y control. Además, las nuevas tecnologías y la ciencia ciudadana están demostrando ser herramientas de gran potencial para recopilar datos relacionados con los mosquitos y sus interacciones con los humanos. España dispone de un Plan de Vigilancia, Prevención y control de Enfermedades Transmitidas por Vectores que desde 2023 se va ampliando y desarrollando y en el que participan el Ministerio de Sanidad como unidad coordinadora, las CCAA y un amplio grupo de expertos nacionales. Durante 2025 se han elaborado las Guías de manejo clínico, los manuales de gestión integrada del vector, y el protocolo de vigilancia éntomo-virológica de enfermedad del Nilo occidental.

Desde el CSIC, se están desarrollando nuevas herramientas de apoyo a la toma de decisiones que combinan datos autoritativos y contribuciones de la ciudadanía y que permiten comprender mejor el proceso de expansión de los mosquitos invasores, detectar patrones estacionales de actividad y posibles anomalías, y anticipar tanto las alertas como las acciones de control. Al mismo tiempo, ayudan a sensibilizar a la población y fomentar buenas prácticas de protección frente a estos vectores.

Medidas clave de la Unión Europea de la Salud

- A nivel europeo, prosigue la implementación del Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo de 23 de noviembre de 2022 sobre las amenazas transfronterizas graves para la salud y por el que se deroga la Decisión nº 1082/2013/UE.
- Todos los EEMM incluido España, continúan con el proceso de Evaluación de las capacidades de preparación y respuesta, derivado del artículo 8 del Reglamento (UE) 2022/2371. España realizó la evaluación en octubre de 2024, e hizo público su informe en julio de 2025.
- En el seno del Comité de Seguridad Sanitaria, se ha establecido un grupo de trabajo de colaboración-cívico militar, para reforzar y cooperar con otras partes interesadas en lo relacionado con las amenazas que deriven de conflictos armados.

- En el contexto del Reglamento (UE) 2022/2372 del Consejo de 24 de octubre de 2022 relativo a un marco de medidas para garantizar el suministro de contramedidas médicas pertinentes para la crisis en caso de emergencia de salud pública a escala de la Unión, España está participando en una Acción Conjunta de la Unión Europea para el desarrollo de una estrategia sostenible e integral de la reserva estratégica y en la Acción Conjunta de la Unión europea para la formación en contramedidas médicas.
- En el marco de las actividades de prevención, preparación y respuesta, la Comisión Europea ha publicado en noviembre de 2025 el Plan europeo de prevención, preparación y respuesta de la Unión para las crisis sanitarias. Este plan incluye el conjunto de herramientas que la UE tiene, abarcando la prevención y preparación, detección y evaluación, respuesta, y recuperación.

Medidas clave de España en el ámbito sanitario

- *La Ley 7/2025, de 28 de julio, por la que se crea la Agencia Estatal de Salud Pública y se modifica la Ley 33/2011, de 4 de octubre, General de Salud Pública*, ha creado la Agencia Estatal de Salud Pública. Actualmente, se está trabajando en el desarrollo del Real Decreto de sus estatutos. La Orden TMD/1467/2025, de 16 de diciembre, ha publicado el informe de la Comisión consultiva para la determinación de la sede de la Agencia Estatal de Salud Pública. La Agencia Estatal de Salud Pública coordinará la Comisión de Biocustodia del Plan Nacional de Biocustodia en el marco del Comité de no Proliferación de armas de destrucción masiva.
- El 6 de octubre finalizó el proceso de audiencia pública del Proyecto de Real Decreto del Plan Estatal de Preparación y Respuesta frente a Amenazas Graves para la Salud. Este Plan contempla los mecanismos de gobernanza y el desarrollo de las capacidades y recursos de preparación y respuesta frente a las amenazas graves para la salud y crisis sanitarias, utilizando mecanismos de coordinación intersectorial y entre los distintos niveles de las administraciones estatal, autonómica y local, incluyendo la disponibilidad de los servicios y recursos esenciales.
- En 2024 se publicó el *Real Decreto 568/2024 de 18 de junio por el que se crea la Red Estatal de Vigilancia en Salud Pública*, que también crea el Sistema de Alerta Precoz y Respuesta Rápida, con el fin de mejorar la detección precoz y favorecer una respuesta más rápida, oportuna y coordinada ante amenazas que supongan o puedan suponer un riesgo para la salud de la población.
- Finalmente, cabe destacar el Plan Nacional de Prevención, Vigilancia y Control de las Enfermedades Transmitidas por Vectores (Plan de vectores) que ha sido desarrollado bajo el enfoque de «Una Sola Salud», entre los sectores de salud humana, sanidad animal, gestión integrada del vector, sanidad ambiental, y medio natural. Dicho Plan recoge los esfuerzos realizados en los últimos años por instituciones y profesionales, con el objetivo de mejorar la capacidad de respuesta ante los riesgos que estas enfermedades suponen para la salud pública. Además, el Plan establece objetivos generales y específicos, así como mecanismos de coordinación entre administraciones, y promueve la integración de sistemas de vigilancia interconectados y sostenibles.

AMENAZAS A LAS INFRAESTRUCTURAS CRÍTICAS

- El incremento de episodios que afectaron a infraestructuras vinculadas al transporte, la energía y la logística en distintos países europeos, puso de relieve la vulnerabilidad de determinados elementos de la cadena de suministro y la creciente recurrencia de operaciones híbridas.
- Las infraestructuras marítimas se consolidan como un ámbito de atención prioritaria debido a su creciente exposición a riesgos físicos, operativos y geopolíticos, así como a su relevancia para la continuidad de servicios esenciales.
- Durante 2025, la participación de España en la Task Force de Resiliencia en Infraestructuras Críticas de la OTAN se centró en el refuerzo de la cooperación aliada y en el intercambio de información sobre amenazas híbridas con impacto potencial sobre servicios esenciales.

AMENAZAS A LAS INFRAESTRUCTURAS CRÍTICAS

Amenazas físicas

Durante 2025, las amenazas físicas sobre las infraestructuras críticas se desarrollaron en un contexto europeo caracterizado por la concurrencia de riesgos de distinta naturaleza, que incluyeron fenómenos naturales extremos, acciones deliberadas con capacidad de generar disrupciones y dinámicas propias de las amenazas híbridas. A diferencia de ejercicios anteriores, el año estuvo marcado por la materialización en Europa de incidentes que afectaron directamente a la continuidad de servicios esenciales.

En este entorno, se constató un incremento de episodios que afectaron a infraestructuras vinculadas al transporte, la energía y la logística en distintos países europeos, lo que puso de relieve la vulnerabilidad de determinados elementos de la cadena de suministro y la creciente recurrencia de operaciones híbridas. Entre ellos destacan los sabotajes a redes ferroviarias en Alemania, los incendios provocados y sabotajes mecánicos en centros logísticos y subestaciones eléctricas en Alemania y Francia, así como incursiones no autorizadas mediante drones sobre instalaciones sensibles, aeropuertos, parques eólicos en el mar del Norte o nodos portuarios. En general, se trata de actuaciones de baja complejidad técnica, pero con capacidad para generar disrupciones relevantes, orientadas a interferir en el funcionamiento normal de los servicios y a explotar vulnerabilidades físicas y operativas. A esta dinámica se sumaron ataques a infraestructuras energéticas estratégicas, como el ciberataque a una presa noruega que permitió la apertura remota de válvulas de control.

El uso indebido de drones adquirió una relevancia creciente como vector de riesgo en el entorno europeo, debido a su accesibilidad, su dificultad de detección y su potencial para ser empleados con fines de vigilancia ilícita o interferencia en operaciones críticas. Los incidentes registrados en torno a aeropuertos y puertos impulsaron el refuerzo de capacidades tecnológicas de detección, neutralización y control, así como la revisión de protocolos operativos. Estas medidas se extendieron a otras infraestructuras expuestas, como estaciones ferroviarias, centros de control de tráfico aéreo y nodos logísticos estratégicos.

En el ámbito nacional, durante 2025 estos riesgos se tradujeron en incidentes que afectaron a la continuidad de servicios esenciales, lo que exigió la activación de dispositivos de protección reforzada y una respuesta operativa sostenida por parte de las autoridades competentes y los operadores implicados. En este contexto, el transporte, y en particular la aviación civil, continuó figurando como un ámbito de atención desde el punto de vista de la seguridad física, manteniéndose dispositivos de

protección en aeropuertos, redes ferroviarias y centros de control, así como la coordinación con los operadores responsables de su gestión.

Las infraestructuras energéticas y logísticas concentraron esfuerzos específicos de protección en el ámbito nacional. La experiencia de incidentes registrados en otros países europeos reforzó la necesidad de incrementar la vigilancia y la prevención en subestaciones eléctricas, centros logísticos y otras instalaciones críticas, con especial atención a aquellas cuya afectación podría generar efectos en cascada sobre otros servicios esenciales.

A estas amenazas de carácter intencionado se sumaron riesgos derivados de fenómenos naturales extremos, como inundaciones, incendios o temporales, que durante 2025 afectaron a diversas infraestructuras críticas y pusieron a prueba su capacidad de resistencia y recuperación. Estos episodios evidenciaron la necesidad de integrar la gestión del riesgo climático en las estrategias de protección física y de reforzar la coordinación entre operadores, servicios de emergencia y autoridades competentes para minimizar el impacto sobre la continuidad de los servicios.

En este escenario, las Fuerzas y Cuerpos de Seguridad del Estado desempeñaron un papel central en la protección física de infraestructuras críticas, mediante la custodia de instalaciones estratégicas, la vigilancia de puertos, aeropuertos y fronteras y la supervisión de accesos y entornos sensibles. En 2025 se llevaron a cabo actuaciones de supervisión en instalaciones de especial relevancia, como centrales nucleares e instalaciones radiactivas, así como ejercicios operativos orientados a mejorar la capacidad de respuesta ante incidentes. Asimismo, se avanzó en la modernización de sistemas de vigilancia, con el refuerzo de capacidades de sensorización y detección en ámbitos como el control marítimo y fronterizo.

En 2025 se produjeron también incidentes de carácter delictivo en territorio nacional que, sin responder necesariamente a una intencionalidad terrorista, generaron impactos relevantes sobre servicios esenciales. La sustracción de cobre y otros materiales estratégicos continuó provocando interrupciones en sectores como el ferroviario, las telecomunicaciones o el alumbrado público, como reflejan las interrupciones temporales de servicios ferroviarios tras robos registrados en distintos puntos del territorio. Estos episodios subrayaron la necesidad de abordar este tipo de amenazas desde una perspectiva integral, que combine prevención física, investigación policial y coordinación con los operadores afectados.

En este contexto operativo se inscribe el cero energético registrado el 28 de abril, que puso de manifiesto la exposición de determinados sistemas y la importancia de disponer de mecanismos eficaces de respuesta ante incidentes de gran impacto. En particular, el incidente subrayó la necesidad de contar con sistemas de alimentación ininterrumpida y fuentes de energía alternativa que garanticen la autonomía de las infraestructuras ante fallos en la red principal. Asimismo, evidenció que la resiliencia de las redes de comunicaciones constituye un elemento esencial para la gestión de crisis, al requerir canales robustos y redundantes que permitan mantener el control operativo y la capacidad de respuesta coordinada en escenarios de pérdida de suministro eléctrico.

Si bien la respuesta coordinada, la activación de comités de crisis y la colaboración con las Fuerzas y Cuerpos de Seguridad del Estado resultaron determinantes para limitar el impacto, la experiencia ha puesto de relieve áreas de mejora necesarias.

Para ello, se hace imprescindible reforzar la autonomía energética, optimizar la gestión de combustible para equipos de emergencia, incrementar la resiliencia de las comunicaciones y perfeccionar la coordinación intersectorial ante incidentes de gran magnitud.

La prevención en el Sistema Nacional de Protección de las Infraestructuras Críticas

A lo largo de 2025, la prevención se consolidó como un eje central del Sistema Nacional de Protección de las Infraestructuras Críticas en un contexto marcado por la materialización de incidentes y por la necesidad de anticipar riesgos de distinta naturaleza. Las actuaciones preventivas se orientaron a reducir la exposición de las infraestructuras críticas frente a amenazas físicas, híbridas y naturales, mediante una planificación más exigente y una coordinación reforzada entre las administraciones competentes y los operadores responsables de la gestión de servicios esenciales.

En este marco, se intensificó la evaluación y supervisión de los planes de protección de las infraestructuras críticas, con un enfoque más riguroso orientado a verificar su adecuación a escenarios operativos reales. Las revisiones de los planes de seguridad y de contingencia permitieron identificar áreas de mejora y ajustar las medidas preventivas a la evolución de las amenazas, con el objetivo de minimizar el impacto de posibles incidentes sobre la continuidad de los servicios. Este enfoque contribuyó a optimizar la capacidad de respuesta y a reducir los tiempos de recuperación ante situaciones de alteración del funcionamiento normal de las infraestructuras.

La coordinación interadministrativa constituyó otro de los pilares de la prevención durante 2025. A lo largo del año se mantuvo y reforzó la colaboración entre el Centro Nacional de Protección de Infraestructuras Críticas, las Fuerzas y Cuerpos de Seguridad del Estado y el Ministerio de Defensa, especialmente en materia de intercambio de información, análisis de riesgos y actualización de planes de contingencia. Esta cooperación facilitó una visión compartida de las amenazas y permitió la adopción de medidas preventivas coherentes en los distintos niveles de la administración.

Desde el ámbito de la Defensa, se impulsó la cooperación operativa entre las Fuerzas y Cuerpos de Seguridad del Estado y los tres equipos de respuesta ante incidentes de ciberseguridad de referencia nacional. Esta colaboración se materializó en el intercambio continuado de información sobre alertas e incidentes, así como en la participación conjunta en grupos de trabajo y dispositivos de seguridad asociados a acontecimientos de especial relevancia, como procesos electorales, cumbres internacionales o eventos de alta visibilidad. Estas actuaciones reforzaron la dimensión preventiva del sistema al permitir una detección temprana de riesgos con potencial impacto sobre infraestructuras críticas.

De forma complementaria, la prevención incorporó de manera progresiva la consideración de riesgos derivados de fenómenos naturales extremos que, durante 2025, afectaron a diversas infraestructuras críticas. La integración de información procedente de los servicios de emergencia y de los sistemas de alerta temprana permitió mejorar la anticipación ante episodios como inundaciones, incendios o temporales, y facilitó la adopción de medidas preventivas orientadas a reducir daños y preservar la continuidad de los servicios esenciales. En este contexto, se reforzó la cooperación con los operadores y con los servicios de emergencia autonómicos y locales para asegurar una respuesta coordinada ante situaciones de riesgo.

Aproximación a las infraestructuras críticas marinas

Durante 2025, las infraestructuras críticas marinas se consolidaron como un ámbito de atención prioritaria debido a su creciente exposición a riesgos físicos, operativos y geopolíticos, así como a su relevancia para la continuidad de servicios esenciales. Puertos, terminales energéticas, cables submarinos, gasoductos e interconexiones eléctricas concentran una parte significativa del tráfico

de datos, energía y mercancías, lo que incrementa el impacto potencial de cualquier incidente que afecte a su funcionamiento. En este contexto, se intensificaron los esfuerzos orientados a mejorar el conocimiento, la identificación y la evaluación del grado de criticidad de estas infraestructuras en aguas bajo jurisdicción española.

A lo largo del año se observó un aumento de aproximaciones no autorizadas y comportamientos anómalos en el entorno de infraestructuras submarinas y marítimas sensibles, incluidos cables de telecomunicaciones, boyas instrumentadas, puertos estratégicos y plataformas energéticas. Estos incidentes se alinean con las advertencias emitidas en el ámbito europeo y aliado sobre el interés creciente de actores hostiles en el dominio submarino, caracterizado por su extensión, su complejidad técnica y las limitaciones inherentes a su vigilancia permanente. Esta evolución refuerza la necesidad de mantener capacidades de detección temprana y de respuesta coordinada ante posibles actos de interferencia, sabotaje o daño accidental.

En el plano internacional, durante 2025 se produjeron avances relevantes en el marco de la OTAN y la Unión Europea orientados a reforzar la protección de las infraestructuras críticas marinas. Entre ellos destacan la intensificación de las actividades de la red aliada de infraestructuras críticas subacuáticas y la puesta en marcha de iniciativas específicas para la protección de cables submarinos, como la operación “*Baltic Sentry*” en el mar Báltico. Asimismo, se avanzó en la actualización de las estrategias marítimas aliadas y europeas, incorporando de forma más explícita la protección de infraestructuras submarinas frente a amenazas híbridas. En este ámbito, España participó activamente en los trabajos desarrollados en el seno del Centro Marítimo para la Seguridad de Infraestructuras Submarinas Críticas (NMCSCUI, en sus siglas en inglés).

En el ámbito nacional, la protección de las infraestructuras críticas marinas se articuló a través de las actuaciones desarrolladas en el marco del Consejo Nacional de Seguridad Marítima, con el objetivo de mejorar la coordinación interadministrativa y reforzar la resiliencia de estas infraestructuras frente a incidentes deliberados, accidentales o derivados de fenómenos naturales. Desde la perspectiva operativa, se reforzó la vigilancia y el control del tráfico marítimo en las proximidades de infraestructuras sensibles, así como la supervisión de accesos y actividades en zonas de especial relevancia estratégica, en coordinación con las autoridades portuarias, Capitanías Marítimas y operadores críticos.

De forma complementaria, durante 2025 se avanzó en el uso de capacidades científicas y técnicas para mejorar la monitorización y el análisis de riesgos en el entorno marino y submarino. En este ámbito, el empleo de técnicas de monitorización geo científica, interferometría radar y observación del fondo marino permitió identificar zonas con deformaciones activas y procesos geológicos susceptibles de afectar a infraestructuras críticas. Estas capacidades contribuyen a mejorar la planificación preventiva y la gestión del riesgo, especialmente en relación con fenómenos como la sismicidad, los deslizamientos submarinos o la erosión, cuya incidencia puede verse agravada por el cambio climático y la actividad humana.

Resiliencia – aplicación de la directiva CER

En 2025, el refuerzo de la resiliencia de las infraestructuras críticas se abordó desde una perspectiva operativa y normativa, con especial atención a la aplicación del marco CER y a la mejora de los mecanismos de coordinación para la gestión de incidentes con impacto potencial sobre servicios esenciales. Este enfoque respondió a un entorno de amenazas cada vez más complejo, en el que confluyen riesgos físicos, cibernéticos e híbridos, y en el que la capacidad de respuesta y recuperación adquiere un papel determinante para garantizar la continuidad operativa.

En el ámbito normativo, durante 2025 se avanzó en el desarrollo del marco legal orientado a reforzar la resiliencia de las entidades críticas, con la aprobación del anteproyecto de la Ley de Protección y Resiliencia de las Entidades Críticas (Ley CER), aún pendiente de tramitación definitiva. Este marco incorpora la obligación de que las entidades críticas adopten un enfoque integral de gestión de riesgos, que incluya la identificación de amenazas físicas, cibernéticas e híbridas, así como la planificación de medidas de prevención, respuesta y recuperación. La articulación de este enfoque con otros marcos normativos de seguridad y resiliencia refuerza la coherencia del sistema a escala nacional.

Desde el punto de vista operativo, durante 2025 se avanzó en la integración de los principios de resiliencia establecidos en la directiva CER, concretamente en los mecanismos de gestión de incidentes que pueden afectar a infraestructuras críticas. Las Fuerzas y Cuerpos de Seguridad del Estado reforzaron su papel en la coordinación, notificación y respuesta ante incidentes con potencial impacto físico o funcional sobre servicios esenciales, contribuyendo a una respuesta más estructurada y a una mejora en la trazabilidad de las actuaciones desarrolladas.

En el ámbito de la Defensa, se continuó reforzando la resiliencia de las infraestructuras críticas con incidencia en la Defensa Nacional mediante la coordinación con las autoridades civiles competentes y la participación en los mecanismos nacionales de gestión de crisis. Durante 2025, estas actuaciones se orientaron a mejorar la capacidad de anticipación y respuesta ante incidentes complejos, así como a reforzar la protección de los sistemas CIS asociados a infraestructuras críticas estratégicas.

En el marco del Grupo Permanente de Coordinación de Resiliencia Nacional, dependiente del Comité de Situación, el Ministerio de Defensa, lidera las tareas de alineamiento entre el planeamiento civil y militar en materia de resiliencia, con la participación de los ministerios competentes y del Departamento de Seguridad Nacional. Este trabajo permitió avanzar en una visión compartida de los riesgos y en la definición de criterios comunes para la protección y recuperación de servicios esenciales ante incidentes de gran impacto.

Sistemas CIS de las IC y Operadores de Servicios Esenciales

A lo largo del año 2025, los sistemas CIS asociados a las infraestructuras críticas y a los operadores de servicios esenciales continuaron desempeñando un papel relevante en la supervisión de operaciones y en la gestión de incidentes con impacto potencial sobre la continuidad de los servicios. En un entorno caracterizado por la coexistencia de riesgos físicos y cibernéticos, las actuaciones se orientaron a reforzar la capacidad de coordinación, detección y respuesta ante incidentes que pudieran afectar al funcionamiento normal de infraestructuras con incidencia directa en la seguridad y el bienestar de la población. En este contexto, se avanzó en la identificación y análisis de operadores esenciales con incidencia en la Defensa Nacional, con el objetivo de mejorar la coordinación y el apoyo entre los distintos organismos competentes. Esta línea de trabajo permitió reforzar los mecanismos de cooperación entre los equipos especializados y facilitar una respuesta más coherente ante incidentes que afecten a sistemas y servicios estratégicos. La naturaleza de los operadores implicados confiere a estas actuaciones una especial relevancia en el ámbito de la protección de infraestructuras críticas.

Por su parte, el Plan estratégico contra la cibercriminalidad del Ministerio del Interior, dotado en 2025 con 9 millones de euros, ha permitido avanzar en la formación de la Policía Nacional y la Guardia Civil, reforzar la coordinación nacional y la cooperación internacional, la concienciación de la sociedad y abundar en la ciberseguridad de los operadores de servicios esenciales, entre otros objetivos.

De forma complementaria, se continuó trabajando en la mejora de la seguridad de los sistemas CIS mediante el refuerzo de procedimientos de supervisión y la atención a vulnerabilidades derivadas de

la coexistencia de tecnologías de información y tecnologías operacionales. La identificación de riesgos asociados a sistemas expuestos y a configuraciones heterogéneas puso de relieve la necesidad de mantener una actualización constante de medidas técnicas y organizativas para reducir la superficie de ataque y limitar el impacto de posibles incidentes.

En el ámbito de la investigación y la gestión de incidentes, la coordinación entre los distintos organismos del Estado permitió canalizar de forma más eficaz la respuesta ante incidentes que pudieran constituir ilícitos penales o comprometer la seguridad de servicios esenciales. La actuación conjunta de los organismos responsables de la protección de infraestructuras críticas contribuyó a reforzar la coherencia del sistema y a mejorar la trazabilidad de las actuaciones desarrolladas ante incidentes que afectan a operadores críticos y a sus sistemas CIS.

Colaboración público-privada

Durante 2025, la colaboración público-privada en el ámbito de la protección de infraestructuras críticas se mantuvo como un elemento operativo del sistema, centrado en reforzar los mecanismos de intercambio de información y la coordinación ante incidentes que pudieran afectar a la continuidad de los servicios esenciales. Las actuaciones desarrolladas se orientaron a consolidar canales ya existentes y a mejorar su funcionamiento en escenarios reales, sin introducir cambios estructurales respecto al marco vigente.

En este contexto, se continuó trabajando en el fortalecimiento de la cooperación entre las administraciones competentes, los operadores de infraestructuras críticas y los servicios de emergencia, con especial atención a la gestión de riesgos de origen natural y a la respuesta ante incidentes con impacto potencial sobre servicios esenciales. El refuerzo de los flujos de información permitió una mejor anticipación ante episodios adversos y facilitó una respuesta más coordinada, especialmente en situaciones que requieren una actuación rápida para minimizar efectos sobre la población y la economía.

Asimismo, la colaboración con los operadores privados responsables de instalaciones estratégicas siguió articulándose a través de planes de seguridad específicos, protocolos de actuación conjunta y ejercicios de coordinación. Aunque la explotación y gestión de determinadas infraestructuras corresponde a operadores privados, durante 2025 se mantuvo el modelo de supervisión y coordinación pública, orientado a garantizar el cumplimiento de las medidas de seguridad y a asegurar una respuesta homogénea ante incidentes que puedan comprometer la prestación de servicios esenciales.

De forma complementaria, las Fuerzas y Cuerpos de Seguridad del Estado continuaron participando en foros y grupos de trabajo junto a asociaciones empresariales, universidades y centros de investigación, con el objetivo de favorecer el intercambio de información, compartir buenas prácticas y reforzar una cultura de seguridad compartida en el ámbito de las infraestructuras críticas. Estas actuaciones contribuyeron a mejorar la confianza mutua y a facilitar la cooperación operativa en un entorno de riesgo cambiante.

I+D+i

En 2025, las actividades de investigación, desarrollo e innovación vinculadas a la protección de infraestructuras críticas se orientaron a reforzar la capacidad de anticipación, detección y respuesta frente a riesgos físicos, cibernéticos e híbridos, con un enfoque aplicado y alineado con las prioridades

de seguridad. Las actuaciones se centraron en apoyar proyectos que contribuyen a mejorar la resiliencia de sistemas esenciales y a reducir el impacto de incidentes sobre la continuidad de los servicios.

En el ámbito nacional, la Agencia Estatal de Investigación financió durante 2025 proyectos de investigación relacionados con infraestructuras críticas, con especial atención a líneas que abordan la protección de sistemas esenciales y la mejora de la resiliencia frente a escenarios disruptivos. Estas actuaciones permitieron consolidar capacidades científicas y técnicas orientadas a generar conocimiento aplicable a la planificación y protección de infraestructuras estratégicas.

En el plano europeo, el Programa Marco Horizonte Europa, a través del Clúster 3 “Seguridad civil para la sociedad”, definió nuevas líneas prioritarias para el periodo 2025–2027 orientadas a la protección de infraestructuras críticas. Estas líneas incluyen el desarrollo de tecnologías para evitar efectos en cascada ante ataques o fallos, la realización de pruebas de estrés sobre infraestructuras esenciales, el refuerzo de la resiliencia frente a catástrofes naturales o acciones deliberadas, y la consideración de factores humanos en la protección de infraestructuras, con especial atención a las amenazas internas.

Durante 2025 se continuó avanzando en la participación de entidades nacionales en proyectos financiados en el marco de Horizonte Europa, con una presencia relevante en iniciativas orientadas a mejorar la seguridad y resiliencia de infraestructuras críticas europeas. Estas actuaciones contribuyeron a reforzar la integración de capacidades nacionales en redes de investigación e innovación a escala europea y a facilitar la transferencia de resultados hacia aplicaciones prácticas.

De forma complementaria, se mantuvo la participación de organismos públicos en proyectos de innovación aplicada orientados a mejorar la sensorización, la detección temprana de anomalías y la automatización de procesos de vigilancia y respuesta. En este contexto, se reforzó el papel de los organismos de seguridad como usuarios finales en proyectos de innovación, contribuyendo a validar soluciones tecnológicas en entornos operativos reales y a mejorar su adecuación a las necesidades de protección de infraestructuras críticas.

Internacional – Task force de la OTAN de resiliencia en IC (Avances)

A lo largo de 2025, la participación de España en la *Task Force* de Resiliencia en Infraestructuras Críticas de la OTAN se centró en el refuerzo de la cooperación aliada y en el intercambio de información sobre amenazas híbridas con impacto potencial sobre servicios esenciales. Las actuaciones desarrolladas se orientaron a mejorar la prevención, la respuesta y la continuidad operativa ante incidentes que puedan afectar a infraestructuras críticas en el entorno euroatlántico.

En este marco, las Fuerzas Armadas españolas contribuyeron mediante la participación en ejercicios aliados, el apoyo a la evaluación de vulnerabilidades y la aportación de experiencia en la protección de infraestructuras con incidencia en la Defensa Nacional. Estas actividades favorecieron el desarrollo de criterios comunes de resiliencia y el fortalecimiento de la interoperabilidad entre aliados ante escenarios de disrupción de infraestructuras críticas.

Entre los avances del año destacaron la realización de ejercicios coordinados de gestión de crisis, como el *NATO Crisis Management Exercise 2025 (CMX25)*, así como la reactivación de los diálogos entre la Unión Europea y la OTAN en materia de seguridad y resiliencia, entre otros aspectos, como se detalla en el X Informe de progreso en las relaciones OTAN-UE (junio 2025). Estas iniciativas contribuyeron a mejorar la coordinación internacional y la capacidad colectiva de anticipación y respuesta ante incidentes con impacto transnacional.

EMERGENCIAS Y CATÁSTROFES

- En 2025 el Centro Nacional de Seguimiento y Coordinación de Emergencias de la Dirección General de Protección Civil y Emergencias ha registrado un total de 75 episodios de fenómenos meteorológicos adversos, siendo los más destacados por su frecuencia e impacto los relacionados con las lluvias intensas y las inundaciones.
- En 2025, se han registrado 63 grandes incendios forestales (que presentan una superficie afectada superior a las 500 ha), una cifra muy superior a los 23 de la media del decenio precedente.
- En el ámbito de la cooperación internacional, España activó el Mecanismo de Protección Civil de la Unión Europea, que respondió ante esta petición con un despliegue de medios sin precedentes, para el control y extinción de los incendios forestales que de forma simultánea afectaban en el mes de agosto a distintas áreas del territorio peninsular.

EMERGENCIAS Y CATÁSTROFES

En 2025 se han registrado 983 sucesos en el Sistema Integrado de Gestión de Emergencias (SIGE) de la Dirección General de Protección Civil y Emergencias (DGPCE) del Ministerio del Interior. (Figura 5.1)

Figura 5.1: Comparativa de los sucesos registrados en el Sistema de Información de Gestión de Emergencias (SIGE) por anualidades

SUCESOS	2025	2024	2023	2022	2021	2020	2019	2018	2017
Riesgo nuclear	3	9	5	7	11	2	0	1	1
Riesgo químico	40	32	27	34	30	26	24	19	16
Transporte de mercancías peligrosas	85	64	76	71	55	40	62	40	37
Incendios forestales	587	433	378	621	588	504	575	342	772
Riesgo climático	75	63	73	70	94	43	124	221	37
Riesgo sísmico	175	162	178	217	4.615	197	213	279	205
Riesgo volcánico	0	0	0	0	1	0	0	0	0
Otros riesgos	18	22	18	24	31	37	14	18	17
TOTAL	983	785	755	1.044	5.425	849	1.012	920	1.085

Fuente: Ministerio del Interior

En el mismo año, el Centro Nacional de Seguimiento y Coordinación de Emergencias (CENEM) de la DGPCE ha registrado un total de 75 episodios de fenómenos meteorológicos adversos, especialmente relacionados con lluvia e inundaciones. (Figura 5.2)



Figura 5.2: Sucesos registrados en el Centro Nacional de Emergencias en 2025

Fenómenos meteorológicos adversos

En 2025 se han registrado varios episodios de lluvias intensas y/o persistentes con efectos sobre el territorio, que han causado inundaciones de menor o mayor gravedad. El episodio más significativo se produjo en el mes de marzo, cuando, a partir del día 6, se desarrolló un tren de borrascas atlánticas de gran impacto (Jana, Konrad, Laurence y Martinho), con precipitaciones intensas generalizadas en todo el país.

Los daños por inundaciones fueron importantes especialmente en Andalucía, Región de Murcia, Madrid y las dos Castillas. La provincia de Málaga fue la zona más castigada con crecidas y desbordamientos de varios ríos, provocando la inundación de viviendas, anegamientos y cortes de agua potable. Se contabilizaron 3 fallecidos por efecto de las inundaciones, además de daños e incidencias de diversa naturaleza.

También se registraron otros episodios de menor amplitud e intensidad, entre los que cabe reseñar el fallecimiento de 2 personas en Sant Quintí de Mediona (Barcelona) en el mes de septiembre, tras un episodio de lluvias intensas que afectó a Cataluña; y 1 fallecido en Gibraleón (Huelva), como efecto de las lluvias torrenciales registradas Sevilla y Huelva a finales del mes de octubre.

El 7 de octubre se formó la Depresión Aislada en Niveles Altos (DANA) Alice, que volvió a provocar chubascos muy fuertes y perseverantes en el levante peninsular y Baleares, activando los avisos

meteorológicos de nivel naranja y rojo, por lo que fue necesaria la intervención de la UME en las Islas Baleares. Posteriormente, el 22 de octubre, la borrasca *Benjamín*, catalogada como ciclogénesis explosiva, generó fuertes vientos y oleaje (con olas de hasta ocho metros) en el litoral cantábrico y en zonas del norte del país. Cerrando el mes, la presencia de otra DANA al oeste de la península ocasionó un episodio de lluvias intensas que afectó inicialmente a Galicia y posteriormente a zonas del centro y sur peninsulares.

El 10 de noviembre hizo su aparición la borrasca *Claudia*, que dejó inicialmente lluvias y viento intenso en Canarias, y que posteriormente se extendió a la península con lluvias muy intensas y persistentes en el oeste de Galicia, el oeste de Castilla y León, Extremadura y, con especial virulencia, en Andalucía (principalmente en Huelva y Sevilla), donde se gestionaron un gran número de incidencias por inundaciones.

Los días 5 y 6 de diciembre llegó la borrasca *Davide*, una profunda borrasca atlántica, que dejó un temporal marítimo significativo en Galicia y Cantábrico, si bien no se produjeron daños e incidencias reseñables. Días después, el 11 de diciembre, la borrasca atlántica *Emilia* permaneció hasta el 15 de diciembre con alto impacto en Península y Canarias. A consecuencia de la misma, se produjeron inundaciones locales (rescates de personas en Castellón), cortes y balsas en viario, interrupciones de suministro y se adoptaron medidas de protección en espacios naturales.

Para terminar el año la borrasca *Francis* asoló especialmente Andalucía y Canarias y se prolongó hasta principios de enero del 2026 con precipitaciones muy abundantes, nevadas en cotas bajas, viento fuerte y marcado descenso térmico. Cabe destacar el fallecimiento de tres personas, una de ellas en la provincia de Granada, y otras dos en la provincia de Málaga.

Por otra parte, el 27 de marzo de 2025 se dio por finalizada la Operación “Inundaciones Valencia 2024” de las FAS, iniciada el 29 de octubre de 2024 a consecuencia de la DANA que afectó severamente a la Comunidad Valenciana. Tras esta emergencia, la UME asumió la dirección y coordinación del esfuerzo militar, compuesto por la totalidad de su capacidad operativa y el refuerzo proporcionado por el resto de las Fuerzas Armadas. En el conjunto de la operación participaron 33.885 militares, con un total acumulado de 69.634 efectivos entre todos los contingentes desplazados, lo que la convirtió en una de las mayores operaciones de apoyo a la población civil desarrolladas en territorio nacional.

También con ocasión de la DANA de Valencia de 2024, cabe mencionar que, a través del Protocolo de Asesoramiento en Desastres y Emergencias (PADE) y al Grupo de Asesoramiento en Desastres y Emergencias (GADE), el CSIC realizó un despliegue científico y técnico sin precedentes: 210 voluntarios procedentes de 27 institutos y centros, apoyados por una inversión de más de 1,3 millones de € y por la activación de cinco proyectos de investigación específicos, que siguen hoy plenamente activos, lo que evidencia que las labores de recuperación continúan muchos meses después del evento. Este esfuerzo ha permitido desarrollar 21 campañas de campo, centradas en la búsqueda de objetos arrastrados al mar, la caracterización de lodos y suelos contaminados, la evaluación de daños estructurales, el análisis de la calidad ambiental y el impacto marino.

La respuesta generó además una intensa actividad de transferencia, con 44 secretos industriales y 4 solicitudes de patente, y una destacada participación de institutos como el Instituto Geológico y Minero de España (IGME), el Instituto Español de Oceanografía (IEO), el Instituto de Diagnóstico Ambiental y Estudios del Agua (IDAEA) o el Centro de Edafología y Biología Aplicada del Segura (CEBAS), demostrando la capacidad multidisciplinar y sostenida del CSIC para acompañar a las administraciones no solo durante la emergencia, sino también en la fase crítica de recuperación y restauración de la normalidad.

En aplicación del Plan Meteoalerta de Predicción y Vigilancia de Fenómenos Meteorológicos Adversos, entre enero y diciembre de 2025, se han emitido 3.525 avisos por Fenómenos Meteorológicos Adversos (FMA) de nivel naranja o rojo sobre un total de 21.715 avisos. Para el cálculo de estos datos se contabiliza como un aviso de FMA a cualquier pronóstico de nivel de aviso rojo, naranja o amarillo de un parámetro concreto de cualquier tipo de fenómeno para una zona de aviso y para un día. El número y el porcentaje de cada uno de los niveles respecto al número total de avisos ha sido el siguiente: avisos de nivel rojo (peligro extraordinario) 153 (0,7%); avisos de nivel naranja (peligro importante) 3.372 (15,5%); y avisos de nivel amarillo (peligro bajo): 18.190 (83,8%).

Además, la Agencia Estatal de Meteorología (AEMET) ha mantenido el sistema AEMET Vialidad Invernal para UVR (Unidad de Valoración de Riesgo) de nevadas que facilita previsiones más ajustadas espacial y temporalmente sobre este tipo de fenómeno, que permiten la anticipación en la toma de decisiones.

Merecen destacarse los fenómenos meteorológicos adversos (heladas y nevadas) constatados en Castilla y León, con afección a la vialidad especialmente en la provincia de Soria en la que, entre los días 2 y 3 de marzo de 2025, hubo de restringirse la circulación en la autovía A-2 (nivel amarillo y rojo), contabilizándose un total de 900 vehículos retenidos y 1800 personas atrapadas en los mismos hasta que pudo normalizarse la circulación.

Durante la campaña de vialidad invernal 2024-2025, la Guardia Civil intervino en 123 cortes de carretera o restricciones a la circulación derivados de las necesidades de preservar la seguridad del tráfico rodado por fenómenos meteorológicos adversos (nevadas). Se produjo el embolsamiento de 3.983 camiones, siendo rescatadas 50 personas de un total de 995 vehículos atrapados y 1.854 personas asistidas.

Por su parte, a lo largo de 2025 la UME participó en una operación por nevada en Medinaceli (Soria), que se suma a las seis operaciones por inundaciones en Toledo, Zaragoza, Ibiza y Cartagena (Murcia) y a otras dos de búsqueda de personas desaparecidas en el Parque Nacional de Ordesa y Monte Perdido (Huesca) y Ribadesella (Asturias).

Temperaturas medias y precipitaciones

Según información de la Agencia Estatal de Meteorología, el año 2025 ha tenido un carácter extremadamente cálido, con un verano tórrido y un régimen de precipitaciones notablemente concentrado. La temperatura media sobre la península ha continuado la tendencia al alza, y la distribución de las precipitaciones mostró anomalías significativas.

Durante este año, el fenómeno más destacado fue el calor estival, haciendo que el conjunto del verano de 2025 se consolidara como el más cálido de la serie histórica desde 1961, superando el récord establecido en 2022. Esta anomalía térmica fue iniciada en junio, clasificado como el mes más anómalamente cálido jamás registrado.

Se observaron dos olas de calor de gran impacto que afectaron a la península e Islas Baleares. La primera ola de calor fue de larga duración, extendiéndose entre el 18 de junio y el 4 de julio, y afectando a gran parte del territorio. La segunda ola de calor se produjo entre el 3 y el 18 de agosto, periodo en el que se registraron los picos de temperatura del verano. Durante el periodo estival se contabilizaron un total de 33 días bajo ola de calor. Agosto fue, además de extremadamente cálido (empatando con agosto de 2024 como el más cálido), el décimo sexto mes de agosto más seco de la serie en la península.

Según el informe final del Plan Nacional de Actuaciones Preventivas frente a las Altas Temperaturas del Ministerio de Sanidad, durante el verano de 2025 se registraron 870 episodios de alto riesgo por calor (nivel 3), frente a los 501 episodios notificados en 2024.

En el periodo comprendido entre el 16 de mayo y el 30 de septiembre, se confirmaron 25 fallecimientos por golpe de calor, principalmente en personas con factores de vulnerabilidad de origen social, laboral o sanitario.

Asimismo, el Sistema de Monitorización de la Mortalidad Diaria (MoMo) estimó 3.832 defunciones atribuibles al exceso de temperatura en 2025, lo que representa un incremento del 87,6% respecto a 2024. El 96% de estas muertes correspondieron a personas mayores de 65 años, y más de la mitad superaban los 85 años.

El invierno 2024-2025 tuvo unas temperaturas excepcionalmente altas, situándose como el sexto más templado desde el inicio de la serie en 1961, y resultó, en conjunto, seco. En 2025 no hubo ningún episodio que pudiera catalogarse como ola de frío, continuando la pauta de años anteriores de baja significancia invernal.

La primavera fue en conjunto muy húmeda, especialmente en los meses iniciales, con valores medios un 151% por encima del normal (la quinta más húmeda desde 1961 y tercera del siglo XXI). El otoño concentró los eventos de inestabilidad más severos, como la entrada, a finales de septiembre, de los restos del huracán *Gabrielle*, que, junto con una situación atmosférica propicia, originó lluvias fuertes y persistentes en el tercio este peninsular.

Incendios forestales

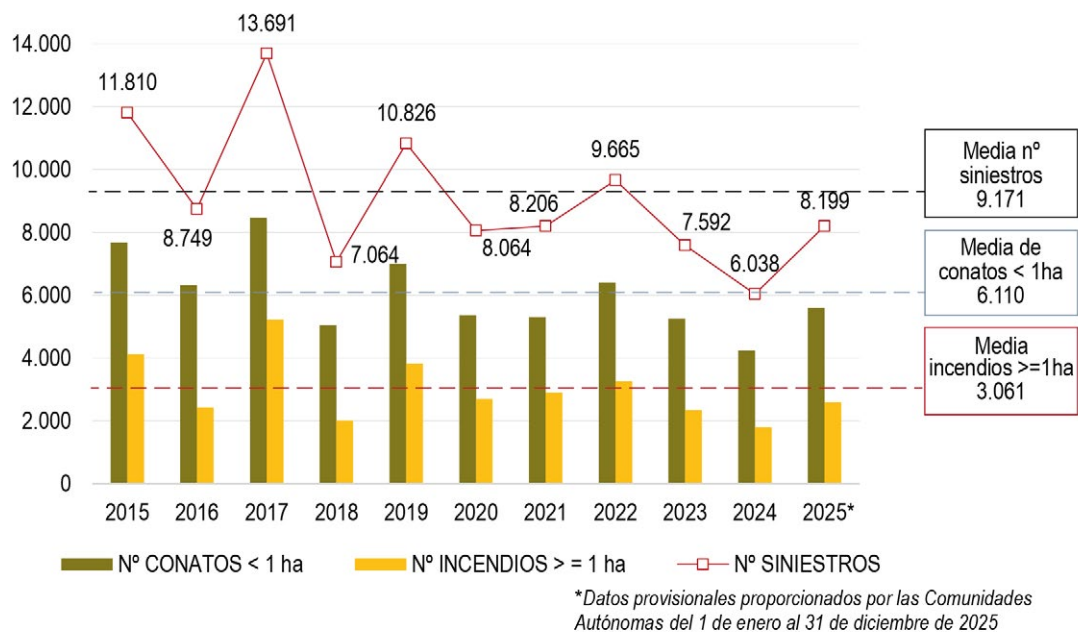
Los incendios forestales se mantienen como uno de los principales problemas a los que se enfrenta España en la época estival, por cuanto generan una gran alarma social no sólo por su impacto sobre el medio ambiente, sino también por la amenaza directa que representa para la seguridad de las personas y los bienes. La situación meteorológica descrita anteriormente durante el período de mayor riesgo de incendios (verano) ha tenido una correlación directa con el desarrollo de los grandes incendios forestales registrados (GIF, que presentan una superficie afectada superior a las 500 ha).

En cuanto a la evolución de la campaña de incendios forestales de 2025, hasta el 31 de diciembre, el número de siniestros (8.199) ha disminuido un 10,60% con respecto a la media del decenio anterior, reduciéndose el número de conatos (siniestros de superficie inferior a 1 ha) en un 8% y el de incendios en un 15%.

De aquellos, 63 han sido grandes incendios forestales, cifra muy superior a los 23 de la media del decenio precedente. En ellos han resultado afectadas 310.108,07 ha, lo que supone un 87% de la superficie total afectada (354.746,67 ha) por incendios forestales. (Figura 5.3)

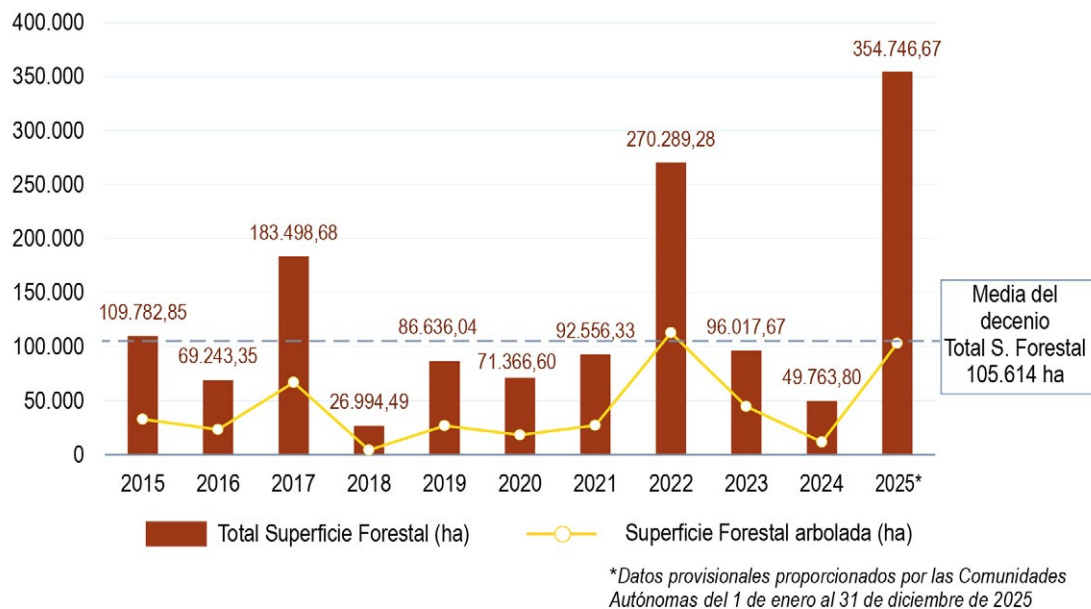
Todos los GIF salvo uno se produjeron dentro de la campaña de incendios forestales, período en el que se concentran los mayores riesgos. Durante la primera ola de calor (18 de junio a 4 de julio) se produjeron 3 GIF; en la segunda ola de calor peninsular (3 a 18 de agosto) se produjeron 42. En total, el 71,4% de los GIF se han producido bajo estos eventos climatológicos, siendo Galicia y Castilla y León las Comunidades Autónomas más afectadas.

En relación con la superficie forestal afectada en los incendios (354.746,67 ha), se ha producido un aumento del 235% con respecto a la media del decenio anterior (105.614 ha), resultando la superficie forestal quemada del año 2025, la quinta más alta de la serie histórica (1969-2025). (Figura 5.4)



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 5.3: Siniestros, conatos e incendios en el último decenio 2015-2025



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 5.4: Superficie forestal quemada en el último decenio 2015-2025

De los 16 incendios mayores de 20.000 ha de toda la serie histórica (1968-2025), 5 se producen en 2025 durante el episodio extraordinario de agosto. Solamente en 4 de estos GIF se han quemado prácticamente la misma superficie (105.978 ha), que la media de superficie forestal del último decenio (105.614 ha). Estos incendios se han concentrado en la zona noroeste de España (sur Galicia-norte de León y Zamora), siendo el mayor en superficie de toda la serie histórica el de Larouco(Ou)-Quiroga (Lu)-Oencia (Le) con más de 37.765 ha forestales quemadas. Le siguen los de Molezuelas de la Carballeda (Za)/Castrocalbón (Le) y Oímbra (Ou) con 24.426 y 22.414 hectáreas de superficie forestal quemadas respectivamente.

En el año 2025 se han producido 138 incendios forestales con consecuencias para la protección civil, en los que 8 personas fallecieron, 86 resultaron heridas -50 de ellas miembros de los equipos de intervención- y 42.913 fueron evacuadas, lo que supone un notable ascenso respecto al año 2024. (Figura 5.5)

Figura 5.5: Incendios con consecuencias de protección civil en 2025. Comparativa últimos 5 años

	2025	MEDIA	AÑOS				
		2020 2024	2024	2023	2022	2021	2020
Nº de incendios registrados	587	484	434	353	588	554	490
Nº de incendios con consecuencias de PC	138	55	65	37	96	52	25
Fallecidos	8	2	5	0	3	1	2
Heridos	86	54	42	70	90	60	9
Incendios con evacuados	110	39	40	29	75	30	20
Nº estimado de personas evacuadas	42.913	15.426	6.827	26.316	30.143	6.346	7.497
Incendios con albergados	13	11	6	9	22	11	7
Incendios con daños en infraestructuras	22	12	5	7	24	13	9
Incendios con cortes de carreteras	83	31	36	14	59	35	13
Incendios con cortes de ferrocarril	15	5	2	3	14	3	1
Incendios con cortes de electricidad	7	5	3	8	8	4	2
Incendios con intervención de la UME	49	21	8	8	54	14	20

Incendios con consecuencias de protección civil en 2025. Comparativa últimos 5 años.

Fuente: Ministerio del Interior

Además, de los GIF (63) registrados, el 71% (45) tuvieron consecuencias sobre la población o sus bienes, en el 79% (50) intervinieron medios del MITECO para su extinción. En 37 fue declarada la Situación Operativa 2 (59%).

Por parte de las Fuerzas Armadas, en el ámbito de apoyo a las autoridades civiles y con el objeto de colaborar con la campaña de prevención de incendios forestales, se ejecutó la *Operación Centinela* desde junio y hasta septiembre. Durante la operación se llegaron a desplegar un total de 60 patrullas junto con sus medios de mando y control y recuperación para la realización de actividades de vigilancia y disuasión en las zonas determinadas en sendos convenios con la Xunta de Galicia y el Cabildo Insular de Tenerife. Durante la segunda quincena de agosto, se incrementó el número habitual de patrullas de la operación Centinela Gallego, debido a la gravedad de los incendios registrados.

En las operaciones de lucha contra los incendios forestales, han participado más de 6.600 militares y se han empleado al menos 2.470 vehículos y medios de la UME, así como del 43 Grupo de Fuerzas Aéreas y del resto de las FAS. La UME intervino en 51 incendios, 24 de ellos fueron GIF, con un despliegue de 4.276 militares y 1.608 vehículos.

En lo que a la actuación de las FCSE se refiere, la Guardia Civil ha investigado 660 incendios susceptibles de tener un origen delictivo, ya sea por negligencia o dolo. A raíz de las investigaciones llevadas a cabo se ha efectuado la detención o investigación como posibles autores de 373 personas. El Instituto Armado contabiliza 236.484 servicios relacionados con el evento nacional de incendios forestales, y ha puesto a disposición de la gestión de incendios una importante cantidad de medios humanos y materiales: 29.566 efectivos que han participado de manera directa en la lucha contra los incendios forestales; 10 helicópteros, 1 avión, 44 drones y 10 Oficinas Móviles de Atención al Ciudadano.

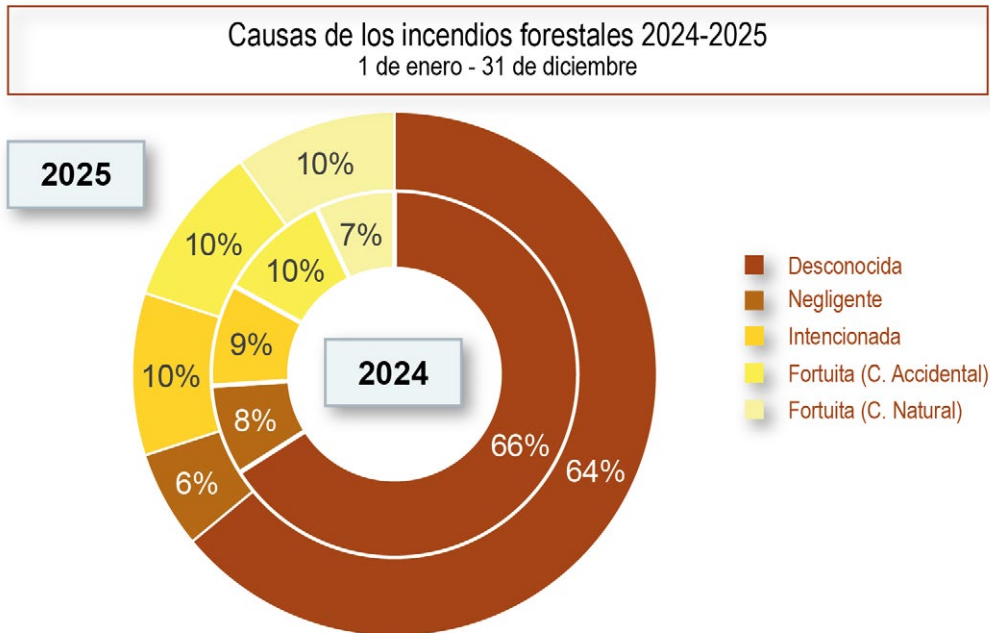
La estadística disponible de campañas anteriores evidencia que en aproximadamente dos terceras partes de los incendios forestales registrados no se llega a establecer la causa que lo originó. Ello pone de manifiesto, por una parte, la gran dificultad que conllevan este tipo de investigaciones y, por otra, que es preciso hacer un mayor esfuerzo en los aspectos relacionados con este ámbito. (Figuras 5.6)

Figura 5.6: Siniestros investigados por la Guardia Civil

	2020	2021	2022	2023	2024	2025
SINIESTROS INVESTIGADOS POR GUARDIA CIVIL	3.251	3.023	3.816	2.840	2.522	3.992

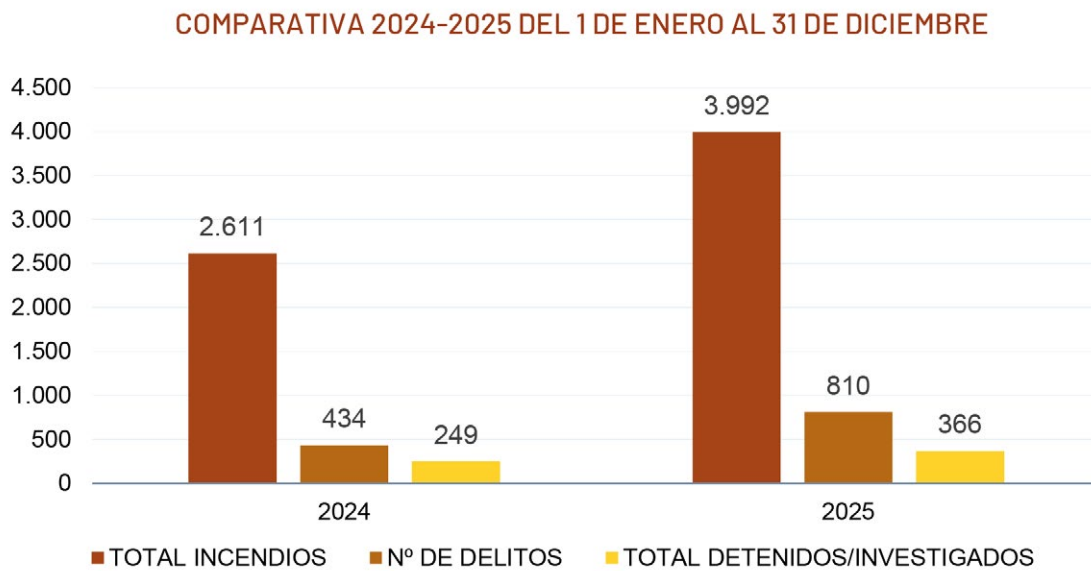
Fuente: Servicio de Protección de la Naturaleza de la Guardia Civil

No obstante, en aquellos incendios en los que se ha podido determinar las causas que los han propiciado se pone de manifiesto que el factor humano se encuentra presente en el 72% de los sucesos. Esto confirma que las conductas humanas, ya sean imprudentes, involuntarias o deliberadas, siguen siendo el principal desencadenante en los incendios esclarecidos. (Figuras 5.7 y 5.8)



Fuente: Dirección General de la Guardia Civil

Figura 5.7: Causas de los incendios forestales 2024-2025



Fuente: Dirección General de la Guardia Civil

Figura 5.8: Comparativa del número de incendios, delitos y detenidos 2024-2025

Por su parte, la Policía Nacional también ha participado en la gestión de estas catástrofes, fundamentalmente en las zonas urbanas afectadas, mediante el control de accesos y la protección de las personas en riesgo, la protección de infraestructuras críticas y edificios sensibles; así como a través de su Unidad Aérea, que se integra en diversos planes de emergencia, como el INFOCA. La importante participación de la Policía Nacional en la campaña incendios de verano de 2025 incluyó un total 14.864 efectivos y 3.281 recursos materiales.

La DGPCE, como punto nacional de contacto del Mecanismo Europeo de Protección Civil (UCPM), ha gestionado durante 2025 la respuesta de nuestro país a las solicitudes de ayuda motivadas por incendios forestales, además de solicitar ayuda a través de este mecanismo para hacer frente a los fuegos registrados en agosto en territorio peninsular. También se ha canalizado ayuda en base los convenios bilaterales suscritos con países vecinos. En el apartado de cooperación internacional se recoge esta información con más detalle.

Además de la actualización continua de los mapas diarios de nivel de peligro de incendios forestales a nivel nacional y autonómico, así como de los archivos a nivel municipal, con alcance hasta 7 días y muy útiles para la prevención, AEMET ha seguido manteniendo en 2025 las mejoras para el apoyo a la lucha contra incendios y a la protección civil asociada a los incendios forestales desarrolladas en 2023, el Visor web AEMET ALCIF, que permite a los organismos de protección civil y de extinción de incendios, tanto estatales como autonómicos, acceder a la última información en tiempo real de observación (datos de estaciones, satélites, radar y descargas eléctricas) y de predicción (la última salida del modelo numérico operativo Harmonie-Arome) de temperatura, humedad, viento, racha máxima de viento, y precipitación; al servidor de mapas georreferenciados focalizados en el punto del incendio, que permite la descarga de mapas de viento, temperatura, humedad y precipitación, centrados en el punto del incendio, meteogramas con la predicción y sondeos; y también la emisión de boletines especiales de predicción meteorológica de apoyo a la extinción de incendios elaborados específicamente por los predictores de AEMET a demanda de los organismos de protección civil y extinción de incendios autonómicos.

Debido a los graves incendios de la campaña 2025, AEMET ha incrementado muy significativamente este apoyo, con 442 boletines especiales emitidos (hasta el 28 de septiembre), que suponen un 76% del total de boletines emitidos desde enero de 2023. De hecho, un 61% del total se emitieron entre el 11 y el 31 de agosto.

Por otro lado, AEMET ha seguido participando en los encuentros virtuales quincenales de seguimiento que se iniciaron en la campaña 2024, coordinados por la Dirección General de Biodiversidad, Bosques y Desertificación, en los que se presta una asesoría sobre la situación meteorológica, el índice de peligro de incendios actuales y la predicción para los próximos días y semanas.

Finalmente, durante la campaña 2025 se ha puesto en fase preoperativa en el visor AEMET ALCIF, un nuevo índice de peligro de incendios forestales que no es solo puramente meteorológico sino más estructural y que sustituirá en la campaña 2026 al índice actual. Además de las condiciones meteorológicas, que ya se tienen en cuenta en el índice actual, las principales novedades de este nuevo índice son: la inclusión del tipo de suelo forestal y su inflamabilidad, junto con el estado de la vegetación; la incorporación de la cobertura de nieve y zonas urbanas; el aumento de la resolución espacial de 5 a 1 km; una nueva calibración incluyendo los últimos años y otras mejoras en estudio (humedad del suelo, relacionada con la humedad del combustible vivo).

Por otra parte, los incendios acaecidos durante el año 2025 han afectado seriamente a la explotación ferroviaria: Taboadela - Ourense (Ourense), Sant Sadurní - Martorell Central (Barcelona), Yeles - La Sagra (Toledo), Os Peares - San Estevo (Ourense), provocando múltiples retrasos y suspensiones del

servicio. Especialmente importante fue la afección a las instalaciones ferroviarias de los incendios en las provincias de Zamora y Orense en el mes de agosto, que mantuvo cortada durante varios días, coincidiendo con el puente de agosto, fechas de gran demanda, la conexión ferroviaria entre Madrid y Galicia.

Por otra parte, en agosto de 2025 se activó el Protocolo y el Grupo de Asesoramiento en Desastres y Emergencias (PADE / GADE CSIC) para el apoyo a las zonas afectadas por los fuegos. De hecho, el GADE Incendios 2025 fue liderado por los coordinadores de emergencias y de riesgos forestales del CSIC y estuvo activado entre agosto y diciembre de 2025.

Además, cabe destacar las actuaciones del Centro para el Desarrollo Tecnológico y la Innovación (CDTI) que, dentro de su programa Misiones Ciencia e Innovación, ha puesto en marcha una acción orientada a la planificación y gestión territorial para mejorar la resiliencia y hacer frente a los riesgos climáticos y que persigue ofrecer soluciones que reduzcan el impacto de fenómenos adversos derivados del cambio climático, como sequías, inundaciones o incendios forestales, además de extender medidas de alerta temprana y de seguridad en infraestructuras energéticas y/o destinadas a servicios públicos.

Finalmente, en el contexto de la gestión de otras emergencias acaecidas en 2025 con trascendencia para la protección civil, el cero energético registrado a nivel nacional (28 de abril) hizo necesaria la activación de la fase de Emergencia Nacional, Situación Operativa 3, del Plan Estatal General de Emergencias (PLEGEM) en ocho comunidades autónomas: Andalucía, Extremadura, La Rioja, Comunidad de Madrid, Región de Murcia, Castilla-La Mancha, Galicia y Comunidad Valenciana.

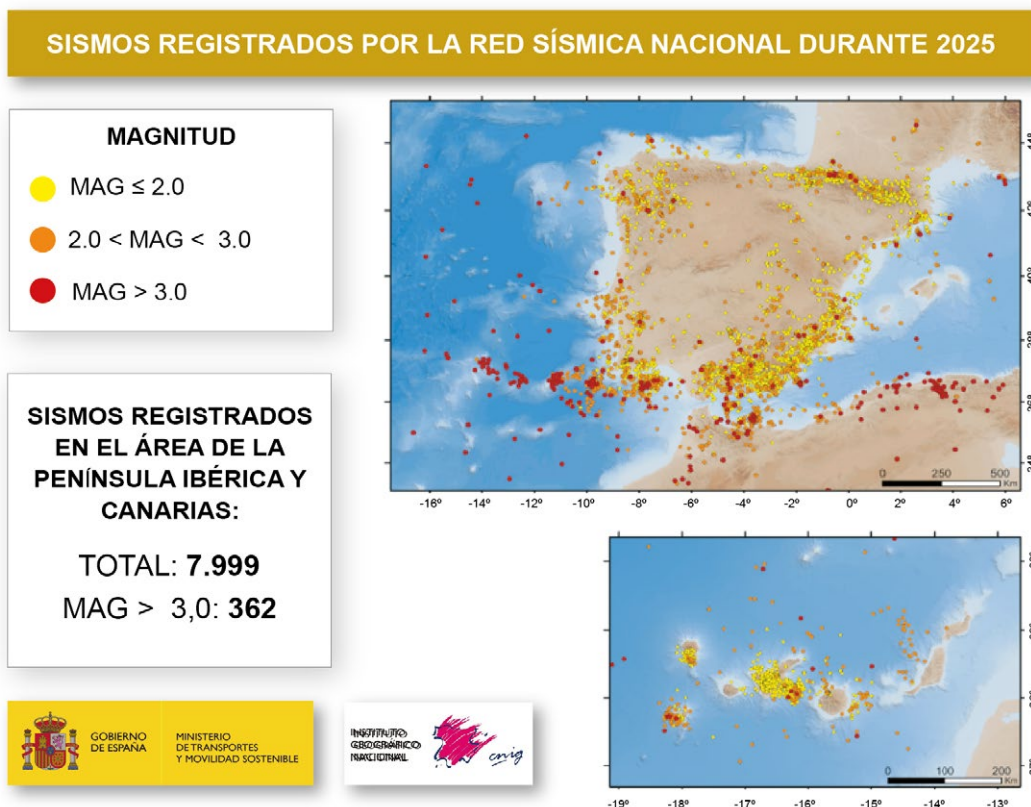
En esta emergencia, y al igual que hicieran otros recursos del sistema nacional de protección civil, las Fuerzas Armadas, con la UME como elemento de primera intervención, prestaron numerosos apoyos en diferentes ámbitos. La UME ejerció la Dirección Operativa de la Emergencia, bajo la superior dirección del ministro del Interior, e intervino con la totalidad de su personal en activo (más de 3.000 militares y 159 medios). El resto de las unidades de Fuerzas Armadas aportaron a la emergencia otros recursos adicionales de naturaleza diversa.

Actividad sísmica y volcánica

La actividad sísmica y volcánica se mantienen como riesgos presentes en nuestra geografía, especialmente en determinadas zonas. El mantener y potenciar los sistemas de vigilancia y monitorización de los fenómenos, así como la adopción de medidas de prevención son la manera de minimizar dentro de lo posible sus efectos en caso de producirse. Así, se sigue trabajando en el desarrollo y transformación de la red sísmica y de los sistemas de vigilancia, con la incorporación de nuevas tecnologías y la optimización y mejoramiento de las ya existentes.

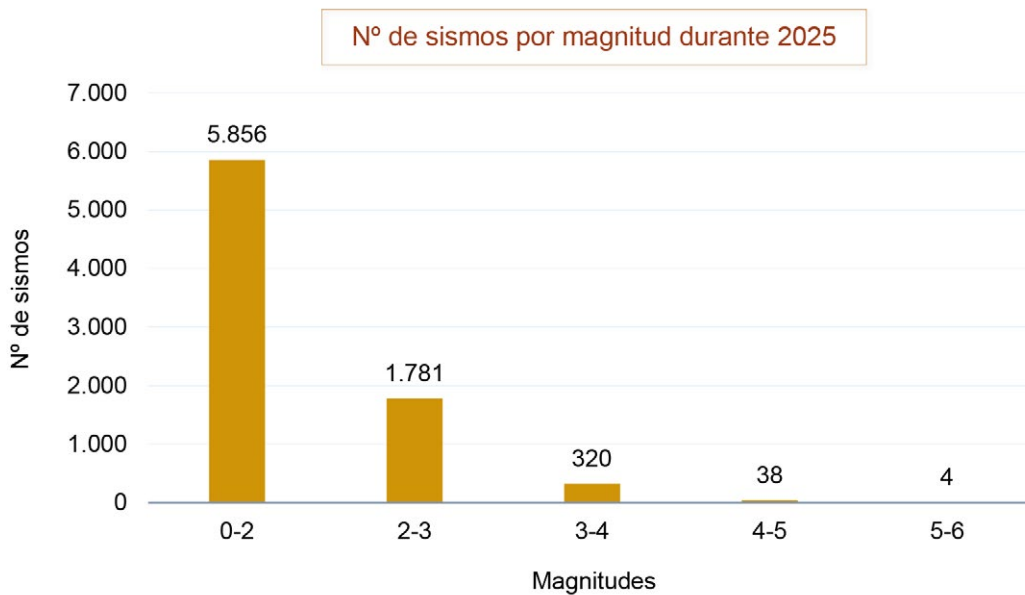
La Red Sísmica Nacional (RSN) del Instituto Geográfico Nacional (IGN) ha registrado en España y zonas próximas 7.999 terremotos durante 2025. De ellos, 362 tuvieron magnitud mayor de 3,0. El número de terremotos sentidos fue de 163. En las se representa la distribución de los terremotos por magnitud y por intensidad macrosísmica (escala EMS-98) desde el año 2000. (Figuras 5.9 a 5.13)

El terremoto de mayor magnitud ha sido el ocurrido en el 25 de julio en el Océano Atlántico, al oeste de Sines (Portugal), con una magnitud de 5,7, aunque no se tiene constancia de que fuera sentido en territorio español. Por el contrario, durante 2025, sí se han sentido cuatro terremotos con intensidad 4: el 27 de febrero de magnitud M3,8 en Cazalla de la Sierra (Sevilla); el 14 de julio, de M5,3 en zona Mediterráneo-Levante sur; el 12 de septiembre, de M3,1 en Santa Fe (Granada); y, finalmente, el 7 de diciembre de M8 en Iruña de Oca (Vitoria).



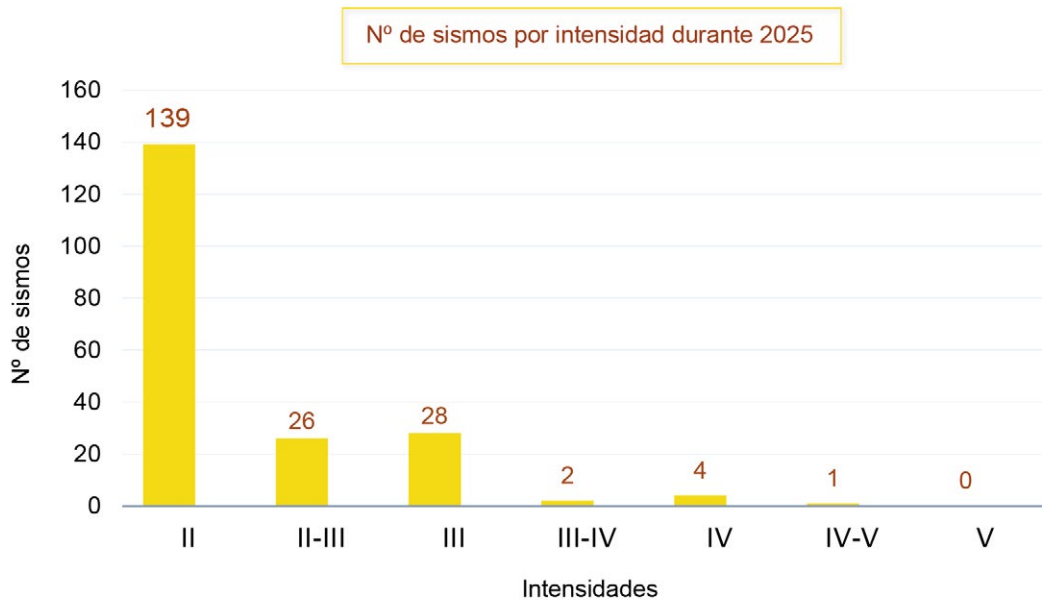
Fuente: Ministerio de Transportes y Movilidad Sostenible

Figura 5.9: Terremotos registrados en 2025 por el IGN en España y zonas limítrofes



Fuente: Ministerio de Transportes y Movilidad Sostenible

Figura 5.10: Distribución del número de terremotos de 2025 por magnitud



Fuente: Ministerio de Transportes y Movilidad Sostenible

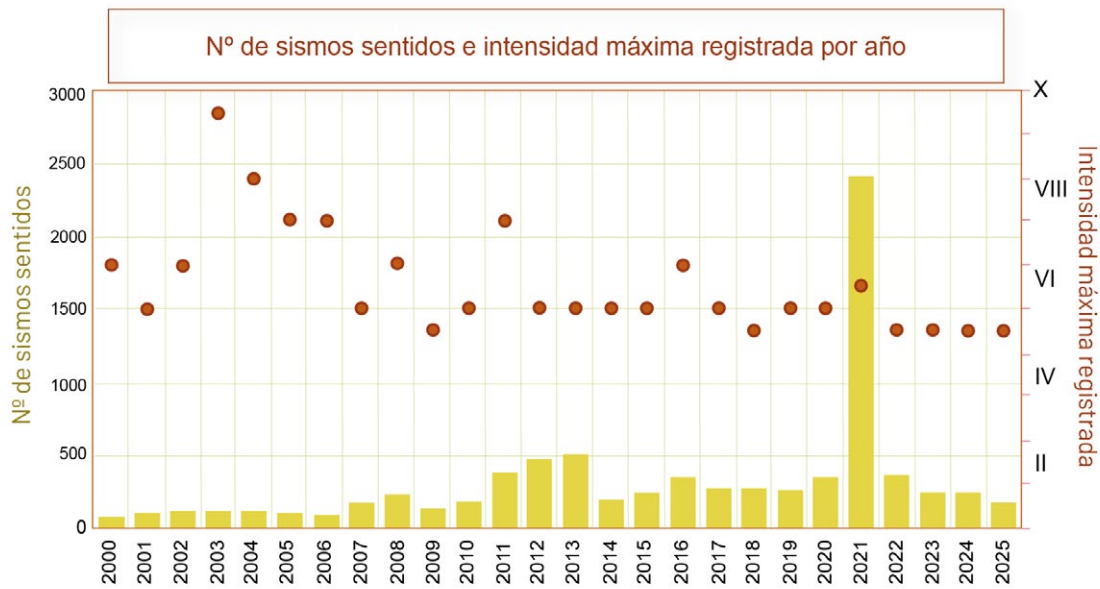
Figura 5.11: Distribución del número de terremotos de 2025 por intensidad macrosísmica máxima (escala EMS-98)



*En marrón sólo aquellos cuya magnitud es mayor de 3,0

Fuente: Ministerio de Transportes y Movilidad Sostenible

Figura 5.12: Número de terremotos por año desde el año 2000



*los puntos rojos indican la intensidad macrosísmica máxima (escala EMS-98) registrada ese año en España y zonas limítrofes

Fuente: Ministerio de Transportes y Movilidad Sostenible

Figura 5.13: Número de terremotos sentidos por la población por año desde el año 2000

Por otro lado, se ha informado por parte del IGN al Centro Nacional de Seguimiento y Coordinación de Emergencias (CENEM) de 14 series sísmicas: 6 en Canarias, 6 en Andalucía, 1 en Navarra, 1 en Huesca.

Sobre el riesgo volcánico, el Plan Especial de Protección Civil de Riesgo Volcánico de la Comunidad Autónoma de Canarias continúa en Situación Operativa 1. Como medida fundamental de protección de la población, el Instituto Geográfico Nacional y el Instituto Volcanológico de Canarias, a través de la red de vigilancia de gases en la Palma, dotada con 1.482 estaciones de monitoreo, prosiguen analizando la evolución de las emisiones de dióxido de carbono, entre otras, en las poblaciones de Puerto Naos y La Bombilla, con objeto de mantener informada a la población y asesorar administraciones locales para la toma de decisiones sobre realojos.

Actividad solar

Durante 2025 se ha alcanzado el máximo de actividad solar del ciclo 25, comenzando la fase de disminución del número de manchas solares, si bien esto no supone una desaparición de eventos solares importantes que se espera que sigan ocurriendo en los próximos años.

El año comenzó con una importante tormenta geomagnética, que tuvo lugar el día 1 de enero de 2025 y fue clasificada como tormenta de categoría G4 (severa), alcanzándose un valor de Kp=8, y valores de K=7 en los observatorios de San Pablo de los Montes y Güímar.

El suceso más importante del año 2025 ocurrió el 12 de noviembre, en el que tuvo lugar un evento que alcanzó la categoría de G4, alcanzándose un valor de Kp=9-, y valores de K=9 en los observatorios del IGN. Otros eventos importantes que han alcanzado la categoría de G4 han ocurrido los días 15 de abril y 1 de junio, para los que se ha determinado un valor de Kp=8-, si bien no se superaron los valores de K=6 en los observatorios del IGN. Además, han ocurrido varios eventos de categoría G3 (fuerte) a lo largo del año.

Cooperación internacional para la gestión de emergencias

A lo largo del año 2025, España ha participado en 25 emergencias en activaciones del Mecanismo Europeo de Protección Civil (UCPM). Las activaciones en el marco de este instrumento han supuesto la aportación distintas capacidades, destacando la actividad desarrollada ante un incendio en un club nocturno en Macedonia del Norte, que facilitó el ingreso en hospitales especializados en el tratamiento de lesiones por quemaduras graves; en Gaza se colaboró en la evacuación médica desde la franja a hospitales españoles de pacientes, principalmente menores, que no podían ser tratados en los hospitales locales; en las inundaciones de Cabo Verde se enviaron 720 kits de higiene personal; en Ucrania se colaboró en el enlace de un conjunto de dispositivos de conexión y protección de equipos eléctricos; y en Jamaica, tras el paso del huracán Melisa, se envió un Equipo de Emergencia Médico de nivel 2 (EMT2) de AECID, que permaneció activo durante más de un mes.

Además de estas actuaciones, también en el marco del UCPM, se desplegó ante graves emergencias acaecidas en Ecuador, tras un derrame de petróleo, donde fue desplegado un experto de la Marina Mercante en gestión de residuos peligrosos, en ecosistemas marinos y terrestres, y en recursos híbridos y calidad del agua; así como en Rumanía, tras un incidente en la mina de sal Praid, donde se envió un experto en impacto medioambiental (IGME).

Junto a los ofrecimientos de ayuda, España también activó el UCPM en dos ocasiones durante el período estival. Por un lado, dos equipos de bomberos forestales de Países Bajos y dos Equipos de

Estonia acudieron a apoyar y formarse con el personal de la Xunta de Galicia y de la Junta de Castilla-La Mancha.

Además, debido a la elevada magnitud y al gran número de incendios simultáneos ocurridos en el mes de agosto, entre el 14 y el 30 de agosto se activó el UCPM para colaborar en la respuesta ante los incendios de Extremadura, Galicia, Castilla y León y Asturias. Se recibió ayuda de nueve países, con un total de 8 medios aéreos, 221 bomberos y 46 vehículos. Además, se contó con la ayuda de un contingente de 6 bomberos forestales desde Andorra.

En aplicación de los convenios bilaterales suscritos con otros países, diversos medios españoles han intervenido en 29 incendios forestales en Portugal. También, en el mismo período, medios portugueses han intervenido en 14 incendios ocurridos en zonas fronterizas de nuestro país. Asimismo, el Principado de Andorra ha participado en la extinción de nuevos focos en los incendios ocurridos en Asturias a finales del mes de agosto.

Por su parte, la UME participó en dos operaciones en el exterior: la operación “Libre Hidalgo” (Líbano), donde instruyó en materia de Protección Civil a los Centros de Defensa Civil de la zona de operaciones; y la operación “NATO Mission Iraq”, en la que impartió el Curso de Apoyo en Emergencias para personal del Ministerio de Defensa y del Ministerio del Interior en Irak. Esta formación se centró en las capacidades con las que el Ministerio de Defensa iraquí podría apoyar al Ministerio del Interior en caso de emergencia nacional, así como en el establecimiento de las relaciones de mando y control necesarias para dicho apoyo, tomando como referencia el modelo español.

También en este período un buque de la Armada transportó material de ayuda humanitaria a Cabo Verde, y se utilizó la Base Aérea de Torrejón para transporte de ayuda humanitaria a Jamaica.

Nuevamente, durante 2025 se ha activado la **Operación Paso del Estrecho (OPE)**, con un dispositivo coordinado a través de la Dirección General de Protección Civil y Emergencias. Se desarrolló entre el 15 de junio y el 15 de septiembre, en sus habituales Fases de Salida (15 de junio - 15 de agosto) y de Retorno (15 de julio - 15 de septiembre).

En esta edición se han embarcado un total de 3.488.885 personas y 857.784 vehículos en 10.536 rotaciones de barcos. Se han alcanzado máximos históricos en todos los datos de embarque de pasajeros y vehículos que se contabilizan en la operación. La normalidad y la fluidez ha sido la tónica general en todos los puertos, sin que hayan llegado a saturarse las capacidades de ninguna instalación portuaria, incluidas las de mayor tráfico (Algeciras, Almería, Ceuta, Tarifa y Melilla).

Durante la Fase de Salida, se ha gestionado el tránsito por la península hacia el continente africano de vehículos y personas procedentes de Europa, así como el embarque en 15 líneas marítimas de 1.720.799 pasajeros (3,5% más que en 2024) y 433.755 vehículos (3,6% más que en 2024) en los puertos españoles de Algeciras, Tarifa, Málaga, Motril (Granada), Almería, Alicante y Valencia.

Durante la Fase de Retorno, se ha gestionado el regreso a Europa y el embarque de 1.768.086 pasajeros (2,3% más que en 2024) y 424.029 vehículos (2,4% más que en 2024) en los puertos ubicados en el Norte de África: Ceuta y Melilla en España; Tánger-Med, Tánger-Ville, Nador y Alhucemas en Marruecos y Argel, Orán, Ghazaouet y Mostaganem, en Argelia.

La fluidez en los tránsitos ha permitido no solo que no haya sido necesario determinar la intercambiabilidad de billetes en Algeciras, al igual que la precedente campaña de 2024, sino incluso que no se hayan declarado fases de preemergencia ni emergencia en ninguno de ambos puertos.

La repercusión que esta operación tiene en las principales rutas por carretera provoca que se desplieguen servicios de las FCSE, combinando un refuerzo de las actuaciones encaminadas a salvaguardar la seguridad vial con las actuaciones en los recintos portuarios. En este sentido, se ha detectado un repunte de la captación de clientes dentro del recinto portuario para la venta ilegal de billetes y tarjetas de embarque por agencias ubicadas fuera de él.

Por su parte, AEMET ha seguido manteniendo el sistema AEMET Operación Paso del Estrecho, que facilita el acceso a la información meteorológica (avisos de fenómenos meteorológicos adversos, predicciones, modelos de oleaje) actualizada en tiempo real para el propio día y los dos siguientes en las principales zonas de interés.

Accidentes e incidentes en el transporte

Las Comisiones de investigación de accidentes dependientes del Ministerio de Transportes y Movilidad Sostenible tienen por función mejorar la seguridad en los distintos medios de transporte.

De esta forma, la Comisión de Investigación de Accidentes e Incidentes de Aviación Civil (CIAIAC) ha abierto en 2025 un total de 35 investigaciones de accidentes e incidentes graves, emitiendo un total de 42 recomendaciones de seguridad operacional.

Por su parte, la Comisión de Investigación de Accidentes e Incidentes Marítimos (CIAIM) ha recibido 282 notificaciones de accidentes e incidentes de las que se han investigado 15, desestimándose 267. Se ha producido el hundimiento de 21 buques y embarcaciones, y se han publicado 15 informes durante el año, en los que se han incluido 20 recomendaciones de seguridad.

La Comisión de Investigación de Accidentes Ferroviarios (CIAF) ha recibido 138 notificaciones de accidentes e incidentes, de los que se ha decidido investigar 4 sucesos (2 accidentes y 2 incidentes). Además, se han elaborado 5 Estudios Preliminares. Este año también se han cerrado las investigaciones de 2 sucesos (un accidente y un incidente) y se han publicado sus informes finales, que incluyen un total de 10 recomendaciones de seguridad.

La Oficina de Asistencia a Víctimas de Accidente Aéreos (OAV) del Ministerio de Transportes y Movilidad Sostenible ha mantenido su actividad en materia de colaboración docente con la Escuela Nacional de Protección Civil, a través de varios cursos sobre gestión de asistencia a familiares por emergencias masivas en transporte colectivo, dentro de su labor de consolidación de una estructura nacional de atención a las víctimas y familiares de accidentes masivos en el transporte.

En la esfera internacional, la OAV ha participado en la 42ª Asamblea General de Organización de Aviación Civil Internacional (OACI) en Montreal, en la que se ha trabajado sobre distintas propuestas en materia de asistencia, en estrecha coordinación con la DG de Aviación Civil. En este foro se han mantenido contactos bilaterales con diversos estados miembros, como Reino Unido, Brasil y Canadá. También ha continuado su actividad con el grupo de trabajo *Asistencia a las víctimas de accidentes de aviación y a sus familias (AAAVF)* de OACI, dirigido a mejorar las capacidades de los estados en la implantación de la normativa y recomendaciones en el campo de asistencia a víctimas.

Junto con acciones de divulgación en el entorno diplomático y consular de la UE y terceros países, en el ámbito de la colaboración público-privada, la Oficina de Asistencia a Víctimas de Accidente Aéreos ha mantenido contactos con representantes de diversas aerolíneas para intercambiar experiencias y compartir buenas prácticas en ese campo.

Desarrollos estratégicos y regulatorios

Además de los trabajos de elaboración de las Directrices Básicas para los distintos riesgos ante emergencias de Protección Civil, los avances sobre el Plan Estatal General de Emergencias de Protección Civil (PLEGEM) se centran en dos aspectos:

En lo que respecta a la **confección del mapa de riesgos**, continúa la actualización de las distintas capas cartográficas de riesgo de ámbito autonómico, que deberán mostrarse en el Mapa Nacional de Riesgos, en función de su tipología (peligrosidad, vulnerabilidad, riesgo u otras). Hasta el momento, se han incorporado nuevas cartografías de 11 Comunidades Autónomas, así como diferentes cartografías a nivel nacional proporcionadas por los distintos organismos de la Administración General del Estado.

En lo respecta al **Mecanismo Nacional de Respuesta**, el desarrollo que se ha realizado durante el año 2025 ha sido la preparación de la Guía Técnica de Módulos Nacionales de Respuesta, que se presentó al Consejo Nacional de Protección Civil en diciembre de 2025. En esta guía se definen las características mínimas que los módulos nacionales de respuesta deben tener para poder ser incluidos en el Catálogo Nacional de Módulos de Respuesta ante emergencias.

El 17 de diciembre de 2025 se celebró el Pleno del Consejo Nacional de Protección Civil, donde se aprobaron varios asuntos por unanimidad. Por un lado, la Guía Técnica de los Módulos Nacionales de Emergencia, así como el impulso de la creación de la Plataforma Nacional para la Reducción de Riesgos de Desastres. Igualmente, se acordó el establecimiento de un calendario de trabajo con los Directores Generales del Conjunto de las Comunidades Autónomas, para abordar la aprobación de las Directrices Básicas del conjunto de riesgos de Protección Civil. Asimismo, se aprobó dar impulso de la creación de la Agencia Estatal de Protección Civil y Emergencias.

El desarrollo de la Plataforma Nacional para la Reducción de Riesgos de Desastres responde a la voluntad de España de implementar los compromisos internacionales adquiridos en esta materia.

El *Marco de Acción de Sendai para la Reducción del Riesgo de Desastres 2015-2030*, adoptado por los Estados miembros de Naciones Unidas y del que España forma parte, establece como objetivos reducir el riesgo existente, evitar la generación de nuevos riesgos y fortalecer la resiliencia. La Dirección General de Protección Civil y Emergencias, como punto focal nacional e interlocutor ante la ONU, coordina e impulsa su implementación a escala estatal, tal y como refuerza la II Estrategia Nacional de Protección Civil (2024), que encomienda a dicha Dirección General consolidar una plataforma nacional multisectorial e interdisciplinar en materia de reducción de riesgo de desastres.

En este marco, la Plataforma Nacional para la Reducción del Riesgo de Desastres se configura como un foro permanente de participación y diálogo entre actores públicos, privados, técnicos, científicos, económicos y sociales, con el fin de promover la colaboración, la transparencia y la rendición de cuentas e incorporar de forma transversal y coherente la reducción del riesgo en las políticas, la planificación y los programas públicos. Su funcionamiento combinará un Pleno para las funciones principales y grupos de trabajo temáticos, integrados por las vocalías implicadas, encargados de analizar cada materia, identificar necesidades y formular propuestas concretas.

Se establece un esquema de gobernanza sencillo orientado a facilitar el trabajo técnico, compuesto por una Presidencia, ejercida por la persona titular de la Dirección General de Protección Civil y Emergencias; una Vicepresidencia, ubicada en el Ministerio para la Transición Ecológica y el Reto Demográfico; y una Secretaría, adscrita a la propia Dirección General, en su condición de punto de contacto nacional para el Marco de Sendai. A ello se suma un número variable de vocalías de carácter voluntario y representativo, procedentes de órganos directivos de la Administración General del

Estado, comunidades y ciudades autónomas interesadas, entidades locales, organismos públicos de investigación, universidades, empresas gestoras de infraestructuras críticas, organizaciones y profesionales vinculados a la reducción del riesgo de desastres, colectivos vulnerables, medios de comunicación, y asociaciones empresariales y sindicales.

Respecto a la **Red de Alerta Nacional**, se ha continuado trabajando en la mejora continua y progresiva, mediante tareas de mantenimiento evolutivo y correctivo, abordándose, entre otras, la integración de datos hidrológicos de las Comunidades Autónomas de Andalucía e Islas Baleares o la visualización de alertas de tsunamis y de los mensajes emitidos por ES-ALERT.

Por otra parte, en el marco de la mejora continua de los estándares de **seguridad industrial portuaria**, durante 2025 se han iniciado los trabajos para la revisión y actualización del Reglamento de Admisión, Manipulación y Almacenamiento de Mercancías Peligrosas en los puertos españoles. Esta iniciativa tiene como objetivo adaptar la normativa vigente, que data del año 1989, a los avances técnicos y a los nuevos requisitos internacionales, reforzando la prevención y gestión de riesgos asociados a la manipulación y almacenamiento de mercancías peligrosas. La redacción de un nuevo reglamento supone la oportunidad de llevar a cabo un análisis profundo de la situación actual, de revisar procedimientos y de adoptar criterios actualizados que permitan mejorar progresivamente las condiciones de seguridad en los puertos, en línea con las mejores prácticas y estándares internacionales.

Finalmente, cabe destacar la propuesta de un **Pacto de Estado frente a la Emergencia Climática**, iniciativa impulsada por el Gobierno de España en septiembre de 2025 para dar respuesta a los impactos, cada vez más extremos, del cambio climático. Con un espíritu de país, con ambición y vocación de perdurabilidad, se busca que el acuerdo trascienda los ciclos políticos y las diferencias territoriales, con el fin de reforzar la capacidad de adaptación, mitigación, respuesta y recuperación ante los fenómenos climáticos.

El pacto se fundamenta en el conocimiento científico, la anticipación y la cooperación institucional, con el objetivo de proteger a la ciudadanía, a la economía y a la rica biodiversidad española. Para ello, propone un marco compartido de compromisos que garantizan el interés general y el bien común, que transitan desde la gestión de agua y bosques a la prioridad de las personas más vulnerables, la disposición de las mejores condiciones de trabajo para los servicios de emergencia y el desarrollo de una nueva cultura de prevención.

Con el horizonte de construir una España más resiliente, segura y próspera en el nuevo contexto climático, la hoja de ruta propuesta para su elaboración tiene como finalidad generar consenso mediante la participación en su desarrollo de todas las administraciones, fuerzas políticas, agentes sociales y ciudadanía.

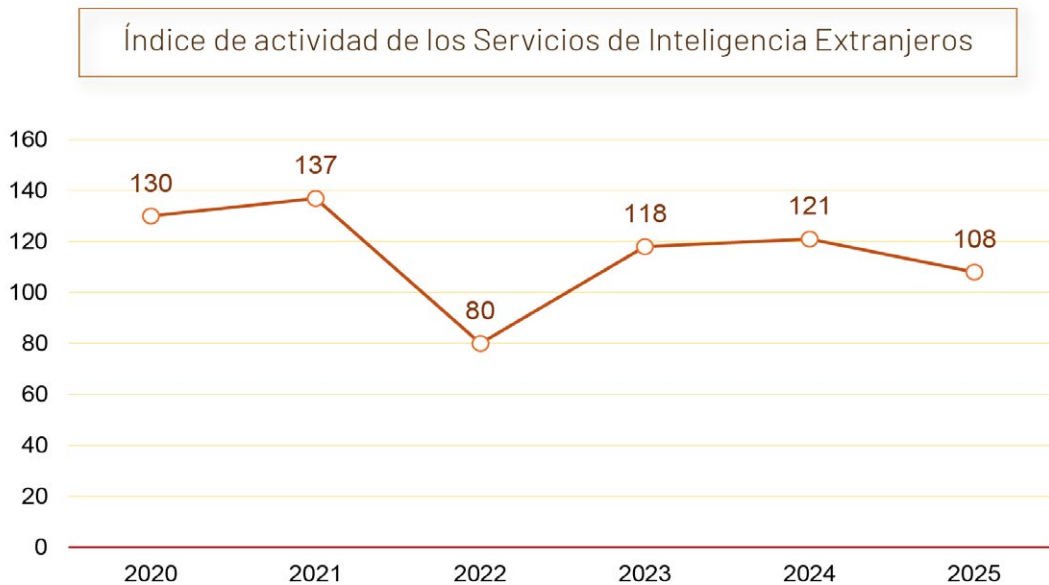
ESPIONAJE E INJERENCIAS DESDE EL EXTERIOR

- Los procesos electorales continúan siendo momentos especialmente críticos que pueden ser aprovechados para promover campañas de influencia utilizando todos los recursos del arsenal híbrido.
- Los correos de *spear-phishing* y la utilización de credenciales de acceso remoto son las técnicas más utilizadas por los delincuentes, para alcanzar y comprometer los servidores de correo electrónico de las organizaciones de su interés.
- Durante 2025 se ha continuado trabajando en la creación de una cultura de seguridad de la protección de la información clasificada, con un aumento en la formación y sesiones de concienciación, tanto en el ámbito de la administración pública como en el ámbito industrial.

ESPIONAJE E INJERENCIAS DESDE EL EXTERIOR

Actividades de los Servicios de Inteligencia extranjeros

Como puede observarse en el gráfico, hay un ligero descenso en el índice de actividad de los Servicios de Inteligencia (SI) extranjeros respecto a 2024. Esto es debido fundamentalmente a que se computan las actividades tradicionales desarrolladas por los SI extranjeros, no así las actividades de estrategias híbridas, realizadas en la denominada “zona gris”, que dificulta enormemente la identificación de sus acciones y la posterior atribución. (Figura 6.1)



Fuente: Centro Nacional de Inteligencia

Figura 6.1: Índice de actividad de los Servicios de Inteligencia Extranjeros

Los Servicios de Inteligencia (SI) rusos, especialmente GRU y SVR, han intensificado sus actividades en Europa, con un periodo de alta e intensa actividad operativa, marcada por la intensificación de actividades de naturaleza híbrida como sabotajes, desinformación y ciberataques, junto con el reclutamiento de agentes mediante redes sociales y otras tecnologías.

Además, durante 2025, se ha observado una evolución hacia el empleo sistemático de métodos híbridos, en algunos casos a través de *proxies*, con objeto de dificultar la atribución: drones que sobrevuelan instalaciones militares o fronterizas, incendios provocados en almacenes logísticos vinculados a la ayuda a Ucrania o infraestructuras críticas, ciberataques dirigidos a redes de comunicación y energía, así como intentos de injerencia electoral. Entre sus principales objetivos estarían, por un lado, probar y medir la capacidad de respuesta ante esta amenaza y, por otro lado, generar presión, desestabilización, miedo y desconfianza en las instituciones del país que sufre estos hechos. Asimismo, también se observa la instrumentalización del crimen organizado para fines geopolíticos, dificultando la detección y aumentando el riesgo para la seguridad interior.

La reacción ante estas operaciones de carácter híbrido procedentes de países hostiles se manifiesta en el reforzamiento de la actividad de Contrainteligencia en los Estados europeos y en su propósito de elevar su cooperación dentro de la OTAN y la UE.

Esta combinación de actividades de inteligencia tradicionales y acciones híbridas evidencia que la Federación de Rusia no solo busca obtener información, sino también debilitar la capacidad de reacción europea y generar inestabilidad.

En general, la actividad de Inteligencia de muchos actores continúa estando principalmente relacionada con sus intereses políticos, económicos e industriales. Por ejemplo, los intereses informativos chinos siguen centrados tanto en el ámbito de la UE como de la OTAN, en aquellas decisiones políticas y comerciales que afecten a sus intereses. Otra de las principales preocupaciones del país es mantenerse informado sobre la diáspora china y la población disidente, contraria a las políticas del Partido Comunista Chino (PCC).

Ciberespionaje

Los actores estatales y los grupos alineados con ciertos Estados, habitualmente asociados a actividades de Amenaza Persistente Avanzada (APT, por sus siglas en inglés), continúan desempeñando un papel central en el ciberespionaje contemporáneo debido a su elevada sofisticación técnica y al respaldo logístico y operativo del que disponen. Estos actores llevan a cabo campañas prolongadas y discretas dirigidas a infiltrarse en redes gubernamentales, militares y corporativas con el objetivo de obtener información sensible o acceder a activos estratégicos.

A lo largo de 2025, su actividad ha mantenido un ritmo sostenido en Europa, con especial incidencia en sectores como la Administración Pública, la Defensa, el Transporte, la Energía, la Salud y la Infraestructura Digital y las Telecomunicaciones, en un contexto geopolítico marcado por la competencia entre potencias y el uso del ciberespacio como un ámbito clave para la recopilación de inteligencia, la influencia estratégica y la proyección de poder estatal.

A nivel nacional, los organismos públicos y gubernamentales españoles continúan siendo objetivo de las campañas de ciberespionaje desarrollados por actores estatales y no estatales rusos, cuya atención se centra en la obtención de información relacionada con la posición de España en materia de política y comercio exterior.

Estos actores estatales, vinculados a los SI rusos, intentan aprovechar la interconectividad de la red de las Administraciones Públicas, utilizando como puertas de acceso los sistemas de organismos de menor tamaño, más desprotegidos y, por tanto, más fáciles de penetrar que otros sistemas de mayor interés para los atacantes.

Los correos de *spear-phishing* y la utilización de credenciales de acceso remoto continúan siendo las técnicas más utilizadas por los atacantes, cuyo objetivo es, mayoritariamente, alcanzar y comprometer los servidores de correo electrónico de las organizaciones de su interés, para después exfiltrar la información de buzones específicos.

Estrategias híbridas

El objetivo que Rusia persigue con el desarrollo de sus estrategias híbridas en Europa y en España combina distintas acciones de diversa índole (sabotajes, ciberataques, desinformación, instrumentalización de redes criminales, incidentes con drones, etc.) y está orientado, fundamentalmente, a influir en la sociedad y en los liderazgos políticos para quebrar el apoyo político, económico y militar a Ucrania.

En su confrontación con Europa, Rusia ha incrementado el empleo de herramientas híbridas y las ha adaptado a las circunstancias particulares de cada país y región, con campañas oportunistas, de bajo coste pero que persiguen gran impacto.

Momentos especialmente críticos son los procesos electorales, en los que desde el Kremlin se promueven campañas que utilizan todos los recursos del arsenal híbrido, desde ciberataques, *hacktivismo*, influencia a través de redes sociales, financiación de todo tipo de actuaciones subversivas y acercamientos a figuras políticas relevantes, a las que accede a través de *proxies*.

Protección de la Información Clasificada

Respecto a la labor de la Oficina Nacional de Seguridad (ONS), se está impulsando la automatización de parte de los procesos internos de la ONS con el objetivo de aumentar la eficacia en las tramitaciones y mejorar la experiencia del usuario.

Durante 2025, destacan las siguientes acciones dirigidas a la protección de la Información Clasificada:

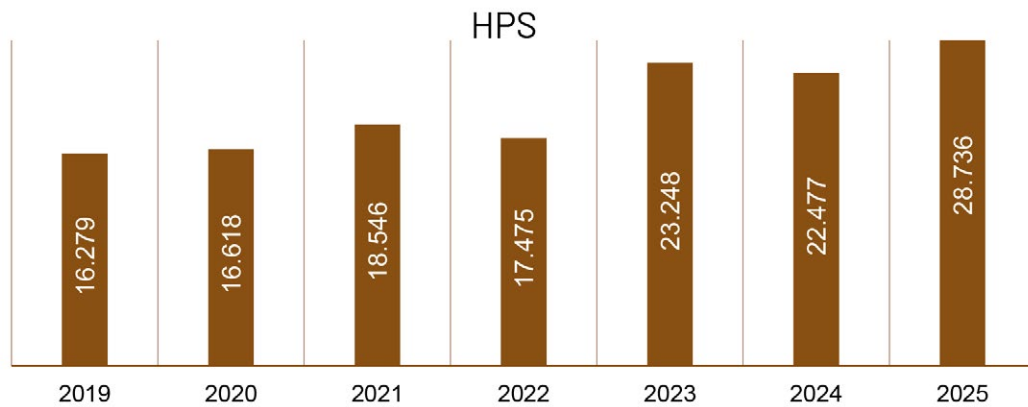
- Se han realizado las inspecciones ordinarias bienales a los subregistros principales correspondientes a 2025 observando que se mantiene un grado aceptable de protección de la información clasificada.
- Se ha consolidado el uso del Formulario de Acreditación de Seguridad (FASE) en las solicitudes de acreditación de locales para el manejo de información clasificada. Se están desarrollando nuevas funcionalidades en MARGA para aumentar la automatización de las tareas derivadas de las solicitudes que recibe la ONS.
- Se ha continuado trabajando en la creación de una cultura de seguridad de la protección de la información clasificada, con un aumento en la formación y sesiones de concienciación, tanto en el ámbito de la administración pública (Ministerio del Interior y Guardia Civil, entre otros), como en el ámbito industrial (Navantia y Santa Bárbara, entre otros).
- Se ha potenciado el número de comprobaciones de seguridad sobre el personal con HPS en vigor, para verificar que las condiciones actuales del habilitado continúan cumpliendo los requisitos para disponer de HPS.
- Se ha creado un nuevo procedimiento de análisis de riesgos de las entidades que solicitan acceso a información clasificada. Este nuevo sistema aporta mayor eficiencia y fiabilidad a las investigaciones.
- Se han cerrado varios acuerdos internacionales de protección mutua de información clasificada, tanto bilaterales (Canadá, Uruguay) como multilaterales (OCCAR).
- Se ha seguido garantizando la representación de España en los comités de seguridad de organismos multilaterales (OTAN, UE, ESA).

A 1 de enero de 2026, España contaba con 114.162 personas y 708 empresas habilitadas, en distintos grados, para acceder a Información Clasificada. Estas cifras, a 1 de enero de 2025, eran 103.561 y 634 respectivamente.

Los datos correspondientes a 2025 reflejan un marcado incremento en la concesión de HPS, por encima del 10%. Las necesidades de acceso a IC han aumentado notablemente tanto en la administración pública como en el ámbito empresarial. (Figura 6.2)

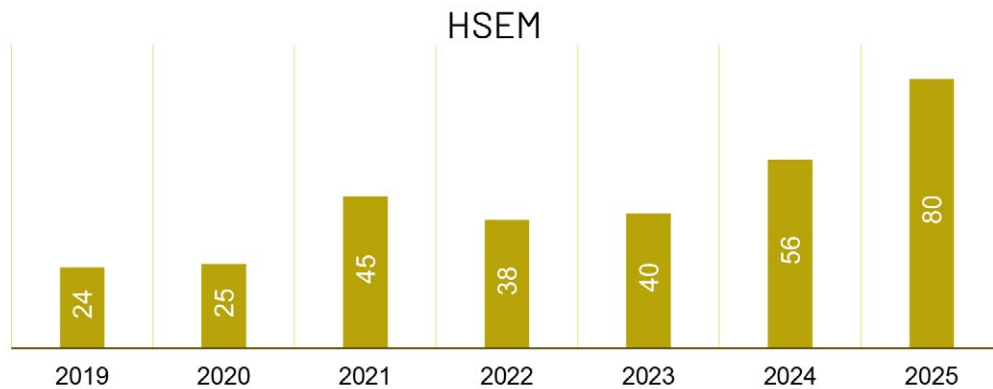
En cuanto al tejido industrial, se mantiene la tendencia alcista y, al igual que en el caso de HPS, el incremento supera el 10% con respecto al año anterior. (Figura 6.3)

Asimismo, se aprecia el cambio de tendencia en el número de sesiones de los Comités de Seguridad de los diferentes organismos multilaterales de los que España es miembro. Sin embargo, cabe señalar que esta cifra no incluye las sesiones técnicas en las que la representación de España la realiza el Centro Criptológico Nacional. (Figura 6.4)



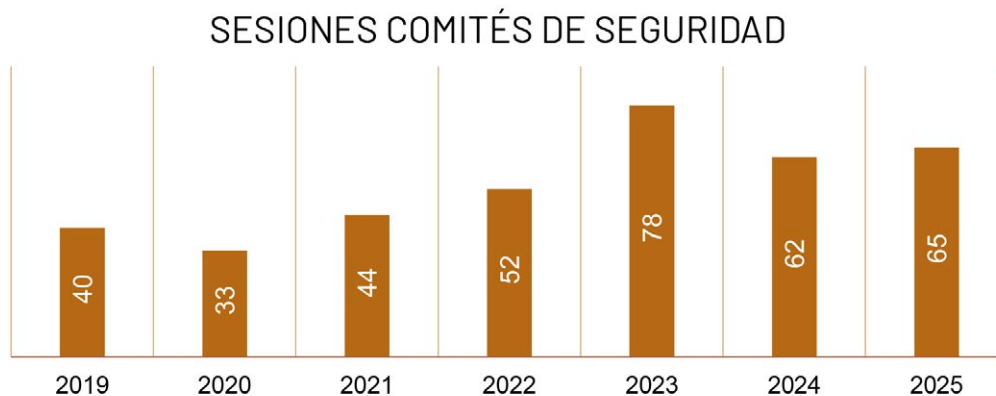
Fuente: Centro Nacional de Inteligencia

Figura 6.2: Número de Habilitaciones Personales de Seguridad concedidas



Fuente: Centro Nacional de Inteligencia

Figura 6.3: Número de Habilitaciones de Seguridad concedidas a empresas



Fuente: Centro Nacional de Inteligencia

Figura 6.4: Número de sesiones participadas en Comités de Seguridad de organismos multilaterales y programas clasificados. 2019-2025

Finalmente, señalar que una parte del volumen de solicitudes de HPS y, en especial, de las HSEM está directamente relacionada con el gasto público en los ámbitos de Defensa y Seguridad, por lo que se prevé que se mantenga la tendencia positiva en los próximos años. Ello, al igual que en años anteriores, pone de manifiesto la importancia y la necesidad de disponer de estructuras de protección de Información Clasificada en la administración pública y en el tejido empresarial.

CAMPAÑAS DE DESINFORMACIÓN

- Las campañas de desinformación se consolidan como un vector destacado de inestabilidad así como un instrumento híbrido que atenta contra la cohesión social y la legitimidad institucional, impactando también en la capacidad operativa de las Fuerzas Armadas.
- La Inteligencia Artificial ha dejado de ser únicamente una herramienta de producción para convertirse en un soporte integral de campañas hostiles a nivel estratégico, táctico y operativo.
- En 2025 (Orden PJC/248/2025, de 13 de marzo) el Consejo de Seguridad Nacional aprobó el procedimiento para elaborar la Estrategia Nacional contra las Campañas de Desinformación, abordando el fenómeno como una amenaza de alta capacidad disruptiva que requiere la colaboración de todos actores relevantes de la sociedad.

CAMPAÑAS DE DESINFORMACIÓN

En 2025 las campañas de desinformación se han consolidado como un vector destacado de inestabilidad. Desde la perspectiva de las relaciones internacionales, las campañas de desinformación proceden principalmente de actores estatales y no estatales y redes transnacionales que buscan influir en procesos políticos, erosionar la confianza en las instituciones, moldear la opinión pública y debilitar la cooperación internacional.

La desinformación aprovecha tensiones estratégicas como la guerra de Ucrania, con narrativas manipuladas sobre sanciones, suministros energéticos o el apoyo occidental, y los conflictos en Oriente Medio y el Sahel, donde han circulado falsos relatos sobre la presencia de actores extranjeros o el control de recursos. También se han explotado debates sensibles sobre flujos migratorios irregulares, por ejemplo, difundiendo rumores de “oleadas inminentes” para fomentar polarización social, y se han reactivado campañas ligadas a la salud pública, desde teorías conspirativas sobre vacunas hasta mensajes manipulados sobre brotes epidémicos, erosionando la confianza institucional y dificultando la respuesta de gobiernos y organismos sanitarios.

Dinámicas de actores estatales y tensiones estratégicas

La Federación de Rusia continúa desarrollando campañas desinformativas, especialmente de naturaleza oportunista, contra España, Europa y regiones de su interés en África e Iberoamérica. Paralelamente, ha expandido sus campañas de influencia en África, consolidando alianzas locales y difundiendo narrativas que cuestionan la legitimidad occidental para erosionar su influencia en regiones clave del continente africano.

Una parte significativa de los intereses del Kremlin se han centrado en influir en las élites y liderazgos políticos de los Estados, para reducir el apoyo que se presta a Ucrania, y generar desconfianza en las instituciones democráticas de países occidentales y difundir posturas prorrusas.

Asimismo, ha potenciado el uso de *proxies* con fines desinformativos para lograr una penetración más orgánica de sus narrativas con mayores posibilidades de negar de manera plausible su vinculación con estrategias híbridas. Asimismo, el Kremlin ha explorado diferentes entornos, hasta la fecha con menor incidencia, como *TikTok* o *Discord*, para la ejecución de estas estrategias.

La Inteligencia Artificial (IA) ha permitido a Rusia ampliar el volumen de desinformación. La facilidad de traducción, elaboración y difusión de contenidos de manera masiva ha potenciado la capacidad de penetración y de saturación de la “infoesfera” occidental. Asimismo, la sofisticación de la herramienta dificulta contrastar la veracidad de la información.

Se aprecia una reducción de la cobertura mediática en China en relación con la guerra en Ucrania. La escasa cobertura mediática ha mostrado una visión favorable a Rusia.

Las narrativas en los medios de comunicación social (MCS) oficiales chinos, así como las utilizadas por la RPC, se han centrado en la región del Sahel, en torno a la “inestabilidad y extorsión” que provocan los países occidentales y su política “neocolonial”.

Narrativas de polarización y explotación de crisis

En este ámbito, durante 2025, se destacan las siguientes tendencias narrativas:

- **Narrativas anti-europeas e identitarias.** Se detecta una intensificación de mensajes hostiles anti-europeos focalizados en el colectivo LGBTQ+ y en la promoción de discursos ultraconservadores, una tendencia especialmente notoria en Europa del Este durante los ciclos electorales. Estas campañas buscan polarizar a la sociedad vinculando la ampliación de derechos con supuestas imposiciones externas que amenazan la identidad nacional.
- **Gestión de emergencias y catástrofes.** Los vacíos informativos en las crisis son explotados sistemáticamente. La experiencia en crisis de los últimos años demuestra que el ecosistema pro-Kremlin actúa de manera oportunista, activando campañas de desinformación con el objetivo de ahondar en el malestar, agravar el descontento social y atacar a las instituciones del Estado, en ocasiones, con menciones concretas a la Monarquía o las FCSE.
- Una narrativa utilizada recurrentemente es la de demostrar que los líderes políticos no socorren a sus ciudadanos ante situaciones de emergencia, mientras desvían recursos a Ucrania para su enfrentamiento con Rusia.
- El carácter general, los vacíos informativos se explotan en tres fases: (i) publicación rápida de hipótesis especulativas (sanciones, sabotaje, guerra híbrida); (ii) amplificación en plataformas; (iii) anclaje mediante piezas audiovisuales de apariencia “testimonial”. La confluencia de estos elementos llena el vacío informativo generado, explotándolo para erosionar la confianza en instituciones y servicios de emergencia, en particular.
- **Migración y seguridad.** Se explotan tensiones intercomunitarias y flujos migratorios irregulares en la región MENA y Sahel. Destaca la difusión de *deepfakes* en Polonia, mostrando falsos solicitantes de asilo, coincidiendo con las elecciones presidenciales. Se consolidan polos de fricción geográficos y simbólicos (Sahel, Ceuta y Melilla, fronteras exteriores de la UE) donde la narrativa sobre migración se entrelaza con la inseguridad y se instrumentalizan episodios de conflictos sociales para proyectar un deterioro de la seguridad pública. La difusión en idiomas locales y el uso de material audiovisual fabricado incrementan su poder de persuasión.

El suceso en Torre-Pacheco (julio 2025) evidenció la capacidad de la desinformación para traspasar dimensiones. Se registró un aumento de actividad digital sobre inmigración ilegal donde la intensidad narrativa precedió a la escalada de violencia física, estableciendo una correlación directa entre la saturación cognitiva en redes y la materialización de riesgos para la seguridad pública.

Impacto en la Defensa Nacional

La desinformación se consolida como un instrumento híbrido que atenta contra la cohesión social, la legitimidad institucional y la capacidad operativa de las FAS. Se categorizan cinco amenazas clave: negación de la amenaza, desconfianza en la capacidad militar, ilegitimidad de misiones exteriores, percepción de debilidad y radicalización.

En misiones exteriores, las campañas atacan la legitimidad del mandato, cuestionan la capacidad operativa y buscan fracturar el apoyo político-social. La respuesta exige comunicación estratégica continua, análisis de narrativas hostiles en tiempo casi real y coordinación con marcos OTAN/UE que aportan indicadores, alertas y estándares de capacitación frente a contenidos sintéticos.

Las Fuerzas Armadas continúan desarrollando su capacidad para la identificación, análisis y respuesta coordinada frente a campañas de desinformación que puedan afectar, entre otros, a sus operaciones en curso.

Entre estos mecanismos de respuesta a la amenaza, son relevantes la cooperación con el Departamento de Seguridad Nacional, la coordinación con el Centro de Inteligencia de las Fuerzas Armadas en el análisis de operaciones de influencia hostiles, y la integración en marcos europeos y OTAN, que proporcionan indicadores y alertas.

Tendencias evolutivas

Más allá de las herramientas tecnológicas y las narrativas temáticas, se observan cambios cualitativos en los objetivos estratégicos de las campañas:

- Injerencia en Fuerzas y Cuerpos de Seguridad y Fuerzas Armadas. Se detectan estrategias hacia la influencia dentro de estos colectivos. Actores vinculados al extremismo, antieuropeísmo y afinidad con Rusia buscan erosionar la neutralidad institucional aprovechando narrativas sobre el “declive moral” de la sociedad europea y la inseguridad, tratando de alinear a los servidores públicos con tesis desestabilizadoras.
- Fabricación de “consensos”. El objetivo último de las nuevas herramientas de automatización trasciende la mera difusión de ruido; se persigue la creación de una “realidad epistémica fragmentada”. Se busca fabricar un falso consenso social mediante la interacción masiva de agentes autónomos, legitimando discursos marginales para fracturar la percepción de la realidad compartida.
- Desestabilización económica. La desinformación amplía su espectro operativo, convirtiéndose en una herramienta para cometer fraudes a mayor escala o incluso manipular sistemas económicos.

La Inteligencia Artificial como agente disruptivo

La Inteligencia Artificial (IA) se ha consolidado en 2025 no solo como herramienta de producción, sino como soporte integral de campañas hostiles en tres niveles:

1. Planificación estratégica, permitiendo el análisis masivo de datos para mapear el “espacio cognitivo” y detectar vulnerabilidades sociales.

2. Planificación táctica, que facilita la generación automatizada de contenidos (texto, imagen, vídeo) y selección algorítmica de canales óptimos.
3. Planificación operativa, donde se adscribe la coordinación de enjambres de *bots/agentes* y ajuste de estrategias en tiempo real según la reacción de la audiencia.

La aparición de “enjambres maliciosos de IA” supone el uso de agentes autónomos y adaptativos que superan a los *bots* tradicionales, capaces de sostener narrativas coherentes y mimetizar el comportamiento humano, dificultando su detección. Asimismo, el uso de *deepvoices* (voces sintéticas clonadas) y *deepfakes* aumenta la eficacia del engaño.

Inversión en I+D+i

La inversión en I+D+i es fundamental para combatir las campañas de desinformación, que han crecido en sofisticación y alcance. Gracias a estos esfuerzos, se desarrollan herramientas avanzadas capaces de detectar patrones anómalos, mejorar la alerta temprana y prevenir acciones FIMI hostiles. Esta actividad es clave ante el desafío que suponen las tecnologías avanzadas usadas tanto para crear campañas de desinformación como para combatir las.

La Unión Europea está consolidando un marco integral para la prevención y lucha contra la desinformación, combinando esfuerzos regulatorios, tecnológicos y educativos.

Entre las iniciativas de la UE destaca el Observatorio Europeo de Medios Digitales (EDMO, por sus siglas en inglés), que reúne verificadores (*fact-checkers*), investigadores, expertos en alfabetización mediática y medios para analizar y contrarrestar desinformación, así como sus 15 centros regionales (ej. *FACT Hub* especializado en combatir campañas de desinformación prorrusa en Ucrania y Moldavia). El Servicio Europeo de Acción Exterior (SEAE) ha intensificado su trabajo sobre lo que denomina “Injerencia y Manipulación Extranjera de la Información Extranjera” (FIMI).

El núcleo regulatorio más relevante es la Ley de Servicios Digitales (DSA, por sus siglas en inglés), que desde 2024 es de aplicación efectiva en la UE. Esta norma obliga a las grandes plataformas digitales y motores de búsqueda a asumir responsabilidades concretas para prevenir la difusión de contenidos ilegales o dañinos, incluida la desinformación, mediante obligaciones de moderación, transparencia y mecanismos de alerta de contenidos. En febrero de 2025, la UE decidió integrar formalmente el Código de Conducta sobre Desinformación, hasta entonces voluntario, dentro del marco de la DSA. Esto convierte muchas de sus recomendaciones en un estándar de referencia al evaluar el cumplimiento de plataformas.

El Programa Marco de I+D+i de la UE, Horizonte Europa, y concretamente el Clúster 3 “Seguridad civil para la sociedad”, define una serie de líneas prioritarias a abordar a través de proyectos, para hacer frente a los riesgos y amenazas como las campañas de desinformación, el discurso del odio y las amenazas híbridas, dentro de su epígrafe de tecnologías para la lucha contra el crimen y el terrorismo, incluyendo cibercrimen y ciberterrorismo sobre las infraestructuras críticas de los países europeos.

Asimismo, el CSIC está desarrollando capacidades de detección temprana de redes de *bots* coordinados, por constituir una amenaza híbrida creciente. Adicionalmente, el Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad, colabora en el desarrollo de herramientas de monitorización mediante iniciativas público-privadas enfocadas en la detección temprana de campañas de desinformación.

En este contexto, cabe mencionar lo siguiente:

- La Agencia Estatal de Investigación ha financiado 15 proyectos por más de 2,1 millones de euros. Se priorizan líneas del Clúster 3 del Programa Marco Horizonte Europa (“Seguridad civil para la sociedad”) para el periodo 2025-2027.
- En el marco del Plan de Impulso de los Espacios de Datos Sectoriales, coordinado por la SEDIA, se están financiando varios proyectos que abordan la lucha contra la desinformación y que tienen una orientación bien definida en cuanto a la verificación de contenidos o la detección automatizada de comportamiento manipulativo. Se identifican los siguientes proyectos financiados:
 - ConflIA: Espacio de datos colaborativo para la verificación de contenidos digitales.
 - EPDATA 2.0: Espacio inteligente de datos abiertos para la generación de información.
 - Proyecto “COD”: Plataforma de análisis y distribución programática de contenidos en el ecosistema de información digital (*content on demand*).
- El proyecto ECLIPSE, financiado bajo el paraguas del programa *Horizonte*, destinado a prevenir y combatir el discurso de odio y la desinformación con gran participación de entidades españolas.
- FERMI (*Fake News Risk Mitigator*). Proyecto también financiado bajo Horizonte Europa que cuenta con la participación de las Fuerzas y Cuerpos de Seguridad del Estado. Incluye la identificación de cuentas falsas, *bots* y contenidos sintéticos generados por IA, afrontando los riesgos emergentes de campañas híbridas que amenazan la seguridad digital y de información en la Unión Europea.
- Detección contenidos sintéticos. Desarrollo por parte de la AESIA (Agencia Española de Supervisión de la Inteligencia Artificial) de una tecnología pública, prevista para 2026, que permitirá al ciudadano identificar contenido generado por IA (audio, vídeo, imagen).

El fortalecimiento del enfoque lingüístico en la lucha contra la desinformación se ha convertido en una prioridad para España, ya que gran parte de los contenidos manipulados que circulan en el espacio digital hispanohablante se adaptan específicamente a códigos culturales, expresiones y marcos narrativos propios. Una encuesta difundida por RTVE en 2025 indica que aproximadamente un 40% de los españoles reconoce no saber distinguir un bulo de una información veraz. Esto exige avanzar en la capacitación para la detección de narrativas construidas para explotar rasgos lingüísticos del español, como la carga emocional de ciertos términos o el uso de etiquetas polarizantes. Como parte de este refuerzo del enfoque lingüístico en la lucha contra la desinformación, España ha impulsado la elaboración de un estudio comparativo sobre los flujos de desinformación en los principales idiomas globales.

Desarrollo normativo-estratégico

España avanza en el desarrollo de una Estrategia Nacional contra las Campañas de Desinformación. En 2025 (Orden PJC/248/2025, de 13 de marzo) se aprobó el procedimiento para elaborar la Estrategia Nacional contra las Campañas de Desinformación, abordando el fenómeno como una amenaza de alta capacidad disruptiva que requiere la colaboración de todos actores relevantes de la sociedad.

La Comisión Permanente contra la Desinformación es el organismo responsable de la elaboración de la Estrategia, dirigiendo el proceso a través de la constitución de un grupo de trabajo técnico.

Concretamente, en relación con la seguridad en servicios digitales, el 24 de enero de 2024, en cumplimiento de su obligación establecida en el artículo 49.3 del Reglamento de Servicios Digitales (DSA), el Ministerio para la Transformación Digital y de la Función Pública designó a la Comisión Nacional de los Mercados y la Competencia (CNMC) como coordinador de servicios digitales nacional. Asimismo, la CNMC forma parte de la Junta Europea de Servicios Digitales.

Las obligaciones relativas a desinformación que contiene el DSA, y que van a ser determinantes del papel del coordinador de servicios digitales, se pueden clasificar en dos grupos:

- i. Obligaciones específicas dirigidas a las VLOPS y VLOPSE respecto a los riesgos sistémicos derivados del diseño y funcionamiento de su servicio y de los sistemas relacionados con este, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios. La supervisión de estas obligaciones del Reglamento es competencia exclusiva de la Comisión Europea, sin perjuicio de las capacidades de la CNMC para, en su caso, dar traslado al coordinador de servicios digitales del estado miembro donde el prestador esté establecido, y a la Comisión Europea, como consecuencia de la obligación de asistencia mutua, toda vez que, actualmente, no hay ninguna VLOPSE establecida en España.
- ii. Obligaciones contra prácticas inapropiadas que pueden ser relevantes en materia de desinformación, que son obligatorias para los VLOPS y VLOPSE, pero también, ciertas de ellas afectan a otro tipo de intermediarios.

La CNMC, como coordinador de servicios digitales de España, tiene competencias de supervisión respecto a los prestadores de servicios intermediarios establecidos en España y respecto a aquellos prestadores sin establecimiento en la UE que nombren representante legal en España.

Dentro de las funciones de los coordinadores destaca también la de certificación en cada Estado miembro de los alertadores fiables y de los organismos de resolución extrajudicial de conflictos.

Por último, en noviembre de 2025 se presentó el “Escudo Europeo de la Democracia”, que se inscribe en el mandato político general fijado por el Consejo Europeo en sus Conclusiones de junio de 2024 sobre resiliencia frente a amenazas híbridas y desinformación. Al mismo tiempo, constituye una pieza estratégica para articular la respuesta de la Unión a Injerencia y Manipulación Extranjera de la Información (FIMI, *Foreign Information Manipulation & Interference*) que además organiza y refuerza todo un ecosistema de normas ya vigentes, como la DSA, el Reglamento sobre Inteligencia Artificial (AI Act) o el Reglamento sobre la Libertad de los Medios de Comunicación (EMFA).

Cooperación internacional y estandarización

España ha reforzado sus acuerdos de cooperación internacional en materia de lucha contra la desinformación, especialmente con países iberoamericanos, en el marco de la Cumbre de Madrid, mediante comunicados especiales, una declaración final conjunta, la creación de una red de verificadores iberoamericanos y un estudio sobre la posible armonización regulatoria en la región. En España, el MAUEC acogió en 2025 una conferencia titulada “El entorno de la información en español como campo de batalla de la desinformación”, organizada en el marco del Foro contra las campañas de desinformación. Paralelamente, se han identificado posibles socios en otras regiones, con especial atención a Canadá, para ampliar la cooperación global. Asimismo, se ha analizado el impacto del giro político de Estados Unidos, Argentina, Paraguay y otros actores en este ámbito, incluyendo las consecuencias del cierre de USAID en proyectos de verificación y alfabetización mediática.

Tanto en la UE como en la OTAN, España defiende un refuerzo de la aproximación integral al concepto de seguridad, incluyendo ámbitos como la desinformación, parte esencial de las acciones híbridas contra la seguridad euroatlántica y europea.

En noviembre de 2025, con ocasión de la visita del presidente Zelensky a España, se firmó un memorando de entendimiento específico sobre cooperación en materia de desinformación y manipulación informativa entre el MAUEC y el MAE de Ucrania, orientado a reforzar la colaboración bilateral frente a campañas de desinformación relacionadas con la guerra y la seguridad.

Por otra parte, se participa activamente en foros de la UE y la OTAN. En este sentido, se destaca la participación del Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad, en el Seminario Conjunto con el IHEMI (Instituto de Altos Estudios del Ministerio del Interior) en París.

Asimismo, se ha participado en el curso “*Advanced FIMI Analysis*” realizado en octubre de 2025 en Bruselas, donde se abordó el concepto de FIMI, cómo desarrollar análisis conjuntos, metodología y las Tácticas, Técnicas y Procedimientos (TTP) de diferentes actores y análisis sobre posibles objetivos estratégicos perseguidos.

Finalmente, en el marco DISARM sigue siendo la metodología de referencia para analizar indicadores técnicos de acciones FIMI, con el objetivo de establecer un modelo común de trabajo y facilitar el intercambio de información.

Alfabetización mediática y sensibilización

Entre las medidas desarrolladas para fortalecer la resiliencia social, destacan:

- En cuanto a formación, la Realización de MOOCs (*Massive Open Online Courses* o Cursos Masivos Abiertos en Línea) para educadores, como “Educar en seguridad y privacidad digital”. También se fomentan talleres de verificación impulsados por la Dirección General del Dato mediante el proyecto *ImpulsaData* para fomentar la *data literacy* (alfabetización en datos).
- El Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional, del que se deriva la publicación de trabajos destinados a promover y elaborar estudios e iniciativas que permiten, directa o indirectamente, aumentar el conocimiento y la sensibilización de la sociedad acerca de los riesgos y amenazas generados por las campañas de desinformación susceptibles de comprometer la Seguridad Nacional.
- En 2025 el lema del Día de las Bibliotecas 2025 ha sido “Bibliotecas contra la censura y la desinformación”, y ha acogido una mesa redonda de mismo título y un *webinar* sobre “Cómo combatir la desinformación desde las bibliotecas”. Asimismo, se ha puesto a disposición de las bibliotecas, un juego de mesa “Noticia oculta”, destinado a usuarios de entre 14 y 18 años.
- Asimismo, el XII Congreso Nacional de Bibliotecas Públicas, celebrado en Granada en noviembre de 2025, acogió varias actividades relacionadas con la lucha contra la desinformación y la alfabetización mediática.

VULNERABILIDAD DEL CIBERESPACIO

- La ampliación de la superficie de exposición y la convergencia de actores marca una creciente complejidad del panorama de ciberamenazas.
- La aceleración tecnológica de 2025 ha precipitado un cambio de escala y de naturaleza en el ámbito de la ciberseguridad. Así, Inteligencia Artificial, computación cuántica, 5G, IoT y cloud actúan de forma simultánea como motores de innovación y como catalizadores de nuevos modelos de ataque.
- España cuenta con una extensa y avanzada red de alerta temprana y de detección lo cual se ve reflejado en una mayor visibilidad sobre los ciberataques y una mayor capacidad para poder actuar sobre ellos.

VULNERABILIDAD DEL CIBERESPACIO

El panorama de ciberamenazas en 2025 muestra una creciente complejidad marcada por la convergencia entre actores estatales, motivaciones criminales y extremistas y una mayor sofisticación de las técnicas ofensivas.

Además, la implantación digital en España lleva a un crecimiento elevado de la superficie de exposición impulsado por la digitalización masiva acompañado de un uso cada vez más sofisticado de la tecnología, de la adopción de servicios en la nube, el consumo de contenidos digitales y el uso extendido de la inteligencia artificial.

España cuenta además con una extensa red de alerta temprana y de detección lo cual se ve reflejado en una mayor visibilidad sobre los ciberataques y una mayor capacidad para poder actuar sobre ellos.

Entre las tendencias predominantes se mantienen, pero con un mayor grado de complejidad, los ataques de denegación de servicios distribuidos (DDoS), el *phishing* y las brechas de datos que generan tanto impacto operacional como reputacional.

A lo largo del año 2025 se ha observado una volumetría elevada de DDoS contra Administraciones Públicas, operadores y servicios esenciales, con repuntes vinculados a grupos *hacktivistas* en contra de Ucrania y países que le prestan apoyo. Pese al volumen, la efectividad de las medidas de detección y de mitigación desplegadas ha permitido disminuir el impacto. En concreto, el 59% de los ciberataques obedecen a una detección proactiva de los sistemas de protección (72.123), mientras que el resto (el 41%, que equivale a 50.100 ciberataques en 2025) se corresponde con notificaciones recibidas por los distintos canales de INCIBE.

En paralelo se ha observado un aumento masivo del *phishing* contra la ciudadanía y empleados públicos, en los que la irrupción de la IA generativa ocupa también un lugar protagonista al facilitar campañas extremadamente convincentes, sin errores gramaticales, adaptadas a perfiles y ámbitos organizativos, y posibilitando *deepfakes* altamente creíbles. El resultado es una dificultad mayor de detección temprana por medios tradicionales y la necesidad de reforzar esta capacidad de detección, así como la concienciación y las buenas prácticas del usuario final.

Los datos personales, especialmente credenciales de acceso, continúan siendo altamente codiciados por la ciberdelincuencia; aunque muchas brechas detectadas resultan obsoletas, la tendencia se mantiene al alza, con un repunte notable en marzo, en gran medida por malas prácticas del usuario. El objetivo final suele ser monetizar el acceso y facilitar intrusiones posteriores.

El *ransomware* se consolida como principal amenaza para empresas y administraciones públicas, con modelos de negocio maduros (plataformas de afiliación, extorsión múltiple) y tácticas avanzadas, incluidas infraestructuras flexibles, células descentralizadas y técnicas *malwarefree*. Su objetivo ya no es solo el beneficio económico, sino también la exfiltración estratégica de datos.

Además, se intensifican los ataques a la cadena de suministro digital, que permiten comprometer a decenas o cientos de organizaciones a partir de un único proveedor vulnerado. Todo ello se ve facilitado por un ecosistema criminal profesionalizado, que adopta modelos *crimeaservice* para la adquisición de herramientas y servicios ilícitos, y por el aumento del *hacktivismo*, ahora más interconectado con intereses estatales y con capacidad para encadenar campañas cuyo impacto trasciende lo simbólico.

En relación con los actores patrocinados por Estados, en especial los que realizan actividades de tipo Amenazas Persistentes Avanzadas (APT), se ha producido un incremento muy elevado de incidentes respecto al año anterior (cerca al 300%) así como un mayor número de acciones coordinadas entre actores en algunas de las campañas. Este aumento también es debido al aumento de recursos dedicados a la detección temprana y análisis de esta actividad. De hecho, parte importante de estos ciberataques se han detectado en fase inicial y han tenido, en estos casos, impacto limitado. Sus objetivos principales son los tradicionales (Gobierno y empresas privadas del sector tecnológico y de defensa).

Las campañas rusas de ciberespionaje son las más numerosas y frecuentes. Durante los últimos años, la Federación de Rusia ha perfeccionado los ataques con APT, en especial los basados en correos maliciosos (*spear-phishing*) como vector de entrada. Para ello, utilizan cada vez más técnicas de Inteligencia Artificial que contribuyen a redactar los mensajes, así como asuntos y “ganchos” centrados en temas de actualidad para engañar a las víctimas. Para el éxito de estas misiones se ha detectado que diferentes APT rusas tradicionalmente enfrentadas desarrollan en la actualidad campañas conjuntas (coordinación entre APT).

Asimismo, se han incrementado las operaciones de desinformación, propaganda y operaciones psicológicas rusas contra la población europea y española, así como contra los procesos electorales, dirigidas a influir en las ideas y el ánimo de los ciudadanos. Para ello, además de las APT, se sirven de los grupos *hacktivistas*, como NoName057(16) y los cibercriminales. Sus campañas de ataques de DDoS (más de 300) han estado relacionadas con sucesos asociados a la guerra en Ucrania.

En el ámbito de las Administraciones Públicas, el impacto es creciente lo que tensiona especialmente a la administración local por su menor disponibilidad de recursos. También Gobierno y personal público figuran de forma recurrente entre los objetivos de campañas de *phishing*, intrusiones y desinformación.

En 2025, las infraestructuras críticas han enfrentado a un entorno de riesgo cada vez más transversal y complejo, afectando por igual al sector público y al privado. La sofisticación de las ciberamenazas, la ampliación de su impacto operativo y la evolución del ecosistema criminal han configurado un escenario donde cualquier vulnerabilidad puede ser explotada, incluso cuando los atacantes no buscan necesariamente objetivos estratégicos, sino oportunidades detectadas en accesos o herramientas comprometidas.

Este panorama está marcado por la convergencia de amenazas híbridas que combinan *ransomware*, extorsión, exfiltración de datos y acciones de sabotaje. La fragmentación del ecosistema criminal, caracterizada por grupos más pequeños, descentralizados y altamente ágiles, incrementa tanto la frecuencia como la gravedad de los incidentes. Estos actores emplean técnicas sin *malware* convencional, herramientas de automatización avanzada e ingeniería social impulsada por inteligencia artificial, lo que reduce los tiempos necesarios para comprometer un sistema y dificulta enormemente la detección temprana de sus operaciones.

Los sectores estratégicos más expuestos incluyen energía, transporte, telecomunicaciones y, con un riesgo especialmente relevante, el del agua. En este último, se han identificado intrusiones dirigidas específicamente a manipular parámetros en Sistemas de Control Industrial (ICS), lo que demuestra la creciente capacidad de los atacantes para influir de forma directa en procesos operativos esenciales.

Frente a este escenario en mayo de 2025 se aprobó por Acuerdo de Ministros la asignación de 1.157 millones de euros para actuaciones complementarias al Plan Nacional de Ciberseguridad de 2022 para reforzar la resiliencia y la respuesta institucional:

El conjunto de actuaciones previsto en el Acuerdo persigue mejorar las capacidades de ciberseguridad y ciberdefensa de amplio espectro, desde la prevención, detección y protección hasta la respuesta y la recuperación, así como el refuerzo de la ciberresiliencia, potenciando la integración de tecnologías avanzadas y la alerta temprana.

El Acuerdo contemplaba la participación de diferentes órganos y organismos relacionados con la ciberseguridad, siendo la Agencia Estatal de Administración Digital la encargada de coordinar e impulsar el cumplimiento del plan.

Estadísticas de ciberincidentes y cibercriminalidad

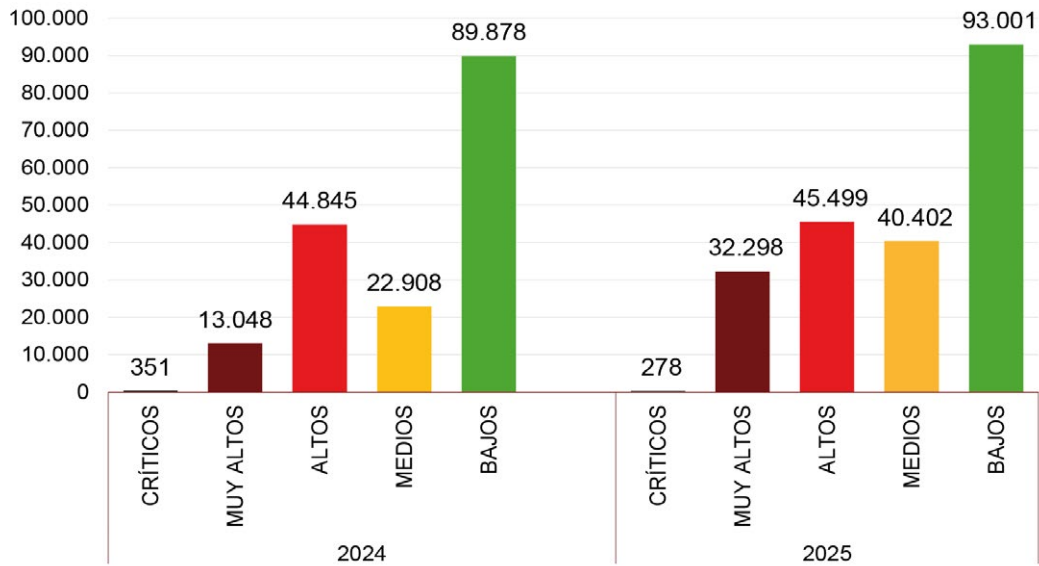
En 2025, el Equipo de respuesta del Centro Criptológico nacional (CCN-CERT) ha gestionado un total de 211.478 incidentes; el Equipo de respuesta del Instituto Nacional de Ciberseguridad de España (INCIBE-CERT) 122.223 y el Equipo de Respuesta del Ministerio de Defensa (ESPDEF-CERT) 231.

Incidentes gestionados por CCN-CERT en el sector público (Figuras 8.1 a 8.4)



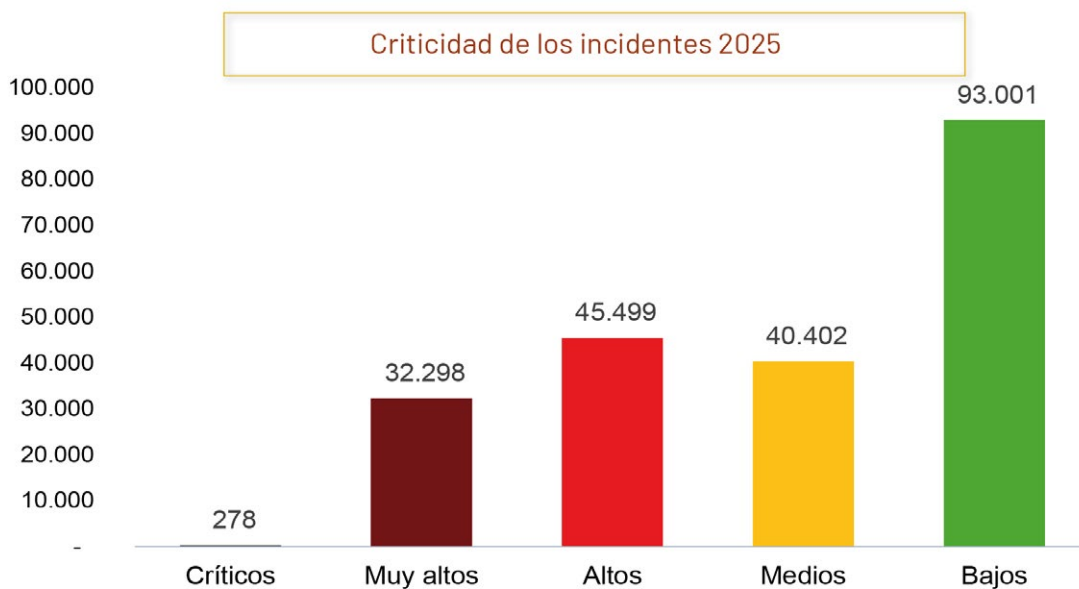
Fuente: Centro Criptológico Nacional

Figura 8.1: Incidentes gestionados por el CCN-CERT



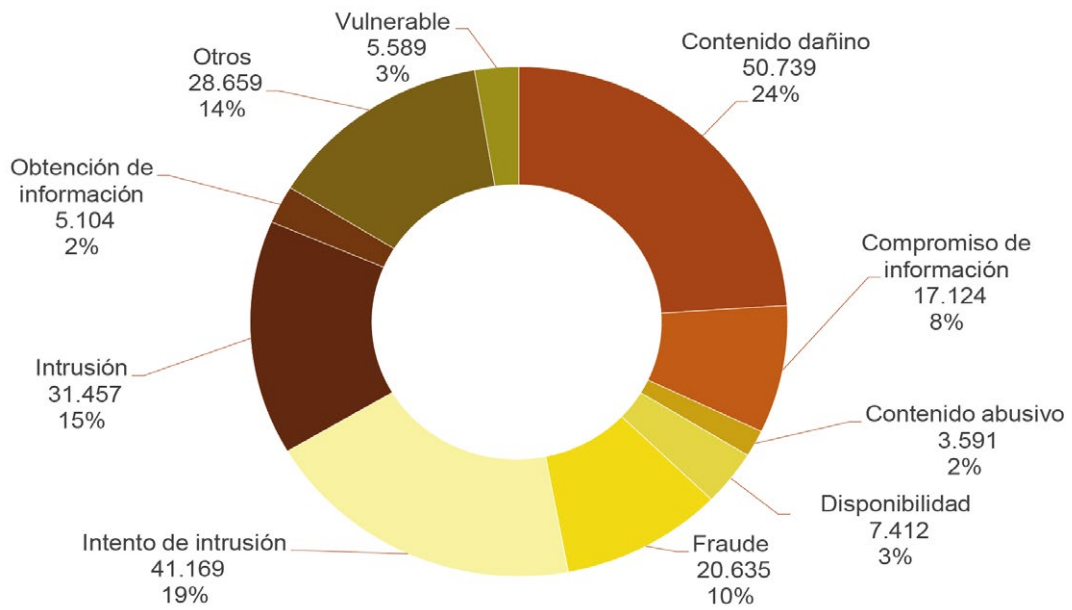
Fuente: Centro Criptológico Nacional

Figura 8.2: Comparativa del número total de incidentes por peligrosidad 2024-2025



Fuente: Centro Criptológico Nacional

Figura 8.3: Clasificación de los incidentes gestionados por el CCN-CERT



Fuente: Centro Criptológico Nacional

Figura 8.4: Tipología de incidentes gestionados en 2025

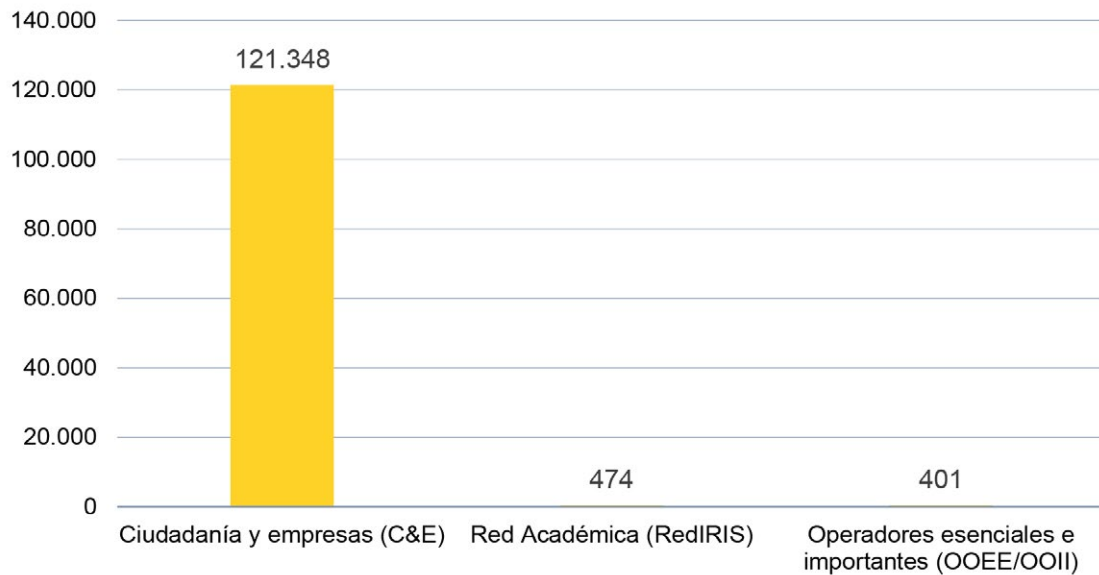
Incidentes gestionados por INCIBE en ciudadanos, sector privado y red académica

(Figuras 8.5 a 8.7)

Figura 8.5: Número de ciberincidentes por público objetivo gestionado por INCIBE en 2025

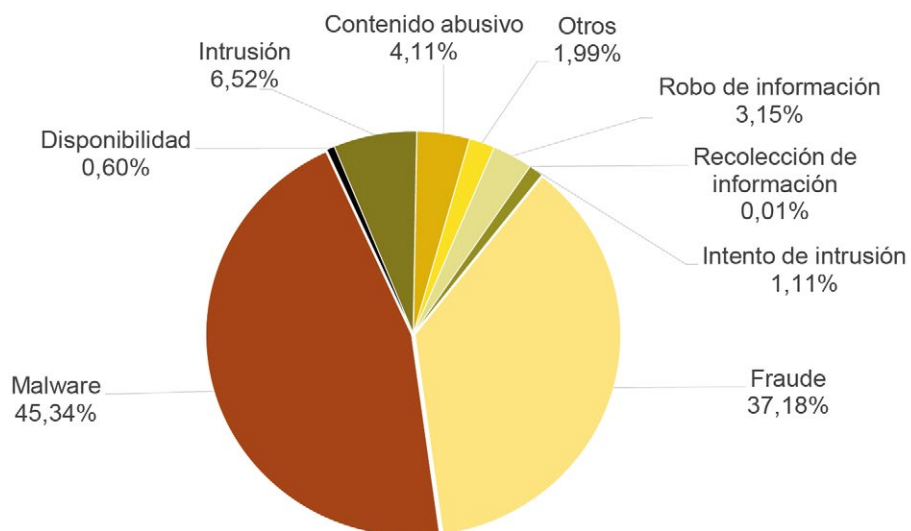
Público objetivo	TOTAL
Ciudadanos y empresas (C&E)	121.348
Red Académica (RedIRIS)	474
Operadores esenciales e importantes (OOEE/OOII)	401
TOTAL	122.223

Fuente: INCIBE



Fuente: INCIBE

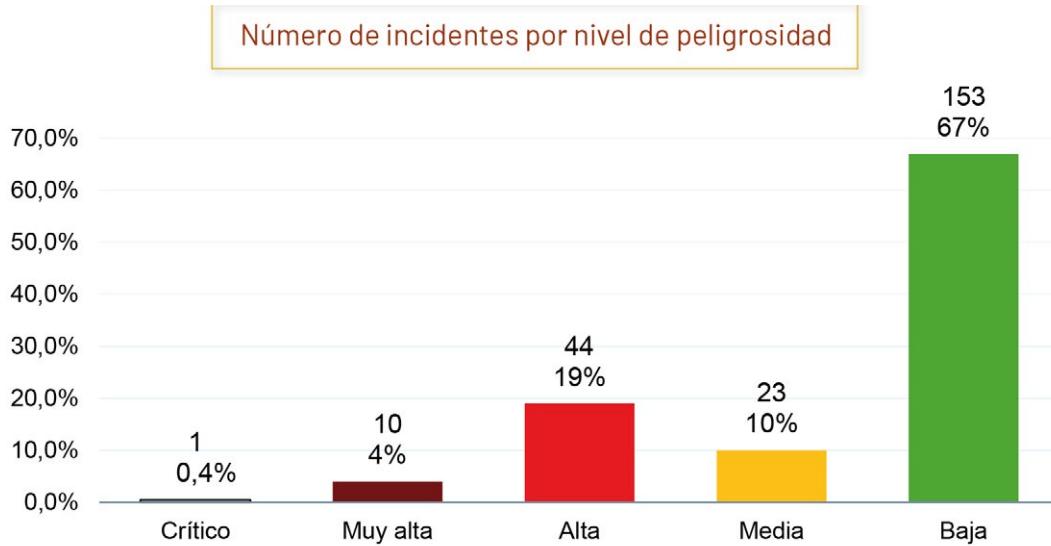
Figura 8.6: Número de ciberincidentes por público objetivo gestionados por INCIBE en 2025



Fuente: INCIBE

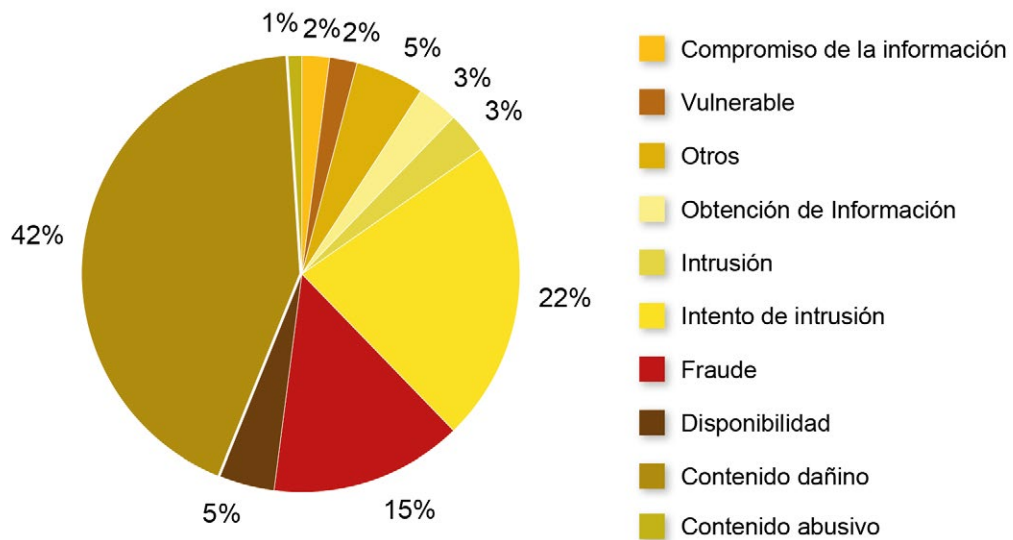
Figura 8.7: Tipología de incidentes gestionados por INCIBE en 2025

Incidentes gestionados por el ESPDEF-CERT en las redes de Defensa (Figuras 8.8 y 8.9)



Fuente: Ministerio de Defensa

Figura 8.8: Peligrosidad de ciberincidentes gestionados por ESPDEF-CERT en 2025

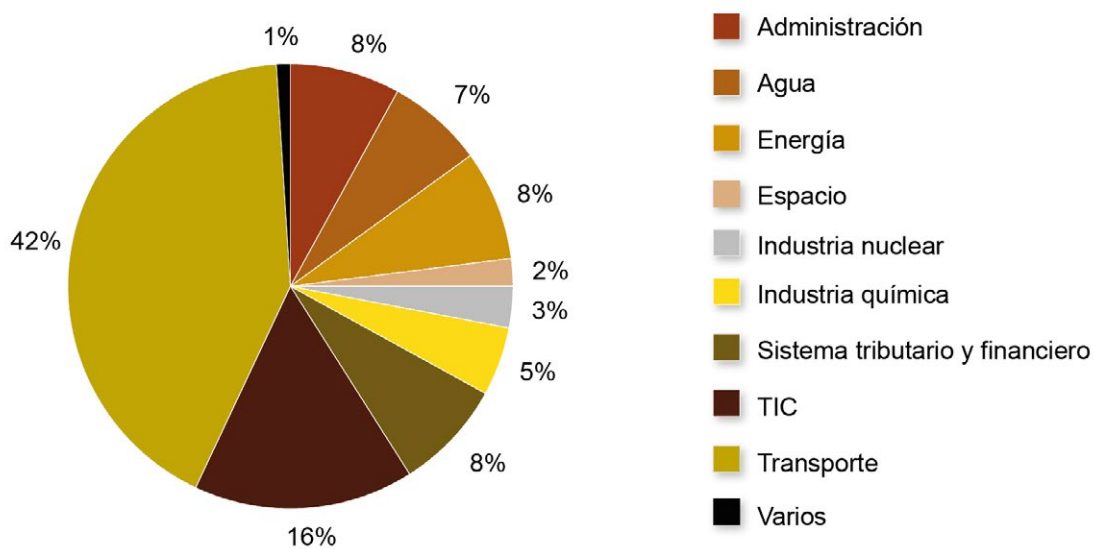


Fuente: Ministerio de Defensa

Figura 8.9: Tipología de incidentes gestionados por ESPDEF-CERT

Incidentes en Operadores de Servicios Esenciales de riesgo alto, muy alto o crítico, notificados a la Oficina de Coordinación de Ciberseguridad (OCC) del Ministerio del Interior (Figuras 8.10 a 8.13)

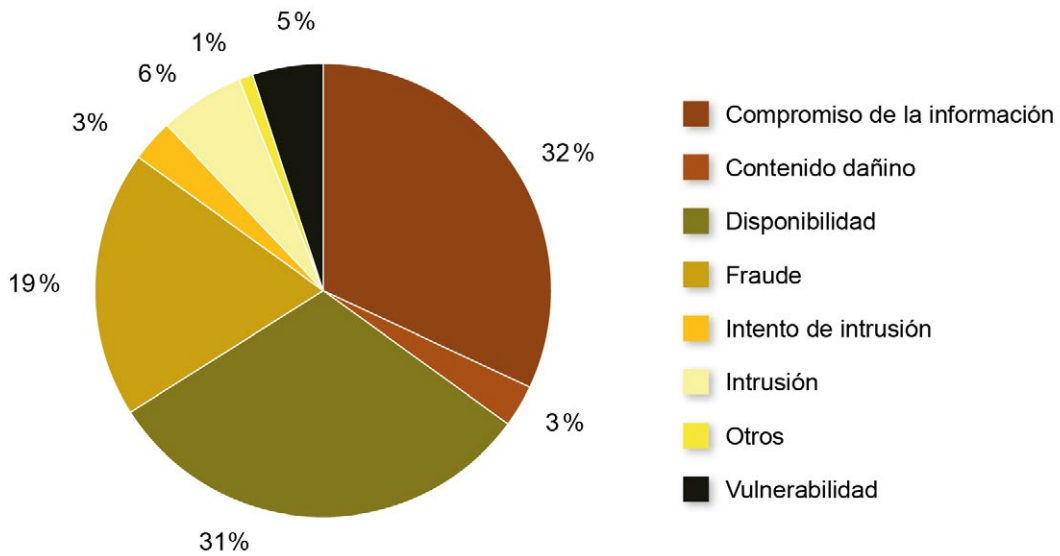
SECTOR ESTRATÉGICO	2021	2022	2023	2024	2025
ADMINISTRACIÓN	7	4	2	2	7
AGUA	4	3	2	12	6
ALIMENTACIÓN	0	0	0	0	0
ENERGÍA	5	11	7	23	7
ESPACIO	0	0	2	0	2
INDUSTRIA NUCLEAR	5	1	3	3	3
INDUSTRIA QUÍMICA	7	8	3	10	5
INSTALACIONES DE INVESTIGACIÓN	0	0	0	0	0
SALUD	0	2	2	2	0
SISTEMA TRIBUTARIO Y FINANCIERO	23	12	18	28	7
TECNOLOGÍAS INFORMACIÓN Y COMUNICACIONES (TIC)	20	11	17	19	14
TRANSPORTE	17	11	23	60	38
VARIOS	3	4	2	1	1
	91	67	81	160	90



Fuente: Ministerio del Interior

Figura 8.10: Número de incidentes por Sector estratégico que presentan niveles de riesgo alto, muy alto o crítico, de obligada notificación a la OCC

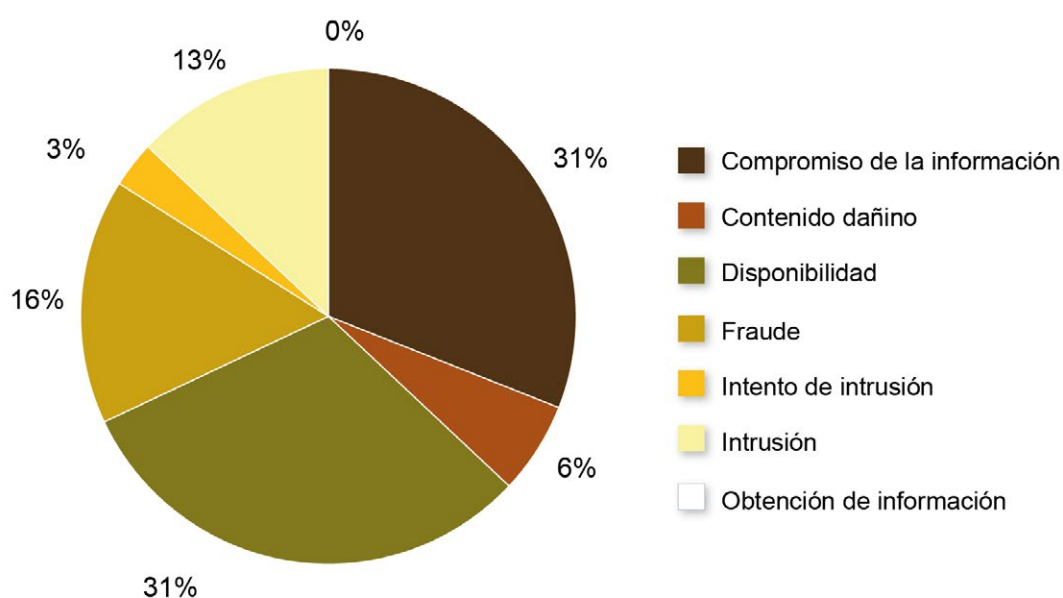
TIPO DE INCIDENTE	2021	2022	2023	2024	2025
COMPROMISO DE LA INFORMACIÓN	19	26	22	62	29
CONTENIDO ABUSIVO	0	0	0	0	0
CONTENIDO DAÑINO	32	11	4	7	3
DISPONIBILIDAD	5	6	28	65	28
FRAUDE	18	15	11	12	17
INTENTO DE INTRUSIÓN	0	1	0	2	3
INTRUSIÓN	10	7	10	8	5
OBTENCIÓN DE INFORMACIÓN	0	0	0	0	0
OTROS	3	0	2	3	1
VULNERABILIDAD	4	1	4	1	4
	91	67	81	160	90



Fuente: Ministerio del Interior

Figura 8.11: Número de incidentes en operadores de Servicios Esenciales por tipología que presentan niveles de riesgo, muy alto o crítico, de obligada notificación a la OCC del Ministerio del Interior

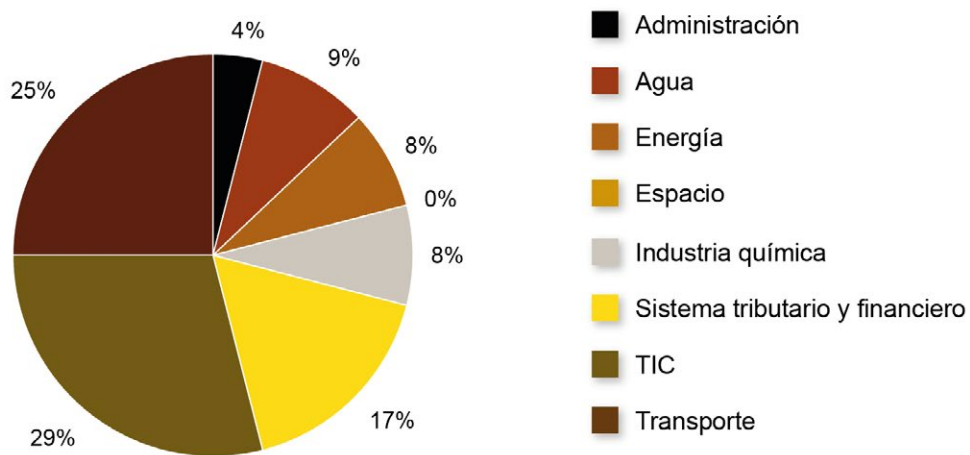
TIPO DE INCIDENTE	2021	2022	2023	2024	2025
COMPROMISO DE LA INFORMACIÓN	4	11	4	9	10
CONTENIDO ABUSIVO	0	0	0	0	0
CONTENIDO DAÑINO	7	1	1	1	2
DISPONIBILIDAD	3	5	15	13	10
FRAUDE	4	0	3	4	5
INTENTO DE INTRUSIÓN	0	1	0	0	1
INTRUSIÓN	4	5	6	3	4
OBTENCIÓN DE INFORMACIÓN	0	0	0	0	0
OTROS	2	0	0	1	0
VULNERABILIDAD	0	0	1	0	0
	24	23	30	31	32



Fuente: Ministerio del Interior

Figura 8.12: Incidentes notificados por tipología a la OCC y agregados al informe anual conforme a lo establecido en el artículo 27.1 de RD 12/2018 de seguridad de las redes y sistemas de información

SECTOR ESTRATÉGICO	2021	2022	2023	2024	2025
ADMINISTRACIÓN	1	1	0	0	5
AGUA	2	0	1	1	1
ALIMENTACIÓN	0	0	0	0	0
ENERGÍA	2	5	2	5	2
ESPACIO	0	0	1	0	1
INDUSTRIA NUCLEAR	0	0	0	0	0
INDUSTRIA QUÍMICA	2	0	1	0	1
INSTALACIONES DE INVESTIGACIÓN	0	0	0	0	0
SALUD	0	0	2	2	0
SISTEMA TRIBUTARIO Y FINANCIERO	4	4	4	4	1
TECNOLOGÍAS INFORMACIÓN Y COMUNICACIONES (TIC)	7	9	8	5	6
TRANSPORTE	6	4	10	13	15
VARIOS	0	0	1	1	0
	24	23	30	31	32



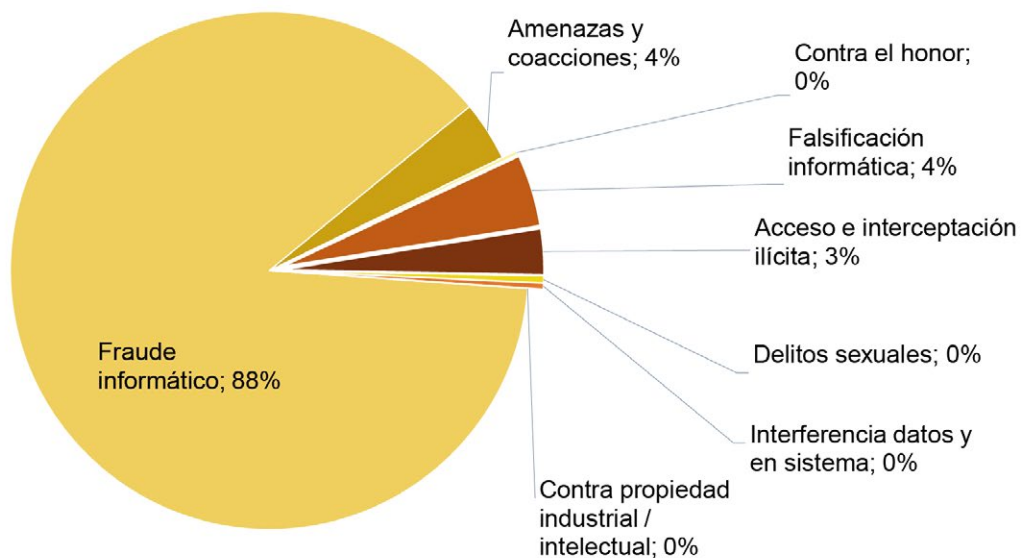
Fuente: Ministerio del Interior

Figura 8.13: Incidentes notificados por Sector Estratégico de incidentes a la OCC y agregados al informe anual conforme a lo establecido en el artículo 27.1 de RD 12/2018 de seguridad de las redes y sistemas de información

Hechos conocidos de infracciones penales relacionadas con la criminalidad

(Figura 8.14)

HECHOS CONOCIDOS	2019	2020	2021	2022	2023	2024	2025
ACCESO E INTERCEPTACIÓN ILÍCITA	4.004	4.653	5.342	5.578	7.367	9.773	13.753
AMENAZAS Y COACCIONES	12.782	14.066	17.319	15.982	17.472	17.738	18.194
CONTRA EL HONOR	1.422	1.550	1.426	1.191	1.174	1.128	1.173
CONTRA LA PROPIEDAD INDUSTRIAL/INTELLECTUAL	197	125	137	114	117	227	145
DELITOS SEXUALES	1.774	1.783	1.628	1.646	1.804	1.676	2.031
FALSIFICACIÓN INFORMÁTICA	4.275	6.289	10.476	12.569	15.137	19.492	21.690
FRAUDE INFORMÁTICO	192.375	257.907	267.011	335.995	427.448	412.850	429.681
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	1.437	1.590	2.138	1.662	1.741	1.917	1.763
TOTAL HECHOS CONOCIDOS	218.302	287.963	305.477	374.737	472.260	464.801	488.430



Fuente: Sistema Estadístico de Criminalidad

Figura 8.14: Evolución de hechos conocidos por categorías delictivas

Tecnologías emergentes

La aceleración tecnológica de 2025 ha precipitado un cambio de escala y de naturaleza en el ámbito de la ciberseguridad. Inteligencia artificial, computación cuántica, 5G, IoT y *cloud* actúan de forma simultánea como motores de innovación y como catalizadores de nuevos modelos de ataque. El resultado es un ecosistema en el que la superficie de exposición crece, los atacantes reducen barreras de entrada y los defensores se ven obligados a repensar sus modelos técnicos y organizativos para preservar la seguridad, la privacidad y la resiliencia.

Si existe una tecnología que define el año 2025, esa es la inteligencia artificial. Tras el despliegue de la IA generativa, ha cobrado especial relevancia la IA agéntica (IA de agentes), un salto evolutivo que dota a los sistemas de una autonomía significativamente mayor para desplazarse por redes, ejecutar operaciones complejas e incluso reescribir su propio software malicioso sin intervención humana. Esta evolución potencia campañas masivas de ingeniería social, facilita la generación de *deepfakes* de alta verosimilitud y reduce aún más las barreras técnicas de entrada para actores criminales y terroristas. En paralelo, en el ámbito defensivo esto debe obligar a utilizar la IA como motor de los mecanismos de detección de anomalías en tiempo real y respuestas automatizadas a incidentes, acelerando una carrera de sofisticación que exige implantar controles estrictos sobre el acceso, el gobierno y el funcionamiento interno de los propios sistemas de IA, convertidos ya en activos críticos y objetivos preferentes para los atacantes.

En respuesta a este escenario de doble filo, el Gobierno ha continuado con el despliegue de la Estrategia Nacional de Inteligencia Artificial (ENIA), enmarcada en la agenda España Digital 2026. Durante 2025, la inversión pública se ha centrado en potenciar la investigación, el desarrollo de talento y la integración ética de la IA en el tejido económico y administrativo.

Iniciativas clave de este año han sido el fortalecimiento del superordenador Mare Nostrum 5 como pilar para el entrenamiento de modelos de IA soberanos y el impulso de proyectos como ALIA para el desarrollo de grandes modelos de lenguaje (LLM) en español y lenguas cooficiales. Estas acciones son consideradas cruciales para asegurar una soberanía tecnológica y reducir la dependencia de modelos desarrollados por terceros países, mitigando así el riesgo de sesgos o manipulaciones externas.

Asimismo el CCN-CNI se encuentra desarrollando una metodología de evaluación de la seguridad de la IA mediante la cual se establecen métricas y pruebas objetivas y reproducibles que valoran las garantías ofrecidas por dicha IA desde diversos puntos de vista (robustez frente a los ataques más comunes a la IA: inyecciones de *prompts*, divulgación de información sensible, envenenamiento de datos y modelos, filtración de *prompts* de sistema y calidad de los resultados ofrecidos por la IA: Evaluación de comportamiento mediante test de respuesta, tolerancia al ruido, todo ello con un nivel de garantía determinado por la categoría del riesgo de los sistemas de IA establecidos dentro del Reglamento de Inteligencia Artificial (RIA) de la Unión Europea.

El Ministerio de Defensa a su vez ha establecido el Centro de Referencia de IA del Estado Mayor de la Defensa, cuyo objetivo es programar y ejecutar actuaciones de carácter innovador, experimental y formativo en materia de IA dentro de las Fuerzas Armadas.

Este 2025 ha sido un año clave para la computación cuántica en Europa, continuando con las acciones ya iniciadas en 2024 (publicación de NIST de los primeros estándares resistentes a ataques cuánticos (FIPS 203, 204 y 205) y, suscripción en noviembre del citado año por parte de 18 Estados miembros de la UE, entre ellos España, una declaración conjunta instando a proteger los casos de uso más sensibles antes de 2030), ha estado marcado por varias novedades estratégicas y políticas que buscan consolidar el liderazgo tecnológico y superar la fragmentación del sector: la Comisión Europea presentó la

Estrategia Cuántica el 2 de julio de 2025, con el objetivo de convertir a la UE en potencia mundial en tecnologías cuánticas de aquí a 2030, estructurándola en cinco pilares (investigación e innovación, infraestructuras cuánticas, fortalecimiento del ecosistema industrial, tecnologías espaciales y de doble uso, y desarrollo de competencias cuánticas) para acelerar la transición de ciencia a mercado y reforzar la soberanía tecnológica.

Además, este año la Comisión ha lanzado una consulta pública para preparar un futuro “*Quantum Act*” (previsto para 2026), con el fin de establecer un marco regulatorio y de gobernanza que coordine inversiones, cadenas de suministro y capacidades industriales en todo el bloque.

Se han dado pasos concretos en proyectos de infraestructura cuántica, como el diseño de instalaciones piloto para chips cuánticos y redes de Internet cuántica europea, y se prepara la Academia Europea de Competencias Cuánticas para 2026 para formar talento especializado.

Paralelamente, informes del *Joint Research Centre* de la Comisión Europea muestran que, aunque Europa alberga cerca de un tercio de las empresas cuánticas globales, solo un pequeño porcentaje de patentes proviene de la UE, lo que impulsa aún más las iniciativas de coordinación y financiación para cerrar esa brecha.

En el plano internacional, 2025 también fue declarado por la ONU Año Internacional de la Ciencia y Tecnología Cuánticas, lo que ha reforzado la visibilidad global de la investigación y cooperación cuántica.

En España destaca el lanzamiento oficial de la Estrategia Nacional de Tecnologías Cuánticas 2025-2030, cuya hoja de ruta busca consolidar el ecosistema cuántico español para fortalecer la soberanía digital y preparar al país para la disrupción que suponen estas tecnologías.

España, a través de plataformas como Quantum Spain, está fomentando la colaboración entre centros de investigación, universidades y el sector privado que están trabajando para posicionarse en áreas clave como las comunicaciones cuánticas seguras y el desarrollo de los nuevos algoritmos de criptografía postcuántica (PQC), convirtiendo esta transición en un imperativo para la seguridad del Estado en la próxima década.

Siguiendo las pautas marcadas por el Consejo de la Unión Europea, que aprobó en junio del 2020 el documento Quantum Transition, el CCN- CNI junto con la industria nacional está llevando a cabo un remarcable esfuerzo en la cripto-modernización de los cifradores nacionales que protegen información clasificada, con el objetivo de que todos ellos sean *Quantum-safe* en el año 2030.

Es necesario también remarcar otros ámbitos tecnológicos, que, si bien no son tan novedosos, contribuyen notablemente a aumentar la superficie de exposición. La implantación del 5G y la dependencia creciente de los servicios en nube, más conocidos como “*cloud*” multiplican los puntos vulnerables, especialmente ante fallos de configuración o accesos indebidos que pueden explotarse gracias a su hiperconectividad. En estos entornos, el cifrado robusto, la autenticación fuerte y la automatización de auditorías se han convertido en pilares básicos para mantener un nivel adecuado de protección. Junto a ello, la proliferación del Internet de las cosas (IoT) y el crecimiento del “*edge computing*” (conmutación en el extremo) plantean retos adicionales. Siguen llegando al mercado muchos dispositivos con configuraciones por defecto poco seguras y sin capacidad de actualización, lo que los convierte en la puerta de entrada ideal para *botnets* o ataques distribuidos. La dispersión geográfica de estos equipos complica la gestión de incidentes, por lo que resulta esencial segmentar las redes, mantener inventarios precisos e integrar su actividad en los sistemas de monitorización corporativos para evitar puntos ciegos.

La cadena de suministro digital también se ha convertido en un objetivo estratégico para los atacantes. Los entornos basados en contenedores y ciclos de desarrollo muy rápidos hacen necesario incorporar la seguridad desde el propio diseño, reforzar las imágenes de contenedores y vigilar de forma continua la integridad de los procesos de CI/CD. Todo ello debe complementarse con una gestión del riesgo de proveedores que tenga en cuenta la resiliencia global del ecosistema.

Cloud: adopción, certificación y soberanía

Si bien no es una tecnología emergente merece una mención explícita ya que el uso de servicios en la nube sigue creciendo con fuerza no solo en España sino en todo Europa, justo en un momento en el que el marco regulador está en plena revisión.

Como se detalla más adelante, aún está pendiente la trasposición de la directiva NIS2, continúa la actualización del “*Cybersecurity Act*” y se sigue avanzando el futuro esquema de certificación EUCS. Este proceso refleja la intención europea de reforzar la seguridad y garantizar que los servicios en nube se desarrollen con mayores garantías y con más control sobre los datos estratégicos.

Tanto administraciones públicas como empresas han acelerado su migración hacia la nube, atraídas por las ventajas que ofrece: mayor flexibilidad, mejor capacidad de procesamiento, posibilidad de integrar tecnologías emergentes como la inteligencia artificial y un mayor aprovechamiento de los datos. En el caso de las administraciones públicas, además, están tomando forma modelos de nube híbrida y servicios compartidos alineados con el Esquema Nacional de Seguridad.

Sin embargo, este avance también está poniendo de relieve desafíos importantes. Uno de los más señalados es la dependencia de proveedores globales y la necesidad de mantener un control real sobre dónde se alojan los datos y quien puede acceder a ellos. De ahí que este cobrando fuerza la idea de desarrollar nubes soberanas, concebidas para asegurar mayor autonomía y una gestión más cercana de la información sensible.

Al mismo tiempo, la generalización de la IA, muy dependiente de la capacidad de cómputo que ofrece la nube, está llevando a las organizaciones a replantearse como garantizar la protección de estos entornos. La gestión segura de infraestructura multi-nube también exige perfiles altamente especializados, algo que hoy en día no siempre está disponible.

No obstante, este cambio de paradigma solo es posible si se realiza de forma segura, para lo cual es imprescindible evaluar y certificar la seguridad de los servicios en la nube. Sin embargo, las metodologías existentes hasta el momento para certificar la seguridad de productos “*on premise*”, como Common Criteria o LINCE, no son adecuadas en aquellos casos en los que el producto se encuentra desplegado en la nube. Por ello el CCN-CNI ha desarrollado CICLON, una nueva metodología de evaluación concebida exclusivamente para adaptarse al paradigma “*cloud*” basándose en la experiencia acumulada a lo largo de la evaluación de dichos productos.

Avances en el ámbito regulatorio

A nivel europeo se desatacan las nuevas iniciativas legislativas y recomendaciones, así como modificaciones a las ya existentes y avances en las mismas durante 2025 y hasta la fecha de publicación de este informe.

Respecto al estado de la Normativa Europea:

Reglamento (UE) 2024/2847 de 23 de octubre de 2024. Ciber Resilient Act (CRA).

Los organismos europeos de normalización CEN (Comité Europeo de Normalización), CENELEC (Comité Europeo de normalización Electrotécnico) y ETSI (Instituto Europeo de normas de Telecomunicaciones) continúan elaborando las normas técnicas para verificar los requisitos esenciales de ciberseguridad. La Comisión ha aprobado el borrador del Reglamento de Ejecución que define las categorías de productos importantes y críticos con elementos digitales, pendiente de publicación en el Diario Oficial de la UE (DOUE). Han comenzado las reuniones de las futuras Autoridades Notificantes, que preparan la hoja de ruta para 2026. Se ha constituido el grupo ADCO para coordinar la aplicación uniforme de la CRA entre las autoridades de vigilancia del mercado y continúan los trabajos de los grupos de expertos (evaluación de riesgos, procesamiento remoto de datos, notificaciones, software libre) y está en proceso de creación un grupo sobre Inventario de componentes de software (*Software Bill of Materials* o SBOM, por sus siglas en inglés).

Reglamento (EU) 2025/38 19 de diciembre de 2024. Ciber solidarity Act (CSoA).

Este instrumento legislativo crea un Sistema Europeo de Alerta de Ciberseguridad, compuesto por centros nacionales y transfronterizos interconectados (*Cyber Hubs*) que emplean tecnologías avanzadas para detectar y compartir alertas de amenazas a nivel transfronterizo. Además, establece un Mecanismo de Emergencia de Ciberseguridad con tres pilares principales: acciones de preparación, incluyendo pruebas de resistencia en sectores críticos como finanzas, energía y salud; la constitución de una Ciber Reserva de la UE, integrada por servicios de respuesta a incidentes de “proveedores de confianza” desplegables a petición de los Estados miembros, instituciones o países asociados; y el refuerzo de la asistencia mutua entre Estados miembros ante ciberincidentes.

Adicionalmente, en octubre de 2025 y hasta marzo de 2016, a través del programa Europa Digital se abrió el plazo de convocatoria para financiar acciones de preparación del Mecanismo de Emergencia en materia de Ciberseguridad (DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP).

Reglamento delegado (UE) 2022/30 de 29 de octubre de 2021, que completa la RED activando los requisitos del art. 3.3 (letras d, e, f) para ciertos equipos conectados (protección de datos y privacidad, protección de la red y contra el fraude). Su aplicación es obligatoria desde el 1 de agosto de 2025.

DIGITAL OMNIBUS 19 de noviembre de 2025.

El Digital Omnibus es una iniciativa de la Comisión Europea orientada a simplificar, racionalizar y armonizar las obligaciones digitales aplicables a empresas y administraciones públicas en la Unión Europea. Su objetivo principal es reducir la carga administrativa derivada de la superposición de requisitos en distintos marcos regulatorios (como NIS2, DORA, GDPR y la *Cybersecurity Act*), especialmente en materia de notificación de incidentes, reporte de información y cumplimiento normativo. En el ámbito de la ciberseguridad, el Digital Omnibus busca avanzar hacia un enfoque de “ventanilla única”, para la notificación de incidentes, mejorar la coherencia entre autoridades competentes y reforzar la eficacia del marco regulatorio europeo, sin rebajar los niveles de seguridad

ni de protección de derechos fundamentales, contribuyendo así a una mayor resiliencia del ecosistema digital europeo.

Borrador COM (2026) 11 20 de enero de 2026- Cybersecurity Act (CSA).

El borrador de revisión de la *Cybersecurity Act* publicado el 20 de enero de 2026, propone una modernización y ampliación del marco europeo de ciberseguridad mediante el fortalecimiento de los mecanismos de certificación, gobernanza y cooperación en materia de ciberseguridad en la Unión Europea.

En primer lugar, refuerza el mandato de ENISA como agencia europea de ciberseguridad, ampliando sus funciones hacia un papel más activo de apoyo técnico, coordinación y asistencia operativa a las autoridades nacionales, con especial atención a la interoperabilidad de los esquemas de certificación y a la gestión de riesgos transfronterizos.

En segundo lugar, introduce una ampliación y racionalización de los esquemas de certificación de ciberseguridad europeos, potencialmente abarcando nuevas familias de productos, servicios y tecnologías, y promoviendo una mayor convergencia y reconocimiento mutuo entre Estados miembros y sectores, lo que incluye componentes de redes, dispositivos críticos y servicios *cloud*.

El borrador también contempla normas para armonizar y simplificar las obligaciones de notificación de incidentes, en coherencia con iniciativas como el *Digital Omnibus* que recoge el Punto único de entrada (*Single Entry Point*), con el objetivo de reducir cargas administrativas.

Plan de Acción Europeo sobre la Ciberseguridad de los Hospitales (enero 2025). Este plan para reforzar la ciberseguridad sanitaria mediante prevención, detección, respuesta y disuasión, además de crear un Centro Paneuropeo de Apoyo bajo ENISA. También incluye alertas tempranas, formación y ejercicios para hospitales y proveedores.

Como parte de una **nueva arquitectura de seguridad, defensa y resiliencia de la Unión Europea** para responder a un entorno geopolítico más inestable, la Unión Europea publicó el **Libro blanco de la Defensa Europea** (marzo 2025) dedicado a reforzar las capacidades militares, la industria de defensa y la cooperación estratégica y la **Estrategia de Preparación de la Unión Europea** (marzo 2025), que define 30 acciones para fortalecer la capacidad de la UE frente a amenazas como ciberataques, crisis geopolíticas y desastres naturales, incorporando criterios mínimos de preparación para servicios esenciales.

El Plan de Acción de la UE sobre la Seguridad de los Cables establece el marco estratégico para reforzar la protección de los cables submarinos europeos mediante medidas de prevención, detección, respuesta, reparación y disuasión, además de fortalecer la vigilancia y la evaluación coordinada de riesgos ante incidentes recientes en aguas europeas.

Como desarrollo operativo de este marco, el **Informe sobre Seguridad y Resiliencia de las Infraestructuras de Cables Submarinos** cartografía detalladamente estas infraestructuras, identifica siete escenarios de riesgo y define pruebas de resistencia, al tiempo que impulsa la creación de Centros Regionales de Cableado para mejorar la vigilancia y la detección temprana en toda la Unión. España, por su situación geográfica debe tener un papel destacado en esta área.

Recomendación del Consejo de 6 de junio de 2025 de Plan director de la UE para la Gestión de Crisis de Ciberseguridad cuyo objetivo es establecer un **marco estratégico y operativo común** que permita a la Unión Europea **gestionar de manera coordinada y eficaz las crisis de ciberseguridad**, reforzando la resiliencia y la capacidad de respuesta frente a ciberamenazas de gran escala.

A nivel nacional, en el marco de las iniciativas legislativas y recomendaciones de la Unión Europea se han llevado acciones tanto para la implementación como el desarrollo de estas.

Respecto a la Transposición de la Directiva Europea (UE) 2022/2555-NIS2, el 14 de enero de 2025, el Consejo de Ministros dio luz verde al anteproyecto de Coordinación y Gobernanza de la Ciberseguridad con el objetivo de incorporar al ordenamiento jurídico nacional las obligaciones de la NIS2. Actualmente, el Ministerio del Interior está estudiando cómo realizar la integración de las observaciones emitidas por el Consejo de Estado mediante dictamen en el mencionado anteproyecto.

Como ya se venía haciendo, los diferentes organismos han sido muy activos en los diferentes grupos de trabajo de Cooperación NIS.

- WS11 – 5G/Telecom Cybersecurity (5 reuniones): España presentó el SOC 5G en la 31ª reunión de Atenas, primera iniciativa de este tipo a nivel europeo. Se ha contribuido a los trabajos sobre implementación de la 5G Toolbox, restricciones a proveedores de alto riesgo y la nueva Toolbox de cadena de suministro TIC.
- WS10 – Digital Infrastructure: definición de servicios sujetos a NIS2, autonomía estratégica de la UE en infraestructuras críticas (incluidos cables submarinos) y coordinación con los requisitos del Reglamento de Ciberresiliencia.
- WS4 – Supervision: elaboración de directrices sobre jurisdicción única y asistencia mutua entre autoridades competentes.
- WS12 – WHOIS: definición del marco de acceso a datos de registro de dominios por parte de solicitantes legítimos, equilibrando trazabilidad y protección de datos.

Reglamento (UE) 2019/881- Cybersecurity Act (CSA)

A nivel europeo, se han desarrollado los procedimientos de la Autoridad Nacional de Certificación de la Ciberseguridad (ANCC) y del Organismo de Certificación del EUCC, según lo establecido en el *Cybersecurity Act*, y ya se ha autorizado al organismo de certificación del Centro Criptológico Nacional, así como a tres laboratorios de evaluación privados, para operar a nivel elevado en el esquema EUCC. También se ha llevado a cabo la notificación como ANCC, de dos organismos de certificación y de dos laboratorios de evaluación privados para operar a nivel sustancial en el EUCC. El Centro Criptológico Nacional ha participado en el Grupo de Expertos del *Ciber Resilient Act* (CRA) para el establecimiento de la ANCC como Autoridad Notificante.

Reglamento (UE) 2024/1183 (eIDAS 2) y EUDI Wallet

A raíz del reglamento europeo eIDAS 2 (Reglamento (UE) 2024/1183) se está empezando a trabajar de forma intensa en temas de futuro como el *wallet* digital. Un paso previo ha sido el DNI en el móvil, que permite a los ciudadanos identificarse en multitud de sitios sin necesidad de portar el documento físico. Igualmente sigue creciendo el uso de la video identificación, aunque existen fundados temores de que la IA y los *Deep fakes* puedan ser obstáculos importantes a la hora de asentar este tipo de tecnologías.

En 2025, continúan los trabajos de desarrollo de eIDAS 2 y la cartera europea EUDI Wallet, lo que exige adaptar sistemas nacionales de identificación y autenticación (CI@ve, DNI electrónico) y reforzar la autenticación fuerte para mitigar el *phishing* y accesos no autorizados. La Comisión Europea publicó en julio directrices y planes para la verificación de edad en el marco del Reglamento de Servicios Digitales permitiendo demostrar mayoría de edad sin revelar datos personales, y en octubre se avanzó en soluciones que integran pasaportes, tarjetas de identificación y APIs (*Application Programming Interface*) de credenciales digitales.

Adicionalmente se detallan el resto de las medidas y desarrollo normativo en proceso a nivel nacional:

- Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales actualmente en tramitación.
- *Real Decreto de Resiliencia*. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETELECO) ha iniciado los trámites para elaborar una iniciativa normativa para regular las condiciones y actuaciones que garanticen la seguridad y resiliencia de las infraestructuras digitales y los servicios de comunicaciones electrónicas, en desarrollo del artículo 63 de la Ley 11/2022. Esta regulación se enfocaría especialmente en situaciones que afecten la integridad, disponibilidad o calidad de las redes y servicios, incluyendo interrupciones o degradaciones importantes.
- El anteproyecto de Ley de digitalización y modernización del sector financiero contiene el régimen sancionador del Reglamento sobre resiliencia operativa digital (*Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero* y por el que se modifican los Reglamentos (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 y (UE) 2016/1011). El objetivo fundamental de esta ley es garantizar que el ordenamiento jurídico nacional se sigue posicionando a la vanguardia en el ámbito de la legislación financiera, teniendo en cuenta los avances en materia de digitalización. Para ello, se requieren actuaciones en cuatro ámbitos principales, tanto para reflejar los últimos avances en la normativa europea como para actualizar herramientas nacionales que promueven la innovación en el sector financiero: ciberresiliencia, criptoactivos, servicios y sistemas de pago, incluyendo una revisión del régimen jurídico de Iberpay, y actualización del *Sandbox* regulatorio financiero nacional. Se encuentra en una fase de tramitación muy avanzada.
- La Estrategia de Ciberseguridad del Sistema Nacional de Salud 2025-2028 que establece el marco integral diseñado para proteger la **a infraestructura de información sanitaria, garantizar la continuidad asistencial y salvaguardar la confianza de los ciudadanos** en el sistema de salud.

Avances en la Estrategia Nacional de Ciberseguridad

La Estrategia Nacional de Ciberseguridad 2019 estructura la acción pública en siete líneas de actuación que guían los desarrollos operativos, tecnológicos y organizativos del Estado en este ámbito. Bajo esta estructura se integran las iniciativas emprendidas por los distintos organismos y entidades con competencias en ciberseguridad. Durante 2025 gracias a la aprobación de las medidas adicionales al Plan Nacional de Ciberseguridad de 2022 se ha dado un gran impulso a estas acciones.

En el contexto de **reforzar las capacidades ante las amenazas provenientes del ciberespacio**, el CCN han impulsado medidas de ciberdefensa activa y se han reforzado las capacidades en materia de ciberinteligencia. Las herramientas destinadas a la prevención, detección y respuesta han incorporado nuevas capacidades apoyadas en desarrollos de Inteligencia Artificial. Se ha continuado el trabajo en la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, adaptándola a los requerimientos de la Directiva NIS2, y la Red Nacional de SOC ha incrementado tanto el número de entidades adheridas como el volumen de información compartida entre organismos públicos y privados. Asimismo, se han publicado guías y procedimientos orientados a reforzar la protección y la defensa en ciberseguridad.

En relación con la línea orientada a **garantizar la seguridad y resiliencia de los activos estratégicos de España**, las herramientas impulsadas por el CCNCNI puestas a disposición del sector público han sido ampliadas mediante inversiones contempladas en el Plan Nacional de Ciberseguridad, incluyendo sistemas de alerta temprana para infraestructuras CTS. Se ha prestado apoyo y acompañamiento a entidades públicas en la adopción del Esquema Nacional de Seguridad, manteniendo la colaboración con organismos autonómicos, de las ciudades autónomas y locales con competencias en ciberseguridad.

Durante este periodo se han evaluado nuevos productos y servicios que han sido incorporados al Catálogo de Productos y Servicios de Seguridad TIC, que constituye una referencia en los procesos de contratación pública en este ámbito.

El modelo español se ha consolidado como referente en el ámbito europeo en materia de procesos y esquemas de certificación. Asimismo, se ha fortalecido la coherencia entre los requisitos de seguridad establecidos en el Esquema Nacional de Seguridad (ENS) y los instrumentos de contratación centralizada, en particular, los Sistemas Dinámicos de Adquisición (SDA), mediante la utilización de productos certificados y del Catálogo de Productos y Servicios de Tecnologías de la Información y las Comunicaciones (CPSTIC).

Según el informe de cobertura de banda ancha de SETID, la cobertura 5G alcanza el 95,76% de la población (datos a junio 2024), con un incremento de 3,46 puntos respecto al año anterior. En el ámbito rural, la cobertura se sitúa en el 80,01%, mejorando 11 puntos porcentuales también respecto al año anterior.

España cuenta con el *Real Decreto-ley 7/2022* y el *Real Decreto 443/2024*, que establecen el *Esquema Nacional de Seguridad de redes y servicios 5G*.

El Centro de Operaciones de Ciberseguridad 5G de referencia, dirigido por la Subdirección General de Seguridad Digital, perteneciente a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETELECO) del Ministerio para la Transformación Digital y de la Función Pública, continúa su desarrollo.

La línea dirigida a **reforzar las capacidades de investigación y persecución de la cibercriminalidad** se ha materializado mediante la puesta en funcionamiento, en el seno de la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior, del Observatorio de la Cibercriminalidad, orientado a monitorizar y detectar tendencias y amenazas relacionadas con la ciberseguridad, la cibercriminalidad y la desinformación, con el fin de elaborar productos de inteligencia y planes preventivos y de respuesta. Asimismo, se ha creado el Centro de Respuesta a Incidentes Cibernéticos del Ministerio del Interior en apoyo a la Policía Judicial (CSIRT MIRPJ), destinado a prestar soporte técnico y coordinar unidades de investigación de las Fuerzas y Cuerpos de Seguridad del Estado. Paralelamente, se han mantenido acciones de concienciación dirigidas a diversos colectivos y se ha avanzado en la formación y coordinación interinstitucional mediante el Plan Estratégico contra la Cibercriminalidad. La Guardia Civil ha reforzado sus capacidades a través de la consolidación de la Jefatura de Transformación Digital y Ciberseguridad, la integración de la UCCIBER y la formación especializada impartida en colaboración con INCIBE. También se ha puesto en funcionamiento la posibilidad de interponer denuncias telemáticas mediante la Oficina Nacional de Recepción Electrónica de Denuncias (ONRED), con disponibilidad permanente y varios procedimientos iniciales habilitados. Por su parte, la Policía Nacional ha desarrollado el Plan de Capacidades Operativas Digitales destinado a mejorar las capacidades de investigación en redes sociales, *Dark Web* y análisis de criptovalores. El CCNCNI ha continuado prestando apoyo a los organismos con competencias en investigación de cibercriminalidad.

En cuanto a la línea dedicada a **impulsar la ciberseguridad de las Entidades Locales** se ha progresado en el marco de colaboración entre la Secretaría de Estado de Función Pública y la Secretaría de

Estado de Política Territorial. Esta línea, bajo el liderazgo y coordinación de la Agencia Estatal de Administración Digital, persigue reforzar la ciberseguridad de las Entidades Locales y de los servicios que estas proveen, garantizando la seguridad de infraestructuras, comunicaciones y servicios digitales, la interoperabilidad con el marco de ciberseguridad de la AEAD y el refuerzo del cumplimiento del Esquema Nacional de Seguridad.

En 2025 ha progresado el proyecto para el despliegue del Centro de Operaciones de Ciberseguridad para Entidades Locales (COCS EELL) que permita ofrecer un servicio básico y que democratice la ciberseguridad en todo el territorio nacional. Con una situación de despliegue que ofrece cifras tales como 48 territorios adheridos al COCS EELL, 41 Diputaciones, 2 Ciudades Autónomas, 6 Comunidades Autónomas uniprovinciales, 7 Cabildos Insulares y 4 Consejos Insulares adscritos a los servicios del COCS EELL; con 7.707 Entidades de menos de 20.000 habitantes y 274 Entidades de 20.000 – 50.000 habitantes adscritas al COCS EELL. para **reforzar la ciberseguridad de las Entidades Locales** y de los servicios que estas proveen, garantizando la seguridad de infraestructuras, comunicaciones y servicios digitales, la interoperabilidad con el marco de ciberseguridad de la SGAD y el refuerzo del cumplimiento del Esquema Nacional de Seguridad. Para ello, se han puesto en marcha **dos actuaciones principales** con despliegue previsto hasta 2026, por un lado, un acuerdo interdepartamental dirigido a municipios de hasta 50.000 habitantes (excepto capitales de provincia), con una parte destinada a evaluar e implementar mejoras y otra destinada a un Convenio SGAD-CCN que permita la implantación de un Centro de Operaciones de Ciberseguridad para Entidades Locales (COCS EELL) único y centralizado y una **oficina técnica** de apoyo, control, coordinación y referencia tecnológica; por otro se han articulado subvenciones a entidades de más de 50.000 habitantes, exigiendo la inclusión de un proyecto de ciberseguridad con el objetivo de garantizar la seguridad de infraestructuras, comunicaciones y servicios digitales y de mejorar las capacidades de prevención, detección y respuesta.

Estas medidas se coordinan con las iniciativas de otros organismos competentes: entre ellas, la participación del CCNCNI en el Centro de Operaciones de Ciberseguridad para Entidades Locales (COCS EELL) de Entidades Locales y las actuaciones de sensibilización desarrolladas por Policía Nacional y Guardia Civil, incluidas campañas, guías y programas de formación dirigidos a colectivos concretos, que se integran de forma complementaria en el esfuerzo de concienciación y protección de la ciudadanía y del tejido empresarial.

Por lo que respecta a las FCSE, en 2025, la Guardia Civil ha reforzado de manera significativa su aportación a las siete líneas de acción de la Estrategia Nacional de Ciberseguridad gracias a la consolidación de la Jefatura de Transformación Digital y Ciberseguridad, que impulsa la modernización tecnológica y la protección digital de la Institución. La integración de la UCCIBER mejora la coordinación con los CSIRT nacionales y con la Oficina de Coordinación Ciberseguridad.

La línea orientada a **potenciar la industria española de ciberseguridad y la generación y retención de talento** se ha desarrollado mediante diversas actuaciones. El Ministerio de Defensa ha apoyado la participación del tejido tecnológico nacional en convocatorias de proyectos del Fondo Europeo de Defensa y en iniciativas de innovación como DIANA de la OTAN. Adicionalmente, las actuaciones de I+D+i del Plan Industrial y Tecnológico para la Seguridad y Defensa 2025 han permitido impulsar avances en tecnologías con impacto en el ciberespacio, como la inteligencia artificial, las tecnologías cuánticas o las comunicaciones avanzadas y destacando los proyectos específicos pioneros del Mando Conjunto del Ciberespacio para la obtención de un sistema de combate en el Ciberespacio (SCOMCE) y para el desarrollo de un Campo de Maniobras Ciber Clasificado para el entrenamiento específico en todos los niveles de las operaciones ciber.

Adicionalmente, el CCNCNI ha promovido el desarrollo de productos y servicios de seguridad TIC por parte de la industria nacional. En el ámbito europeo, el programa Horizonte Europa, a través

del Clúster 3, ha lanzado convocatorias orientadas al desarrollo de tecnologías de ciberseguridad, incluyendo IA generativa, protección de la privacidad, criptografía postcuántica, *cyberranges*, *hardware* y *software* ciberseguros, así como sistemas criptográficos híbridos. En este contexto, se señala que las características del régimen de contratación pública y del sistema de acceso al empleo público en el ámbito tecnológico condicionan las posibilidades de potenciación y retención de talento especializado en determinados organismos.

En cuanto a la línea destinada a **contribuir a la seguridad del ciberespacio en el ámbito internacional**, se está desarrollando un proyecto liderado por el CCNCNI con la participación de siete países europeos para la creación de una red europea de Centros de Operaciones de Ciberseguridad destinada al intercambio de información sobre ciberamenazas, siguiendo el modelo de la Red Nacional de SOC.

Por su parte, la Secretaría de Estado de Telecomunicaciones ha participado activamente en el Grupo de Planeamiento de Comunicaciones Civiles de la OTAN, donde ostenta la vicepresidencia y en el que ha participado en un ejercicio Table Top diseñado para poner a prueba la capacidad de respuesta de los participantes ante un escenario de crisis en comunicaciones civiles.

En el marco de la línea orientada a Desarrollar una cultura de ciberseguridad, se han desarrollado actuaciones de sensibilización y capacitación orientadas a ciudadanía, menores y familias, tejido empresarial, personal del sector público y colectivos específicos.

En este contexto, INCIBE ha desplegado acciones formativas y de concienciación dirigidas a público general, pymes y profesionales (a través de “Ciudadanía/OSI”, “Menores/IS4K” y “Empresas/Protege tu Empresa”), con recursos estructurados por audiencias y materias (cursos en línea, talleres, materiales didácticos, actividades interactivas, juegos y kits de concienciación), así como itinerarios para empresas (plan director, buenas prácticas, evaluación de riesgos y contenidos temáticos como *phishing*, *ransomware*, ingeniería social o teletrabajo). Estas iniciativas se encuentran centralizadas en el portal institucional de INCIBE y su sección de formación y concienciación.

Asimismo, INCIBE mantiene catálogos formativos que ordenan la oferta de capacitación reglada y especializada (Formación Profesional, formación universitaria y otras vías de especialización), con el objetivo de facilitar el acceso a titulaciones y trayectorias en ciberseguridad para distintos perfiles académicos y profesionales.

Dentro de las iniciativas de fomento del talento y la capacitación práctica, el portal de INCIBE integra programas y actividades de entrenamiento y divulgación técnica, entre los que figuran Academia Hacker, Talento Hacker, Conecta Hacker y Emplea Hacker, junto con eventos como Cybersecurity Summer BootCamp, ENISE, CyberCamp, International CyberEx o el Día de Internet Segura, que incluyen formatos formativos, retos, talleres o sesiones técnicas.

Como canal de apoyo y orientación complementario a la formación, INCIBE opera la Línea 017 – Tu ayuda en ciberseguridad, con atención técnica, psicosocial y legal para ciudadanía, empresas y menores, y materiales asociados (guías, recursos y derivaciones), lo que posibilita reforzar la prevención y la respuesta temprana en el ámbito educativo y formativo.

En el sector público, el CCNCNI mantiene un programa de formación STIC (en colaboración con el INAP) con convocatorias periódicas y cursos específicos, por ejemplo, ciberinteligencia, gestión de incidentes, seguridad en la nube, trazabilidad del dato, dispositivos móviles o ENS, combinando fases sincrónicas y asincrónicas en calendario oficial.

Además, las Jornadas STIC, en las que se unen CCN, Mando Conjunto del Ciberspacio y Rooted-CON incorporan jornadas técnicas con sesiones formativas y prácticas encuadradas en el programa del evento (talleres y laboratorios), constituyendo un marco adicional de capacitación sectorial.

En el ámbito de las Administraciones Locales (EELL), el despliegue del COCS EELL mencionado anteriormente incluye un Plan de Formación y Concienciación en Ciberseguridad con webinars en vivo, calendarios de sesiones, material audiovisual e infografías para personal municipal y provincial, así como repositorios documentales y comunicaciones periódicas para facilitar la asistencia y el seguimiento. Estas acciones se articulan en coordinación con diputaciones y la Agencia Estatal de Administración Digital, sin sustituir soluciones existentes, y se enmarcan en el Plan de Digitalización de las Administraciones Públicas 2021-2025 y en la iniciativa estatal de refuerzo de la ciberseguridad en EELL.

De forma complementaria, distintas diputaciones han convocado sesiones de formación y concienciación alineadas con el servicio del COCS EELL; por ejemplo, la Diputación de Sevilla (INPRO) ha anunciado sesiones online de “Seguridad de la información” para personal de diputación y ayuntamientos dentro de su Plan de Formación y Concienciación en Ciberseguridad (PRE.7).

En cuanto a colectivos específicos, las jornadas Ciberwall de la Policía Nacional y la Ciberliga de la Guardia civil se han convertido en uno de los referentes anuales en el ámbito formativo.

Complementariamente, la Policía Nacional y la Guardia Civil en colaboración con Canal Sénior y en el marco del Plan Mayor Seguridad, desarrollan un programa formativo gratuito online para personas mayores de 55 años, con videoclases, podcasts, juegos e infografías sobre prevención de estafas, fraudes digitales y protección de la información personal. Estas acciones se difunden a través de la web de Canal Sénior y de los canales institucionales, con participación de especialistas de la Unidad Central de Participación Ciudadana.

Por lo que respecta a la capacitación de personal especializado que contribuye a esta cultura de seguridad, en 2025 la Guardia Civil ha impartido formación especializada a más de 6.000 agentes en materia de ciberseguridad en colaboración con INCIBE, lo que se inserta en el esfuerzo formativo orientado a la mejora de capacidades en investigación y respuesta y, de manera indirecta, a la extensión de prácticas de ciberseguridad en su relación con ciudadanía y operadores.

En abril de 2025, el Consejo de Seguridad Nacional aprobó el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad, decisión que fue publicada oficialmente en el BOE el 26 de mayo de 2025. Esta aprobación marca el inicio de la actualización del marco estratégico vigente desde 2019, impulsada por el notable incremento en la sofisticación de las amenazas, la expansión de la ciberdelincuencia y la necesidad de adaptarse a nuevos desafíos tecnológicos, incluida la inteligencia artificial y la transposición de la Directiva NIS2. El acuerdo establece un proceso participativo liderado por el Consejo Nacional de Ciberseguridad y apoyado por un grupo técnico con representación de administraciones, sector privado, sociedad civil y expertos, con el objetivo de definir una estrategia alineada con las políticas europeas y orientada a reforzar la resiliencia nacional en un entorno digital cada vez más complejo.

Capacidades nacionales en Ciberseguridad

En 2025 se ha consolidado el despliegue y operación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS-AGE), previsto en la Medida 9 del Plan de Digitalización de las Administraciones Públicas 2021–2025. Este servicio compartido y centralizado ofrece capacidades de prevención, protección, detección, respuesta, asesoramiento e intervención ante incidentes, mejorando la eficacia mediante economías de escala y una gestión unificada.

La Agencia Estatal de Administración Digital (AEAD) ejerce la dirección técnica y estratégica del COCS-AGE, mientras que el CCN aporta capacidades de despliegue, operación, herramientas especializadas y respuesta experta ante incidentes complejos. En 2025, el COCS-AGE ha alcanzado la certificación ENS de categoría ALTA, un hito especialmente relevante dada su complejidad y alcance, y que se suma a la certificación “ALTA” del servicio Cloud de NubeSARA. Con ello, la AEAD refuerza su papel como referencia estratégica en infraestructuras de Administración Digital. En términos de despliegue, en 2025 el COCS-AGE ha alcanzado 27 servicios de ciberseguridad ofrecidos a 131 entidades integradas en el COCS-AGE, que protegen a más de 200.000 usuarios, lo que supone un 125% de servicios disponibilizados en relación con las previsiones iniciales de despliegue; a lo anterior se añaden más de 198.000 servidores y puestos personales monitorizados por el agente de seguridad de punto final EDR que supone un 132% en relación con las previsiones iniciales.

En paralelo, se ha avanzado en el despliegue del Centro de Operaciones de Ciberseguridad para Entidades Locales (COCS-EELL), dirigido a entidades de menos de 50.000 habitantes (excepto capitales de provincia).

El CCNCERT mantiene y opera el **Sistema de Alerta Temprana (SAT)**, una infraestructura de detección en tiempo real que identifica comportamientos anómalos e intrusiones en los sistemas y redes de los organismos públicos. El SAT se compone de sondas distribuidas, cuyos eventos se correlacionan en un sistema central que emite avisos inmediatos a los organismos conectados. Actualmente, el SAT permite detectar amenazas tanto en conexiones a internet (SATINE) como en redes operacionales (SATICS).

Asimismo, el CCN contribuye al desarrollo de políticas de actualización tecnológica en instituciones científicas como el CSIC, apoyando la implantación progresiva del Esquema Nacional de Seguridad mediante pruebas piloto, iniciativas de formación, campañas de concienciación y asesoramiento técnico.

De igual modo, el CCN es responsable de la **Red Nacional de SOC (RNS)**, principal plataforma de intercambio de alertas de ciberamenazas activas. Con 283 organismos adheridos, 114 proveedores de seguridad gestionada y 23 compañías privadas, la red comparte unas 400 alertas diarias, consolidándose como un modelo nacional e internacional de colaboración público-privada.

En el ámbito de ciudadanos y empresa, el Ministerio de Transformación Digital y de la Función Pública, a través de INCIBE y su servicio de identificación proactiva ha emitido “durante 2025” 7.708 avisos y alertas de incidentes, y amenazas de ciberseguridad. Los tipos de avisos más frecuentes notificados por este servicio continúan siendo los relacionados con el alojamiento de sitios web de *phishing*, que representan el 63% del total. A pesar de haber experimentado una ligera disminución del 3% en comparación con el año anterior, este tipo de amenaza sigue siendo la predominante. Le siguen las alertas de detección de campañas de SPAM, que constituyen el 27% del total de los avisos emitidos. Finalmente, cabe destacar las alertas relacionadas con dominios identificados como maliciosos,

comprometidos o potencialmente fraudulentos dentro del ámbito español, las cuales representan el 9,3% del total de notificaciones realizadas.

Como parte del operativo especial de Ucrania se han emitido durante 2025, hasta el 31 de octubre, 279 avisos y alertas de incidentes, que incluyen información de 4.914 eventos distintos de ciberseguridad.

Dentro del servicio CNA (Autoridad de Numeración de CVE -*Common Vulnerabilities and Exposures*), durante 2025 se han gestionado un total de 243 casos con múltiples notificaciones, publicándose 415 nuevos CVE correspondientes a nuevas vulnerabilidades. Además, en el rol de INCIBE de CNA-ROOT, los 9 CNA coordinados y supervisados por INCIBE a través de su CERT gestionaron un total de 6 nuevas vulnerabilidades durante el mismo periodo.

Durante 2025 el servicio de Alerta Temprana de INCIBE ha difundido un total de 933 avisos de seguridad a través de la página web así como por distintos canales de RRSS, con la siguiente distribución: 84 avisos de seguridad dirigidos para la ciudadanía, 76 avisos de seguridad para empresas, 409 avisos de seguridad para profesionales IT y 364 avisos de seguridad para profesionales en SCI (Sistemas de Control Industrial); difundiéndose además por diferentes boletines por correo electrónico. Además, se han generado 13 alertas *ad-hoc* ante amenazas de especial relevancia para operadores y entidades estratégicas españolas.

El servicio de Tiresias, durante el 2025, lleva remitidos 1.933 informes de exposición, dando servicio a 166 entidades.

El servicio ICARO de intercambio de ciberamenazas cuenta con más de 149.500 eventos de información y da servicio a 121 entidades españolas.

Dentro del Servicio *Antibotnet* de INCIBE, a lo largo del 2025 se han proporcionado un total de 542.046 evidencias a los ISPs involucrados en el servicio. A partir de estas evidencias se ha notificado de una posible infección a un total de 4.451 usuarios únicos (8.952 usuarios si se contabilizan las notificaciones reiteradas).

Desde el ámbito de Defensa se promueve un contacto estrecho y continuo con las Fuerzas y Cuerpos de Seguridad del Estado mediante la integración de oficiales de enlace de la Guardia Civil y del Cuerpo Nacional de Policía. Asimismo, se mantiene una cooperación activa con los CERT nacionales, CCNCERT, INCIBECERT y ESPDEF CERT, mediante el intercambio permanente de información, el trabajo coordinado en grupos especializados y la participación en proyectos conjuntos.

El Mando Conjunto del Ciberespacio (MCCE), actuando como ESPDEF CERT, participa habitualmente en dispositivos de ciberseguridad nacionales.

Aunque persiste el reto de lograr una coordinación estatal completamente integrada ante amenazas complejas, los esfuerzos conjuntos del ámbito público y privado continúan avanzando para comprender mejor la naturaleza de la amenaza y desarrollar herramientas más eficaces de respuesta y resiliencia.

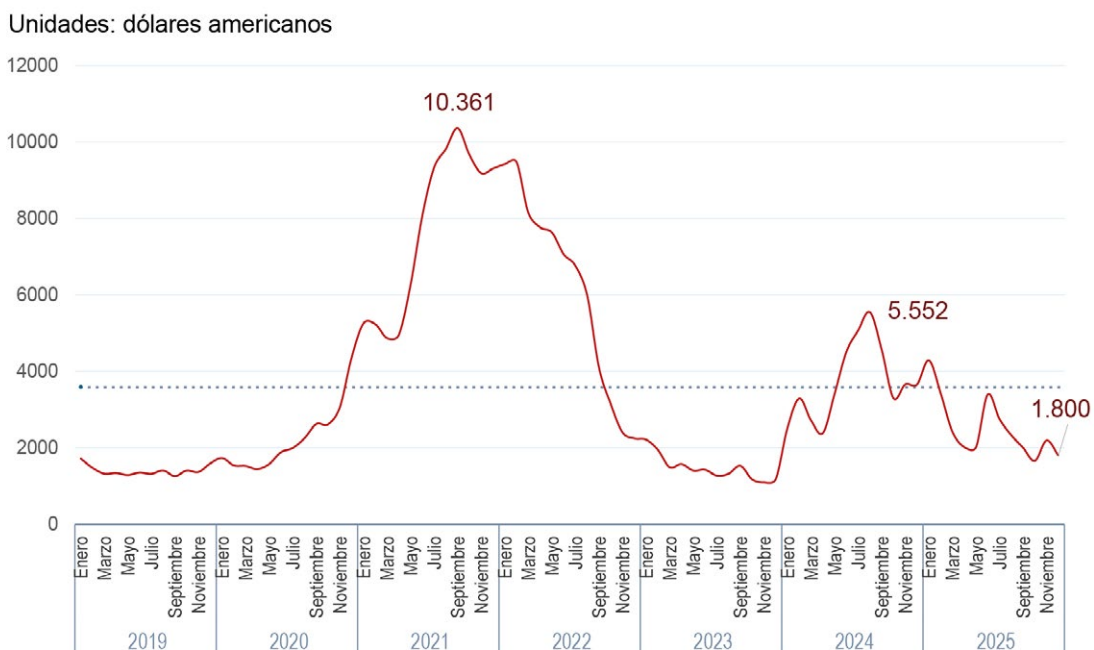
VULNERABILIDAD DEL ESPACIO MARÍTIMO

- Aunque la piratería en el Cuerno de África ha disminuido significativamente gracias a la operación Atalanta de la UE, que España lidera, persisten riesgos esporádicos que afectan la navegación comercial.
- La protección de los cables submarinos es una de las principales preocupaciones en lo que respecta a las amenazas híbridas y su proyección en los espacios marítimos.
- El año 2025 ha marcado un punto de inflexión respecto a la gobernanza marina global con la adopción del Pacto Europeo por los Océanos y el avance en el proceso de ratificación del Tratado de Alta Mar, que han sentado las bases para una mejor protección de las aguas internacionales.

VULNERABILIDAD DEL ESPACIO MARÍTIMO

Amenazas a las rutas marítimas internacionales

Tras la elevada volatilidad de 2024, marcada por aumentos significativos en las tarifas de flete debido a la inseguridad en el Mar Rojo, 2025 muestra señales del comienzo de regreso a la normalidad. El movimiento hutí anunció el 12 de octubre de 2025 que detendría los ataques contra territorio israelí y contra los buques en el mar Rojo, una vez firmada la tregua por Hamás y avanzando sus fases de implementación con Israel, no sin dificultades, en la Franja de Gaza. De esta forma, el 2025 puede considerarse un año de corrección gracias a la estabilización del mercado a raíz de ajustes operativos de las navieras, una mayor coordinación en la gestión de rutas y mejoras en la seguridad de algunas zonas estratégicas. Estos factores han permitido una disminución progresiva de las tarifas de flete de contenedores. (Figura 9.1)



Fuente: Elaboración del DSN con datos del Freightos Baltic Index (FBX)

Figura 9.1: Evolución del Índice mundial de tarifas de flete de contenedores (dólares americanos)

Por otra parte, la Flota Fantasma rusa constituye una plataforma desde la que Rusia puede impulsar acciones híbridas capaces de comprometer la seguridad de infraestructuras y rutas estratégicas. Al tiempo, el Golfo de Guinea y la costa occidental de África permanecen expuestos a piratería, redes de contrabando de personas, armas y drogas, muchas con origen en el Caribe y destino a Europa. Aunque la piratería en el Cuerno de África ha disminuido significativamente gracias a la operación Atalanta de la UE, persisten riesgos esporádicos que afectan la navegación comercial.

En relación con la invasión de Ucrania, el 18 de diciembre de 2025, el Consejo de la Unión Europea impuso medidas restrictivas a otros 41 buques que forman parte de la flota clandestina de petroleros de Rusia y contribuyen a los ingresos de Rusia procedentes de la energía. Esta medida va dirigida a los buques cisterna no pertenecientes a la UE que forman parte de la flota clandestina de Putin que elude el mecanismo de limitación de los precios del petróleo o apoya al sector energético de Rusia, o a los buques que transportan equipos militares para Rusia o cereales y bienes culturales ucranianos robados. Esta decisión eleva el número de buques en la lista hasta casi los 600.

En cuanto a las consecuencias para España, en 2025 se ha mantenido el nivel de protección marítima para todos los buques de pabellón español que naveguen en aguas del Mar Negro al Nivel 2 del Código PBIP, que fue acordado con fecha 4 de marzo de 2022 por la Secretaría de Estado de Seguridad, con ocasión de la agresión rusa contra Ucrania.

Implicaciones para la seguridad marítima de la inestabilidad en el Mediterráneo

La Estrategia Nacional de Seguridad Marítima 2024 declara el Mediterráneo como un espacio marítimo de interés para España. En este sentido, en 2025, la Armada ha contribuido a las agrupaciones navales permanentes de la OTAN en el Mediterráneo Oriental (SNMG-2 y SNMCMG-2), con la integración de la fragata “Álvaro de Bazán” y los buques de aprovisionamiento de combate “Patiño” y “Cantabria”, durante un periodo de tres meses cada uno, así como de los cazaminas “Duero” y “Sella”, también por periodos de tres meses. Por otro lado, se ha contribuido a la Operación *Sea Guardian* de la OTAN, que tiene como principal objetivo la seguridad marítima en el mar Mediterráneo, con la participación de las fragatas “Reina Sofía” y “Canarias”, por periodos de 35 días, y los submarinos “Galerna” e “Isaac Peral”, por periodos de 90 días.

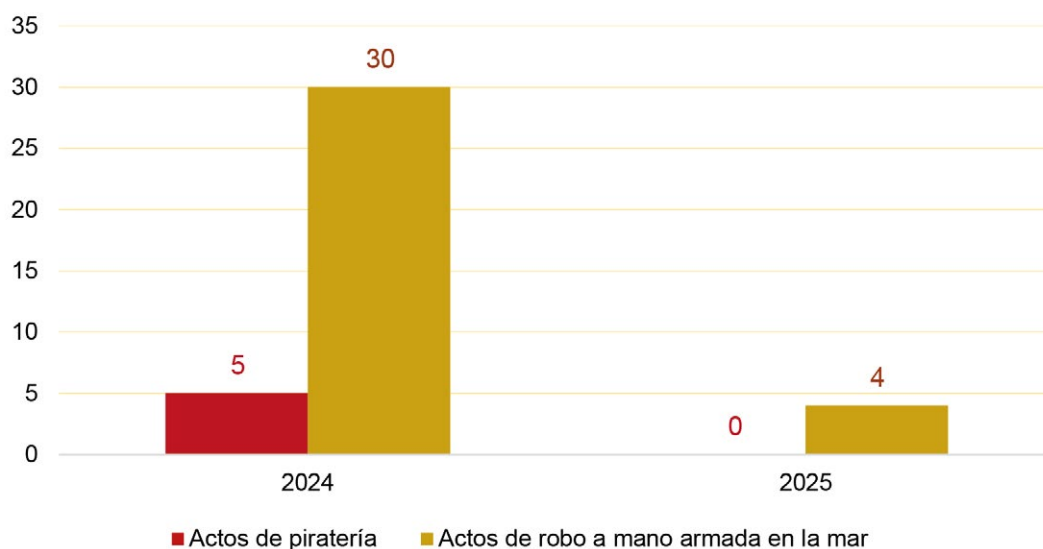
La inestabilidad en estas zonas supone un aumento de la presión operativa en el Mediterráneo occidental y el Estrecho de Gibraltar. La posibilidad de desbordamiento de rutas migratorias, el riesgo de infiltración de actores terroristas y la afectación de rutas comerciales obligan a reforzar la vigilancia, intensificar la cooperación internacional y a mantener la capacidad de respuesta rápida ante posibles incidentes de seguridad o emergencias humanitarias.

Por otra parte, la inestabilidad en el Mediterráneo Oriental está ligada a la explotación de recursos y a la delimitación de las Zonas Económicas Exclusivas (ZEE), donde contrastan las diferentes interpretaciones entre países ribereños.

Cuerno de África y golfo de Adén

La situación de seguridad en el golfo de Adén y la cuenca de Somalia se caracteriza por la amenaza relativa a la piratería y el robo armado en la mar en aguas somalíes. En 2025, se han producido cuatro casos de robo a mano armada en las aguas territoriales somalíes, sobre embarcaciones de pesca que son utilizadas posteriormente para llevar a cabo ataques sobre mercantes, como el acaecido sobre el buque “Hellas Aphrodite”, el 6 de noviembre, que fue asaltado a 700 millas de la costa de Mogadiscio y liberado en unas horas, al no poder acceder los piratas a la ciudadela donde se había refugiado la tripulación, y tras la presión ejercida por las unidades de la operación “Atalanta” de la Unión Europea. Estas cifras están muy por debajo de los incidentes acaecidos en 2024, donde se confirmaron 5 actos de piratería y 30 de robo armado en la mar en aguas de Somalia. Estos ataques siguen siendo más habituales en los periodos intermonzónicos, donde las condiciones meteorológicas son más favorables.

Por otro lado, la amenaza yihadista de Al-Shabaab es la principal amenaza de la región, presentando un grave riesgo para la seguridad en Somalia. No obstante, y a pesar de que este grupo terrorista controla algunas áreas costeras en el sur del país, no constituye una amenaza relevante para el dominio marítimo. Además de ostentar el mando operacional de Atalanta, España mantiene una presencia permanente. En el año 2025, se han desplegado en el área las fragatas “Santa María”, “Victoria”, “Reina Sofía” y “Navarra”, incluyendo la capacidad de helicóptero, medios aéreos no tripulados y equipos de operaciones especiales. Todo lo anterior junto al destacamento Orion, desplegado en Yibuti. (Figura 9.2)



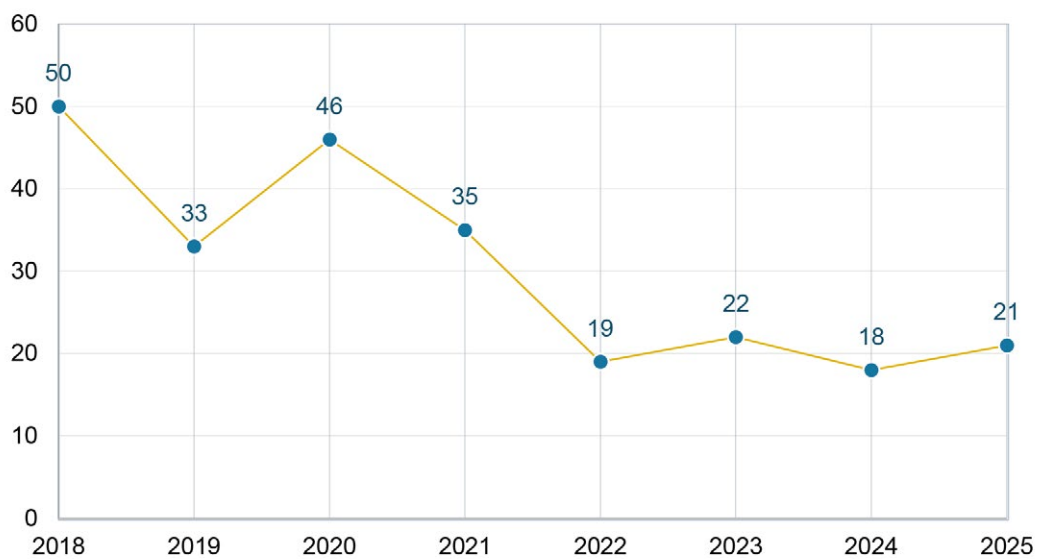
Fuente: Elaboración del DSN con datos proporcionados desde el Ministerio de Defensa

Figura 9.2: Actos de piratería y robo a mano armada en la mar (2024 y 2025)

En cuanto al Mar Rojo, la situación mejoró levemente tras el alto el fuego en Gaza y la menor actividad de los hutíes en Yemen. No obstante, existen otros focos de tensión en la zona que pueden afectar a la seguridad: la aproximación entre Sudán (en guerra civil desde 2023) e Irán, así como la ambición rusa para incrementar su influencia mediante un acuerdo firmado en febrero de 2025 para establecer una base naval en Port Sudán. También destaca la intención de Etiopía por recuperar una salida al Mar Rojo, que perdió tras la independencia de Eritrea, y que motivó movimientos de tropas etíopes en marzo.

Amenazas a la seguridad marítima en el Golfo de Guinea y la costa occidental de África

La piratería y el robo a mano armada en la mar siguen constituyendo una de las principales amenazas en el golfo de Guinea. En 2025, el número de ataques parece estabilizarse, con 21 incidentes registrados según el informe de la ICC *International Maritime Bureau*. La progresión hacia la costa del Golfo de Guinea de la influencia rusa y de la presencia de contingentes armados patrocinados por su gobierno es motivo de preocupación. (Figura 9.3)



Fuente: Elaboración del DSN con datos de ICC International Maritime Bureau

Figura 9.3: Ataques de piratería en el Golfo de Guinea

La Armada está presente en la costa occidental africana y, en particular, en el Golfo de Guinea durante la mayor parte del año, participando en la iniciativa de la Unión Europea denominada “Presencias Marítimas Coordinadas”, por la que se tratan de sincronizar todos los esfuerzos de los países miembros de la UE en la región, fomentar el intercambio de información y apoyar a los países ribereños en el desarrollo de sus capacidades de seguridad y defensa. Durante las visitas a puerto (desde Mauritania, Senegal y Cabo Verde, hasta Angola, incluyendo Nigeria, Ghana, Gabón, Camerún, Benín y Costa de Marfil) se realizan actividades de cooperación militar, así como diversas iniciativas en el ámbito de la diplomacia de defensa.

Las Fuerzas y Cuerpos de Seguridad del Estado participan en la zona en labores de cooperación internacional, intercambio de inteligencia y apoyo logístico a misiones europeas, contribuyendo con capacidades navales a la detección de buques sospechosos y al control de mercancías procedentes de zonas de alto riesgo que arriban a puertos españoles; y mediante personal en tierra colaboran en el marco del control de la migración en los destacamentos que tiene ubicados en países de la costa occidental de África como Mauritania, Gambia o Senegal.

Amenazas híbridas para las infraestructuras marítimas

El 86% de las averías producidas en las infraestructuras submarinas se relaciona con actividades de pesca y fondeo de embarcaciones. Los fenómenos naturales (corrientes o actividad sísmica submarina) representan el 11%, mientras que los fallos de instalación suponen el 3%.

El tiempo medio de reparación de averías en el Atlántico y el Mediterráneo oscila entre 7 y 20 días, debido a procesos que incluyen permisos, preparación de buques y pruebas. A pesar del aumento de cables desplegados, el número de fallos en Europa ha disminuido un 7% anual, pasando de 56 en 2020 a 41 en 2024.

Las principales infraestructuras en España se encuentran en:

- **Mediterráneo:** Esta región cuenta con el mayor número de cables submarinos intracomunitarios, 37 en total, con una capacidad total de 811 Tbit/s. El Proyecto Medusa, con una inversión de 342 millones de euros y respaldado por la UE y el Banco Europeo de Inversiones, constituye una infraestructura estratégica que conectará 11 países, entre ellos España, mediante 21 puntos de amarre y alcanzará una capacidad de 480Tbit/s, cuadruplicando la capacidad actual de la región. Se prevé que parte de la red esté operativa en 2026.
- **Atlántico Sur:** La región cuenta con una elevada presencia de cables submarinos que enlazan Portugal y España con países de África occidental y meridional. En el caso de España los cables conectan la península ibérica con Canarias y los que interconectan las islas, con una capacidad total de 6 Tbit/s, son propiedad de Canalink y Telefónica.

La protección de los cables submarinos es una de las principales preocupaciones en lo que respecta a las amenazas híbridas y su proyección en los espacios marítimos, habida cuenta del actual panorama de seguridad. Esta amenaza es particularmente intensa en aguas del mar Báltico, en el contexto de la invasión de Ucrania por la Federación Rusa. De tal forma que, en enero de 2025, la OTAN lanzó en enero la operación *Baltic Sentry* (Centinela del Báltico) con despliegue de buques, aeronaves y sistemas no tripulados, para la protección de esta infraestructura marítima.

También en el plano internacional, en 2024, la Comisión Europea aprobó la *Recomendación (UE) 2024/779 para reforzar la seguridad y resiliencia de las infraestructuras de cables submarinos*. Como parte de esta iniciativa, se creó un Grupo informal de expertos sobre infraestructuras de cables submarinos con representación de todos los Estados miembros, destinado a coordinar esfuerzos, asesorar a la Comisión y facilitar el intercambio seguro y eficaz de información. España participa en este Grupo a través del Ministerio para la Transformación Digital, que ostenta la representación nacional.

Posteriormente, en 2025, la Comisión Europea publicó un informe que incluye cartografía, evaluación de riesgos y pruebas de estrés de las infraestructuras de cables submarinos. Este informe fue preparado y acordado con los Estados miembros, en el marco del citado Grupo de Expertos creado bajo la *Recomendación de la Comisión (UE) 2024/779 sobre infraestructuras submarinas de cable seguras y resilientes*. El informe identifica como principales amenazas a las infraestructuras de cables submarinos de la UE tanto ataques intencionados (sabotaje físico, intrusiones cibernéticas, ataques a la cadena de suministro, acciones de actores estatales y no estatales, y amenazas híbridas o de “zona gris”) como daños no intencionados (actividades humanas como pesca, anclaje, obras civiles, minería submarina, y fenómenos naturales como terremotos, volcanes, corrientes marinas o tormentas). Entre las vulnerabilidades destacan la insuficiente seguridad física y cibernética en puntos críticos (estaciones de aterrizaje, centros de operación), la falta de redundancia, la exposición pública de la localización de

infraestructuras, la carencia de sistemas avanzados de monitorización y la dependencia de equipos y componentes no europeos.

Los riesgos se agravan por dependencias estratégicas de la UE respecto a proveedores y tecnologías de terceros países (Estados Unidos, China, Reino Unido, Rusia), la concentración del tráfico en rutas y puntos geográficos críticos (como el Mar Rojo), la escasez de capacidad de mantenimiento y reparación, la falta de coordinación y planes de respuesta entre Estados miembros y la necesaria cooperación con otros estados (Turquía) para asegurar y estabilizar zonas estratégicas (Mar Negro y Mediterráneo). El informe define siete escenarios de riesgo principales, que incluyen sabotajes coordinados, ataques a estaciones de aterrizaje, cortes de energía, interrupciones en la capacidad de mantenimiento o suministro, daños accidentales y eventos naturales, subrayando que la combinación de amenazas, vulnerabilidades y dependencias puede provocar interrupciones graves en la conectividad y la economía digital europea). Asimismo, el informe proporciona una guía dirigida a los Estados miembros y los operadores de infraestructuras críticas para desarrollar pruebas de estrés y aplicar indicadores de resiliencia para infraestructuras de cable submarino.

Esta guía se alinea, entre otros, con el manual para tests de estrés cibernéticos de ENISA (2025) y la metodología aplicada en el sector energético.

El Grupo de Expertos trabajó durante el año 2025 en la elaboración de un informe para ofrecer una Caja de Herramientas de Seguridad de Cables con medidas de mitigación, en respuesta a los resultados de la evaluación de riesgos de la UE; y una lista prioritaria de Proyectos de Cable de Interés Europeo (CPEI), a priorizar para el apoyo público futuro, como en el marco del Mecanismo de Conexión a Europa (CEF) y otros programas. (NOTA: este informe ha sido publicado en febrero de 2026).

Financiación de proyectos para proteger las infraestructuras submarinas

El Centro Europeo de Competencia en Ciberseguridad ha publicado en 2025 una convocatoria de 10 millones de euros dedicada al establecimiento de Centros Regionales de Cable, financiada bajo el Programa de Europa Digital. Los Centros Regionales de Cable apoyarán la monitorización y detección de amenazas a los cables submarinos agregando los datos e información relevantes, desarrollarán análisis de amenazas basados en IA para establecer una imagen situacional casi en tiempo real y permitirán una respuesta más rápida en caso de incidentes. El objetivo es financiar un centro por cuenca marítima. La Comisión está trabajando con todos los Estados miembros interesados en los *Hubs*, con especial atención a la región nórdica del Báltico, que será un banco de pruebas para dicha infraestructura.

Además, el Centro está lanzando una campaña de 10 millones de euros para apoyar la preparación y la puesta a prueba de estrés de la resiliencia de infraestructuras críticas, bajo la *Ley de Solidaridad Cibernética*.

Un total de 51 proyectos de *Digital Global Gateways* han sido financiados bajo convocatorias digitales de CEF, por un total de 420 millones de euros, con una nueva oleada de proyectos cuya convocatoria se realizará en el primer cuatrimestre de 2026.

A nivel nacional, en 2025, el Grupo de Trabajo para la Vigilancia, Protección y Resiliencia de las Infraestructuras Marítimas, dependiente del Consejo Nacional de Seguridad Marítima, se ha reunido en cuatro ocasiones con dos objetivos prioritarios: la elaboración de un análisis de riesgos sobre las

infraestructuras marítimas, especialmente las submarinas, en áreas de interés prioritario, y definir y desarrollar un plan de vigilancia que garantice su protección.

Por su parte, la actividad de la flota fantasma en España se focaliza en aguas cercanas al archipiélago de las islas Canarias y en el tránsito por el mar de Alborán y por el estrecho de Gibraltar. Se trata, habitualmente, de buques de transporte de hidrocarburos que se dedican a transbordar (de buques pequeños a buques de mayor porte) petróleo crudo y refinados de origen ruso, aunque también venezolano e iraní, para luego ser transportado a países asiáticos. En el último año, se ha quintuplicado la presencia de barcos rusos transitando próximos a las costas canarias. El COVAM monitoriza este tipo de buques e informa de una media de 50 buques semanales, tomando como criterio la lista de buques sancionados por la UE. La posibilidad legal de actuar contra los buques de la flota fantasma en la mar es un asunto de difícil resolución.

Estos buques también pueden emplearse en actividades ilícitas o incluso en acciones de sabotaje contra infraestructuras críticas. Por tal motivo las Fuerzas y Cuerpos de Seguridad del Estado intensifican la vigilancia de zonas sensibles mediante sus capacidades navales, como gasoductos submarinos, puertos y áreas de fondeo, empleando sistemas como el SIVE, sensores costeros y patrullas oceánicas, además de cooperar con la Armada y la Agencia Europea de Seguridad Marítima (EMSA) en la identificación de flotas fantasmas y el control del tráfico marítimo anómalo.

Degradación medioambiental y efectos del cambio climático en el medio marino

La degradación ambiental del medio marino es una realidad y supone un riesgo y amenaza a la seguridad marítima, en tanto los efectos de esta degradación ambiental tienen una incidencia directa en la seguridad marítima. Un ejemplo de escala global es la disminución de tráfico por el Canal de Panamá y la consecuente reorientación de rutas marítimas a consecuencia de la sequía del canal.

En este sentido, el año 2025 ha marcado un punto de inflexión en la gobernanza marina global. La adopción del *Pacto Europeo por los Océanos*, el 9 de junio, y el avance en el proceso de ratificación del *Tratado de Alta Mar* han sentado las bases para una mejor protección de las aguas internacionales.

En el ámbito económico y estratégico, el *Pacto por los Océanos* redefine el concepto de Economía Azul al integrar la sostenibilidad ambiental con la seguridad nacional y alimentaria. La movilización de recursos financieros, que superan los 8.700 millones de euros a nivel global, está orientada a transformar industrias tradicionales como la pesca y el transporte marítimo hacia modelos de bajas emisiones. Este enfoque reconoce que la salud de los ecosistemas marinos es intrínseca a la resiliencia económica de las naciones costeras, promoviendo una infraestructura marítima más segura y tecnológicamente avanzada frente a los desafíos geopolíticos actuales. No obstante, estos avances institucionales se enfrentan a una realidad climática alarmante, marcada por el noveno año consecutivo de temperaturas oceánicas récord.

En España, para abordar estas presiones, desde las distintas unidades del Ministerio para la Transición Ecológica y el Reto Demográfico se llevan a cabo actuaciones conducentes a mejorar el estado ambiental del medio marino y la ordenación sostenible de los sectores marítimos, proteger la biodiversidad marina, y luchar contra el cambio climático.

Tráficos ilícitos por vía marítima

La seguridad marítima se encuentra ante amenazas crecientes, debido a nuevas modalidades de transporte ilícito de mercancías que, requiriendo alteraciones estructurales de los cascos, incrementan el riesgo de accidentes y de contaminación marítima. Surgen nuevas modalidades delictivas con el fin de prestar apoyo logístico a los narcotraficantes, como el abastecimiento de combustible a narco embarcaciones en alta mar. El incremento del uso de embarcaciones rápidas, buques nodriza, recientes avistamientos e incautación de narco-submarinos y rutas alternativas exige una respuesta integral basada en inteligencia, patrullas combinadas, y cooperación con la Vigilancia Aduanera, la Armada y cuerpos policiales internacionales.

En particular, a lo largo del 2025 se constató el incremento de informes internacionales sobre embarcaciones semi-sumergibles para el transporte transoceánico de grandes volúmenes de drogas, con rutas no tradicionales que eluden sistemas de vigilancia estándar, así como el incremento de embarcaciones semirrígidas de alta velocidad (RHIB) transportando cocaína en la zona central de Atlántico Norte. Estas embarcaciones navegan sin luces y a altas velocidades, lo cual supone un gran peligro a la navegación y a la seguridad marítima.

Las zonas del Estrecho de Gibraltar y del arco Canarias-Atlántico presentan una vulnerabilidad creciente para España. Algunos grupos organizados podrían estar utilizando las rutas y medios originalmente diseñados para el tráfico de drogas para realizar actividades vinculadas a la inmigración ilegal, diversificando de esta manera su actividad delictiva. En concreto, desde el COVAM se ha informado de más de 600 embarcaciones tipo *go-fast*, sospechosas de llevar a cabo operaciones relacionadas con el tráfico de estupefacientes, principalmente en el área del estrecho de Gibraltar.

La *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2025* considera uno de los puntos clave en esta amenaza el narcotráfico en puertos y aeropuertos, señalando factores como la corrupción como multiplicador delictivo, enfoque que resulta crucial en el comercio marítimo que canaliza cerca del 90% del comercio mundial. Esta vía es un instrumento esencial para las actividades vinculadas al crimen organizado, lo que posiciona a los puertos en *hubs* logísticos clave para las organizaciones criminales y, en consecuencia, la infiltración portuaria por parte de estas redes representa una de las mayores amenazas para la economía legal y la seguridad nacional.

Asimismo, debe contemplarse el riesgo de utilización de la vía marítima, tanto para el transporte ilícito de materiales, productos o tecnologías vinculados a la proliferación de armas de destrucción masiva, como para la elusión de regímenes internacionales de sanciones. El carácter global del comercio marítimo, la complejidad de las cadenas logísticas, el recurso a pabellones de conveniencia, las transferencias buque a buque, la manipulación de sistemas de identificación automática (AIS) o el empleo de estructuras societarias opacas —como se ha evidenciado en relación con la denominada “flota fantasma” vinculada a la Federación Rusa— pueden dificultar la trazabilidad de los cargamentos y la identificación de los beneficiarios finales. Estos riesgos tienen especial importancia en España, debido a su posición geoestratégica y al papel de sus puertos como nodos esenciales del comercio internacional.

El Departamento de Aduanas e Impuestos Especiales de la Agencia Estatal de Administración Tributaria (AEAT) y el Servicio Marítimo de la Guardia Civil han reforzado su presencia operativa ante el incremento de amenazas híbridas que afectan a infraestructuras críticas portuarias y a la cadena logística marítima. Como respuesta, se han desplegado tecnologías avanzadas de geolocalización, monitorización en tiempo real y colaboración operativa con los organismos europeos.

A este respecto, se considera también la necesidad de adaptar el marco normativo internacional, por ejemplo de la Convención de las Naciones Unidas sobre el Derecho del Mar (UNCLOS), para

permitir el ejercicio del derecho de visita ante una sospecha fundada de tráfico ilícito (artículo 110) y la incorporación en la legislación marítima internacional de disposiciones similares a las 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.

La Policía Nacional y la Guardia Civil participan en el “Proyecto de cooperación portuaria” (SEACOP VI), financiado por la Comisión Europea, cuyo objetivo es apoyar la lucha contra el tráfico marítimo ilícito (sustancias estupefacientes, especialmente cocaína) y las redes criminales internacionales en América Latina y el Caribe.

El tráfico de cocaína sigue siendo la principal actividad delictiva de los grupos de delincuencia organizada con actividad en España. El liderazgo de estos grupos se mantiene en manos de colombianos, si bien es muy significativo el avance de grupos de albaneses y dominicanos.

Además de Madrid y Barcelona, existen principalmente tres zonas de actividad prioritaria: la vertiente atlántica de Galicia (sobre todo Pontevedra), la zona más próxima al Estrecho de Gibraltar (Cádiz y Málaga) y la vertiente mediterránea (Valencia, Alicante y Murcia). La presión policial en las zonas afectadas por el Plan Estratégico de Seguridad para el Campo de Gibraltar ha provocado la redistribución geográfica de las organizaciones criminales que operan en la zona hacia otras limítrofes.

Los buques de la Armada también contribuyen a luchar contra este fenómeno, particularmente, mediante la colaboración con el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), del Ministerio del Interior, en la ejecución de operaciones de lucha contra este tipo de tráfico ilícito. Para ello, se despliegan buques con objeto de seguir, interceptar y asaltar las embarcaciones sospechosas de realizar actividades vinculadas con el narcotráfico.

Pesca ilegal, no declarada y no reglamentada

La pesca ilegal, no declarada y no reglamentada (INDNR), constituye una amenaza directa para la sostenibilidad de los recursos marinos, la economía pesquera legal y la seguridad marítima. Además, provoca un impacto muy significativo sobre los recursos naturales y sobre las poblaciones de especies pesqueras vulnerables, hasta el punto de poner en riesgo su continuidad y alterar el equilibrio de los ecosistemas marinos. Se caracteriza por el uso de buques sin identificación, transbordos ilegales, documentación falsificada y aparejos prohibidos, operando con frecuencia con el Sistema de Identificación Automática (AIS) apagado o bajo banderas de conveniencia. La detección y el control de estas actividades son esenciales para proteger la biodiversidad marina y asegurar que el pescado que llega al consumidor sea legal y sostenible.

En la Secretaría General de Pesca del Ministerio de Agricultura, Pesca y Alimentación, a través de las actuaciones llevadas a cabo en este año (1 enero 2025 – 31 diciembre 2025), tanto a nivel nacional como internacional destinadas a combatir la pesca INDNR, se han llevado a cabo 10.112 inspecciones, incluyendo todos los ámbitos de actuación: inspecciones portuarias, en la mar, avistamientos (incluyendo el empleo de drones), en mercados y/o instalaciones, de transporte, documentales, etc., que derivaron en unas 927 presuntas infracciones en materia de pesca marítima.

Por otra parte, desde la Secretaría General de Pesca, en este periodo, se han analizado 49.339 expedientes de importación de productos pesqueros y que se correspondieron a la solicitud de autorización de importación de unas 1.010.974 toneladas procedentes de 80 países ribereños.

Como resultado del control e inspección de estas importaciones, durante este periodo, desde la Secretaría General de Pesca se ha procedido a la denegación de 25 lotes de mercancía que ascendían a más de 681 toneladas de introducción de pescado ilegal en territorio español.

En este ámbito, la Guardia Civil, a través del Servicio de Protección de la Naturaleza (SEPRONA), ha desarrollado diversas operaciones frente a la pesca ilegal de atún rojo en el Mediterráneo, donde el *modus operandi* se basa en superar los cupos autorizados mediante la ocultación de capturas reales, el uso de asentamientos y pesajes no declarados, el desvío de parte de la producción a canales paralelos y la falsificación de documentación para presentar como legal un volumen de atún que en realidad excede las posibilidades de pesca asignadas.

El control de actividades pesqueras es fundamental para garantizar las sostenibilidades de los recursos marinos y evitar su sobre explotación. Por ello, la Guardia Civil continúa participando activamente en el Plan Anual de Control Integral de Actividades Pesqueras (PACIAP), efectuando el seguimiento y control del cumplimiento de la normativa pesquera en el mar, respecto de las artes y capturas, y la tenencia de especies con tallas inferiores a las reglamentadas.

En este contexto, en el año 2025, el Servicio Marítimo de la Guardia Civil ha realizado 2.502 inspecciones, de las cuales 1.614 lo son en el ámbito del PACIAP y los 888 restantes como policía administrativa. De todo ello se deduce un total de 780 infracciones administrativas en materia de pesca. (Figura 9.4)

Figura 9.4: Actuaciones realizadas por la Guardia Civil en el marco del programa anual de control integral de actividades pesqueras (PACIAP)

MESES	TOTAL PESCADO CONTROLADO	TOTAL PESCADO INCAUTADO	Nº TOTAL INFRACCIONES
ENERO	16.313,130	16.302,130	15
FEBRERO	7.540,560	5.647,560	15
MARZO	1.930,000	320,400	11
ABRIL	33.903,449	1.392,599	25
MAYO	17.712,490	8.953,420	88
JUNIO	120.211,840	117.335,640	51
JULIO	4.606,855	4.281,950	48
AGOSTO	4.653,150	1.553,150	21
SEPTIEMBRE	1.742,080	905,850	45
OCTUBRE	21.054,950	13.191,950	20
NOVIEMBRE	5.372,460	5.367,640	20
DICIEMBRE	5.553,100	113,100	7
TOTAL	240.594,064	175.365,389	366

Fuente: Servicio de Protección de la Naturaleza de la Guardia Civil

La Armada, en coordinación con la Secretaría General de Pesca, realiza despliegues en los principales caladeros donde operan buques españoles. En 2025, se han llevado a cabo los despliegues de los patrulleros “Alborán”, “Tarifa” y “Arnemendi”, tanto en caladeros nacionales del mar Mediterráneo y mar Cantábrico, como en campañas internacionales de vigilancia de pesca, como la NAFO (*Northwest Atlantic Fisheries Organization*), acumulando alrededor de 8 meses de navegación.

Asimismo, tanto en el marco de la operación “Atalanta”, en el océano Índico, como en los despliegues a lo largo de la costa occidental africana, los buques de la Armada llevan a cabo actividades de vigilancia y monitorización de la flota pesquera nacional; en ambas zonas la pesca ilegal es una realidad que puede afectar a los intereses nacionales.

Seguridad marítima y salvamento de la vida en el mar

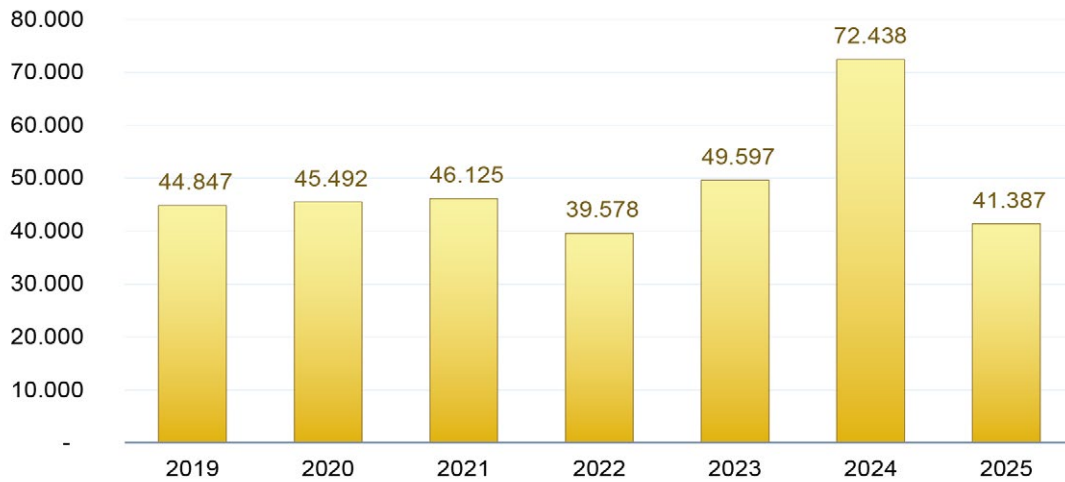
El 4 de febrero de 2025, el Consejo de Ministros aprobó el nuevo *Plan Nacional de Salvamento Marítimo 2025-2027*, con una inversión de 162,7 millones de euros para modernizar los medios de Salvamento Marítimo e impulsar la sostenibilidad. Este plan incluye la construcción de dos buques remolcadores, dos nuevas patrulleras de salvamento, seis embarcaciones ligeras de acción rápida, un helicóptero, un centro de coordinación en Palma de Mallorca y la incorporación de drones. El objetivo es fortalecer el sistema de respuesta a incidentes y accidentes marítimos, implementar nuevas tecnologías, reforzar la lucha contra el cambio climático y promover la seguridad y la protección de los mares y océanos.

La zona de búsqueda y salvamento asignada a España es tres veces el territorio nacional. (Figura 9.5)



Figura 9.5: Zonas de búsqueda y salvamento marítimo responsabilidad de España

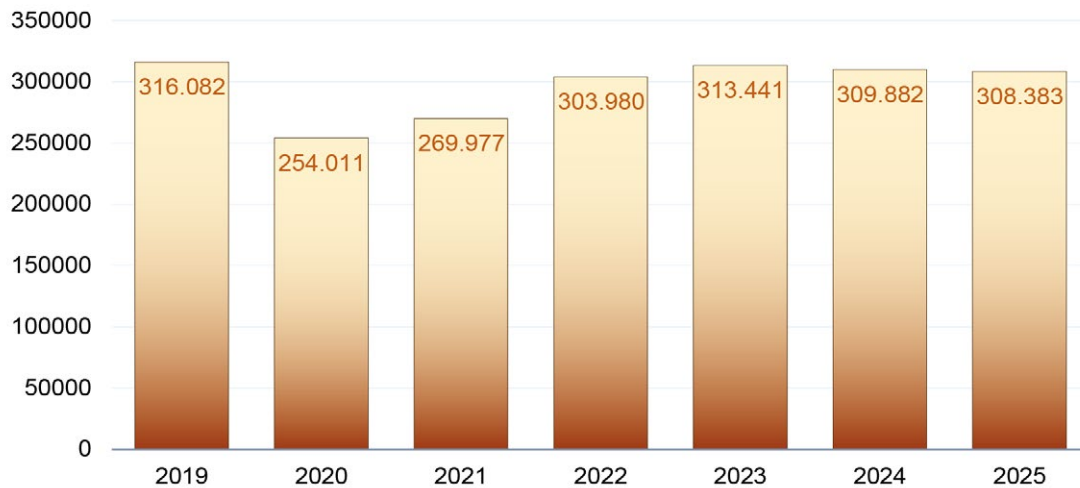
La Sociedad Española de Salvamento Marítimo (SASEMAR), ha coordinado durante el año 2025, el rescate, asistencia y búsqueda de 41.387 personas (una media de 113 personas al día), de las cuales 14.479 fueron rescatadas por las unidades propias de la Sociedad. En 2024 Salvamento Marítimo coordinó el rescate, la asistencia y búsqueda de 72.438 personas en peligro en la mar (198 al día), de los cuales 24.913 fueron rescatadas con las unidades propias de Salvamento. (Figura 9.6)



Fuente: SASEMAR

Figura 9.6: Rescate, búsqueda y asistencia de personas en la mar

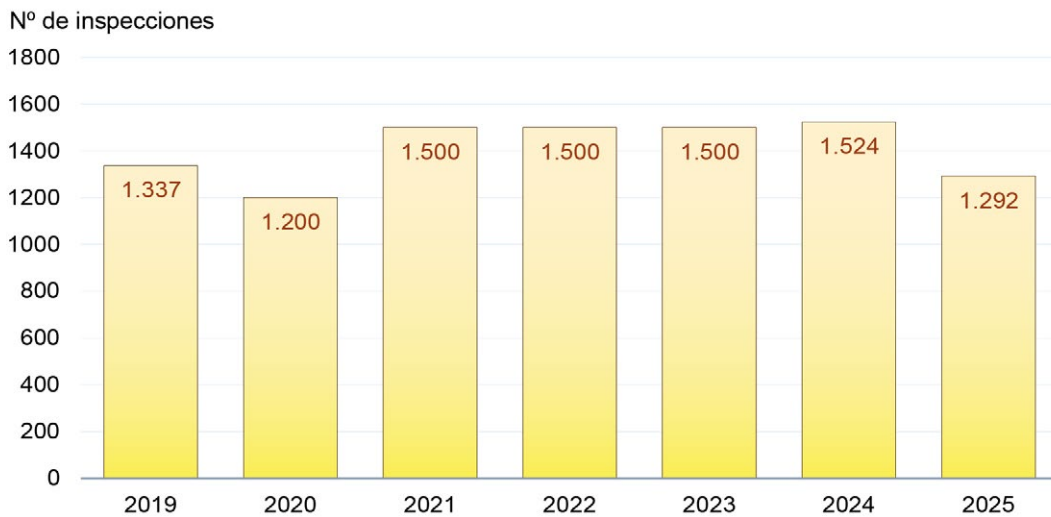
Por otro lado, Salvamento Marítimo vigila intensamente la superficie marina mediante aviones y satélites con objeto de prevenir posibles contaminaciones procedentes de barcos. Durante el año 2025, se ha vigilado una superficie igual a 226 millones de km², equivalente a 446 veces el territorio nacional.



Fuente: SASEMAR

Figura 9.7: Control de Tráfico Marítimo en España

Asimismo, con el fin de incrementar la seguridad marítima, Salvamento Marítimo supervisó en 2025 el tráfico de 308.383 buques tanto en los Dispositivos de Separación de Tráfico como en las zonas portuarias. (Figura 9.7)



Fuente: SASEMAR

Figura 9.8: Inspecciones a buques mercantes de pabellón extranjero en puerto o fondeaderos españoles

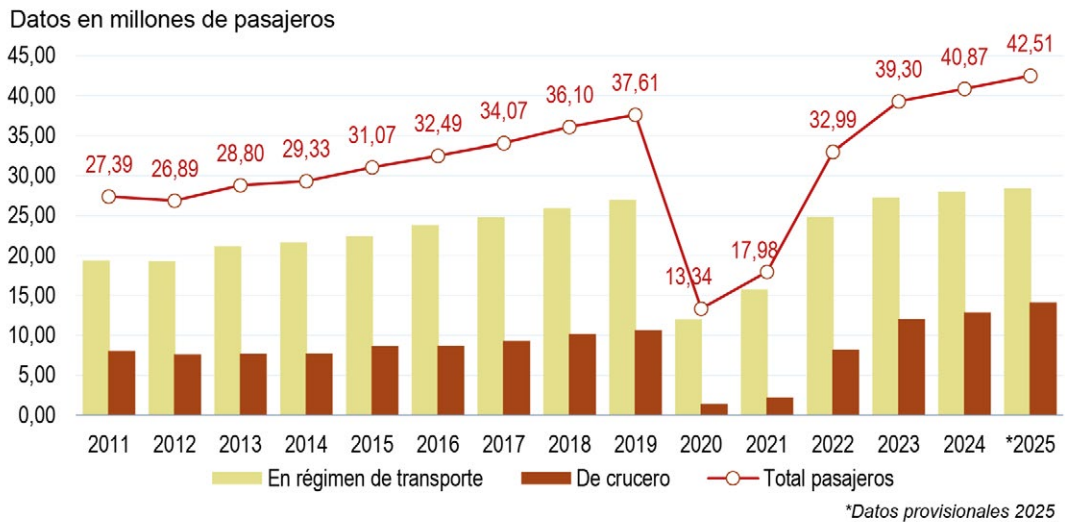
En 2025, el Ministerio de Transportes y Movilidad Sostenible, a través de la Dirección General de la Marina Mercante, realizó 1.292 inspecciones a buques mercantes de pabellón extranjero que arribaron a puerto o fondeadero español, en aplicación del Memorando de París. De estas inspecciones, se produjeron 34 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. (Figura 9.8)

Sistema portuario español

Los puertos son puntos neurálgicos y garantizar su protección es esencial para la soberanía económica, la defensa de las fronteras marítimas y la prevención de riesgos híbridos. Su vigilancia no solo protege el tráfico comercial, sino también la seguridad energética, medioambiental y social de España y de la Unión Europea.

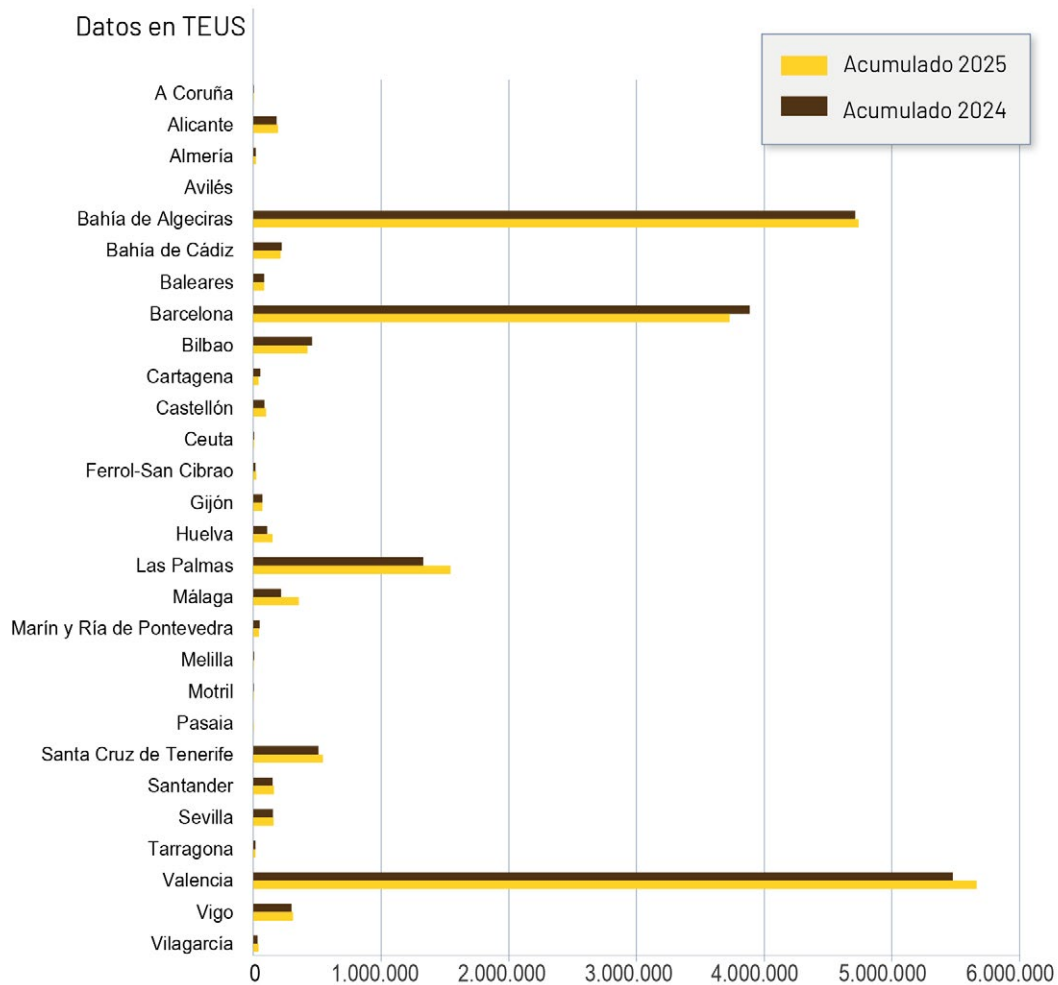
La infiltración en los puertos del crimen organizado es una de las mayores amenazas para la economía legal y la seguridad de la Unión Europea y requiere ser abordada, desde una perspectiva global.

El número de pasajeros que se reciben tanto de tránsito como de desembarque para visitas diarias en las costas españolas en las que arriban cruceros ha crecido exponencialmente en los últimos años, lo que obliga a un control de fronteras que ha de ser igual de seguro pero más rápido por lo que se dota de un mayor número de medios humanos de Policía Nacional y recursos materiales a dichos Pasos Fronterizos, tales como verificadores o analizadores de documentos y con la entrada del Sistema Entry Exit System, se dota de los nuevos Puestos de Control Manual (PCM). (Figuras 9.9 a 9.12)



Fuente: Elaboración del DSN con datos procedentes de Puertos del Estado

Figura 9.9: Evolución del número de pasajeros en régimen de tránsito y crucero

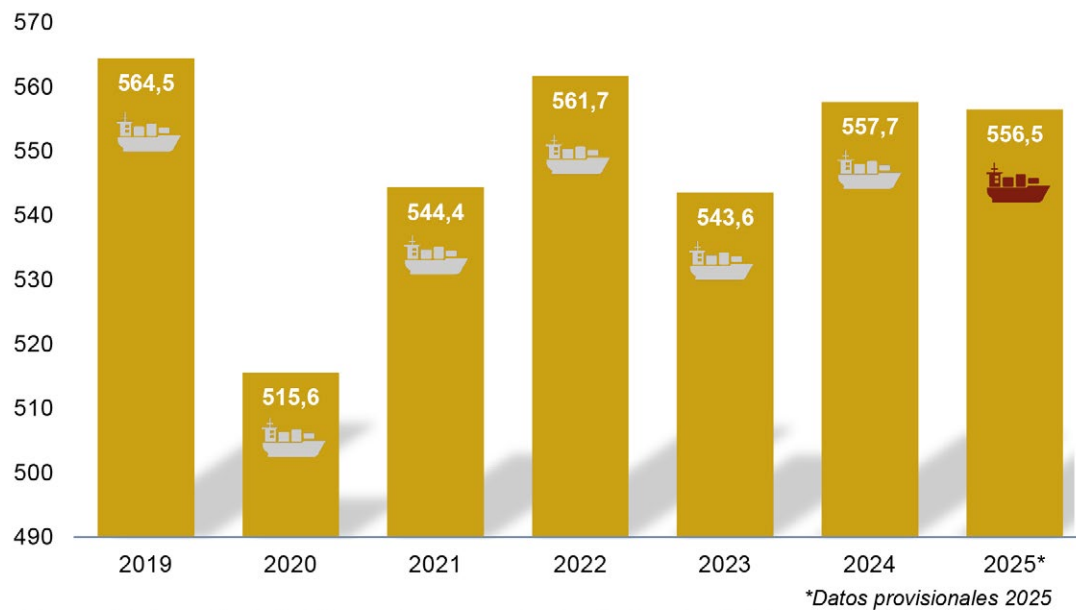


Fuente: Puertos del Estado

Incluye cargas, descargas, tránsito y transbordo

Figura 9.10: Comparativa 2024-2025 del tráfico en los puertos españoles de contenedores en España (datos en TEU)

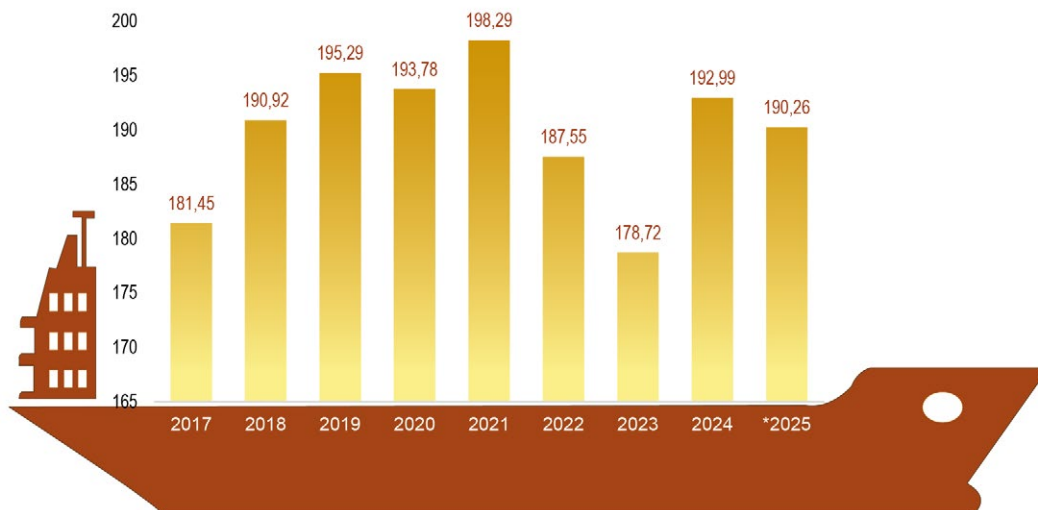
Unidades: millones de toneladas



Fuente: Elaboración del DSN con datos procedentes de Puertos del Estado

Figura 9.11: Evolución histórica del tráfico portuario en España 2019-2025

Unidades: millones de toneladas



*Incluye cargas, descargas, tránsitos y transbordos

Fuente: Puertos del Estado

Figura 9.12: Tráfico de contenedores en España

Principales avances en materia de capacidades de seguridad marítima

La mejora de capacidades es uno de los tres objetivos centrales de la *Estrategia Nacional de Seguridad Marítima*. Para avanzar en este objetivo, a lo largo de 2025, el Ministerio de Defensa ha realizado un arduo trabajo de planeamiento, adquisición e integración de nuevas capacidades de seguridad marítima, en coordinación con las principales empresas nacionales del sector de la seguridad y defensa. En cuanto a buques, se continúa trabajando en la construcción de las fragatas F-110 (la F-111 “Bonifaz” se botó el 11 de septiembre de 2025 y las F-112 “Roger de Lauria” y F-113 “Menéndez de Avilés” ya se encuentran en la grada de construcción), los submarinos S-80 (con la puesta a flote del S-82 “Narciso Monturiol” y el inicio de la construcción del S-83 “Cosme García”), el buque de intervención subacuática, y dos buques hidrográficos costeros. Asimismo, se avanza en la adquisición de nuevos helicópteros para la Flotilla de Aeronaves (como el H-135, el NH-90 o el MH-60R) y en el planeamiento de la modernización de los cazaminas clase “Segura” y las fragatas F-100 clase “Álvaro de Bazán”. Por otro lado, continúan los trabajos de construcción de un nuevo buque de aprovisionamiento de combate y del proyecto *European Patrol Corvette* (EPC), desarrollado conjuntamente entre varios países de la UE. Por último, se destacan los avances llevados a cabo en el ámbito de las comunicaciones y, en particular, de los sistemas vía satélite y de los desarrollos en materia de vehículos no tripulados, cuyo protagonismo en los escenarios actuales de conflicto ha ido aumentando de forma muy significativa.

En lo que respecta al Ministerio del Interior, el Servicio Marítimo de la Guardia Civil mantiene su despliegue y capacidades en el entorno marítimo, y ha incrementado a la flota actual dos nuevas patrulleras de alta velocidad con altas capacidades, así como con la botadura en noviembre de un nuevo buque oceánico de 82 metros de eslora.

Con ello, la Guardia Civil ha reforzado de forma significativa sus capacidades operativas especialmente con la incorporación a la flota del Buque Oceánico Multipropósito (BOM) “Duque de Ahumada”, y el fortalecimiento de la inteligencia marítima en coordinación con la Armada, FRONTEX y la Agencia Europea de Seguridad Marítima (EMSA). Esta adquisición incorpora medios con sistemas avanzados que ayudan a mejorar de manera sustancial su capacidad operativa en su misión de vigilancia y control de las costas y aguas territoriales.

Además, entre los principales avances en materia de capacidades de seguridad marítima destaca la dotación a los Pasos Fronterizos Marítimos de accesorios para prevenir la inmigración irregular, tales como detectores de latidos, detectores de Co2 o terminales de lectura de DNI electrónico para un control efectivo de los Documentos Nacionales de Identidad Españoles electrónicos.

Por su parte, el Instituto Español de Oceanografía (IEO-CSIC) tiene una flota compuesta por seis buques oceanográficos. Tres de ellos litorales: el Francisco de Paula Navarro, que opera principalmente en el Mediterráneo; el Lura y el Mytilus, que operan en aguas del Cantábrico y Galicia. A ellos se suman dos buques oceanográficos regionales, el Ángeles Alvariño y el Ramón Margalef, que operan en aguas nacionales de todo el Estado, tienen 46 metros de eslora y una capacidad para 27 personas entre personal científico y tripulación. Por último, el Odón de Buen es un buque oceanográfico oceánico, capaz de operar en aguas de todo el mundo hasta 6000 metros de profundidad, con categoría polar CP7, una eslora de 85 metros, capacidad para 58 personas entre personal científico y tripulación.

Por otra parte, el Ministerio de Hacienda ha incorporado dos patrulleras de la serie RODMAN 111 (“PEREGRINO I” y “PEREGRINO II”, de 35 m de eslora, hasta 35 nudos y 1.400 millas náuticas de autonomía) para reforzar la vigilancia oceánica.

Además, la AEAT (a través de su Servicio de Vigilancia Aduanera) participa en dos proyectos europeos clave:

- CONNECTOR: desarrolla un entorno interoperable CE-CISE (*Customs Extended Interoperable Common Information Sharing Environment*) que integra aduanas, guardias de fronteras y guardacostas para la evaluación compartida del riesgo y el intercambio de información entre Estados miembros.
- I-SEAMORE (*Integrated Surveillance Ecosystem for European Authorities responsible for Maritime Operations*): crea una plataforma de vigilancia marítima que combina sensores, vehículos no tripulados, datos satelitales e Inteligencia Artificial, para optimizar la conciencia situacional y la capacidad operativa frente a amenazas en el mar.

La implicación de Vigilancia Aduanera de la AEAT en estos programas refuerza sus competencias operativas, mediante el intercambio avanzado de información y tecnologías de frontera marítima, en línea con la política de Seguridad Nacional.

VULNERABILIDAD AEROESPACIAL

- El 14 de julio de 2025, el Consejo de Seguridad Nacional aprobó la Estrategia de Seguridad Aeroespacial Nacional, que establece las líneas estratégicas para la protección y resiliencia del dominio aéreo y espacial.
- El ámbito aeroespacial se consolida como un entorno estratégico de fuerte competencia, con una creciente importancia para la provisión de servicios esenciales y para la Seguridad Nacional.
- El uso indebido de drones adquiere una relevancia creciente como vector de riesgo en el entorno europeo, debido a su accesibilidad, su dificultad de detección y su potencial para ser empleados con fines de vigilancia ilícita o interferencia en operaciones críticas.

VULNERABILIDAD AEROESPACIAL

Riesgos y amenazas a la seguridad aeroespacial

El ámbito aeroespacial se consolida como un terreno cada vez más disputado entre las grandes potencias, organizaciones y actores no estatales. En la ESAN 2025 se ha producido una evolución sustancial en línea con los cambios en OTAN y en la Unión Europea y se ha preferido utilizar el término “dominio” para designar las operaciones en el espacio aéreo y el espacio ultraterrestre. La introducción de ese término supone un paso significativo para subrayar la importancia clave para el suministro de los servicios y recursos esenciales del espacio, y permite resaltar sus características propias. Por otra parte, se reserva el término ámbito aeroespacial para subrayar, que desde el punto de vista de la seguridad nacional es necesario mantener una visión integral y unificada de la seguridad del espacio aéreo y ultraterrestre.

Las grandes potencias han incrementado sus capacidades militares espaciales al tiempo que los grandes grupos tecnológicos han intensificado el despliegue de satélites comerciales, aumentado la densidad del entorno orbital e intensificando el riesgo de saturación de las frecuencias y órbitas que impidan la prestación de nuevos servicios o la entrada de nuevos operadores.

A su vez, la revolución tecnológica ha alcanzado el sector aéreo con la aparición de nuevas aeronaves no tripuladas (drones), misiles hipersónicos, aeronaves de sexta generación o tecnologías de guerra electrónica, entre otros avances, en un marco cada vez más vulnerable debido a la convergencia física y cibernética.

La seguridad aeroespacial se enfrenta a un entorno de riesgo cada vez más complejo y exigente, caracterizado por la aparición de amenazas diversas que combinan factores tecnológicos, operativos y regulatorios. Entre las más relevantes se encuentran la concentración industrial del sector, los ataques a las infraestructuras críticas, la proliferación y uso indebido de drones, así como los riesgos asociados a la reentrada de desechos espaciales. A ello se suman las interferencias de radiofrecuencias, en particular sobre los sistemas de navegación por satélite (GNSS), ya sean provocadas de forma intencionada o accidental, que pueden degradar la señal y afectar a funciones esenciales como la navegación, el funcionamiento de infraestructuras críticas o la sincronización temporal de sistemas. En paralelo, las limitaciones del actual marco regulatorio dificultan la respuesta coordinada ante estas amenazas, incrementando la vulnerabilidad del sistema en su conjunto.

En este contexto, adquiere especial relevancia el riesgo asociado a la concentración de la industria espacial europea, particularmente en el desarrollo de servicios *Direct-to-Device* (D2D), que permiten la conexión directa entre satélites, principalmente en órbita baja, y dispositivos finales, como teléfonos móviles, sin necesidad de infraestructuras terrestres intermedias. La eventual consolidación de un único

actor dominante, capaz de integrar constelaciones, capacidades de red y servicios de conectividad global, conlleva implicaciones estratégicas de primer orden para España. Esta dinámica resulta coherente con el diagnóstico de la Estrategia de Seguridad Aeroespacial Nacional 2025, que subraya la creciente dependencia de capacidades espaciales críticas y la intensificación de la competencia en el entorno aeroespacial.

En este sentido, un escenario de elevada concentración no solo reduciría la competencia efectiva y limitaría la innovación, sino que también debilitaría la resiliencia de la cadena de suministro, generando dependencias estructurales críticas. Asimismo, incrementaría la exposición frente a fallos sistémicos, ciberataques o decisiones unilaterales del proveedor, comprometiendo la continuidad de servicios esenciales y dificultando el cumplimiento de los objetivos estratégicos nacionales en materia de seguridad, resiliencia y autonomía en el ámbito aeroespacial.

Para mitigar estos riesgos, resulta imprescindible fortalecer mecanismos regulatorios efectivos, incluyendo controles antimonopolio y salvaguardias de acceso abierto al mercado institucional europeo, que protejan la diversidad empresarial y la autonomía estratégica, y promuevan la entrada de proveedores especializados en grandes contratos y proyectos innovadores.

Además, en el contexto europeo, se han detectado ataques a infraestructuras críticas del sector aeroespacial, incluyendo ciberataques dirigidos a sistemas y redes, así como incidentes de sobrevuelos de drones en entornos aeroportuarios, con impacto potencial en la seguridad operacional. Igualmente, se han registrado en Europa diversos casos de alteración de las señales del sistema GPS (GNSS), cuya degradación afecta directamente al geoposicionamiento de las aeronaves y genera riesgos operacionales significativos para la navegación aérea.

Otro de los riesgos, cada vez más frecuente, es la utilización de drones para introducir sustancias estupefacientes en territorio nacional, para hacer contravigilancias a nuestras Fuerzas y Cuerpos de Seguridad del Estado y para introducir sustancias y objetos prohibidos en centros penitenciarios.

En relación con los desechos espaciales, comienza a ser cada vez más frecuente la activación de mecanismos estatales de alerta y protección ante el riesgo de reentrada no controlada de objetos en la atmósfera. Estos episodios pueden generar incertidumbre sobre las zonas de impacto y obligan a adoptar medidas preventivas para garantizar la seguridad de la población. De forma ilustrativa, la reentrada de la sonda soviética COSMOS 482, que finalmente se produjo en el océano Pacífico, motivó la activación de la Célula de Coordinación de Alertas Espaciales, evidenciando la creciente necesidad de sistemas de vigilancia y respuesta ante este tipo de riesgos.

Otra de las amenazas a la seguridad aérea son los incidentes relacionados con artefactos incendiarios en aviones. Tras los incidentes ocurridos en centros logísticos de DHL en Leipzig (Alemania) y Birmingham (Reino Unido) en 2024, que resaltan la constante evolución de las amenazas a la seguridad aérea y la necesidad de una vigilancia continua y la cooperación internacional para frustrar complots de sabotaje, las autoridades de Aviación Civil han reaccionado con protocolos estrictos para prevenir y gestionar incendios a bordo.

Finalmente, en cuanto a los retos normativos y regulatorios que afectan a la seguridad aeroespacial, destaca la fragmentación del actual panorama regulatorio europeo, con diferentes enfoques nacionales que aumentan la complejidad y los costes para las empresas, que ha propiciado la propuesta comunitaria de la “*Ley Espacial de la UE*”. Dicha ley, actualmente en negociación, tiene como objetivo crear un marco claro y armonizado a nivel europeo que garantice la seguridad, la resiliencia y la responsabilidad medioambiental de los activos espaciales nacionales y de la UE.

En materia de seguridad y resiliencia espacial, la propuesta más reciente, en lugar de establecer un marco exhaustivo como *lex specialis*, mantiene un núcleo básico de obligaciones, dejando el desarrollo

técnico a futuras normas y facilitando su alineación con los marcos horizontales existentes (NIS2 y CER), así como su coordinación con los esquemas de certificación de ciberseguridad (como la EUCS), a fin de que dicho Reglamento garantice al mismo tiempo la necesaria coherencia y evitando duplicidades de obligaciones para los operadores espaciales.

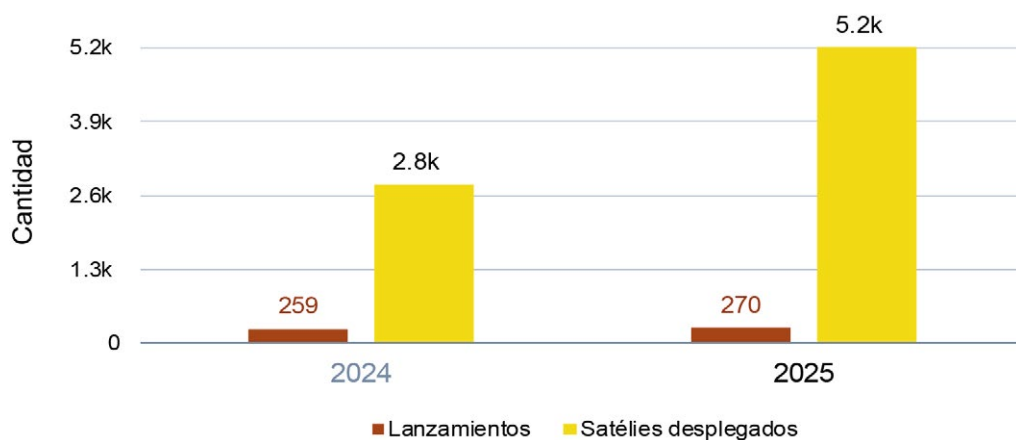
A nivel regulatorio internacional, el incumplimiento de la normativa vigente, en particular en materia de gestión del espectro radioeléctrico, puede generar limitaciones operativas en la prestación de servicios. En este sentido, la falta de adecuada coordinación o registro conforme a los procedimientos de la Unión Internacional de Telecomunicaciones (UIT) puede derivar en la denegación de derechos de uso de frecuencias frente a otros operadores con mayor prioridad internacional, afectando a la disponibilidad y continuidad de los servicios espaciales.

Incremento de la actividad espacial

El aumento de objetos en órbita y la multiplicación de actores privados en actividades espaciales han elevado los riesgos de congestión orbital, colisiones, interferencias, así como la generación de nueva basura espacial. También es de destacar que hubo más re entradas incontroladas (de promedio tres diarias) en la atmósfera, y más frecuentes y probables fragmentaciones.

La actividad espacial global ha mantenido una tendencia claramente expansiva durante 2024 y 2025, alcanzando niveles sin precedentes. En 2024 se registraron aproximadamente 259 lanzamientos orbitales, que permitieron situar en órbita cerca de 2.900 objetos, en gran medida vinculados al despliegue de satélites comerciales. Esta dinámica se ha intensificado en 2025, impulsada fundamentalmente por el crecimiento de las megaconstelaciones en órbita baja (LEO). En este contexto, destaca especialmente la constelación *Starlink*, que superó los 10.000 satélites lanzados acumulados, con aproximadamente 8.500–8.700 satélites operativos, prestando servicio a millones de usuarios a escala global.

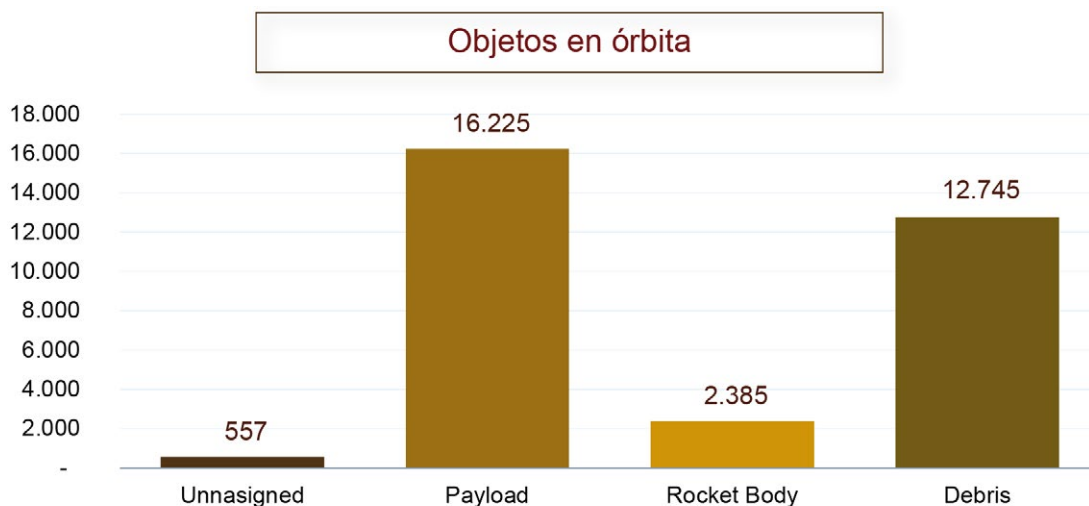
Asimismo, el acceso al espacio presenta un elevado grado de concentración geopolítica, con Estados Unidos, China y la Federación Rusa como actores predominantes. En 2025, Estados Unidos concentró en torno al 60–62% de los lanzamientos orbitales, seguido por China con aproximadamente el 28–30%, mientras que Rusia mantuvo una cuota cercana al 5–6%. Este reparto evidencia una marcada asimetría en las capacidades de acceso al espacio, reforzando la dimensión estratégica del entorno orbital. (Figura 10.1)



Fuente: Agencia Espacial Española (AEE)

Figura 10.1: Aumento de la actividad espacial de 2024 a 2025

Según datos de *Space-Track*, hay más de 30.000 objetos catalogados en órbita, de los cuales unos 16.225 son satélites activos. Asimismo, según el informe 2025 de la ESA (Agencia Espacial Europea) sobre el Entorno Espacial, se estiman que existen más de 1,2 millones de fragmentos mayores a 1 cm, de los cuales más de 50.000 tienen un tamaño superior a 10 cm. (Figura 10.2)



Fuente: Space-Track

Figura 10.2: Número de objetos en órbita

Además, se muestra un aumento creciente en los residuos generados, a pesar de que también se detecta un incremento en la adherencia de los operadores de satélite a la implementación de medidas voluntarias como la pasivación (apagado de los satélites) o reentradas controladas en la atmósfera en órbitas bajas. Estos procedimientos no son suficientes para contener el problema creciente del incremento de la actividad en el espacio.

Finalmente, iniciativas europeas como el EU SST, de la que la Agencia Espacial Española es coordinadora, o como TraCSS (Departamento de Comercio de EEUU) y el enfoque “Zero Debris” de la ESA, reflejan un reconocimiento de la comunidad internacional sobre la necesidad crítica de gestionar el tráfico y los residuos orbitales.

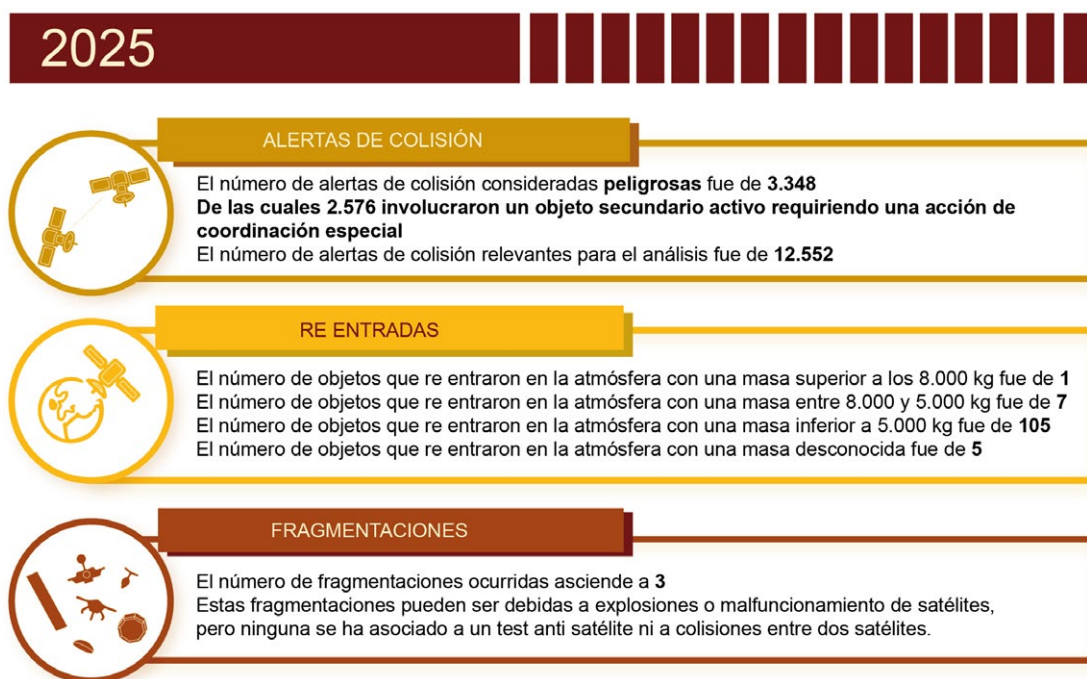
Con el objetivo de hacer frente a estos riesgos España dispone de capacidades civiles y militares para dar cobertura a nivel nacional y europeo.

El Centro de Operaciones de Vigilancia Espacial (COVE) del Ejército del Aire y del Espacio (EA) ha llevado a cabo el seguimiento de reentradas no controladas de objetos espaciales en la atmósfera, elaborando informes de análisis y predicciones, en el marco del Protocolo de Alertas espaciales aprobado por el Consejo de Seguridad Nacional, que permiten informar con el mayor detalle posible sobre la ventana temporal y las zonas potencialmente afectadas.

El Centro Español de Vigilancia y Seguimiento Espacial, (S3TOC), es centro de referencia para la provisión del servicio de prevención de colisiones en órbita en nombre de la Unión Europea, junto con Francia. El S3TOC durante 2025 ha proporcionado servicios de alertas de prevención de colisiones a más de 90 usuarios internacionales con más de 600 satélites, incluyendo el establecimiento de un protocolo de intercambio de información con los satélites de *SpaceX* para fomentar la coordinación

y la seguridad de las operaciones espaciales y ha emitido un total de 358 informes técnicos relativos a 103 eventos de re entrada, de los cuales uno fue clasificado como de riesgo alto y nueve como de riesgo medio.

Estos episodios ponen de manifiesto la relevancia del sistema español de vigilancia y seguimiento espacial, en el que el S3TOC, como proveedor operativo de servicios SST, se complementa con las capacidades del COVE del Ejército del Aire y del Espacio, contribuyendo de forma coordinada a la monitorización del entorno orbital y al apoyo a los mecanismos nacionales de gestión de riesgos. (Figura 10.3)



Fuente: EU SST

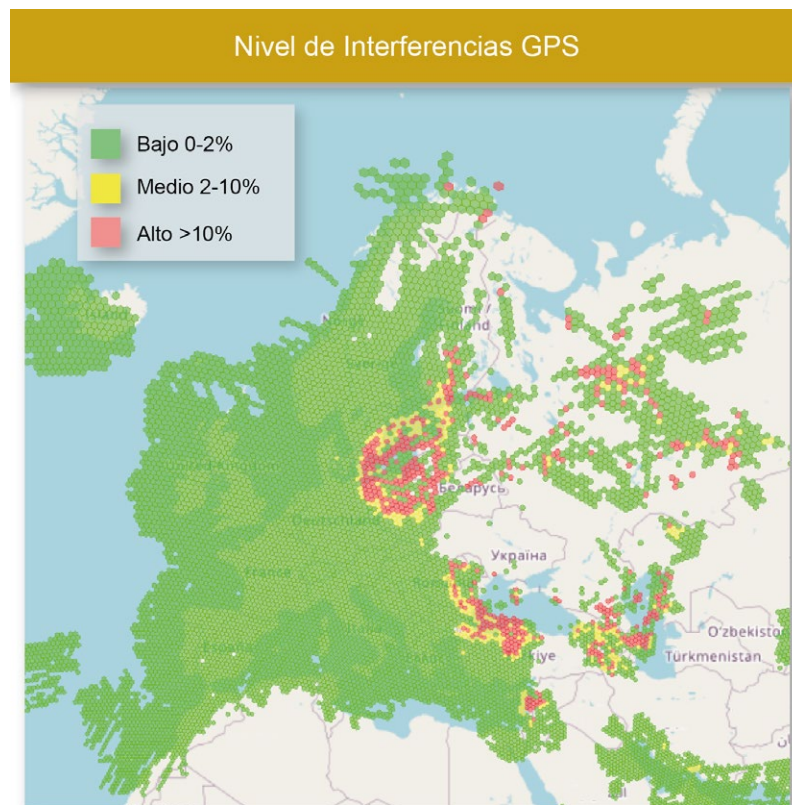
Figura 10.3: Número de eventos en el año 2025

En 2025 los incidentes por peligrosidad en el sector espacial han seguido aumentando como consecuencia del incremento exponencial de objetos en órbita, lo que ha elevado la importancia de las amenazas tanto no intencionadas, entre ellas las re entradas, conjunciones con riesgo de colisión, los fenómenos de meteorología espacial, como deliberadas, caso de las perturbaciones de las señales GNSS.

En este último ámbito, adquieren especial relevancia las operaciones de proximidad (*Rendezvous and Proximity Operations*, RPO) llevadas a cabo por terceros actores, que permiten el acceso físico a satélites y otros activos orbitales con fines potenciales de inspección, interferencia, degradación o espionaje. Este tipo de capacidades introduce un elevado grado de ambigüedad operativa y estratégica, dificultando la distinción entre actividades legítimas y hostiles, lo que refuerza la necesidad de disponer de capacidades avanzadas de vigilancia, caracterización y atribución en el dominio espacial.

Durante el año 2025 el COVE ha elaborado 193 informes de meteorología espacial en los que ha monitorizado los fenómenos de meteorología espacial, con especial atención a una tormenta geomagnética de categoría G5, de nivel extremo, el nivel más alto en la escala de la NOAA (Administración Nacional Oceánica y Atmosférica de EE. UU.), y 3 tormentas geomagnéticas de categoría G4, de intensidad severa, capaces de afectar a satélites, redes eléctricas y sistemas GNSS.

A lo largo de 2025 se ha observado un incremento significativo de las perturbaciones en las señales GNSS, especialmente en Europa y Asia occidental, atribuible principalmente a interferencias externas de carácter intencionado, como *jamming* y *spoofing*, aunque en menor medida también a causas accidentales o fenómenos de meteorología espacial, lo que ha afectado a la fiabilidad de los servicios de posicionamiento, navegación y sincronización. (Figura 10.4)



Fuente: Datos obtenidos en GPSJAM a 31 de diciembre de 2025

Figura 10.4: Perturbación de GPS

Por otra parte la Agencia Espacial Española, en colaboración con el Centro Criptológico Nacional, ha desarrollado un programa piloto a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (PNNSC), para contribuir a que el sector espacio pueda cumplir con algunas de las obligaciones previstas por la *Directiva EU 2022/2555* (NIS2) que se encuentra en proceso de transposición a normativa nacional.

A través de esta plataforma se han notificado un total de 2.466 ciberincidentes (a fecha 31 de diciembre de 2025) en el sector espacio, frente a los casi 6.106 del mismo periodo de 2024. (Figura 10.5)

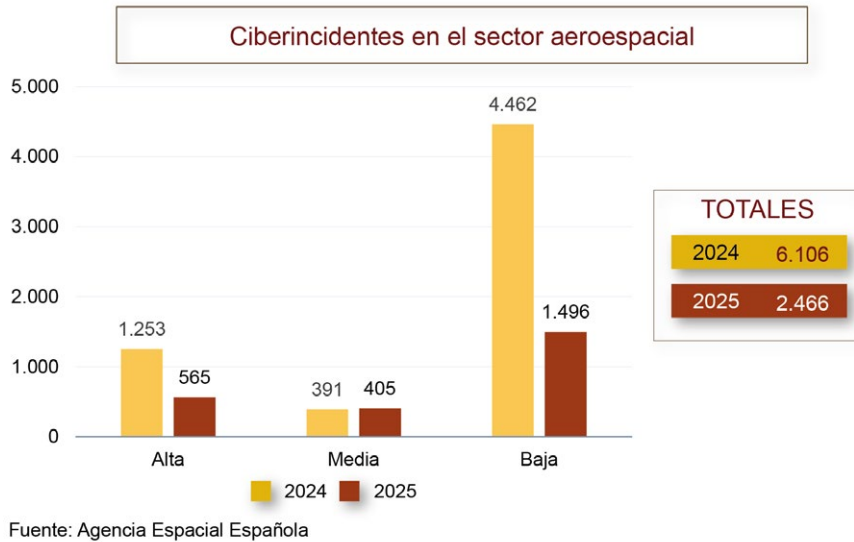


Figura 10.5: Ciberincidentes en el sector aeroespacial

Cambios normativos y regulatorios que afectan a la seguridad aeroespacial

En 2025 se han producido avances significativos en el marco normativo que sustenta la seguridad espacial.

Especialmente, en el marco del Sistema de Seguridad Nacional, el 14 de julio, el Consejo de Seguridad Nacional aprobó la Estrategia de Seguridad Aeroespacial Nacional, que establece las líneas estratégicas para la protección y resiliencia del dominio aéreo y espacial.

Este documento busca dar respuesta los profundos cambios tecnológicos, estratégicos y normativos que han alterado el equilibrio en el espacio aéreo y ultraterrestre en los últimos años y modifica la anterior estrategia de 2019, respondiendo a la necesidad de proteger intereses nacionales frente a amenazas crecientes en el entorno espacial.

La Estrategia de Seguridad Aeroespacial Nacional 2025 (ESAN 2025), se estructura en torno a tres grandes objetivos estratégicos: proteger España “en” y “desde” el Aire y el Espacio; mejorar las capacidades de seguridad y defensa aérea y espacial; y, contribuir a un Aire y a un Espacio seguro y sostenible, cada uno de los cuales se acompaña de líneas de actuación propuestas para su cumplimiento. Además, como novedad respecto a la Estrategia de 2019, se ha elaborado un Anexo con un catálogo de medidas identificadas, orientadas a la consecución de dichos objetivos estratégicos.

Por su parte, el Consejo Nacional de Seguridad Aeroespacial ha activado la Célula de Coordinación del Grupo de Trabajo de Alertas Espaciales, para resolver un



simulacro de OTAN donde se veían afectadas varias infraestructuras espaciales, tanto en tierra como en el espacio, que anulaban las comunicaciones y los sistemas de geoposicionamiento.

Junto a la aprobación de la ESAN 2025, se ha impulsado también la modificación del *Real Decreto 765/2022*, relativo al uso de aeronaves motorizadas ultraligeras, elevando el peso máximo de aquellas que quedan desreguladas y exentas de matrícula de setenta a ciento veinte kilogramos, con el objetivo de introducir mayor flexibilidad en el ámbito de la aeronavegabilidad.

Igualmente, se ha aprobado la Instrucción del Jefe de Estado Mayor del Ejército del Aire y del Espacio, como Autoridad Aeronáutica Competente Militar, que establece las normas y procedimientos para la operación de sistemas de aeronaves no tripuladas de carácter militar y de otros dispositivos aéreos análogos.

Además, continúa el curso de la tramitación de la Ley Nacional de Actividades Espaciales, con la consulta pública lanzada en noviembre de 2025. Esta norma configurará el marco nacional para las actividades espaciales, integrando las prioridades de seguridad, defensa e impulso industrial y alineándose con el futuro Reglamento europeo. Además, España es un socio comprometido y respetuoso con el cumplimiento del marco normativo establecido en las diferentes organizaciones internacionales de las que es miembro. En coherencia, los objetivos fijados en la agenda “Espacio 2030” se han tenido en cuenta en la preparación de los borradores de Estrategia Espacial Nacional, Política Espacial Nacional y Ley Nacional de Actividades espaciales, que se encuentran en proceso de desarrollo normativo.

Mientras, en el marco normativo aeronáutico, destaca la promulgación de la *Ley 8/2025, de 29 de septiembre*, por la que se modifican la *Ley 48/1960, de 21 de julio, sobre Navegación Aérea*, y la *Ley 21/2003, de 7 de julio, de Seguridad Aérea*.

A su vez, a nivel europeo, la Comisión publicó del 25 de junio de 2025 una propuesta de Reglamento sobre seguridad, resiliencia y sostenibilidad de las actividades espaciales (*EU Space Act - EUSA*) que ha suscitado un amplio debate sobre si la futura trasposición de las directivas NIS2 (UE) 2022/2555 y la CER (UE) 2022/2557 harían conveniente disponer de un complemento normativo en la EUSA (i.e. *Lex Specialis*). No obstante, la última versión de la propuesta evidencia una reducción del alcance normativo, desplazando parte del contenido técnico hacia futuros actos de ejecución, estándares y orientaciones. La supresión del anexo específico de resiliencia y de diversos preceptos técnicos confirma el abandono de un sistema autónomo y exhaustivo de requisitos de ciberresiliencia espacial, en favor de un núcleo normativo más reducido, flexible y evolutivo. Este enfoque facilita su alineación con los marcos horizontales existentes y otorga mayor margen de interpretación a los Estados miembros, aunque introduce menor claridad inmediata para los operadores transnacionales.

Estado de la implantación de la Estrategia Europea de Seguridad y Defensa Espacial

La implantación de la Estrategia Europea de Seguridad y Defensa Espacial avanza de forma sostenida y tangible, con hitos claros como la puesta en marcha y expansión del *EU Space ISAC*, bajo el paraguas de la Estrategia, lo que evidencia una consolidación del pilar de cooperación e intercambio de información de seguridad del sector espacial europeo. La Agencia Espacial Española (AEE) es miembro de esta iniciativa desde junio de 2025.

Igualmente, sobre las acciones destinadas a reforzar la Arquitectura de Respuesta a las Amenazas Espaciales (*Space Threat Response Architecture, STRA*), derivado de la Estrategia Europea de Seguridad y Defensa Espacial, la revisión en curso amplía el alcance de la norma más allá del Programa Espacial

de la UE para incluir, de forma voluntaria, sistemas de los Estados miembros. El objetivo es dotarla de mayor agilidad, con activación automática ante amenazas a sistemas de la UE y voluntaria para activos nacionales, además de mejorar el intercambio de información, establecer puntos de contacto permanentes y realizar ejercicios anuales de evaluación.

Mientras, en lo que respecta a la gobernanza y ciber resiliencia, se afianza el papel de la Agencia de la Unión Europea para el Programa Espacial (EUSPA), como garante de seguridad en todos los componentes del programa espacial de la UE y se alinean instrumentos horizontales como NIS2 y CER con el marco espacial. La propuesta de *EU Space Act* preveía actuar como *lex specialis* en aquellos casos no cubiertos por los mencionados instrumentos. En su versión más reciente, el Reglamento ya no se presenta como una *lex specialis* plenamente autónoma frente a dichos instrumentos, sino como un complemento específico que establece un núcleo básico de obligaciones, dejando el desarrollo técnico a actos de ejecución y estándares posteriores y facilitando su coherencia con el acervo horizontal en materia de ciberseguridad y resiliencia.

Por otra parte, el potencial que las tecnologías duales y de doble uso suponen en el actual entorno geopolítico abren nuevas oportunidades a la industria, y contribuirán a ganar autonomía en el desarrollo de la soberanía tecnológica de Europa.

Capacidades y seguridad en el dominio aéreo y espacial

En 2025 el Ejército del Aire y del Espacio ha continuado reforzando de manera significativa las capacidades y la seguridad en el dominio aéreo, mediante la modernización progresiva del Sistema de Vigilancia y Control Aeroespacial, p. ej. la provisión de datos modo 5. A lo largo del año se han completado nuevas fases de actualización en los sensores radar, incrementando la precisión, la cobertura y la capacidad de identificación, incluido el seguimiento de amenazas asociadas a misiles balísticos.

Paralelamente, se han consolidado los avances en ciberdefensa y en la protección de los sistemas de comunicaciones, y se ha avanzado en la renovación de los centros de control de defensa aérea, aumentando su resiliencia.

En 2025, ya se encuentran operativos los radares tácticos desplegados, que permiten extender la red de vigilancia, proporcionar capacidades avanzadas de *picket* radar y cubrir huecos temporales cuando la situación operativa lo requiere. También se mantiene el impulso al sistema de vigilancia, control y coordinación en el entorno UAS de baja cota, ámbito especialmente crítico ante el incremento de amenazas de tipo *low, small, slow*.

Todo este conjunto de sensores se integra en un sistema activo las veinticuatro horas del día y los siete días de la semana, sostenido por la labor diaria de más de cinco mil aviadores de todos los empleos y especialidades dedicados a cometidos de mando y control, vigilancia y alerta, que garantizan el uso libre y seguro del espacio aéreo de responsabilidad nacional, un área muy superior a la superficie del territorio español e indispensable para la defensa y la movilidad aérea.

La capacidad de control se completa con aeronaves de caza dispuestas en un servicio de alerta rápida capaces de llevar a cabo interceptaciones y acompañamiento cuando la situación lo requiere. Estas capacidades, además de garantizar la defensa del espacio aéreo nacional, se proyectan en misiones de policía aérea en el flanco oriental de la OTAN, reflejando el carácter solidario de España con sus Aliados, y consolidando el papel de las Fuerzas Armadas como elemento esencial de la resiliencia y de la defensa aeroespacial del Estado.

El Real Decreto 443/2024, que aprueba el *Esquema Nacional de Seguridad de redes y servicios 5G*, establecía en su artículo 41 la creación del Centro de Operaciones de Seguridad 5G de referencia (SOC5G), como órgano de apoyo y supervisión para garantizar la protección de los sistemas, redes y servicios 5G. Durante 2025 se han desarrollado sus capacidades para contribuir a la seguridad en el dominio aéreo, centrándose en sus principales funciones: ofrecer asistencia operativa a los sujetos obligados en tareas de prevención, protección, detección y respuesta frente a amenazas, incidentes y ciberataques; así como promover medidas de prevención en el ámbito de las redes y servicios 5G. Además, el SOC5G también hace un seguimiento de las iniciativas relacionadas con la seguridad aeroespacial, en lo referente a las telecomunicaciones.

Paralelamente, las capacidades espaciales del Ejército del Aire y del Espacio han experimentado un refuerzo significativo, especialmente tras la entrega oficial al COVE, el 31 de octubre de 2025, del Sistema de Conocimiento y Control de la Situación Espacial (CCSE), desarrollado por GMV y ya plenamente operativo.

Complementariamente, se hace imperativo avanzar en estrategias de “Reposición en el Espacio” (*Responsive Space*) que permitan a España y sus aliados recuperar capacidades operativas mediante lanzamientos tácticos. Ante la degradación de activos en órbita, ya sea por ataques intencionados o incidentes fortuitos, la resiliencia del sistema depende de una respuesta ágil. En defensa, no basta con observar el dominio; es crítica la capacidad de reponer satélites dañados en el menor tiempo posible para garantizar la continuidad de las capacidades esenciales.

Durante 2025, el COVE ha seguido ampliando su conocimiento del dominio espacial mediante la participación en la iniciativa *Joint Commercial Operations* (JCO) del Centro Nacional de Defensa Espacial de Estados Unidos, y ha continuado avanzando en los requisitos para una red de sensores ópticos robotizados y para la futura capacidad de vigilancia basada en antenas de radiofrecuencia pasiva.

Además, desde el Ministerio del Interior, continúa la expansión de la Fase II del programa del Sistema global contra Drones (SIGLO-CD), con planes para mejorar sus capacidades tecnológicas y aumentar la cobertura en áreas claves.

Asimismo, en el ámbito de la cooperación con la AEE y en continuidad con el Estatuto aprobado en 2023, durante 2025 se han iniciado los trabajos para la definición de un mecanismo de coordinación y colaboración entre la AEE y el Ministerio de Defensa, con la participación del Ejército del Aire y del Espacio. Así, la AEE ha incorporado a su plantilla la totalidad de efectivos del Ministerio de Defensa previstos. Por su parte, el personal de la AEE está participando activamente en los foros nacionales e internacionales de relevancia relacionados con la seguridad de los activos espaciales.

En el marco de la Unión Europea, también continúan los esfuerzos para reforzar las capacidades de defensa europeas con el objetivo de disuadir amenazas y responder a cualquier agresión. Entre ellos, destaca el emblemático proyecto denominado “Escudo Espacial Europeo” (*EU Space Shield*), que se concibe como un mecanismo civil-militar para proteger los activos espaciales europeos frente a amenazas físicas, cibernéticas o híbrida, integrando la vigilancia y respuesta rápida entre instituciones, Estados miembros e industria, con el fin de fortalecer la resiliencia del dominio espacial europeo.

En este contexto, la Comisión Europea ha iniciado conversaciones preliminares para el desarrollo de un potencial *flagship* para desarrollar el *EU Space Shield*, que busca proteger y reforzar la resiliencia de los activos y servicios espaciales de la UE para que puedan utilizarse de forma fiable por usuarios gubernamentales, especialmente en el ámbito de la defensa. El desarrollo y adquisición de las capacidades necesarias para el *EU Space Shield* superan la capacidad de un solo Estado miembro, y se agruparán recursos a través del Fondo de Competitividad Europeo y posibles proyectos europeos de defensa de interés común (EDPCI), entre los que se destacan los de drones y contra drones, espacio o alerta temprana y defensa aérea misil integrada (IAMD). (Figura 10.6)



Fuente: European Parliamentary Research Service

Figura 10.6: Ruta de Defensa 2030

Proliferación de vehículos aéreos tripulados de forma remota

La tecnología de los UAS está evolucionando a un ritmo rápido, haciéndolos más pequeños y asequibles, con la capacidad de transportar cargas útiles más pesadas. Su bajo coste y facilidad de manejo hace que estén al alcance de cualquier usuario. Además de poder causar accidentes y situaciones potencialmente peligrosas debido a un uso imprudente, pueden ser utilizados por actores estatales y no estatales con fines hostiles o maliciosos, incluyendo contra infraestructuras críticas.

El empleo de estos medios también ha evolucionado por el uso de sensores más avanzados, sistemas autónomos (sin enlace para el control del UAS *Low Slow Small*, LSS), menos emisiones electrónicas (menos detectabilidad y posibilidades de neutralización electrónica), tecnologías furtivas o “*stealth*” y el control a través de tecnología 5G que hace que sean más difíciles de discriminar y detectar. Los UAS de pequeño tamaño, que vuelan a baja altura y velocidad (LSS), suponen una particular amenaza, al ser difíciles de detectar, identificar y neutralizar.

Los drones son utilizados por actores no estatales para inteligencia, vigilancia, reconocimiento, enrutamiento logístico y contrabando, producción y difusión de propaganda o interrupción de eventos. En el ámbito internacional, algunas organizaciones terroristas han desarrollado un programa completo de drones. Entre ellas se encuentran Dáesh, el Partido de los Trabajadores del Kurdistán (PKK), Hayat Tahrir al-Sham (HTS) y otros grupos respaldados por Irán como Hamás, Hezbolá o los hutíes. Igualmente, se ha detectado el incremento en la utilización drones, además de un aumento en capacidades en cuanto a armamento de defensa antiaérea, por parte JNIM, en Malí, principalmente, aunque también en Níger y Burkina Faso. En la actualidad, utilizan drones comerciales modificados con Inteligencia Artificial para realizar operaciones cada vez más letales y en una zona cada vez más amplia. De esta manera, no solo multiplican la frecuencia de sus ataques, sino también expanden el ámbito geográfico. Se ha observado, igualmente, un incremento en la utilización de drones modificados en el noreste de Nigeria, por parte de ISWAP. Con relación a la actividad en internet, 2025 habrían continuado publicándose abundante cartelería señalando el uso de drones para cometer ataques en Occidente, así como diferentes publicaciones formativas al respecto.

Con relación al capítulo de respuestas, la mayoría de los aeropuertos comercialmente activos, incluidos los españoles, utilizan sistemas antidrones basados en tecnologías de detección por radar, sensores ópticos y acústicos y herramientas de neutralización mediante el “secuestro” por radiofrecuencia.

En el espacio de la Unión Europea que se han llevado a cabo varias operaciones contraterroristas relacionada con el uso de drones, concretamente en Francia, Dinamarca y Bélgica. Cabría destacar que, desde inicios de septiembre de 2025, se han producido avistamientos de drones en varios países europeos entre los que se encuentran Dinamarca, España, Alemania, y Bélgica. Estos han afectado principalmente a aeropuertos e instalaciones militares, y en muchos casos han provocado la suspensión de vuelos y cierres temporales del espacio aéreo. Estos incidentes servirían para visibilizar las vulnerabilidades a las que el sector aeroportuario puede quedar expuesto ante acciones disruptivas de diferente grado de sofisticación y etiología. Por ello, la UE está considerando ampliar las competencias para abordar las amenazas de los UAS y para hacer frente a las amenazas híbridas, incluidas las violaciones del espacio aéreo y la protección de activos estratégicos.

Así, aeropuertos de todo el mundo se enfrentan cada vez con mayor frecuencia a cierres como consecuencia de la presencia de drones no autorizados en sus inmediaciones. En 2025, al menos diez instalaciones aeroportuarias europeas se han visto afectadas por esta práctica que afecta seriamente a la seguridad aérea y provoca serios daños en las economías nacionales, entre ellos el aeropuerto de Fuerteventura. Además, se han reportado incidentes en Polonia, Rumanía, Lituania, Letonia y Francia, aunque no todos derivaron en cierres completos.

En España, el Ministerio del Interior ha puesto a disposición de las Fuerzas y Cuerpos de Seguridad del Estado, del Sistema Siglo-CD (Sistema Global Contra Drones), para la detección remota de UAS, su identificación y, en su caso, neutralización. Este sistema ha ampliado su red nacional de unidades de detección y neutralización a través de la combinación de antenas fijas y unidades portátiles que permiten localizar y rastrear drones en tiempo real y consigue la interoperabilidad con otros sistemas de gestión del espacio aéreo. Se está a la espera de la decisión para instalar este Sistema en los entornos aeroportuarios, empezando por Madrid-Barajas. En España, las Fuerzas y Cuerpos de Seguridad han creado unidades específicas para el uso de sistemas de detección e interferencia de drones. Estas unidades cuentan con sistemas tanto fijos como móviles, distribuidos estratégicamente por todo el territorio español para cubrir las principales entidades críticas.

Además, el Programa Nacional de Seguridad para la Aviación Civil aprobado el 1 de diciembre de 2025 establece que se desarrollará un procedimiento para reducir el nivel de riesgo y responder ante la materialización de la amenaza de presencia de sistemas de aeronaves pilotadas a distancia (RPAS) en el entorno aeroportuario. Este procedimiento estará basado en las directrices nacionales establecidas por la Autoridad competente (protocolo coordinado de respuesta ante la amenaza de presencia de drones en el entorno aeroportuario).

Así, la protección de los activos de la aviación civil contra interferencias y/o ataques que pretendan causar graves daños, será primordial durante los próximos años tanto en el entorno aeroportuario como de otras infraestructuras críticas. La Agencia Estatal de Seguridad Aérea (AESA) continúa trabajando en la regulación del uso del espacio aéreo por parte de los vehículos aéreos con el desarrollo de los entornos U-Space (conjunto de sistemas, servicios y procedimientos específicos que han sido diseñados para permitir el acceso seguro, eficiente y asequible al espacio aéreo de operaciones de UAS numerosas o complejas, sobre la base de desarrollos técnicos con un alto grado de digitalización y automatización) para un mayor control de los mismos.

Por otro lado, merece destacar que el Ejército del Aire y del Espacio realiza la monitorización continua del espacio aéreo de responsabilidad nacional, empleando para ello los recursos humanos y materiales

del Sistema de Vigilancia y Control Aeroespacial (SVICA), los aviones de reacción rápida (QRA, por sus siglas en inglés, *Quick Reaction Alert*) y los sistemas de comunicación que permiten el cumplimiento de la misión. A su vez, cuentan con equipos de detección e inhibición y se han desarrollado trabajos con los organismos implicados, a través de la Subsecretaría General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS), de la Secretaría de Estado de Seguridad, para la integración de sus sistemas en Siglo-CD.

En el marco de las actuaciones de protección del espacio aéreo se ha apostado por la realización de trabajos de coordinación entre Fuerzas y cuerpos de Seguridad del Estado y las Fuerzas Armadas en operaciones conjuntas para la defensa de un objetivo común o en espacios en el que existan instalaciones o infraestructuras a proteger que compartan el mismo espacio aéreo, o se requiera el apoyo de diferentes unidades para mayor eficacia de la defensa de la Seguridad Nacional. A modo de ejemplo, la Guardia Civil ha participado en el ejercicio ATLAS 25 organizado por el Estado Mayor de la Defensa relacionado con la integración de medios y procedimientos para responder de manera efectiva ante una amenaza aérea multi-capa y, en especial, UAS.

Además, se han fortalecido los foros de coordinación y los mecanismos de intercambio de información entre las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad, cuya cooperación resulta clave para incrementar la eficacia en la respuesta frente a este fenómeno. Todo ello ha visto su reflejo en la mencionada nueva Estrategia de Seguridad Aeroespacial Nacional y en el proceso de negociación de la nueva normativa europea EUSA, cuyo objetivo es armonizar y reforzar la regulación de estas actividades en el entorno aéreo europeo.

La rápida proliferación de los UAS tanto en los conflictos armados como en los ataques terroristas ha acelerado notablemente el desarrollo a nivel mundial y el continuo avance tecnológico. Comprar constantemente no es una solución válida, pues no hace sino agrandar nuestra brecha tecnológica, depender de terceros y no tener tiempo de reacción. Debemos generar toda la cadena de valor desde la I+D+i hasta la producción final y su comercialización internacional, para ser partícipes del futuro y la evolución de los UAS.

Dado el mandato interministerial del PERTE Aeroespacial, se lanzó esta visión a finales de 2024 con un documento conceptual sobre la necesidad de “Desarrollar una capacidad industrial nacional de UAS para Seguridad y Defensa”, algo que destacó el JEMAD en sus conclusiones de la presentación de la ESAN 2025.

Desarrollo de la política industrial aeroespacial nacional

En 2025, la política industrial aeroespacial nacional ha seguido consolidándose a través del Proyecto Estratégico para la Recuperación y Transformación Económica Aeroespacial (PERTE) con el que se quiere impulsar el desarrollo y la competitividad del sector espacial nacional y que tiene como objetivo financiar proyectos de I+D en el sector para aumentar la competitividad de su tejido productivo, centrando su atención en la capacidad productiva de constelaciones de satélites y en avanzar el grado de madurez de tecnologías con alto potencial disruptivo, alcanzando al ámbito académico y al empresarial.

Así, el PERTE incluye programas de I+D+i de alcance estatal, como el Programa Tecnológico Aeronáutico (PTA), que cuenta con una dotación pública acumulada cercana a los 190 millones de euros, procedente de las convocatorias iniciales del programa y vigente en su ejecución a 2025, y el Programa Tecnológico Espacial (PTE), con 70 millones, ambos orientados a fortalecer la innovación y la participación de pymes, *startups*, centros de investigación y consorcios público-privados. A ello

se suma la continuidad de las Misiones de Ciencia e Innovación del CDTI, que impulsan proyectos colaborativos de alto impacto tecnológico. Al término del tercer trimestre de 2025, se han asignado más de 75 millones de euros a 22 proyectos en el ámbito aeronáutico y espacial, de los cuales 32,3 millones han sido en forma de subvención a partir de las convocatorias del programa Misiones del CDTI y el resto mediante los créditos a proyectos de I+D con que cuenta este organismo, vinculados al PERTE Aeroespacial.

Así, al finalizar el tercer trimestre del año, el PERTE Aeroespacial ha movilizado los cerca de 2.900 Me asignados. El incremento de la contribución de la ESA, con una dotación de 625 millones de euros procedentes de los Fondos *Next Generation* del PRTR, consolida aún más la inversión en el PERTE Aeroespacial que se consolida como una opción política y estratégica a nivel de país para ser un instrumento que articule en los próximos la máxima cooperación interministerial para afrontar con instrumentos público-privados los retos de país y hacer avanzar el del sector aeroespacial español y ganar en relevancia en la economía aeroespacial global.

En coherencia con la vocación de permanencia de los PERTE establecida en el Real Decreto-ley 36/2020, el Proyecto de Ley de Industria y Autonomía Estratégica prevé que estos instrumentos puedan desarrollarse más allá del Plan de Recuperación, permitiendo articular proyectos tractores estratégicos.

En este contexto, y dado el buen desempeño del PERTE Aeroespacial y su alineación con la Estrategia de Seguridad Aeroespacial Nacional, se plantea un nuevo impulso estratégico mediante la iniciativa Alianza por España Aeroespacial, orientada a consolidar los avances alcanzados y a posicionar a España como un actor relevante y sostenible en la futura economía aeroespacial global con visión de largo plazo.

Por su parte, la Agencia Estatal de Investigación ha financiado 12 proyectos de investigación e innovación relacionados con la vulnerabilidad aeroespacial por un importe de 2.120.655,35 €. Además, ha financiado, dentro del subárea temática “Espacio”, 33 proyectos de investigación por 6.368.300 €.

A su vez, el Sistema SIGLO-CD ha sido desarrollado con la colaboración de Telefónica y ASDT, que han aportado tecnología para la detección y neutralización de drones. El gran desafío será incorporar capacidades de inteligencia artificial y *big data* para mejorar la previsión de incidentes y la gestión de riesgos en tiempo real.

Acciones realizadas para reducir el impacto medioambiental por el sector aeroespacial

En 2025 se han seguido adoptando medidas para reducir el impacto medioambiental del sector aeroespacial, destacando los avances en la implantación progresiva del combustible sostenible de aviación (SAF), cuyo uso no requiere modificaciones en las aeronaves y permite una adopción inmediata y segura tanto en el ámbito civil como en el militar.

El Centro para el Desarrollo Tecnológico y la Innovación (CDTI), dentro de su programa Misiones Ciencia e Innovación ha puesto en marcha en 2025 una misión orientada a la movilidad sostenible y descarbonización del transporte colectivo y de grandes volúmenes. Concretamente, en el ámbito de la aviación, la UE ha adoptado el reglamento *ReFuelEU Aviation*, que promueve el uso de combustibles de aviación sostenibles (SAF, por sus siglas en inglés), al objeto de que el SAF suponga hasta un 70% del combustible utilizado por las aerolíneas en 2050. Con esta misión, se propone a las empresas abordar líneas de trabajo como el impulso de soluciones de propulsión más eficientes, la generación de nuevos

combustibles sostenibles y la reducción de costes, con vistas a favorecer la reducción de emisiones, en línea con las estrategias del Pacto Verde Europeo.

En coherencia con los objetivos de reducción del impacto medioambiental del sector aeroespacial, la Estrategia de Seguridad Aeroespacial Nacional de 2025 destaca la conveniencia de mantener y reforzar, en el contexto actual, los programas de apoyo a la I+D+i orientados al desarrollo de tecnologías más sostenibles y eficientes.

En este sentido, iniciativas como el Programa Tecnológico Aeronáutico (PTA), desarrollado en el período 2021–2023 y vigente en su fase de ejecución y efectos en 2025, han permitido financiar 59 proyectos estratégicos, ejecutados en consorcio por cerca de 170 empresas nacionales, en su mayoría pymes, movilizando una inversión total de aproximadamente 315 millones de euros. Estos proyectos han continuado contribuyendo en 2025 al avance en nuevos combustibles sostenibles, sistemas de propulsión más eficientes y soluciones orientadas a la reducción de emisiones, consolidándose como un instrumento clave para la transición ecológica y la sostenibilidad del sector aeroespacial español.

INESTABILIDAD ECONÓMICA Y FINANCIERA

- Durante 2025, la rivalidad sistémica entre grandes potencias ha derivado en políticas comerciales coercitivas y un proteccionismo tecnológico.
- El complejo entorno geopolítico internacional, y el recrudecimiento de los conflictos bélicos, ha incrementado la importancia del comercio del material de la defensa y doble uso.
- La expansión acelerada de los mercados de criptoactivos plantea desafíos relevantes para la estabilidad financiera, especialmente en un contexto de creciente interconexión entre estos activos y el sistema financiero tradicional.

INESTABILIDAD ECONÓMICA Y FINANCIERA

El ejercicio 2025 ha consolidado la tendencia ya iniciada años atrás hacia un modelo de fragmentación geoeconómica. La seguridad económica ha desplazado a la eficiencia de costes como prioridad en las cadenas de valor globales.

Contexto geoestratégico y tensiones globales

En el plano internacional, la rivalidad sistémica entre grandes potencias ha derivado en políticas comerciales coercitivas y un proteccionismo tecnológico. El uso de instrumentos económicos como palanca de poder estratégico, incluyendo el control de exportaciones, subsidios selectivos o restricciones tecnológicas y comerciales, ha acelerado la transición global hacia la geoeconomía. En este nuevo entorno, garantizar la competitividad, reducir dependencias e impulsar la reindustrialización es una cuestión que afecta a la seguridad nacional.

La UE y España deben acelerar la adaptación sus marcos económicos, tecnológicos e industriales a esta realidad, reconociendo que sin capacidades productivas propias no existe margen real de decisión estratégica. Integrar criterios de resiliencia y autonomía estratégica en la política económica es una condición necesaria para corregir vulnerabilidades estructurales y proteger el interés nacional sin caer en dinámicas autárquicas ni comprometer la competitividad.

La economía global en 2025 ha operado bajo un paradigma de seguridad caracterizado por tres factores de tensión:

El primer factor está relacionado con consideraciones de naturaleza geopolítica y con el proteccionismo: las principales economías han intensificado el uso de instrumentos de defensa comercial. Concretamente, la guerra arancelaria se ha consolidado como una dinámica que afecta no sólo a la competición entre Estados Unidos y China, sino también a bloques terceros, como es el caso de la UE en sectores estratégicos, tales como el vehículo eléctrico, las tecnologías verdes, el sector alimentario y también el sector industrial de la seguridad y la defensa. Además, se identifica una instrumentalización creciente de las dependencias tecnológicas. De esta forma, el control de exportaciones sobre minerales críticos y tecnologías de doble uso se ha normalizado como herramienta de presión diplomática.

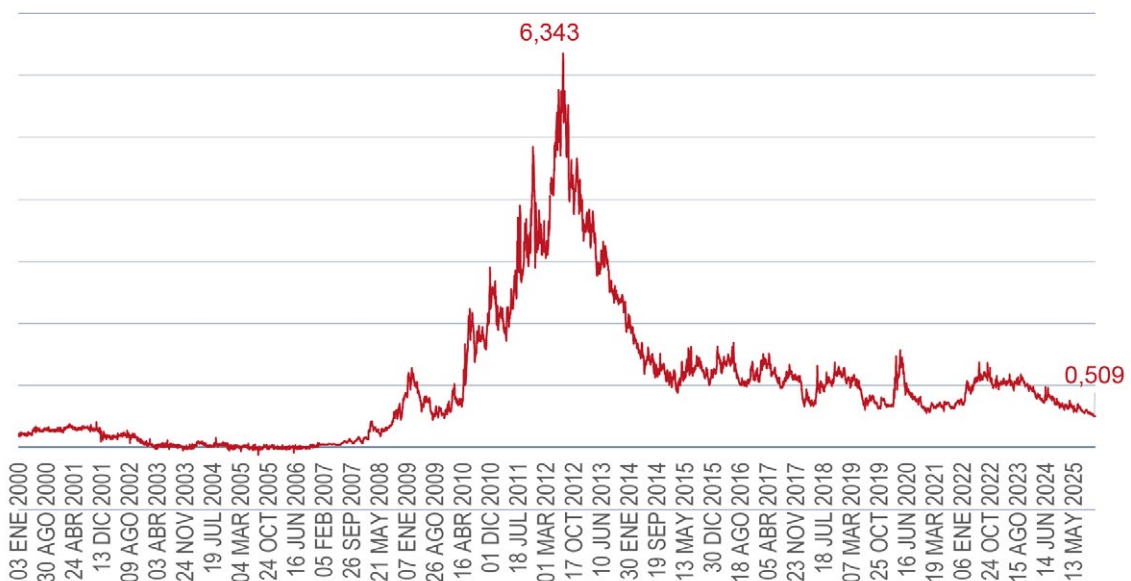
El segundo factor está relacionado con la seguridad financiera y deuda: el entorno de tipos de interés, aunque moderado respecto al bienio anterior, ha revelado la fragilidad del endeudamiento global. La falta de sincronización entre los bancos centrales de las economías avanzadas ha generado volatilidad en los mercados de divisas, encareciendo la financiación para economías emergentes y aumentando el riesgo de fragmentación financiera. Además, la deuda ha consumido un porcentaje creciente de los recursos públicos, limitando el margen fiscal para responder a *shocks* externos.

El tercer factor es la soberanía tecnológica. La adopción de tecnología emergente, entre ellas Inteligencia Artificial (IA), por parte de la ciudadanía, administración pública y tejido empresarial es un avance positivo de digitalización de la sociedad, que a su vez conlleva riesgos. El uso de IA sin una gobernanza de datos, y sin un control por parte del regulador puede conllevar la vulnerabilidad de derechos, puede agrandar la brecha digital y desigualdad en la sociedad, además de establecer una dependencia tecnológica con grandes empresas tecnológicas de países terceros. En 2025, el gran desafío es que la digitalización, y especialmente la IA, se traduzca en servicios más eficientes y seguros, sin dejar atrás a territorios, sectores o colectivos. Además, el acceso a semiconductores de última generación y la capacidad de procesamiento para IA se consideran ahora activos de seguridad nacional, provocando una fragmentación de los estándares tecnológicos internacionales y restringiendo el flujo de conocimiento científico.

Frente a este escenario central, y en lo que se refiere a las políticas monetarias, el Banco Central Europeo (BCE) ha consolidado su ciclo de relajación monetaria durante 2025. Con los tipos de interés de referencia descendiendo hasta el 2%, en la segunda mitad del año el BCE ha optado por mantener los tipos constantes, con el foco de la política monetaria rotando hacia el apoyo de un crecimiento económico que, aunque positivo, se muestra moderado y heterogéneo entre los países miembros. Esta transición hacia un entorno de tipos “neutrales” ha aliviado la presión hipotecaria y corporativa.

En este nuevo entorno, siguen existiendo riesgos vinculados a la estabilidad financiera en los mercados de renta variable y fija. Las valoraciones bursátiles, impulsadas por las bajadas de tipos y el optimismo en torno al sector tecnológico global, han alcanzado niveles elevados que podrían no estar totalmente respaldados por los fundamentales. En la zona euro no ha habido un contagio de los episodios de volatilidad vinculados a la situación política y fiscal en Francia y un factor de riesgo a futuro sería que esto dejase de ser así. Adicionalmente, persisten vulnerabilidades vinculadas al entorno geopolítico. En la coyuntura actual, el BCE dispone de margen para reanudar las bajadas y apoyar la estabilidad financiera. Sin embargo, el dilema surgiría si las nuevas barreras comerciales o tensiones geopolíticas provocasen un repunte inflacionario de oferta.

Con todo, en España, la prima de riesgo en 2025 ha continuado su tendencia decreciente, marcando cifras lejanas a los más de 600 puntos básicos que se llegaron a registrar en verano de 2012, en el peor momento de la crisis de deuda soberana y cuando España estuvo al borde del rescate internacional. (Figura 11.1)



Fuente: Elaboración propia DSN

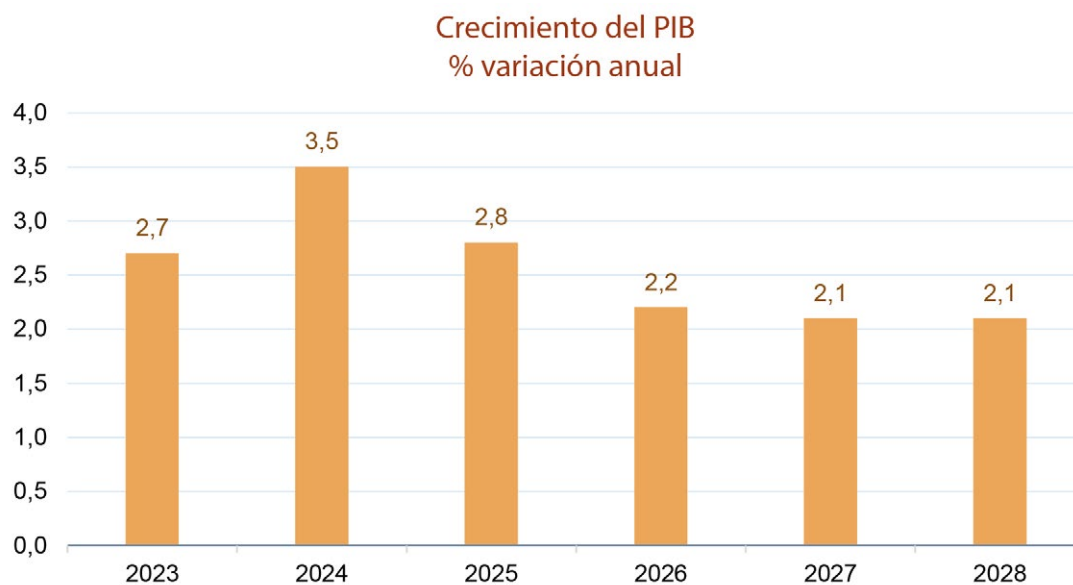
Figura 11.1: Prima de riesgo

Economía española en España en 2025

En 2025, España volvió a liderar el avance del Producto Interior Bruto (PIB) entre las economías desarrolladas, con un crecimiento del 2,8%, según datos preliminares conocidos a finales de enero 2026. En noviembre, el Gobierno mantuvo en el 2,2% la previsión de crecimiento para 2026 y estableció en el 2,1% la de 2027 y la de 2028. Estas estimaciones confirman la sólida evolución de la economía española en un contexto de incertidumbre internacional al registrar un crecimiento más fuerte, más equilibrado y responsable que en etapas anteriores. (Figura 11.2)

De esta forma, tras la recuperación del shock de la pandemia, este crecimiento se asienta en cambios estructurales de la economía española, que muestra un patrón diferente al de otras épocas de la historia económica de España, compatibilizando creación de empleo simultáneamente con una mejora de la productividad por hora trabajada, una reducción del endeudamiento de las empresas y una mejora de la posición fiscal. Además, este crecimiento estable transcurre en un contexto de elevada capacidad de financiación con el exterior y ahorro del sector privado, en especial de los hogares.

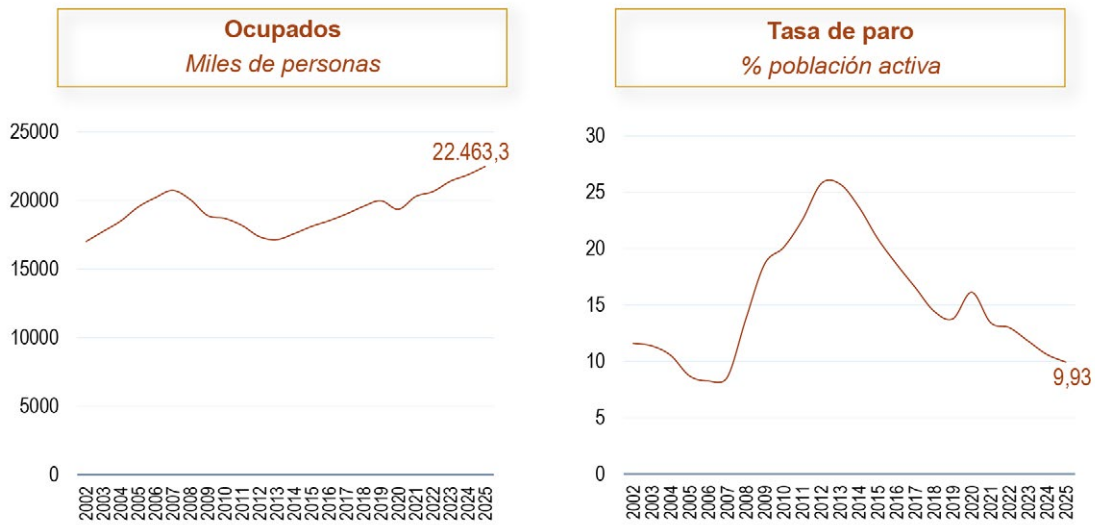
Sin perjuicio de lo anterior, las exportaciones españolas podrían verse negativamente afectadas ante un aumento de las fricciones geopolíticas o ante un potencial giro proteccionista.



Fuente: Ministerio de Economía, Comercio y Empresa

Figura 11.2: Crecimiento del PIB

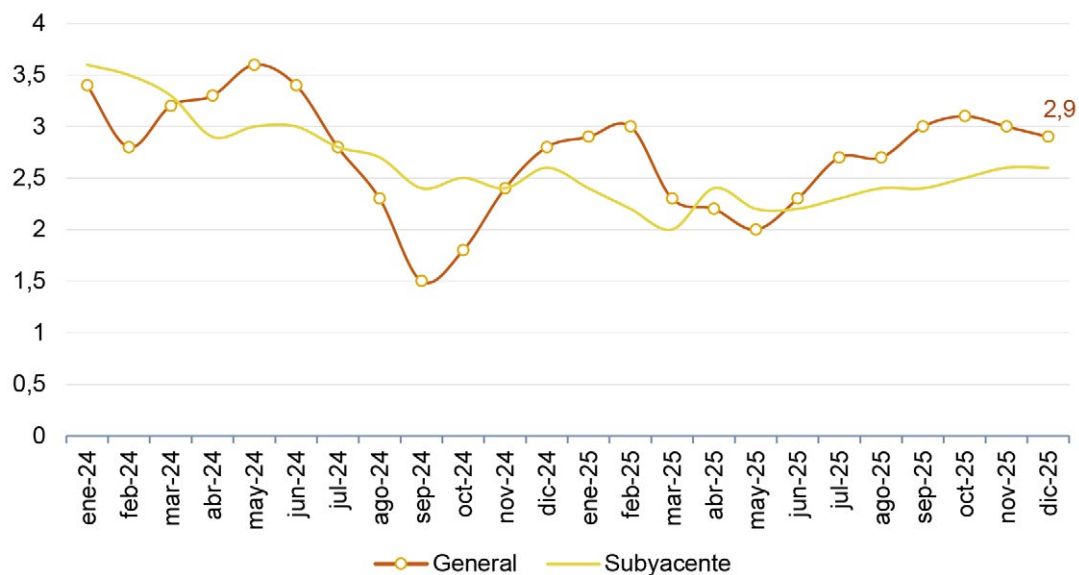
El crecimiento económico viene acompañado de unos indicadores de mercado laboral positivos. La ocupación sigue una senda al alza, impulsada tanto por el crecimiento de la población como por el aumento de la tasa de ocupación. La tasa de desempleo se aproxima a niveles de 2008 y se situó en el 9,9% a finales de 2025. (Figura 11.3)



Fuente: Encuesta de Población Activa

Figura 11.3: Indicadores del mercado laboral: ocupados y tasa de paro

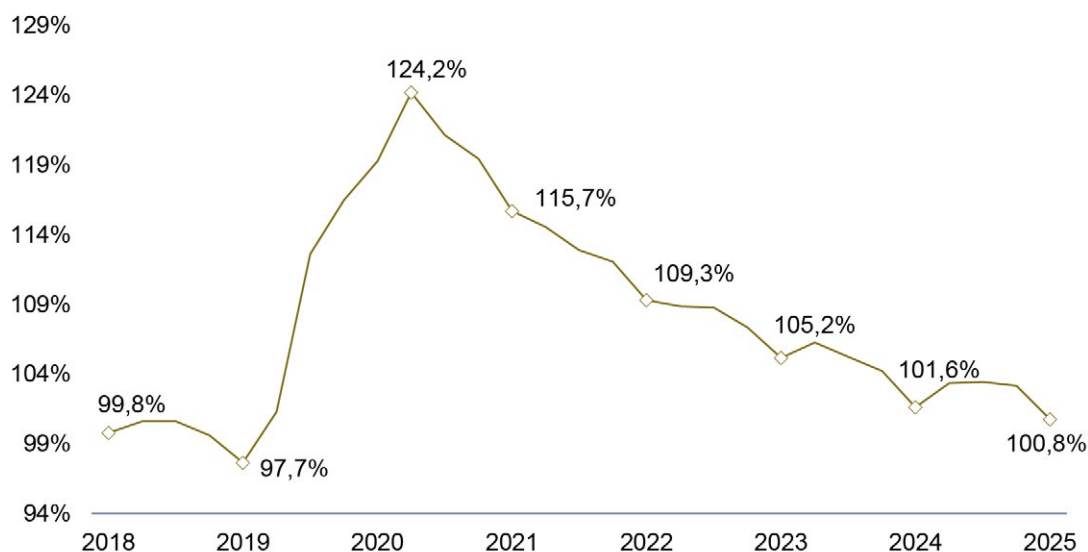
En lo que respecta a la inflación anual estimada en diciembre de 2025, este indicador terminó 2025 con una tasa interanual del 2,9%, según datos del Instituto Nacional de Estadística, superior en 1 décima a la del año anterior, debido a los servicios, los bienes industriales no energéticos y los alimentos no elaborados. Su evolución con respecto al año anterior es debida, principalmente, a la bajada de los precios de los carburantes y lubricantes para vehículos personales, frente al incremento de diciembre de 2024. (Figura 11.4)



Fuente: Instituto Nacional de Estadística

Figura 11.4: Tasa anual del IPC. Índice general y subyacente. Porcentaje

La ratio deuda pública/PIB encadena cinco años de caídas consecutivas desde la pandemia y ha finalizado 2025 en el 100,8%, acumulando así más de 23 puntos porcentuales de caída desde su nivel máximo durante la pandemia. Aunque este nivel es alto en términos históricos, se espera que continúe disminuyendo en los próximos años para situarse en torno al 99% en 2028, gracias a la consolidación de las finanzas públicas y el crecimiento económico. Esta resiliencia de la cartera de deuda pública, junto con el fuerte dinamismo de la economía española han ayudado a limitar el aumento de la carga de intereses, que sigue contenida en términos históricos en torno al 2,4% del PIB. (Figura 11.5)



Fuente: Ministerio de Economía, Comercio y Empresa

Figura 11.5: Deuda pública

El 15 de octubre de 2024, el Gobierno de España remitió a la Comisión Europea el Plan Fiscal y Estructural de medio plazo, en cumplimiento del nuevo marco de gobernanza económica y fiscal de la Unión Europea. El 30 de abril de 2025, el Gobierno remitió a la Comisión Europea el Informe de Progreso Anual, que recoge el cumplimiento de los compromisos fiscales y en materia de política económica incluidos en el Plan Fiscal y Estructural de Medio Plazo.

La Comisión Europea ha concluido que España cumplió con la regla de gasto comprometida con la Comisión Europea para 2024, que es la variable clave que tiene en cuenta la Comisión para evaluar el cumplimiento del Plan Fiscal Estructural por parte de un Estado miembro. En concreto, el gasto primario neto, o gasto computable, creció en España un 4,3% en 2024, por debajo del 5,3% recogido en el Plan Fiscal-Estructural presentado a Bruselas y permite cumplir también con el Consejo de la UE en su Recomendación del 21 de enero.

Por otra parte, el documento remarca que España cumplió en 2024 su objetivo de déficit por quinto año consecutivo. Así, cerró el pasado ejercicio con un déficit del 2,9% del PIB, si excluimos los efectos de la DANA, es decir, 0,5 puntos porcentuales menos que en 2023 y por debajo del objetivo del 3%.

La reducción del déficit se basa en un sólido crecimiento de la economía española y en el dinamismo del mercado laboral. La senda descendente del déficit muestra el rápido saneamiento de las cuentas

públicas. Desde el máximo alcanzado en la pandemia en 2020 con un 9,9% del PIB, el déficit público se ha reducido más de siete puntos porcentuales, casi 70.000 millones de euros.

Si se tiene en cuenta el gasto destinado a paliar los efectos de la DANA, que afectó principalmente a municipios de Valencia, el déficit en 2024 se sitúa en el 3,2%. No obstante, las reglas fiscales permiten excluir del déficit los impactos presupuestarios derivados de las catástrofes naturales, como ocurrió con el terremoto de Lorca. Por tanto, a efectos de las reglas fiscales el déficit de 2024 se situó en el 2,9%.

Gobernanza de seguridad económica

España cuenta con el mecanismo nacional de control de inversiones extranjeras conformado por el artículo 7 bis de la ley 19/2003 de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior, desarrollado en el *Real Decreto 571/2023, de 4 de julio, sobre inversiones exteriores*, y acompañado de la Disposición Transitoria Única del *Real Decreto-ley 34/2020*, para evaluar los riesgos que generan operaciones de inversión extranjera en materia de seguridad nacional y en los sectores estratégicos de nuestra economía. En particular, el mecanismo somete a autorización previa aquellas inversiones extranjeras directas en España que supongan la adquisición de un porcentaje mínimo del 10% del capital social de sociedades españolas cuando se produzcan en sectores clave, como en infraestructuras críticas, las tecnologías críticas, sensibles y claves para el liderazgo industrial, medios de comunicación, ciberseguridad, acceso a datos sensibles e insumos fundamentales, como el sector energético, sanitario y de alimentación. Asimismo, se exige también autorización para aquellas operaciones en las que los atributos del inversor pueden aumentar el riesgo, bien porque esté controlado o bajo influencia de gobiernos de terceros países, o porque exista un riesgo grave de que ejerza actividades ilegales o delictivas por haber sido sancionado en los ámbitos judicial o administrativo, con independencia del sector económico en el que se produzca la operación.

A estas herramientas, cabe añadir la creación, en 2025, del Comité de Inversiones Estratégicas. Este nuevo órgano colegiado, con el fin de impulsar la facilitación y agilización de nuevos proyectos de inversión, tiene las siguientes funciones:

- Contribuir a desarrollar una estrategia de inversión nacional, estableciendo líneas de acción para facilitar e impulsar la inversión nacional y extranjera en aquellos sectores de actividad que se consideren claves en España.
- Apoyar a los órganos y organismos competentes en el análisis y evaluación de proyectos de inversión, de forma que se tengan en cuenta sus efectos sobre la seguridad económica, el impacto socioeconómico, la sostenibilidad y todas aquellas otras dimensiones que se consideren relevantes.
- Impulsar la toma de decisiones por parte de los órganos competentes en materia de inversiones, a fin de agilizar la implementación de los proyectos de inversión.
- Fomentar la colaboración y coordinación entre los órganos competentes de las distintas Administraciones públicas en materia de inversiones.

Nuevas dinámicas en materia de seguridad económica

Tras las vulnerabilidades evidenciadas durante la pandemia y ante un entorno geopolítico cada más complejo, el *Trade Policy Review* de 2021 de la UE impulsó el desarrollo de un conjunto de instrumentos destinados a reforzar su autonomía estratégica abierta. En esta línea, la *Estrategia Europea de Seguridad Económica* (junio 2023) busca minimizar los riesgos de dependencias sin sacrificar la apertura, basándose en tres pilares: la protección contra los riesgos, la promoción de la competitividad, y el partenariado con socios.

En diciembre de 2025 se alcanzó un acuerdo político provisional entre el Parlamento Europeo, el Consejo de la UE y la Comisión Europea sobre un nuevo Reglamento para el control de las inversiones extranjeras con el fin de proteger mejor la seguridad y el orden público de la UE. En dicho texto se refuerza el control de las inversiones extranjeras en la UE mediante una armonización mínima que garantiza que todos los Estados Miembros dispongan de un mecanismo de control con un ámbito sectorial común mínimo, se incrementa la seguridad jurídica para los inversores al armonizar los procedimientos nacionales y se refuerza la cooperación entre Estados Miembros y la Comisión.

Posteriormente, la Comunicación de la Comisión Europea “*Un Enfoque Estratégico para el fortalecimiento de la Seguridad Económica Europea*” (diciembre 2025) reclama un cambio de paradigma: pasar de una postura reactiva a un despliegue más estratégico, proactivo y sistemático de todos los instrumentos de la UE para reforzar la seguridad económica, incluso si no fueron concebidos explícitamente con este objetivo. España está participando activamente los debates con el objetivo de garantizar una respuesta pragmática al entorno actual, lo cual debe ser compatible con el respeto a las normas internacionales del comercio y la profundización de la cooperación con socios fiables.

Nuestro país presenta dependencias significativas en sectores industriales clave, especialmente en materias primas críticas, tecnologías intermedias y etapas de procesado, con una fuerte concentración geográfica. Para identificar con precisión estas vulnerabilidades, se ha constituido desde el Ministerio de Economía, Comercio y Empresa una *Task Force* interministerial, en la que participan, (según los asuntos a debatir) todos o algunos de los demás departamentos con competencias en materia económica, existiendo una coordinación muy activa con la Oficina de Asuntos Económicos y G-20.

Estos trabajos ya han permitido localizar dependencias concretas en cadenas como tierras raras, semiconductores, metales estratégicos y productos químicos esenciales, así como evaluar su impacto sobre la competitividad y la seguridad económica. Una vez identificadas estas dependencias, se llevará a cabo un trabajo coordinado con las Oficinas Económicas y Comerciales y con el Instituto de Comercio Exterior (ICEX), con el objetivo de proponer mecanismos de apoyo y soluciones prácticas para las empresas españolas, promoviendo la diversificación de proveedores, el acceso a nuevos mercados, la inversión en capacidades estratégicas y la reducción de riesgos en las cadenas de suministro.

En otro orden de cuestiones, cabe señalar que el efectivo (el dinero en metálico) también actúa como un pilar fundamental de la resiliencia financiera y económica, estrechamente vinculado a la seguridad nacional, la autonomía estratégica y la estabilidad social. Para asegurar su disponibilidad, la FNMT contempla los riesgos a lo largo de toda la cadena, desde la producción, almacenamiento y distribución hasta su entrega al ciudadano, como un servicio esencial. La crisis de efectivo, o cualquier interrupción en la disponibilidad de dinero en metálico, constituye un riesgo crítico en un contexto marcado por la fragilidad del ecosistema digital y la creciente dependencia de los medios de pago electrónicos. Estos sistemas son vulnerables a interrupciones tecnológicas, ciberataques y fallos energéticos, como se evidenció durante el cero energético del pasado abril, la DANA, o los ciberataques procedentes de regiones en conflicto.

Ámbitos concretos: material de doble uso

El complejo entorno geopolítico internacional, y el recrudecimiento de los conflictos bélicos, ha incrementado la importancia del comercio del material de la defensa y doble uso. A esto se suma la dificultad de actualizar las listas internacionales de productos que deben estar sometidos a controles de exportación debido a la necesidad de alcanzar un consenso en órganos internacionales como el Arreglo de Wassenaar, donde Rusia es miembro y ha bloqueado sistemáticamente los avances.

En materia de Control de exportaciones de material de defensa y doble uso, España cumple con sus compromisos internacionales mientras protege los intereses esenciales de la Defensa Nacional y la política exterior del Estado, garantizando que el comercio de material de defensa y doble uso se realice con las máximas garantías de seguridad y transparencia.

La evaluación de las exportaciones se realiza con un análisis individualizado de cada solicitud por parte de la Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Doble Uso (JIMDDU), que está compuesta por Ministerio de Economía, Comercio y Empresa, el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, el Ministerio de Defensa, Ministerio de Hacienda, el Ministerio de Industria, Ministerio del Interior, Centro Nacional de Inteligencia y el Departamento de Seguridad Nacional. Este examen tiene en cuenta tanto las características del producto como el perfil del receptor. Además, se analizan antecedentes de denegaciones previas, tanto nacionales como de otros países, en operaciones similares de destino, usuario y producto, garantizando así la coherencia y el cumplimiento de los estándares internacionales. El análisis es especialmente exhaustivo en el caso de países considerados de especial sensibilidad.

En 2025, con el objetivo de garantizar que el régimen de control de exportaciones de material de defensa y doble uso da una respuesta eficaz al entorno internacional, se amplió la cobertura del control a otros productos y tecnologías de doble uso relacionados con la computación cuántica, circuitos integrados, materiales para fabricación aditiva, equipos para fabricación de semiconductores, inteligencia artificial, así como sus tecnologías asociadas, materiales explosivos y tecnología para la fabricación de armas ligeras y de asalto. Se trata de productos que se habían identificado y debatido en el marco del Arreglo de Wassenaar como de especial relevancia desde el punto de vista de los criterios de lucha contra la proliferación. Así, *la Orden ECM/551/2025, de 30 de mayo, por la que se modifican los anexos I.1, III.1, III.3, III.4 y III.5 del Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso, aprobado por el Real Decreto 679/2014, de 1 de agosto* ha supuesto un hito en la defensa de los intereses industriales españoles y el compromiso de nuestro país en la lucha contra la proliferación. España se adelanta así al resto de los Estados miembros que están trabajando en la actualización del Reglamento (UE) 2021/821 en relación con estos mismos productos, ante la dificultad de hacerlo en los órganos internacionales.

Cadenas de suministro, dependencias económicas y protección de sectores estratégicos

El riesgo asociado a las cadenas de suministro en 2025 se vincula principalmente a la vulnerabilidad logística y a la volatilidad del comercio global. Los cuellos de botella persistentes en rutas marítimas, la presión sobre el transporte terrestre y la competencia por capacidades portuarias han afectado la fluidez en sectores como automoción, agroalimentación, farmacia y electrónica. Episodios puntuales de disrupción, desde conflictos regionales hasta eventos meteorológicos extremos, han mostrado lo rápido que un incidente puede escalar en costes, retrasos y desabastecimiento temporal. Para España, el impacto se ha notado especialmente en importaciones críticas y en la planificación industrial,

reforzando la necesidad de diversificar rutas, fortalecer puertos estratégicos y aumentar la trazabilidad y resiliencia de la cadena.

Existen relevantes riesgos en la cadena de suministros de las infraestructuras de IA y cuánticas, dados los escasos proveedores de chips, su concentración en muy pocos países y la actual situación geopolítica. En esta línea se hacen urgentes las iniciativas para potenciar la soberanía en infraestructuras de IA, cuántica y chips de la UE.

El dilema entre eficiencia y resiliencia sigue sin resolverse plenamente. Aunque persiste la prioridad empresarial por costes bajos y proveedores globales, las recientes crisis de suministro y tensiones energéticas han reforzado la importancia de disponer de capacidades industriales propias. España ha dado pasos en esta dirección con medidas orientadas a fortalecer sectores críticos. No obstante, se estima necesario continuar con políticas que incluya incentivos comunes, financiación estable y objetivos estratégicos compartidos.

La desventaja competitiva que enfrentan sectores estratégicos como las tecnologías limpias, la defensa, la salud o la digitalización frente a economías dirigidas o fuertemente subvencionadas ha sido el principal detonante de la reciente intensificación regulatoria en la UE. En respuesta, la UE ha desplegado un conjunto creciente de instrumentos, tanto defensivos como proactivos, para contrarrestar prácticas desleales, proteger capacidades críticas y reforzar su autonomía estratégica. Entre ellos destacan los mecanismos de control de inversiones extranjeras, el régimen sobre subsidios distorsionadores, los instrumentos comerciales y antidumping, y el impulso normativo a sectores clave como los semiconductores (*Chips Act*), las materias primas críticas (*CRMA*), las tecnologías limpias (*Net Zero Industry Act*) o el seguimiento de crisis de recursos (*IMERA*).

Asimismo, persisten limitaciones en la capacidad de respuesta a nivel europeo, al no existir aún mecanismos plenamente operativos para activar de forma coordinada capacidades industriales ante crisis de suministro, lo que reduce la eficacia de las medidas adoptadas a nivel nacional.

La efectividad de todos los instrumentos dependerá, de su integración en una estrategia más ambiciosa que combine protección con creación de capacidad. Como señalan los informes de Draghi, Letta, y Niinistö, el reto europeo se concentra en tres frentes interdependientes: industria, tecnología y financiación. A nivel industrial, es urgente escalar proyectos y cadenas de valor continentales con velocidad suficiente para competir globalmente y de forma equilibrada intra-europea, garantizando el acceso a insumos estratégicos. En el plano tecnológico, Europa debe concentrar recursos en innovación disruptiva —inteligencia artificial, computación cuántica, *deep tech*— para reducir su dependencia y asegurar la soberanía digital y de defensa. Finalmente, en el plano financiero, es imprescindible crear un instrumento de capital estratégico europeo, ágil y con volumen suficiente, que refuerce los presupuestos nacionales y permita financiar proyectos industriales de gran escala, cerrando la brecha frente a potencias como EEUU y China. El reto no es abandonar el libre comercio, sino redefinir sus condiciones en función de la seguridad económica.

En este sentido, en la Unión Europea se está promoviendo el Fondo Europeo de Competitividad para el periodo 2028-2032, cuyo desarrollo e implantación marcará la agenda industrial, tecnológica europea de la década entrante.

Autonomía estratégica abierta

La inestabilidad económica y financiera se manifiesta como una amenaza multidimensional que no solo compromete el crecimiento, sino también la soberanía industrial y la autonomía estratégica. La dependencia de España de cadenas de suministro globales –con vulnerabilidades en minerales críticos, componentes tecnológicos o energía– agrava la exposición ante crisis geopolíticas o disrupciones logísticas. A estas vulnerabilidades se añade un cambio en la naturaleza de las dependencias, con terceros países condicionando el acceso a tecnologías avanzadas y recursos estratégicos, lo que limita el desarrollo de capacidades productivas propias y genera dependencias estructurales más difíciles de revertir. Por eso, resulta esencial proteger sectores estratégicos de la economía (como la industria energética, tecnológica o manufacturera intensiva) que, en caso de deslocalización o agotamiento de capacidad, producirían un golpe directo a la seguridad nacional. En este contexto, la autonomía estratégica abierta se convierte en una prioridad para reducir dependencias externas y fortalecer la producción interna.

En este contexto, la autonomía estratégica abierta debe entenderse como la capacidad de la Unión Europea y de España para reducir dependencias críticas y reforzar capacidades propias en sectores estratégicos, energía, tecnologías digitales, defensa, materias primas críticas o semiconductores, sin renunciar a la apertura económica, al comercio internacional basado en reglas y a la cooperación con socios afines.

La *Ley de Industria y Autonomía Estratégica* (pendiente de aprobación parlamentaria) se erige como instrumento clave para afrontar esta amenaza. Esta norma promueve la reindustrialización y modernización del tejido productivo español, reforzando la gobernanza industrial y creando una Reserva Estratégica de Capacidades Nacionales de Producción Industrial (RECAPI), capaz de movilizar rápidamente recursos críticos en caso de crisis. Prevé medidas de estímulo para el impulso a proyectos industriales estratégicos que incentiven la inversión y el empleo, extiende la posibilidad de impulsar Proyectos Estratégicos para la Recuperación y Transformación Económica (PERTE) más allá de la vigencia del Plan de Recuperación – consolidando inversiones industriales que permitan disminuir la exposición a choques externos- y sistematiza por primera vez la ordenación de los procesos de reindustrialización, entendidos como un proceso para gestionar crisis empresariales que reduzcan la volatilidad de los centros productivos más expuestos a fluctuaciones económicas internacionales. Además, la ley introduce medidas para desalentar la deslocalización: cuando las empresas que han recibido ayudas públicas deslocalicen su producción, deberán devolver esas ayudas bajo ciertas condiciones. También refuerza la coordinación institucional mediante la regulación de la Estrategia Española de Industria y Autonomía Estratégica y el Plan Estatal de Impulso Industrial, que definirán las líneas de actuación sobre los ecosistemas industriales prioritarios, y fortalece la gobernanza con la creación de órganos como el Consejo Estatal de Política Industrial y un Foro de Alto Nivel. En conjunto, estas iniciativas permiten mitigar riesgos sistémicos: fortalecen la autonomía estratégica, reducen la vulnerabilidad ante interrupciones de las cadenas globales y protegen los pilares industriales del país, contribuyendo de forma tangible a la seguridad económica nacional.

La autonomía estratégica continúa siendo un objetivo prioritario para la UE, pero su implementación efectiva sigue enfrentando importantes obstáculos. Persisten brechas estructurales en sectores clave como defensa, salud, tecnologías digitales o manufactura avanzada. Tal como diagnostica el informe Draghi, la falta de integración real entre las políticas industrial, energética, fiscal y diplomática impide construir una capacidad de acción coherente, tanto a escala europea como nacional.

Pese al consenso político alcanzado en los últimos años, la autonomía estratégica sigue limitada por la ausencia de instrumentos financieros comunes y por una elevada dependencia externa en fases críticas de las cadenas de valor. La implementación de la guía estratégica resultante de la revisión de

la competitividad europea (el Informe Draghi) y la definición de nuevos mecanismos de financiación, actualmente en debate, marcarán su evolución entre 2026 y 2028.

En este contexto, la autonomía estratégica requiere no solo marcos regulatorios e instrumentos de protección, sino también capacidades industriales y financieras que puedan activarse de forma efectiva en escenarios de disrupción.

En 2025, uno de los principales riesgos relacionados con la autonomía estratégica se centra en la limitada capacidad nacional y europea para desarrollar, controlar y operar tecnologías, infraestructuras y capacidades industriales esenciales sin depender de terceros países. Las tensiones internacionales han puesto de relieve la necesidad de contar con capacidades propias en ámbitos como el *cloud*, la microelectrónica, la ciberseguridad o la inteligencia artificial. La falta de alternativas europeas maduras en estas áreas expone a España a condicionamientos externos que pueden afectar a la continuidad operativa, la protección de datos sensibles y la toma de decisiones soberanas. Durante 2025, este riesgo se ha manifestado en debates sobre certificación de infraestructuras críticas, en retrasos de proyectos industriales de alto valor y en la creciente presión para acelerar consorcios europeos estratégicos.

Otro riesgo en política industrial tiene que ver con la dificultad de consolidar un tejido productivo fuerte y preparado para competir en sectores que están cambiando muy rápido. España sigue dependiendo en exceso de tecnologías y componentes fabricados fuera de la UE, lo que limita la capacidad de nuestras empresas para crecer y abrirse hueco en industrias clave como los semiconductores, las baterías o la energía limpia. Esta situación se nota en retrasos de proyectos, inversiones que no terminan de aterrizar y en la brecha que aún existe entre grandes compañías y pymes para incorporarse a las nuevas cadenas de valor. Todo ello hace que, en 2025, el reto no sea solo atraer industria, sino asegurar que las condiciones, financiación, regulación, talento y colaboración europea, permiten que esa industria se quede, escale y genere autonomía real para el país.

Así, la autonomía estratégica abierta se articula también como un instrumento de seguridad económica, que combina políticas industriales, diversificación de cadenas de suministro, mecanismos de control de inversiones y protección frente a coerción económica, reforzando la resiliencia nacional y europea ante escenarios de fragmentación geopolítica.

Desarrollo del Plan de Recuperación, Transformación y Resiliencia

El Plan de Recuperación, Transformación y Resiliencia (PRTR), se encuentra en una fase de ejecución avanzada. En diciembre de 2025, el Gobierno aprobó la Adenda de Simplificación al PRTR, con el objetivo de agilizar los procesos de verificación y ejecución, reducir cargas burocráticas, reforzar prioridades estratégicas y optimizar el uso de los recursos disponibles antes de la finalización del Mecanismo de Recuperación y Resiliencia, prevista para junio de 2026. La Adenda de Simplificación de España fue aprobada por el Consejo ECOFIN de la UE de 20 de enero de 2026.

Asimismo, en marzo de 2026, se ha presentado la sexta solicitud de desembolso, que en términos netos asciende a 6.467 millones de euros, lo que situaría a España en cerca de 60.511 millones de euros recibidos en transferencias no reembolsables del PRTR.

Esta solicitud de pago está asociada al cumplimiento de 78 hitos y objetivos. Esta solicitud está siendo evaluada por la Comisión, y, en caso de ser evaluada positivamente, supondrá elevar a 343 los hitos y objetivos cumplidos por España.

Prevención y lucha contra el fraude fiscal y financiero

La Agencia Estatal de Administración Tributaria tiene establecidos como objetivos estratégicos tanto la prevención como la lucha contra el fraude fiscal. En enero de 2024 se aprobó el vigente Plan Estratégico 2024-2027 cuyos ejes vertebradores son la asistencia al contribuyente, las actuaciones preventivas, el control del fraude y la estrategia de comunicación institucional.

En 2025, en línea con este Plan Estratégico, se publicó la Resolución de 27 de febrero de 2025, de la Dirección General de la Agencia Tributaria, por la que se aprueban las directrices generales del Plan Anual de Control Tributario y Aduanero de 2025, que desglosa las actuaciones a llevar a cabo por la organización en 2025.

Asimismo, en 2025, la Agencia Tributaria ha hecho públicos los resultados de sus actuaciones de control tributario efectuadas en 2024. Como consecuencia de su labor en la prevención y lucha contra el fraude, en 2024 la Agencia Tributaria obtuvo unos resultados recaudatorios de 18.928 millones de euros, lo que supone un 13,28% más que el año anterior.

En el ámbito normativo, en 2025 se han aprobado diversas normas de lucha contra el fraude, en particular de desarrollo de la Ley 7/2024, que traspuso la Directiva (UE) 2022/2523 del Consejo, de 15 de diciembre de 2022, por la que se establecen un Impuesto Complementario para garantizar un nivel mínimo global de imposición para los grupos multinacionales y los grupos nacionales de gran magnitud.

Así, en primer lugar, se ha aprobado el Reglamento del Impuesto Complementario, por Real Decreto 252/2025, de 1 de abril. Igualmente, en el ámbito de la Unión Europea, se ha aprobado, en relación con el Impuesto Complementario, la Directiva (UE) 2025/872 del Consejo, de 14 de abril de 2025, por la que se modifica la Directiva 2011/16/UE. Esta Directiva, conocida como DAC 9, establece la obligación de presentar una declaración informativa del Impuesto Complementario y regula el sistema de intercambio de su contenido entre las autoridades de los Estados miembros de la UE.

Por otra parte, la Ley 7/2024 adoptó medidas contra el fraude en hidrocarburos, así como contra el fenómeno de los llamados “carburantes de diseño”. Estos carburantes son productos con características técnicas muy similares a los carburantes de automoción convencionales, especialmente al gasóleo, pero con pequeñas modificaciones deliberadas para quedar excluidos del sistema de control aplicable a los hidrocarburos destinados a su uso como carburante de automoción.

En desarrollo de estas medidas incluidas en la Ley 7/2024, el 22 de diciembre de 2025 se publicaron en el Boletín Oficial del Estado tres Órdenes Ministeriales con el objeto de prevenir, y en su caso combatir, el fraude en el mercado correspondiente a las entregas de gasolinas, gasóleos y biocarburantes posteriores a la ultimación del régimen de depósito distinto del aduanero:

- La primera Orden aprueba el modelo 319 que regula el pago a cuenta del IVA correspondiente a dichas entregas.
- La segunda aprueba el procedimiento para reconocer la condición de operador confiable y regula la creación y el mantenimiento de un registro de operadores confiables, en materia de garantías del ingreso del IVA correspondiente a las citadas entregas.
- Por último, la tercera Orden establece los requisitos y los aspectos generales correspondientes a los avales que deben constituirse en garantía del ingreso del IVA con ocasión de dichas entregas, y aprueba el modelo de aval.

Por otra parte, el *Real Decreto 253/2025, de 1 de abril*, por el que se modifican, en materia de obligaciones de información, el Reglamento del Impuesto sobre la Renta de las Personas Físicas, aprobado por el Real Decreto 439/2007, de 30 de marzo, y el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos, aprobado por el *Real Decreto 1065/2007, de 27 de julio*, refuerza de forma significativa las obligaciones de información de las entidades financieras, permitiendo a la Administración tributaria, a partir del 1 de enero de 2026, obtener información de cuentas en entidades financieras con frecuencia mensual en lugar de anual, información relativa a los cobros efectuados mediante cualquier tipo de tarjetas y mediante pagos asociados a números de teléfono móvil e información relativa a operaciones realizadas con todo tipo de tarjetas. Entre las entidades financieras obligadas a informar se incluyen también las entidades que operen en España en régimen de libre prestación de servicios. Esto aumenta de forma notable la capacidad de control y cruce de información en la lucha contra el fraude.

En el ámbito de la lucha contra el fraude en el IVA, en la Unión Europea se ha aprobado en 2025 la *Directiva (UE) 2025/516 del Consejo, de 11 de marzo 2025*, conocida como *Directiva ViDA (VAT in the Digital Age* o IVA en la era digital), que se aplicará de forma progresiva hasta 2035 y que introduce medidas, que deberán ser traspuestas por los Estados miembros, para mejorar el control sobre el IVA, en materia de facturación electrónica en operaciones intracomunitarias, de ventanilla única de importación, y para que se conviertan en sujetos pasivos las plataformas de alquiler de corta duración y de transporte de pasajeros en determinadas circunstancias.

En España son varios los actores que participan en la prevención, detección e investigación de las tipologías delictivas vinculadas tanto a la corrupción como al fraude de ayudas y subvenciones. Entre otros pueden destacar, el Servicio Nacional de Coordinación Antifraude (SNCA) que ejerce de punto de contacto nacional de OLAF (Oficina de la Lucha Antifraude de la UE), la Fiscalía Europea, la propia OLAF, la Intervención General de la Administración del Estado (IGAE) y las Fuerzas y Cuerpos de Seguridad del Estado. Asimismo, la AEAT cuenta con funcionarios especializados de Vigilancia Aduanera con competencias específicas para colaborar en la investigación del fraude fiscal y del blanqueo de capitales derivado del delito fiscal.

Igualmente, el papel de los agentes de las FCSE en la contención y represión del fraude fiscal continúa siendo una prioridad, resultando esencial la continua profesionalización mediante la organización de unidades policiales especializadas, a través de formaciones *ad hoc*, como la impartida en el Curso de Investigación de delitos Económicos, asegurando así que dispongan de las capacidades técnicas necesarias para hacer frente a las organizaciones criminales de manera efectiva y con la contundencia necesaria. Del mismo modo, en julio de 2025, la Guardia Civil aprobó su Plan de Acción de Ética Profesional (PLAEP), el cual incluye medidas y acciones que contribuyen a la lucha contra la corrupción y a la prevención y detección de las conductas contrarias a la ética profesional por parte de sus efectivos; todo ello en el marco de su Sistema de Integridad, el cual vio la luz durante el año anterior. Entre sus elementos, también se incluye la implementación de un Sistema Interno de Información, que entró en funcionamiento en enero de 2025.

En el marco de la colaboración habitual con las distintas autoridades supervisoras, y detección de este tipo de hechos delictivos, para su posterior investigación en coordinación con las autoridades judiciales, se han desarrollado diferentes reuniones en el marco del Plan de Medidas Antifraude del Ministerio del Interior, a fin de profundizar en la colaboración y cooperación de investigaciones de corrupción y fraudes vinculados a las ayudas y subvenciones públicas, y de forma específica, con aquellas que derivarán del fondo de recuperación de la UE.

En cuanto a herramientas normativas, la aprobación de la *Ley 7/24 de 20 de diciembre* y su regulación de desarrollo, mejora la regulación y la prevención de los grandes fraudes en la venta de hidrocarburos al obligar al adelanto del pago del IVA, lo que previsiblemente supondrá una reducción o anulación de este tipo de fraudes.

En el plano de la cooperación internacional, la AEAT ha intensificado su cooperación con la Fiscalía Europea (EPPO), colaborando mediante la designación de funcionarios de apoyo a investigaciones que afectan a los intereses financieros de la UE (entre ellas fraudes transfronterizos de IVA superiores a 10 millones de euros).

Asimismo, la AEAT ejerce el liderazgo en el marco del LEWP Aduanas (*Law Enforcement Working Party - Customs*) del Comité del Consejo de la UE dedicado al refuerzo de la cooperación aduanera, asumiendo una acción específica para sensibilizar sobre el rol de la EPPO en la lucha contra el fraude aduanero y fiscal, identificar mejoras en el marco de cooperación bilateral y multilateral, e impulsar plenamente las capacidades que esta institución ofrece. Esta iniciativa, iniciada en 2024 y extendida al ejercicio 2025, incluye la celebración de un seminario en España en noviembre cuyo objetivo fue extraer conclusiones y desarrollar una guía de buenas prácticas para el análisis e investigación del fraude.

Por otra parte, continúa el esfuerzo de mejora en el intercambio de información internacional como herramienta para la prevención y la lucha contra el fraude fiscal, así como la incorporación de nuevos intercambios automáticos en materia fiscal en línea con lo establecido en la *Directiva 2011/16/UE del Consejo, de 15 de febrero de 2011, relativa a la cooperación administrativa en el ámbito de la fiscalidad* y por la que se deroga la *Directiva 77/799/CEE*, y los impulsados en el seno de la OCDE. Durante 2025, España ha continuado cumpliendo con los compromisos internacionales adquiridos, intercambiando la información dentro de los plazos establecidos.

Riesgos para la seguridad económica derivados de nuevas tecnologías: Fintechs, criptomonedas

El *Informe Estabilidad Financiera otoño 2025* del Banco de España, señala que la expansión acelerada de los mercados de criptoactivos plantea desafíos relevantes para la estabilidad financiera, especialmente en un contexto de creciente interconexión entre estos activos y el sistema financiero tradicional. Aunque su tamaño relativo sigue siendo relativamente limitado, su rápida expansión y la volatilidad que los caracteriza, en particular a los criptoactivos sin respaldo de activos financieros tradicionales, pueden amplificar escenarios de crisis en los mercados financiero.

El *Reglamento sobre Mercados de Criptoactivos (MiCA)* entró en vigor en junio de 2023, y en aplicación, en su totalidad, el 30 de diciembre de 2024, estableciendo normas de aplicación directa en todos los países de la Unión Europea para la emisión de determinados criptoactivos y la actividad de los proveedores de servicios. A lo largo de 2025 esta normativa ha continuado desarrollándose mediante la adopción de reglamentos delegados de la Comisión que incorporan normas técnicas de regulación o implementación, previamente planteadas por las Autoridades Europeas de Supervisión. Estos reglamentos desarrollan el Reglamento MiCA en diversos ámbitos: conflictos de intereses, la clasificación de los libros blancos de cripto activos, la gestión de la liquidez, etc. Asimismo, la publicación de distintas directrices a lo largo de 2025 ha contribuido al desarrollo del marco normativo de cripto activos. Estas directrices abordan distintos ámbitos: las condiciones y los criterios para la calificación de los criptoactivos como instrumentos financieros (*European Securities and Markets Authority, ESMA, 19.03.2025*) y la especificación de normas de la Unión para el mantenimiento de sistemas y protocolos de acceso de seguridad para los oferentes y las personas que soliciten la admisión a la negociación de criptoactivos distintos de las fichas referenciadas a activos y las fichas de dinero electrónico (ESMA,

26.02.2025), o las directrices sobre las prácticas de supervisión de las autoridades competentes para prevenir y detectar el abuso de mercado en virtud del Reglamento relativo a los mercados de criptoactivos (MiCA) (ESMA, 09.07.2025).

En el ámbito fiscal relativo a los criptoactivos, se destaca que 2025 es el segundo ejercicio en el que se han presentado las declaraciones informativas a la Administración tributaria sobre saldos y operaciones con monedas virtuales, así como la declaración de monedas virtuales situadas en el extranjero.

Paralelamente, se está tramitando la transposición al ordenamiento interno de la *Directiva (UE) 2023/2226 del Consejo, de 17 de octubre de 2023*, por la que se modifica la *Directiva 2011/16/UE relativa a la cooperación administrativa en el ámbito de la fiscalidad* (conocida como Directiva sobre cooperación administrativa 8, DAC 8), que incorpora el estándar internacional de intercambio automático de información sobre criptoactivos elaborado por la OCDE. En este proceso, se revisan también las obligaciones informativas nacionales sobre monedas virtuales, y se prevé sustituir el concepto de “moneda virtual” por el más amplio de “criptoactivo” y eliminar la obligación de informar sobre operaciones correspondiente al modelo 173 y reemplazarla por las nuevas obligaciones ligadas a la transposición de la DAC 8, aplicables tanto a residentes como a no residentes.

Asimismo, también destaca que, para articular el futuro intercambio internacional de información, España ha suscrito el Acuerdo Multilateral de Autoridades Competentes relativo al marco de información sobre criptoactivos y la Adenda correspondiente al estándar común de comunicación de información de cuentas financieras, lo que permitirá el intercambio de datos no solo con otros Estados miembros de la Unión Europea, sino también con terceros países. Se prevé que el primer intercambio de información amparado en estos instrumentos tenga lugar en 2027 respecto de la información correspondiente a 2026.

Todo ello se coordina, como ya se ha señalado anteriormente, con la nueva regulación financiera europea sobre mercados de criptoactivos (Reglamento UE 2023/1114, conocido como Reglamento MiCA) y sobre la información que debe acompañar a las transferencias de fondos y determinados criptoactivos (Reglamento UE 2023/1113).

Por su parte, también cabe señalar que la IA está transformando la forma en que se diseñan, operan y consumen los servicios digitales. En la Fábrica Nacional de Moneda y Timbre se ha aprobado una política de uso responsable de la IA, que establece los cimientos para implantar un marco de Gobernanza de la IA. Su objetivo es proteger la información institucional, prevenir riesgos asociados al uso de IA y asegurar que los recursos tecnológicos se empleen conforme a los principios de confidencialidad, legalidad y supervisión establecidos por la organización.

CRIMEN ORGANIZADO Y DELINCUENCIA GRAVE

- El 14 de julio de 2025, el Consejo de Seguridad Nacional aprobó la Estrategia Nacional contra el Crimen organizado y la Delincuencia Grave 2025, marco de referencia político-estratégico para prevenir y luchar contra los fenómenos criminales que causan un grave daño a la sociedad.
- La situación del crimen organizado en España se caracteriza por la prevalencia de actividades criminales relativas a los tráficos ilícitos, especialmente de cannábicos y de cocaína, seguidas, en menor medida, por actividades delictivas contra el patrimonio y el orden socioeconómico.
- El uso creciente de las nuevas tecnologías y de las herramientas digitales representan un desafío para la identificación y neutralización de estas actividades delictivas, así como la adecuada protección de las víctimas y personas vulnerables.

CRIMEN ORGANIZADO Y DELINCUENCIA GRAVE

El crimen organizado y la delincuencia grave se mantienen como una amenaza central para la seguridad nacional debido a su carácter flexible, opaco y con gran capacidad desestabilizadora, además del aumento progresivo de sus sinergias con otras tipologías delictivas. Esta evolución se ve reforzada por la proliferación de nuevas operativas ilícitas apoyadas en innovaciones tecnológicas.

Los mecanismos de respuesta, tanto nacionales como internacionales, se han reforzado de forma notable durante 2025. Por un lado, la cooperación las FCSE con otros organismos, como los servicios de vigilancia aduanera, ha permitido la desarticulación de organizaciones de crimen organizado. También se han fortalecido los planes nacionales de seguridad y se ha continuado en el análisis de información de inteligencia con el fin de identificar amenazas, tendencias y patrones vinculados al crimen organizado. En el ámbito internacional, España sigue participando en foros como Europol, Interpol y Eurojust, que juegan un papel clave en el intercambio de información, la coordinación de operaciones transfronterizas, la identificación de redes criminales y el apoyo en análisis de inteligencia.

Tendencias del crimen organizado y la delincuencia grave

La situación del crimen organizado en España se caracteriza por la prevalencia de actividades criminales relativas a los tráfico ilícitos, especialmente de cannábicos y de cocaína, seguidas, en menor medida, por actividades delictivas contra el patrimonio y el orden socioeconómico.

La situación geoestratégica de España, los lazos y vínculos con América Latina, junto al hecho de ser país de tránsito hacia el resto de Europa confieren a nuestro país la condición de punto estratégico clave para el narcotráfico mundial. Así, el narcotráfico en España representa una de las mayores amenazas proveniente del entorno del crimen organizado y de la delincuencia grave.

Gran parte de los episodios de violencia ocurridos en España están directamente vinculados al narcotráfico y se manifiestan a través de enfrentamientos armados, ajustes de cuentas, secuestros, amenazas, o ataques a las fuerzas de seguridad, con afectación directa, en algunos casos, a la ciudadanía.

Las organizaciones criminales siguen experimentando una transformación muy significativa, predominando aquellas más descentralizadas y flexibles, que cuentan con una cierta autonomía de sus integrantes.

El crimen como servicio (*crime as a service*) sigue, año tras año, ganando relevancia y moldeando el panorama de la criminalidad organizada, haciéndola más compleja y adaptable.

Se observa una instrumentalización de las redes como herramienta de amenaza híbrida, además de una creciente coordinación entre actores criminales y ciertos servicios de inteligencia hostiles, que buscan desestabilizar y explotar las vulnerabilidades internas mediante el desarrollo de actividades delictivas.

Igualmente, las organizaciones criminales se adaptan a un mundo cada vez más caracterizado por la digitalización y las tecnologías emergentes, lo que les permite perfeccionar, impulsar y ampliar sus actividades delictivas. En este punto destaca la utilización de la Inteligencia Artificial (IA) como vector potenciador y disruptivo del crimen organizado, el desarrollo de softwares específicos adaptados a la comisión de actividades delictivas o el incremento del uso de drones, especialmente para el tráfico de drogas, lo que constituye un verdadero desafío en la lucha contra esta amenaza.

En cuanto al uso de la IA, las organizaciones criminales y las bandas de delincuencia grave están adoptando tecnologías avanzadas en este campo para potenciar actividades como la falsificación documental, la suplantación de identidad, el *phishing* de alta sofisticación o la extorsión.

Esta evolución, junto con la dispersión y flexibilidad operativa de las organizaciones criminales, dificulta en gran medida la labor policial, resultando más difícil su detección e identificación, lo que complica la posibilidad solicitar el uso de las técnicas especiales de investigación para la obtención de indicios o pruebas de su actividad delictiva.

Por otro lado, todas las medidas llevadas a cabo en el marco de la Instrucción 9/2018 de la Secretaría de Estado de Seguridad, por la que se puso en marcha el *Plan Especial de Seguridad para el Campo de Gibraltar*, y sus sucesivas actualizaciones, han modificado sustancialmente la operativa de los grupos criminales dedicados al narcotráfico especialmente en esta zona. La necesidad de establecer en alta mar las narcolanchas con el fin de no ser intervenidas está suscitando un incremento de las actividades dirigidas al abastecimiento de combustible en este entorno. Se viene observando, así, un incremento exponencial de apoyos esenciales de tipo logístico, como el suministro de combustibles (“petaqueo”), que implica un riesgo añadido asociado a la volatilidad de estas sustancias.

Además de lo anterior, otro de los aspectos que más preocupan también es el reclutamiento de menores por parte de las organizaciones criminales para la comisión de delitos, que van desde los delitos más leves hasta la subcontratación de actos violentos, como amenazas, agresiones e, incluso, asesinatos a cambio de la oportuna remuneración.

En el ámbito de los delitos contra la Hacienda Pública cometidos por grupos organizados, sigue siendo destacable la defraudación del Impuesto sobre el Valor Añadido (IVA). Se trata de un fraude transnacional de especial complejidad, difícil acreditación y que supone un extraordinario perjuicio para el erario. Se ha detectado que personas vinculadas a otro tipo de delitos, como el narcotráfico, se integran en las organizaciones criminales dedicadas a cometer el fraude de IVA. Asimismo, en los últimos años se han detectado importantes vinculaciones entre las organizaciones criminales especializadas en la comisión de esta tipología delictiva con redes dedicadas al blanqueo de capitales, destacando la participación de ciudadanos de origen asiático en la fase de ocultación y desvío al extranjero de los fondos ilícitamente obtenidos.

En este campo viene siendo clave la actividad de la Fiscalía Europea que, desde 2021, se ha demostrado una vía efectiva para la investigación y represión del fraude al IVA transnacional, al ser competente para investigar y ejercer la acción penal de aquellos delitos contra la Hacienda Pública en materia de IVA transfronterizo, que afecten a dos o más Estados Miembros y que supongan un perjuicio de al menos diez millones de euros.



Fuente: Ministerio del Interior

Figura 12.1: Grupos de crimen organizado con actividad en España 2019-2024

Tráfico de drogas

El tráfico de drogas y, particularmente de cocaína, se mantiene como una de las mayores amenazas para la salud y seguridad de la ciudadanía, así como para la integridad de las instituciones públicas y privadas.

Atendiendo a los datos provisionales disponibles sobre incautaciones de esta sustancia, y a diferencia de la tendencia al alza de años precedentes, en 2025 se observa un ligero descenso con respecto al año anterior.

La principal vía de entrada de esta droga a nuestro país continúa siendo la marítima, a través de contenedores en grandes puertos, como los de Algeciras, Barcelona, Valencia, aunque se están produciendo algunas incautaciones en otros puertos secundarios, como el de Bilbao o Marín.

Si bien el uso de contenedores es el método más habitual de entrada, es destacable la utilización de embarcaciones de alta velocidad (EAV) que recogen grandes cantidades de cocaína en alta mar. En el último año se ha observado un significativo incremento del uso de estos medios para transportar la cocaína al continente europeo.

En cuanto al número de contenedores incautados con droga en 2025 en España, y aún con datos provisionales, se observa una tendencia a la baja respecto del año 2024.

Además de la ruta directa hacia Europa, sigue siendo frecuente el transporte de la droga hacia el Golfo de Guinea para posteriormente dirigirla hacia nuestro continente, patrón ya observado en años anteriores. Por ello, las rutas que transitan por la zona de África Occidental son un punto de especial interés para los operativos policiales.

Por su parte, se ha detectado un nuevo método de tráfico de drogas que, si bien es conocido en América Latina, no ha sido hasta fechas recientes que se ha detectado en Europa. Consiste en cargar la droga en un país de esta área geográfica en un contenedor que viaja en un buque portacontenedores, que posteriormente es abordado en alta mar por una lancha rápida (EAV o Go-Fast), a la que se transborda la droga.

En este contexto, se observa también un aumento de la presencia de organizaciones criminales sudamericanas en territorio español, que han pasado de desempeñar un papel logístico a implicarse directamente en la importación, distribución y control del mercado minorista. Estas organizaciones destacan por su movilidad, capacidad de adaptación y elevado grado de violencia, lo que contribuye al incremento de la conflictividad entre grupos.

Los métodos de ocultación de la droga son cambiantes, están en continua evolución y son cada vez más sofisticados. Una muestra de esta aseveración es la ocultación en el interior de maquinaria pesada o de palés de madera, o incluso en dobles fondos realizados mediante modificaciones estructurales de los cascos y compartimentos internos de los buques, lo que hace que la carga sea prácticamente indetectable. Otro método habitual es la ocultación en los componentes de refrigeración de los contenedores dedicados al transporte de mercancías refrigeradas (sistema *reefer*). Igualmente, se ha observado un incremento en el empleo de semi-sumergibles para su transporte, especialmente procedentes de Colombia y Brasil.

A excepción de los casos de incautación puntuales, ninguna incautación de los servicios aduaneros suele superar las 1,5 toneladas, lo cual sugiere hipótesis operativas de diversificación, limitación del tamaño del envío o mayor infiltración y sofisticación en las instalaciones portuarias.

Asimismo, en estas actuaciones se ha constatado la presencia de armas de guerra u otro material bélico, así como sofisticados medios de monitorización por parte de las organizaciones criminales, lo que incrementa considerablemente la complejidad de las operaciones.

En lo que respecta a la vía aérea, mientras que en 2024 se experimentó un notable incremento de las incautaciones de cocaína, en 2025 se ha mantenido estable el número de actuaciones, si bien la cantidad de droga incautada ha sido menor.

En lo concerniente a la **marihuana**, España continúa siendo el principal productor y exportador de Europa, consolidándose como un centro de acopio que aglutina a numerosas organizaciones criminales de diferentes nacionalidades que compiten por un mismo mercado. Esta situación ha derivado en un aumento de la rivalidad y del clima de tensión entre grupos, con el consiguiente riesgo de incremento de la violencia. Además, la marihuana producida en España presenta concentraciones de THC (principal componente psicoactivo del cannabis) cada vez más elevadas, lo que incrementa tanto su rentabilidad como su peligrosidad sanitaria.

Respecto de las incautaciones realizadas, cabe destacar que, tras el descenso significativo registrado en los dos años previos, los datos provisionales de 2025 muestran, sin embargo, un repunte de las aprehensiones.

En cuanto a las rutas de este tráfico ilícito hacia Europa, la Agencia de la Unión Europea sobre Drogas (EUDA) destaca la apertura de dos nuevas vías de distribución, una procedente de Canadá y Estados Unidos y otra desde Tailandia. En España se han incautado en 2025 dos contenedores marítimos con marihuana procedentes de Canadá y Tailandia respectivamente.

Por otro lado, cabe señalar la existencia de cierta preocupación a nivel europeo al haberse detectado un gran incremento de envíos tanto aéreos como marítimos, de marihuana hacia países del noroeste

europeo, como Irlanda, Países Bajos y Bélgica, y al hecho de que el porcentaje del THC del cannabis herbal norteamericano parece ser más elevado que el cultivado en Europa.

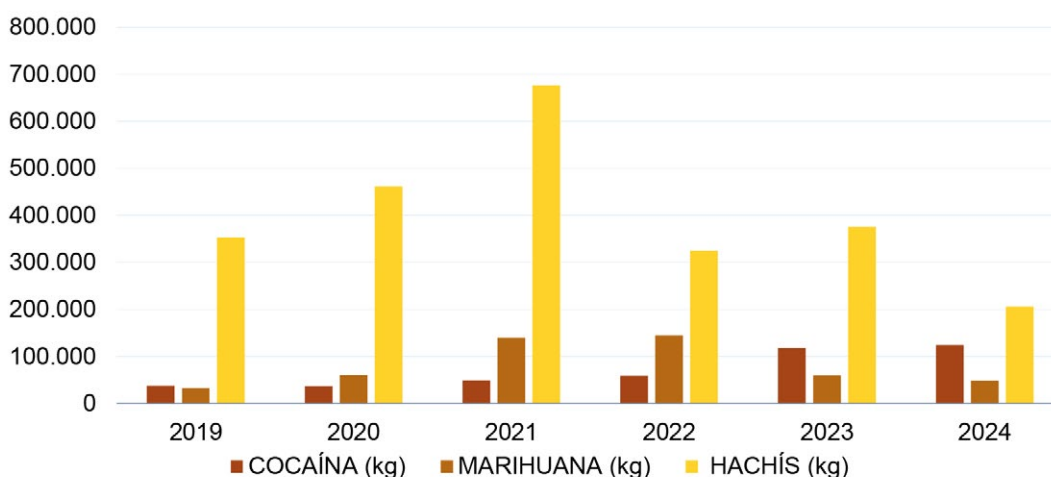
En lo que respecta al tráfico de **hachís**, tras el gran descenso en las aprehensiones experimentado en 2023, que se mantuvo durante el año 2024, en 2025 parece haberse reactivado la ruta desde Marruecos, principal productor mundial, hacia España. Si bien el tráfico de esta sustancia se canaliza principalmente por vía marítima, una vez introducida resulta significativa la cantidad de hachís transportada oculta en camiones, tendencia ya detectada en 2023 y que continúa en aumento, persistiendo rutas terrestres desde Almería, Granada y Cádiz hacia Francia y el resto de Europa.

Asociado al tráfico por mar, y tal y como se ha comentado anteriormente, también es importante resaltar el sensible incremento de aprehensiones de combustible en el sur de España, en particular en las provincias de Cádiz y Huelva, destinado a abastecer a las narcolanchas. (Figura 12.2 y 12.3)

Figura 12.2: Evolución de la droga intervenida de 2019 a 2024

EVOLUCIÓN DEL TRÁFICO DE DROGAS DE 2019 A 2024						
	2019	2020	2021	2022	2023	2024
COCAÍNA (kg)	37.768	36.888	49.159	58.508	118.325	124.040
MARIHUANA (kg)	32.568	59.888	139.711	144.803	59.235	48.466
HACHÍS (kg)	352.342	461.020	676.182	324.709	375.290	205.991

Fuente: Ministerio del Interior



Fuente: Ministerio del Interior

Figura 12.3: Evolución de la droga intervenida de 2019 a 2024

En cuanto a las plantas de cannabis, los datos provisionales disponibles de 2025 apuntan a un importante descenso en las aprehensiones dado que se ha incautado prácticamente la mitad de la cantidad intervenida en 2024. Continúa la prevalencia de las plantaciones *indoor*, en viviendas.

Cabe destacar que se han mantenido las agresiones y hostigamientos a miembros de las FCSE. Los narcotraficantes, en ocasiones, no dudan en embestir vehículos terrestres y embarcaciones cuando perciben riesgo de interceptación o pérdida de la droga, evidenciando una mayor agresividad hacia los agentes. Aunque el número de incidentes violentos registrados contra las FCSE en 2025 no ha sido especialmente elevado en comparación con años anteriores, se está detectando una mayor capacidad ofensiva (uso de armas de guerra). El fallecimiento de un agente de la Gendarmería de Portugal en el río Guadiana, al ser embestida su embarcación oficial por una narcolancha, evidencian esta circunstancia.

La presión ejercida sobre el narcotráfico en el Golfo de Cádiz y la desembocadura del río Guadalquivir ha provocado que las organizaciones dedicadas a esta actividad ilícita hayan desplazado su zona de influencia a la provincia de Huelva, río Guadiana y zona del Algarve, en Portugal. Conscientes de la gravedad del problema, las autoridades y fuerzas de seguridad españolas y portuguesas mantienen un esfuerzo continuo y coordinado para combatir esta amenaza.

La presión policial en combinación con lo establecido por el *Real Decreto-Ley 16/2018, de 26 de octubre*, a partir del cual las embarcaciones de alta velocidad pasan a considerarse como género prohibido, ha provocado que las organizaciones criminales modifiquen las rutas y los métodos de traslado e introducción de la mercancía, así como el establecimiento de redes logísticas para hacer posible la fabricación, el transporte, el abastecimiento y la reparación de dichas embarcaciones.

Así, las zonas de alijo se van ampliando cada vez más hacia el oeste (costa de Huelva y Portugal) y hacia el este (arco de Levante- desde las costas de Murcia hasta las de Gerona e Islas Baleares), detectándose incluso llegadas de embarcaciones al sur de Francia y a Italia.

Relacionado con estos cambios en los modos de actuación, se ha variado el lugar habitual para la fabricación de estas embarcaciones, eligiendo zonas del norte de Portugal donde no se les considera como género prohibido. Desde allí son trasladadas a distintos puntos de España, principalmente hacia la zona del levante español y Cataluña, tomando especial relevancia la zona del delta del Ebro.

Finalmente, y ante el temor de perder las embarcaciones, con el consiguiente menoscabo económico, también las organizaciones criminales operan desde Marruecos, evitando acercarse a las costas españolas para no ser intervenidas. Ante ello, junto al desembarco directo en costa, se recurre a otras embarcaciones (pequeñas semirrígidas, pesqueros, veleros, recreativas, yates, etc.), que son las que las introducen en nuestro territorio a través de puertos pesqueros, deportivos, o mediante los tradicionales alijos en playa con embarcaciones menores.

En la emergente “ruta atlántica del hachís”, la droga es cargada frente a las costas atlánticas marroquíes y se traslada en embarcaciones a países africanos más al sur, como Senegal, Guinea Bissau y Guinea Conakry, donde es alijada para su posterior transporte por vía terrestre a través del Sahel hacia Libia, desde donde puede enviarse a Europa o seguir hacia países de Oriente Próximo.

Del mismo modo, esta ruta atlántica también tiene otra variante, donde el destino final de la droga serían los países latinoamericanos. Para maximizar los beneficios y evitar que se pueda rastrear el dinero, las organizaciones criminales están haciendo trueques entre la cocaína y el hachís, utilizando la misma embarcación que importa la cocaína a África y Europa para transportar el hachís hacia dichos países.

También se han modificado los procedimientos de actuación y reactivado algunas tácticas que habían caído en desuso, como el de la modalidad aérea, consistente en el empleo de aeronaves de diferente tipología, incluidos drones, que realizan vuelos clandestinos entre Marruecos y España para transportar partidas de hachís. La detección de incursiones aéreas ilegales ha permitido el desarrollo de importantes operaciones durante el último año.

Por otra parte, respecto de la **heroína**, los datos provisionales de 2025 muestran un ligero aumento de cantidad aprehendida en España con respecto a 2024. La prohibición del cultivo de opio en Afganistán no parece tener, por el momento, efectos directos en este ámbito, probablemente debido a la existencia de importantes remanentes almacenados.

En cuanto a las **drogas sintéticas**, estas proceden en gran medida de laboratorios europeos, especialmente de Países Bajos y Bélgica, aunque en los últimos años también se ha observado un notable crecimiento de la producción en varios países asiáticos. Paralelamente, en España ha aumentado la fabricación local de derivados cannabinoideos y de catinonas sintéticas, lo que refuerza la oferta interna. En conjunto, estas sustancias se destinan tanto al consumo dentro del país como a su distribución en los distintos circuitos europeos.

En 2025, en España se han desmantelado 17 laboratorios: 10 de cocaína, 3 de sulfato de anfetamina (*speed*), 2 de metanfetamina y 2 de MDMA. Destaca la intervención de 582 kilogramos de MDMA en Tarragona en junio de 2025, siendo el mayor laboratorio de esta sustancia desmantelado en nuestro país. Los detenidos en dicha intervención tenían conexiones en Colombia y Países Bajos. Asimismo, se mantiene la tendencia de aprehensiones de MDMA y metanfetamina ocultos en equipajes de viajeros, así como en paquetería aérea. El resto de las sustancias de síntesis parecen mantenerse o, incluso, descender. En resumen, el número de laboratorios identificados y desmantelados en España durante 2025 se mantiene en cifras similares al año 2024.

Cabe señalar el aumento de incautaciones a nivel europeo de ketamina. Grandes cantidades de esta sustancia son enviadas de forma legal desde el denominado *triángulo de oro asiático* hacia Países Bajos, Bélgica y Alemania principalmente, desde donde son introducidas en el mercado ilícito para su exportación hacia África y Norteamérica. En contraposición, en España, aunque las aprehensiones se mantienen estables, se detectan numerosos envíos a través de paquetería postal con destino a Reino Unido, Estados Unidos, Australia y Nueva Zelanda.

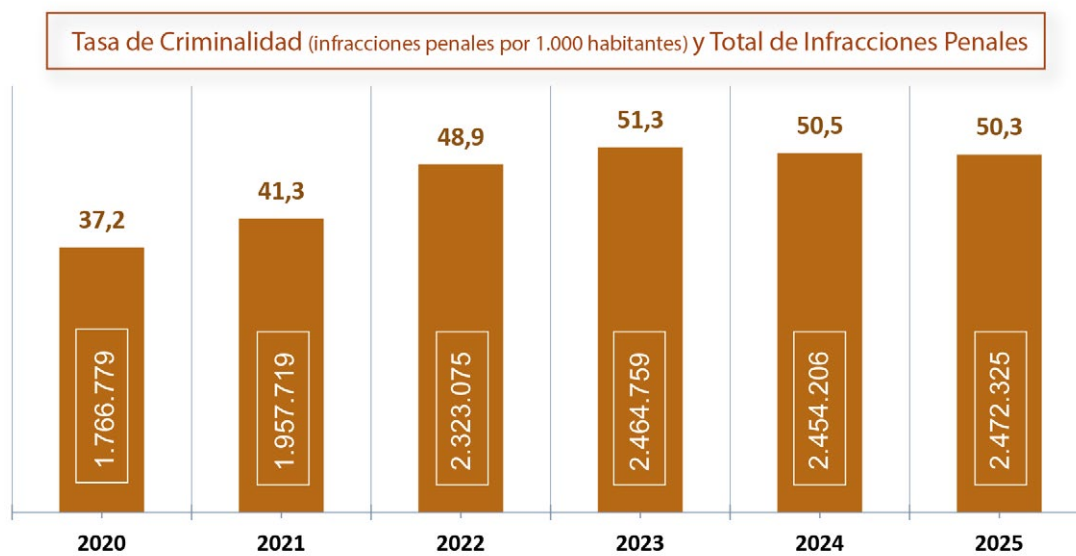
Finalmente, en cuanto a las nuevas sustancias psicoactivas (NPS), una de las novedades a nivel internacional es el aumento de incautaciones de sustancias de la familia de las orfinas, opioides de alta potencia que podrían actuar como sustitutos de los nitazenos (opioides sintéticos).

Pese a la no detección de estas sustancias en España, dada su relevancia y los graves problemas de salud que ocasionan, las FCSE mantienen una alerta continua ante cualquier indicio de detección o tráfico. Idéntica alerta se mantiene ante la proliferación de los cannabinoideos sintéticos, de los cuales se ha detectado un aumento a nivel global tanto de su potencia como de las formas de presentación en las que aparecen en los mercados (como golosinas y productos alimenticios).

Por último, continúan siendo regulares las incautaciones de benzodiazepinas, que aparecen en ocasiones en grandes cantidades en el sur de España con destino a Marruecos. Asimismo, especialmente en época estival y en localidades costeras, son recurrentes las incautaciones de óxido nitroso (“gas de la risa”), que viene sufriendo un aumento exponencial desde el año 2023.

Cibercriminalidad, otros tráficos ilícitos y graves formas delictivas

El total de **infracciones penales** con datos consolidados de 2025 asciende a 2.472.325, frente a 2.454.206 en 2024, lo que supone una variación porcentual 2024/2025 del 0,7%. (Figura 12.4)



Fuente: Ministerio del Interior

Figura 12.4: Tasa de criminalidad y total de infracciones penales

En el ámbito de la **cibercriminalidad**, destacan el fraude *online* (estafas informáticas) y la lucha contra la explotación infantil en la red. Con respecto a los primeros, es reseñable el uso de *malware* avanzado y de técnicas de ingeniería social para acceder ilícitamente a equipos y redes, manipular datos e interrumpir los sistemas buscando el enriquecimiento ilícito, aprovechando vulnerabilidades tecnológicas y falta de concienciación del usuario.

El fraude *online* se caracteriza por ataques dirigidos a obtener beneficios económicos mediante la suplantación de identidad, la manipulación de cuentas bancarias y el robo de información personal, utilizando ingeniería social y campañas de *phishing* cada vez más sofisticadas. Por su parte, la explotación sexual infantil representa una grave amenaza vinculada a la distribución y el consumo de material ilegal, la captación de menores mediante redes sociales y la creación de contenidos abusivos empleando tecnología emergente (especialmente la IA). Todo ello exige una respuesta legal y operacional basada en la detección proactiva, en la colaboración internacional y en el uso de herramientas avanzadas de investigación digital.

Además, se ha observado una clara profesionalización de los grupos de *ransomware*, que operan con estructuras organizativas similares a las de una empresa (con equipos especializados en desarrollo de *malware*, gestión de accesos, negociación y finanzas), lo que les permite ampliar su alcance y mantener una actividad criminal sostenida. A su vez, han orientado sus ataques hacia objetivos estratégicos

cuyo compromiso puede generar efectos desestabilizadores, especialmente en el sector público y en servicios esenciales, incrementando la presión sobre las víctimas para forzar el pago de rescates.

Esta evolución se ha visto reforzada por la expansión de modelos de negocio (*crime as a service*), que facilitan la comercialización de herramientas maliciosas y accesos comprometidos, generalizando capacidades ofensivas antes reservadas a actores altamente especializados y favoreciendo un incremento en la frecuencia, escala y sofisticación de los ataques.

En conjunto, estas dinámicas convierten al ciberespacio en un entorno de amenaza creciente para la seguridad y la estabilidad nacionales.

Entre las actuaciones de las FCSE destaca el desarrollo de la Cibercomandancia de la Guardia Civil, en funcionamiento desde julio de 2025 a través de la Oficina Nacional de Recepción Electrónica de Denuncias (ON-RED), la cual surge para gestionar la denuncia telemática con firma electrónica, a través de su Sede Electrónica. Hasta la fecha se han recibido 14.720 solicitudes de denuncias, de las cuales más de la mitad han sido catalogadas como delito y han derivado en las oportunas gestiones de investigación.

Por otra parte, las cuestiones asociadas a **precursores relacionados con el narcotráfico** se proyectan en el uso de productos adulterantes que facilitan el corte de las sustancias y en determinados disolventes de uso industrial o doméstico, cuyo marco regulatorio resulta más laxo que el de los precursores estrictamente catalogados. Esta flexibilidad normativa permite que organizaciones criminales utilicen sustancias de uso cotidiano para ocultar actividades ilícitas vinculadas a la fabricación de estupefacientes o psicotrópicos, aprovechando su amplia disponibilidad y su legítima circulación comercial.

Aunque no figuren en las listas más restrictivas, estas sustancias desempeñan un papel importante en la elaboración de drogas, como la cocaína, la heroína o drogas de tipo sintético. Por ello, las autoridades competentes prestan especial atención a patrones de compra inusuales, movimientos transfronterizos irregulares y empresas pantalla que intentan adquirir grandes volúmenes. La cooperación con el sector privado se configura como un pilar esencial para detectar operaciones sospechosas, complementada con la formación y sensibilización que facilitan la identificación de señales de alerta. En conjunto, la vigilancia de estos disolventes y sustancias “de bajo control” constituye un elemento clave para cerrar brechas de vulnerabilidad en este ámbito.

En el marco de la lucha contra el **contrabando de tabaco** se observa un aumento en el tráfico tradicional de cajetillas, así como en los kilogramos de picadura y otras labores del tabaco. No obstante, las importantes variaciones interanuales de los datos no implican una reducción del problema, sino un cambio en las dinámicas operativas.

Además, la nueva fiscalidad introducida desde enero de 2025 sobre productos, como los líquidos para cigarrillos electrónicos y otros productos relacionados con el tabaco, plantea un mayor riesgo de defraudación y de impacto sobre la salud pública, al tratarse de productos de moda entre los jóvenes.

Respecto al **desvío de precursores de explosivos**, en los pocos casos donde se ha constatado la fabricación ilegal de artefactos explosivos improvisados (IED) u otros tipos de explosivos, como mezclas pirotécnicas o pólvoras, los autores han recurrido a su adquisición en comercios legales, realizando su fabricación de materia artesanal y en cantidades poco significativas. Los comercios han incumplido, en la mayor parte de los casos, la obligación de requerir licencias a los particulares que son preceptivas en determinados productos, o bien no han comunicado al Punto de Contacto Nacional (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, Ministerio del Interior) esas ventas

sospechosas. En el caso de la fabricación de pólvora, sus componentes pueden ser adquiridos fácilmente en los comercios y posteriormente mezclados, al no haber restricciones en cuanto a su venta.

En relación con las **armas de fuego y explosivos**, a través de controles e inspecciones la Guardia Civil contribuye al mantenimiento de la seguridad pública, evitando que sean desviados al tráfico ilícito y utilizados por la delincuencia organizada o por grupos terroristas. En este ámbito, el Sistema de Control de Explosivos para la Prevención y Lucha contra el Terrorismo (SCEPYLT), representa una herramienta clave para la gestión segura de las transferencias intracomunitarias de explosivos.

Se ha detectado el uso de artificios pirotécnicos para la comisión de diversas actividades ilícitas, como la fabricación de mezclas explosivas utilizadas con el fin de violentar cajeros automáticos o el uso de bengalas en acontecimientos deportivos. De los contactos mantenidos con autoridades policiales de otros países europeos, se ha tenido conocimiento que se trata de un problema que está agravando cada vez más, llegando incluso a utilizarse dispositivos fabricados con pirotecnia para atacar a centros y agentes policiales.

El Punto Focal Nacional de Armas (PFNA), que recae en la Guardia Civil, se configura como un elemento clave de cooperación internacional y de coordinación nacional en la lucha contra el tráfico ilícito de armas de fuego, sus componentes y municiones.

Según los datos estadísticos de los últimos años, recogidos en el Cuestionario Anual de Flujos Ilícitos de Armas de Fuego de la ONU, en España se intervienen una media anual de unas 7.335, de las que menos del 1% del total son armas de guerra (56).

En lo que respecta al tráfico ilícito de armas de fuego, se observan nuevos *modus operandi*, como la transformación ilícita de pistolas empleando armazones originales de marcas especializadas en la fabricación de armas, así como el uso de armas de caza (rifles y escopetas) con estética táctica o de armas de guerra por parte de organizaciones criminales dedicadas al tráfico de drogas, que las obtienen a través de personas interpuestas que poseen licencias de armas en vigor.

Por otro lado, en línea con la protección de la sociedad frente a amenazas relacionadas con el consumo, los **medicamentos ilegales** de distinta naturaleza continúan siendo introducidos y distribuidos en España mediante redes que aprovechan el comercio electrónico y el transporte transfronterizo, principalmente por vía aérea.

Por su parte, el aumento del **tráfico internacional de productos falsificados** y sus repercusiones siguen siendo objeto prioritario de seguimiento y acción. Ello se refleja en las actuaciones derivadas de la Recomendación de la Comisión Europea 2024/915 de 19 de marzo de 2024, que identifica la falsificación como delito de alto impacto y establece medidas para fortalecer la cooperación entre titulares de derechos, proveedores de servicios y autoridades competentes, así como fomentar el uso de herramientas tecnológicas modernas en el control aduanero.

En aplicación de esta política, la AEAT participa en cauces permanentes de cooperación con organismos internacionales (OMA, INTERPOL, LEWP-Customs, OLAF, EUROPOL) y contribuye a operaciones sistemáticas de control intensivo en el entorno de la UE. A nivel nacional, la AEAT forma parte del Grupo de Trabajo para la Lucha contra las Falsificaciones de la Oficina Española de Patentes y Marcas (OEPM), desde donde se analizan las acciones de observancia de derechos de propiedad intelectual e industrial en España y se reportan a la Comisión Europea, en cumplimiento de la recomendación citada anteriormente.

De igual modo, el **tráfico ilícito de productos fitosanitarios** ha evolucionado drásticamente hasta convertirse en un fenómeno de carácter transnacional. A todo ello hay que sumar la fácil disponibilidad para su compra y la utilización de productos ilícitos procedentes de cualquier parte del mundo. Esto

no ha pasado desapercibido por los grupos criminales, quienes han identificado un nicho de mercado altamente lucrativo.

Por otro lado, cabe citar el **comercio ilegal de especies protegidas**, que ha pasado de ser considerado un simple delito ambiental para ser entendido como una amenaza de primer nivel por su impacto transversal en diferentes ámbitos.

Estas organizaciones utilizan las mismas rutas, estructuras logísticas y mecanismos financieros que son empleadas para otros mercados ilegales, lo que refuerza su capacidad operativa. En este contexto, durante el 2025, la Guardia Civil participó en la Operación THUNDER coordinada por INTERPOL a nivel mundial, para la lucha contra el tráfico de flora y fauna protegida. A nivel nacional se desarrollaron 741 inspecciones, se formularon 65 denuncias por infracciones administrativas, se identificaron 25 delitos relacionados con 35 personas detenidas o investigadas.

Asimismo, el Departamento de Aduanas e Impuestos Especiales y Vigilancia Aduanera de la AEAT desempeñan un papel esencial cuando estas conductas presentan dimensión transfronteriza o afectan al comercio exterior.

Los elevados beneficios económicos obtenidos mediante **delitos contra el medio ambiente**, en los que junto al tráfico de especies están otros, como la producción o uso de productos prohibidos y el desvío de residuos, exigen un refuerzo de los esfuerzos internacionales, que en el ámbito de los servicios aduaneros se proyecta intensificando los controles específicos (contenedores, residuos, especies reguladas) y colaborando activamente con organismos europeos e internacionales en operaciones transnacionales para combatir estas formas de criminalidad organizada.

Así, continúan siendo objeto de investigación múltiples entramados delictivos empresariales dedicados a la introducción ilegal de diferentes tipos de residuos, procedentes principalmente de Francia e Italia, en territorio nacional. Entre las actuaciones relacionadas con la delincuencia organizada en materia de contaminación, el SEPRONA de la Guardia Civil destacan: (Figura 12.5)

Operaciones destacadas de SEPRONA	
FINOPLAST	tráfico ilegal de residuos plásticos, procedentes en su mayoría de Francia, y almacenados en León para ser exportados al continente asiático
SUNRISING	tráfico ilegal de residuos textiles, procedentes de terceros países, almacenados en Valencia
RIFIUTI	tráfico ilegal de residuos desde Italia a España
LAYS	traslado ilícito de residuos desde la isla de Tenerife del continente africano
DASHBOARD	traslado de vehículos en desguace con origen en Reino Unido sin autorización, emitiendo residuos de emisiones de efluentes del aire acondicionado y sin certificado de destrucción o contaminación
MUGARIK	sustracción de residuos en Francia que son vendidos a empresas gestoras en España

Fuente: SEPRONA

Figura 12.5: Operaciones destacadas del SEPRONA contra la delincuencia organizada en materia de contaminación

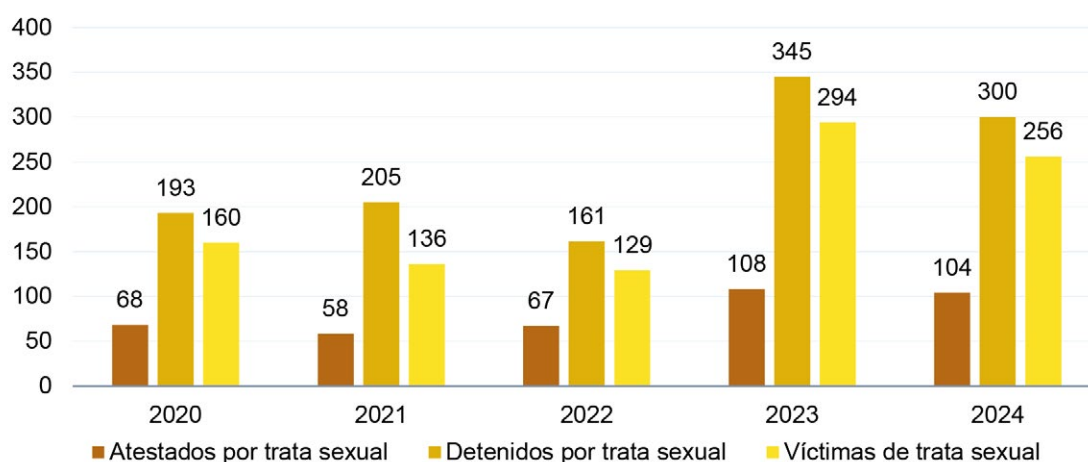
Las **explotaciones ganaderas y mataderos clandestinos** representan también una amenaza directa para la seguridad, con incidencia directa en la salud, al operar fuera de los sistemas de inspección sanitaria y control oficial. La falta de control veterinario, su desarrollo en condiciones higiénicas deficientes y la ausencia de trazabilidad convierten la carne procedente de estas instalaciones en un producto potencialmente peligroso para los consumidores, al tiempo que generan una competencia desleal frente a los productores legales, afectando a las cadenas de suministro reguladas y debilitando sectores productivos estratégicos para la economía nacional.

Las actividades ilícitas vinculadas al sacrificio clandestino de animales y a la introducción de carne y productos de origen animal sin control veterinario en la cadena alimentaria responden a un modelo de delincuencia estructurada que puede encuadrarse en la delincuencia grave y el crimen organizado. Estas redes articulan un ciclo completo, que abarca la captación y movimiento irregular de ganado, el sacrificio y despiece en instalaciones ocultas o no autorizadas, la falsificación o eliminación de la trazabilidad, el transporte y almacenamiento en condiciones higiénico-sanitarias deficientes y la posterior distribución de la carne de forma encubierta a establecimientos de restauración, comercios minoristas o canales de venta informal.

En relación con la **trata de seres humanos**, España continúa siendo principalmente un país de tránsito y destino de las **víctimas en sus distintas formas de manifestación**, tanto en su modalidad de explotación sexual como de explotación laboral. Ésta última ha venido experimentado un notable aumento en los últimos años, en línea con lo que está sucediendo a nivel mundial. El resto de las finalidades de la trata continúa presentando escasa incidencia.

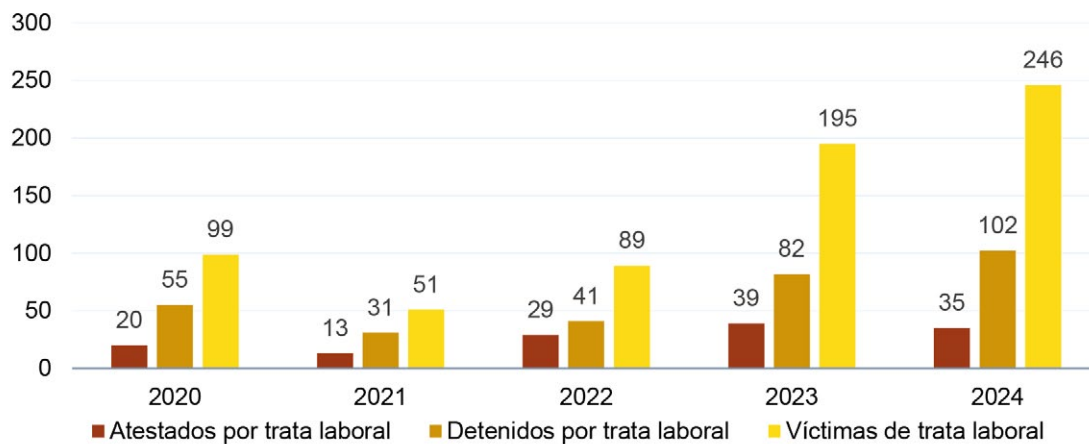
Al igual que otras formas delictivas, la trata de seres humanos se está viendo influenciada por el uso creciente e imparable de las nuevas tecnologías y de las herramientas digitales, que facilitan a los tratantes la comisión del delito al permitirles contactar con personas especialmente vulnerables. Internet ofrece a los autores un alto grado de anonimato, lo que dificulta su identificación y complica la obtención de pruebas, pues la información digital es volátil y las víctimas quedan aún más invisibilizadas, dificultando su localización y protección. A la vez, facilita la publicidad de los servicios ofrecidos por las víctimas, así como una gestión más eficiente y deslocalizada de los mismos.

Resulta imprescindible subrayar el emergente papel de la IA, que ya plantea amenazas significativas, especialmente en la producción de material de explotación sexual infantil o la generación de mensajes de captación de manera automática, aprovechando de manera individualizada la vulnerabilidad de las víctimas. (Figuras 12.6 y 12.7)



Fuente: Ministerio del Interior

Figura 12.6: Atestados, detenidos y víctimas de trata sexual 2020-2024



Fuente: Ministerio del Interior

Figura 12.7: Atestados, detenidos y víctimas de trata laboral 2020-2024

En el ámbito de la trata y explotación sexual, las mujeres continúan sufriendo de forma desproporcionada las consecuencias de esta grave violación de los derechos humanos. En su mayoría provienen de América Latina, con Colombia como principal país de origen. En el caso de la trata y explotación laboral, las víctimas son en su mayoría hombres, y proceden de América Latina y también del Norte de África, siendo los sectores agrícolas y el textil los más afectados.

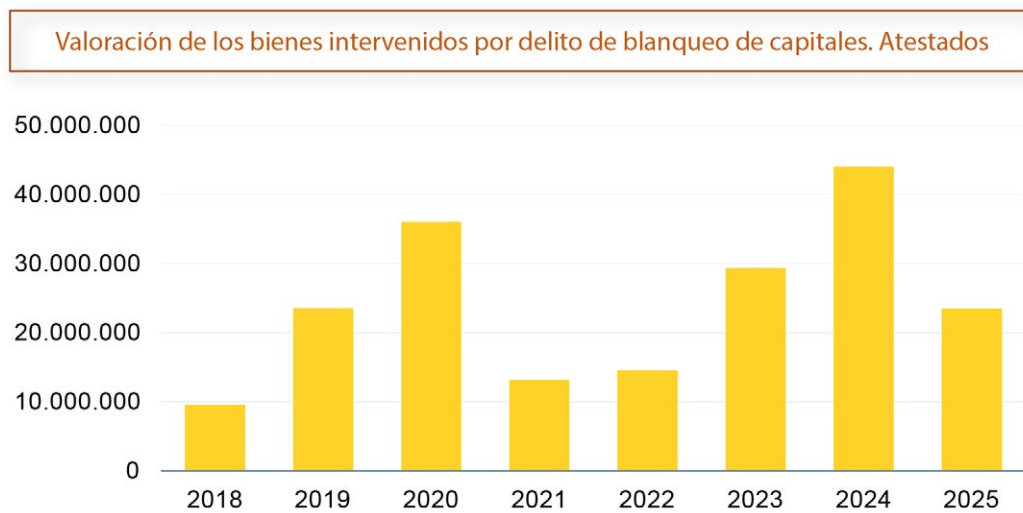
En muchos casos, las víctimas se encuentran en situación de estancia irregular en España o carentes de cualquier tipo de contrato laboral. Pese a que los menores de edad no presentan una elevada incidencia, se presta una especial atención a la capacidad de las redes criminales para ocultarlos hasta su mayoría de edad. También debe tenerse en consideración la específica vulnerabilidad que presentan los Menores Extranjeros No Acompañados (MENA).

Es esencial considerar el mayor riesgo que enfrentan los niños, niñas y adolescentes en los entornos digitales. Los tratantes aprovechan esta situación para acceder a ellos a través de redes sociales o incluso de plataformas de videojuegos con funciones de chat privado, con el fin de captarlos y conducirlos a situaciones de explotación, especialmente en el ámbito sexual o de la pornografía. Respecto de la explotación sexual infantil online, durante 2025 se ha reforzado la cooperación policial internacional, destacando la participación activa de España en EMPACT CSE (*Child Sexual Exploitation*), a través del cual se han intensificado las operaciones conjuntas, el intercambio de inteligencia y el desarrollo de capacidades especializadas orientadas a la persecución de autores, la desarticulación de infraestructuras criminales en línea y a la identificación de víctimas que, en algunos casos, apenas alcanzan el año de edad. (Figuras 12.8 y 12.9)



Fuente: Ministerio de Hacienda

Figura 12.8: Valoración delito de blanqueo de capitales. Atestados



Fuente: Ministerio de Hacienda

Figura 12.9: Valoración de los bienes intervenidos por delito de blanqueo de capitales. Atestados

Las tendencias actuales en materia de **blanqueo de capitales** muestran una combinación de métodos tradicionales y nuevas estrategias impulsadas por la tecnología. Continúan siendo comunes las estructuras opacas, como los complejos entramados societarios configurados sobre gran cantidad de empresas pantalla, las inversiones en el sector inmobiliario, así como el uso de redes informales (*hawala* o el flujo de efectivo).

Sin embargo, el auge de las criptodivisas constituye una de las tendencias más prominentes en el panorama actual del blanqueo de capitales, por gozar de una serie de características que los hacen especialmente atractivos: anonimato o pseudo-anonimato, capacidad de remisión 24/7 sin dependencia de ningún servicio o entidad, ínfimas comisiones y amortiguamiento de la tradicional volatilidad del precio mediante el uso de *stablecoins* (monedas virtuales emparejadas al valor de sus contrapartes en monedas de curso legal, normalmente el dólar estadounidense). Por ello, se confirma la evolución de esta amenaza hacia un uso más intensivo.

En este contexto, los delincuentes están aprovechando cada vez más las plataformas de intercambio de criptomonedas para mover y ocultar las ganancias ilícitas obtenidas de actividades como el cibercrimen, el narcotráfico o las estafas, dificultando significativamente el rastreo de los activos por parte de las autoridades y obligando a los reguladores a intensificar los esfuerzos para incorporar a los proveedores de servicios de activos virtuales en los marcos de prevención de blanqueo de capitales.

Por todo lo expuesto, podemos concluir que el blanqueo de capitales a través de las criptomonedas representa un riesgo creciente para la estabilidad financiera y la seguridad internacional. Una de las amenazas más señaladas es el uso de dispositivos de almacenamiento físico, que permiten transportar grandes cantidades de valor de forma discreta a través de fronteras sin necesidad de declarar dinero en efectivo. Esto dificulta el rastreo por parte de las autoridades, ya que las criptomonedas pueden ser transferidas de manera casi instantánea y con cierto grado de anonimato. Además, la portabilidad y el cifrado de estos dispositivos hacen que sea complicado detectar y confiscar los fondos, lo que facilita operaciones ilícitas como la financiación del terrorismo, la evasión fiscal o el lavado de dinero provenientes del crimen organizado.

Por otro lado, se viene detectando con cada vez más frecuencia las organizaciones criminales de origen asiático especializadas en blanquear las ganancias de otras organizaciones a cambio de una comisión (de nuevo, en formato *crime as a service*).

Además, dentro de las medidas previstas en el Plan Especial de Seguridad para el Campo de Gibraltar, las Fuerzas y Cuerpos de Seguridad del Estado llevan a cabo actuaciones para detectar actividades de blanqueo de capitales, actuando sobre la estructura económica de los grupos criminales dedicados al narcotráfico al objeto de limitar su capacidad operativa, dando continuidad a la intensa labor en el ámbito de las investigaciones económicas y patrimoniales que se vienen desarrollando en los últimos años.

Finalmente, cabe señalar que, en paralelo, en el ámbito preventivo, las autoridades españolas han intensificado las medidas supervisoras y regulatorias, incluyendo la ampliación de sujetos obligados, la mejora en la identificación del titular real y el reforzamiento de los sistemas de control transfronterizo de los movimientos de efectivo y medios de pago.

La *Ley Orgánica 1/2025, de 2 de enero*, de medidas en materia de eficiencia del Servicio Público de Justicia, estableció la eliminación del programa *Golden Visa*. A pesar de que el riesgo de blanqueo en el sector inmobiliario no desaparece, sí se limita la entrada de grandes capitales con controles migratorios débiles; y el atractivo de España como destino de legitimación patrimonial mediante inversión inmobiliaria para grupos criminales.

Por último, cabe reseñar que en los recintos aduaneros se mantiene el control de los movimientos de medios de pago, con el fin de impedir la incorporación de efectivo al circuito de blanqueo de capitales.

En 2025 se ha puesto en marcha un Plan de Investigación de Blanqueo de Capitales que tiene por objeto identificar los nuevos esquemas mediante los cuales organizaciones criminales emplean el sistema financiero digital. Esta línea incluye investigaciones orientadas a *neobancos* -plataformas 100% digitales que operan bajo licencia bancaria de terceros-, y que han sido identificados como posibles canales de entrada o legitimación de fondos ilícitos, aprovechando las ventajas tecnológicas y los vacíos regulatorios existentes.

Los **delitos de odio** constituyen una forma de delincuencia especialmente grave, porque no solo atentan contra bienes jurídicos universales como la integridad física o la libertad, sino también contra la dignidad y la igualdad de los colectivos más vulnerables. De acuerdo con los datos actualizados de 2025, el racismo y la xenofobia continúan siendo uno de los ámbitos discriminatorios con mayor incidencia, al haber pasado de 804 hechos investigados en 2024 a 854 en 2025, lo que supone un incremento del 6,2%. Por su parte, uno de los ámbitos que experimenta el mayor crecimiento es el antisemitismo, que pasa de 37 a 68 hechos investigados, con una variación aproximada del 83,8% respecto al año anterior.

Entre los peligros más relevantes se encuentran en la normalización de discursos discriminatorios en redes sociales, que propician amenazas o agresiones, y especialmente en la infradenuncia, por cuanto muchas agresiones quedan ocultas y no llegan ni siquiera a las estadísticas policiales, debilitando, así, tanto la respuesta institucional como el apoyo a las víctimas.

El Ministerio del Interior, a través de la Oficina Nacional de Lucha Contra los Delitos de Odio (ONDOD), publicó en marzo de 2025 un análisis basado en una encuesta a víctimas y testigos de delitos de odio que profundiza en las barreras que dificultan la denuncia: vergüenza, desconocimiento de los recursos o miedo a represalias son motivos recurrentes apoyados por datos reales. En respuesta, el III Plan de Acción de Lucha contra los Delitos de Odio (2025-2028) tiene por objeto reforzar la prevención, la asistencia a víctimas y la persecución penal.

Durante el último ciclo anual, se ha observado una tendencia sostenida al alza en las denuncias por delitos de odio en España, con especial incidencia en los ámbitos relacionados con racismo/xenofobia, orientación sexual e identidad de género. Este incremento responde tanto a una mejora en los mecanismos de detección y denuncia, como a un repunte de la polarización social amplificadas por entornos digitales, que constituyen un vector clave en la difusión de discursos de odio, susceptibles de evolucionar hacia procesos de radicalización violenta.

Cooperación internacional y desarrollos estratégicos

La cooperación internacional frente a la criminalidad en todas sus manifestaciones resulta esencial para su neutralización, tanto a nivel bilateral con los países socios y aliados, como en el seno de las organizaciones e iniciativas multilaterales de las que España forma parte.

Este tipo de cooperación continúa reforzándose con nuevas iniciativas en materia de lucha contra el crimen organizado, redes de expertos y grupos de trabajo centrados en diferentes ámbitos de la amenaza. Se mantiene la participación de FCSE en los mecanismos de cooperación internacional, colaborando para ello con Instituciones y Agencias europeas, así como con los diferentes socios existentes a nivel global.

Durante 2025 se ha avanzado en la definición e implementación de la Estrategia Europea de Seguridad Interior (ProtectEU). Esta estrategia configura la visión común para reforzar la preparación, la resiliencia y la respuesta de la UE frente a amenazas transnacionales o los fenómenos híbridos, y establece un marco integral que combina prevención, cooperación operativa e interoperabilidad de sistemas. Para articular su implementación destaca la necesidad de que la Comisión informe de manera periódica al Comité de Seguridad Interior (COSI) sobre el progreso de las iniciativas clave, así como el papel de la Presidencia al elevar cuestiones estratégicas al propio COSI y al Consejo de la UE en materia de Justicia y Asuntos de Interior (JAI).

Además, se está colaborando con EU-LISA en la puesta en marcha de una plataforma llamada *Joint Investigation Teams Collaboration Platform* (Plataforma de Colaboración para Equipos Conjuntos de Investigación), que permitirá mejorar la cooperación entre los miembros de los equipos conjuntos y contar con una herramienta común a nivel europeo para compartir información, coordinar actividades y mantener una comunicación ágil.

En materia de tráfico de drogas, el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), como representante del Ministerio del Interior, participa en diversos proyectos, foros y grupos de trabajo internacionales sobre drogas, como el Grupo Horizontal de Drogas (GHD) del Consejo de la Unión Europea y sus Diálogos con terceras regiones y Estados; iniciativas y foros de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC); o la Junta Internacional de Fiscalización de Estupefacientes.

Además, desde su lanzamiento en enero de 2024, CITCO es el punto nacional de contacto del Ministerio del Interior para la *Alianza Europea de Puertos*, una iniciativa europea que nace con el objetivo de luchar contra las organizaciones criminales que utilizan estos nodos logísticos para el tráfico de drogas.

El Ministerio del Interior participa activamente en la “*Coalición de países europeos contra el crimen organizado*”, de la que también forman parte Alemania, Bélgica, España, Francia, Italia, Países Bajos y Suecia. España codirige dos de las acciones recogidas en el Plan de Acción Multianual de la Coalición. Asimismo, organizó la IV reunión Ministerial de la Coalición, que se celebró el 14 de febrero de 2025 en Cádiz con la presencia de los ministros de Interior y de Justicia de países miembros de esta iniciativa.

En 2025 el Ministerio del Interior también ha participado en diferentes proyectos financiados por la Unión Europea, dirigidos al fortalecimiento institucional y a la formación y capacitación de

las fuerzas de seguridad de estados de diferentes áreas geográficas en materia de lucha contra el crimen organizado, mediante la aportación de funcionarios de las FCSE y de la Secretaría General de Instituciones Penitenciarias. Entre ellas, están las siguientes:

- En América Latina, España lidera el Programa de la UE “Europa Latinoamérica - Programa de Asistencia contra el Crimen Transnacional Organizado 2.0” (EL PACCTO 2.0), cuya finalidad es contribuir a reforzar el Estado de Derecho y la seguridad en América Latina y Caribe.
- Expertos del Ministerio del Interior participan en el Proyecto SEACOP VI, cuyo objetivo es apoyar la lucha contra el tráfico marítimo ilícito de sustancias estupefacientes, así como las redes criminales internacionales, liderando el componente regional dirigido a los países de América Latina y el Caribe.
- En Ecuador, España lidera el “Programa de Seguridad, Esperanza y Resiliencia para la Paz en Ecuador” (SERPAZ), cuyo objetivo es fortalecer la capacidad del país en la lucha contra el lavado de dinero y la recuperación de activos financieros de grupos del crimen organizado, así como apoyar la reestructuración del sistema penitenciario.
- En Bolivia, lidera el proyecto “Apoyo europeo a las fuerzas especiales de lucha contra la droga (fase II)” y “Apoyo a la prevención de la trata de personas, el tráfico ilícito de migrantes y delitos conexos”.
- En Perú, lidera el proyecto “Apoyo contra el tráfico de drogas y el crimen (fase II)”.
- La Guardia Civil lidera el proyecto “*Global Drug Intelligence Network*” (GDIN), que tiene por objeto dismantelar las redes delictivas y reducir el flujo internacional de drogas mediante el intercambio de información entre los organismos encargados de la aplicación de la ley de distintos países europeos y latinoamericanos.
- En Jordania, la Policía Nacional lidera un proyecto de hermanamiento, dirigido a apoyar a la Dirección General de Seguridad Pública de dicho país en la lucha contra el crimen organizado.
- En Nigeria, la Policía Nacional participa en el proyecto liderado por ONUDD “Apoyo a la gestión migratoria en Nigeria”, en materia de lucha contra la trata de seres humanos.

Por otra parte, como parte de los mecanismos de respuesta, destaca que el Reglamento de Inteligencia Artificial (IA) de la UE, en su artículo 5, prohíbe de forma general la utilización de sistemas de identificación biométrica en tiempo real a distancia, pero permite específicamente su uso, previa autorización judicial, para la identificación de delincuentes en delitos graves (considerados como tales aquellos que están castigados con una pena de al menos 5 años).

Asimismo, dado el contexto en materia de criminalidad organizada y grave, las autoridades aduaneras españolas han reforzado su cooperación internacional en diferentes direcciones y áreas geográficas, tanto con países clave de América Latina, o con agencias como Europol, con la Plataforma Multidisciplinar Europea contra las Amenazas Criminales y con la Alianza Europea de Puertos. Internamente, el Departamento de Aduanas e Impuestos Especiales de la AEAT ha fortalecido la

seguridad en los principales puertos mediante su Plan de Seguridad Portuario, en coordinación con la Fiscalía Antidroga, las autoridades portuarias y los operadores privados.

En cuanto a los **desarrollos estratégicos realizados durante 2025**, el 14 de julio de 2025, el Consejo de Seguridad Nacional aprobó la Estrategia Nacional contra el Crimen organizado y la Delincuencia Grave 2025, marco de referencia político-estratégico para prevenir y luchar contra los fenómenos criminales que causan un grave daño a la sociedad. Esta nueva Estrategia se apoya en el convencimiento de que la lucha contra el crimen organizado y la delincuencia grave es una responsabilidad compartida por los organismos públicos, el sector privado y la sociedad en su conjunto.

Su aprobación puso fin al proceso de revisión de su antecesora, con vigencia 2019-2023, que fue encomendado al Ministerio del Interior, mediante Acuerdo del Consejo de Seguridad Nacional de 19 de marzo de 2024. En este Acuerdo se establecieron unas directrices para elaborar una nueva Estrategia adaptada a la evolución de la amenaza. A tal fin se creó un Grupo de Trabajo creado al efecto, de naturaleza interministerial, liderado por el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), y constituido por representantes del Departamento de Seguridad Nacional y de los distintos departamentos ministeriales y otros organismos con competencias en la materia, de la comunidad académica, así como de otros expertos en la materia. Las Comunidades y Ciudades Autónomas también participaron en este proceso. El borrador final fue sometido a la consideración del Comité Especializado contra el Crimen Organizado y la Delincuencia Grave, principal órgano de apoyo del Consejo de Seguridad Nacional para el ámbito de esta amenaza.

Una vez finalizada la vigencia del Plan Estratégico Nacional de lucha contra la trata y explotación de seres humanos 2021-2023 (PENTRA), el CITCO ha coordinado su evaluación, contando para ello con los organismos públicos implicados en su implementación, así como con entidades especializadas de la sociedad civil. Como resultado se ha elaborado un informe de evaluación que recoge las principales medidas desarrolladas, así como un listado de conclusiones y recomendaciones para una acción futura.

Entre las recomendaciones del Plan se encuentra la elaboración de un segundo Plan que deberá partir de la base de las recomendaciones aprobadas, así como de la nueva *Directiva 1712/2024*, que modifica la *Directiva 2011/36*, relativa la prevención y lucha contra la trata de seres humanos y a la protección de sus víctimas. Tras la presentación de esta evaluación, el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) ejercerá las funciones de coordinación del grupo de trabajo para la elaboración de este.

FLUJOS MIGRATORIOS IRREGULARES

- En el año 2025 la migración irregular hacia España (entradas por vía marítima y las terrestres por Ceuta y Melilla) se ha reducido cerca de un 43% respecto del año 2024, alcanzando las cifras más bajas desde el año 2022.
- La Ruta Atlántica, a pesar de la tendencia general de descenso, sigue siendo la más transitada hacia nuestro país en número absolutos, con aproximadamente el 50% de las entradas irregulares totales.
- La presión derivada de la inestabilidad política, económica, social y de seguridad, agravada por las consecuencias que arrastra el factor climático, incrementa los retos desde la perspectiva de la gestión integrada de las fronteras.

FLUJOS MIGRATORIOS IRREGULARES

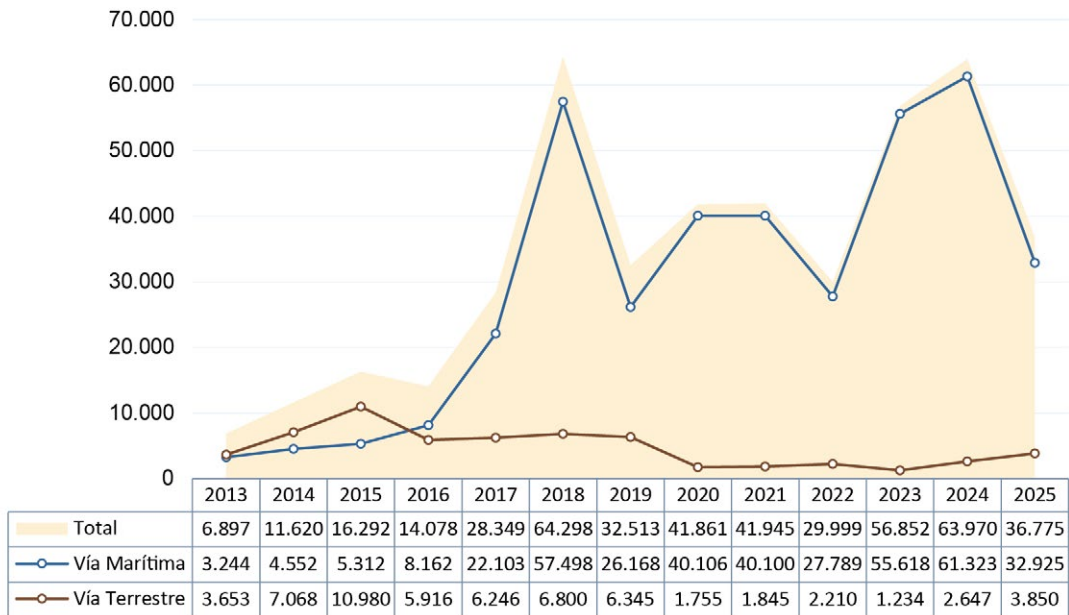
En 2025, los flujos migratorios irregulares internacionales se desarrollan en un contexto marcado por tensiones geopolíticas, conflictos prolongados, desigualdades económicas persistentes y los efectos del cambio climático, factores que continúan actuando como principales motores estructurales de la movilidad humana.

Un elemento con mayor impacto estructural es la contracción de la financiación destinada al sistema multilateral de gestión migratoria y protección, que está reduciendo la capacidad operativa de agencias y programas internacionales en ámbitos como la asistencia humanitaria, la gestión de flujos o el reasentamiento. Aunque el sistema internacional de reasentamiento depende cada vez más de decisiones nacionales, los principales foros multilaterales continúan desempeñando un papel relevante como espacios de coordinación, intercambio de información y alerta temprana.

En África, la reducción de la financiación multilateral contribuye a complicar la gestión de la mayor presión migratoria intraafricana, al tiempo que varios países del norte de África y del África subsahariana han mostrado un interés creciente en reforzar la cooperación con la Unión Europea en materia de gestión de flujos, desarrollo de capacidades y abordaje de las causas profundas de la migración.

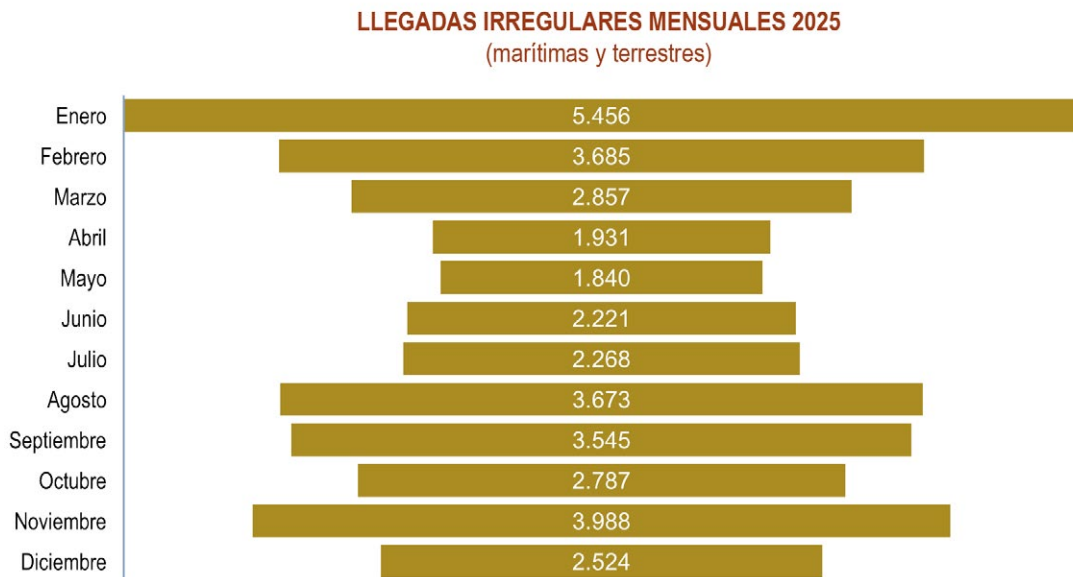
Visión general en el plano nacional

En el año 2025 la migración irregular hacia España (entradas por vía marítima y las terrestres por Ceuta y Melilla) se ha reducido cerca de un 43% respecto del año 2024, alcanzando las cifras más bajas desde el año 2022. A pesar del descenso, cabe destacar el notable aumento de llegadas a las Islas Baleares, así como el incremento de entradas a través del perímetro fronterizo en la Ciudad Autónoma de Ceuta. (Figuras 13.1 y 13.2)



Fuente: Ministerio del Interior

Figura 13.1: Evolución anual de entradas irregulares a España por vía de entrada (2013-2025)



Fuente: Elaboración DSN

Figura 13.2: Llegadas irregulares mensuales 2025

De esta forma, el número de llegados por vía irregular marítima se sitúa en 32.925, frente a los 61.323 del año anterior. No obstante, hay que tener en cuenta que existe una inmigración irregular por vía aérea, o a través de movimientos secundarios procedentes de países Schengen, que no es posible contabilizar. (Figura 13.3)

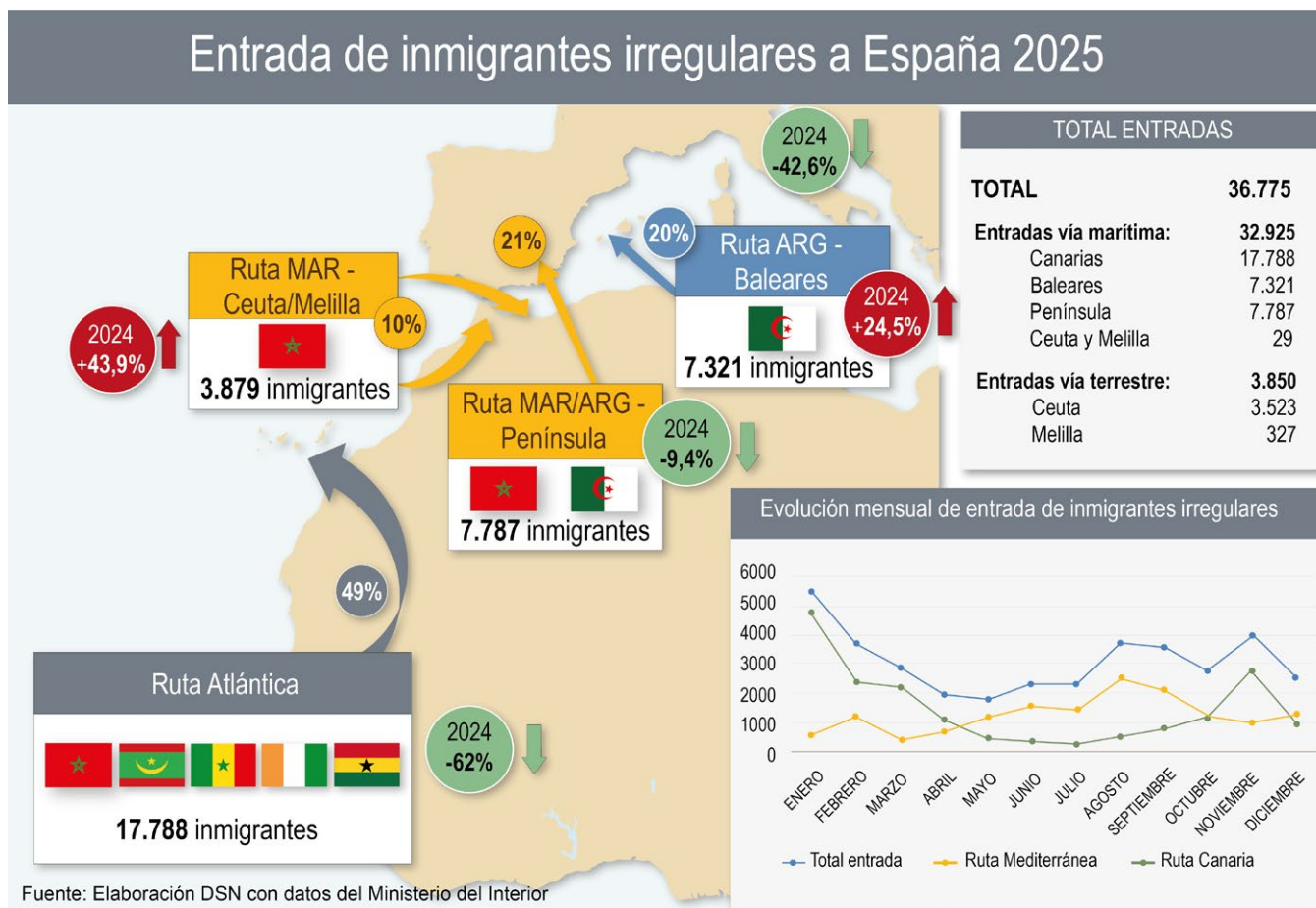


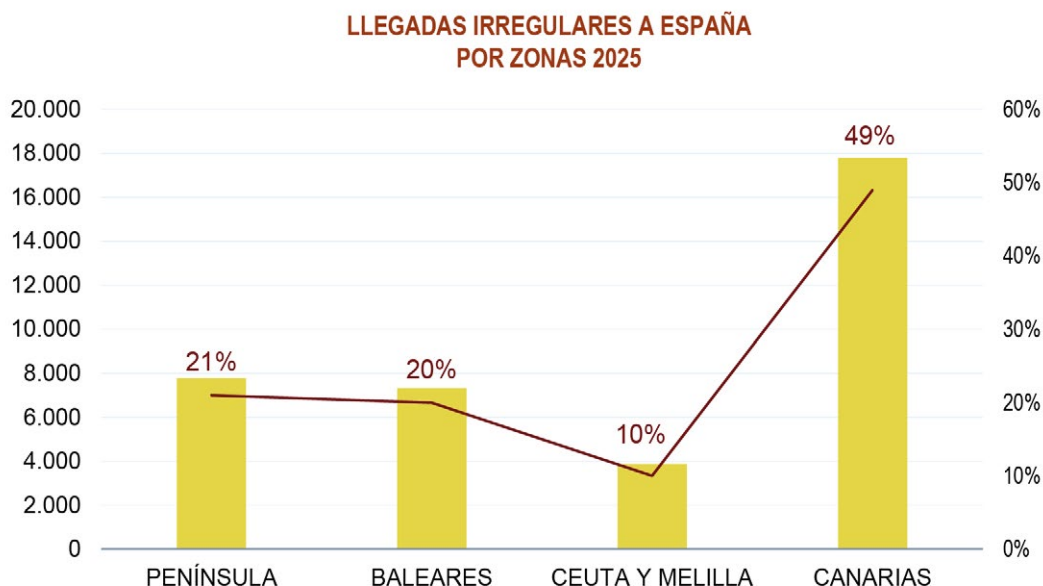
Figura 13.3 Entrada de inmigrantes irregulares a España 2025

Así, aunque España continúa enfrentando una notable presión migratoria, las cifras registradas en 2025 han mostrado un cambio de tendencia a la baja en las llegadas totales, especialmente gracias al positivo cambio de tendencia de los flujos en el frente Atlántico. La presión migratoria afecta de manera directa la costa peninsular del Estrecho, el mar de Alborán y Levante, además de los archipiélagos Canario y Balear.

En lo que se refiere a la Ruta Atlántica (Islas Canarias), a pesar de la tendencia general de descenso, sigue siendo la más transitada en número absolutos, suponiendo aproximadamente el 50% de las entradas irregulares totales a España (las llegadas irregulares a España son las menores de toda la frontera sur de la UE). Las actividades preventivas llevadas a cabo en la costa occidental africana han modificado los patrones de navegación, optando por salir de latitudes cada vez más meridionales, con especial mención a las salidas detectadas desde Port Kamsar (Guinea-Conakry), lo que ha convertido a la isla de El Hierro en uno de los principales destinos dentro del archipiélago.

Respecto a la Ruta del Mediterráneo Occidental (Balears), contrariamente a la tendencia general, ha experimentado un incremento en la intensidad de los flujos migratorios. Las llegadas a las islas Baleares han aumentado un 24,5%, representando el 20% de las entradas. Destaca asimismo el aumento relativo en la presencia de nacionales procedentes del África Oriental, siendo particularmente reseñable el aumento en el número de migrantes de origen somalí.

En lo que se refiere a las rutas a las Ciudades Autónomas de Ceuta y Melilla, la presión migratoria se ha visto notablemente incrementada debido principalmente al fenómeno de nadadores que tratan de acceder sorteando el perímetro fronterizo a través del mar, lo que supone en sí mismo un grave riesgo para sus propias vidas. Respecto a los intentos de saltos masivos a través del vallado, el gran despliegue perimetral de la Gendarmería Real Marroquí y sus Fuerzas Armadas han permitido mantener un control bastante riguroso que ha contenido este fenómeno. (Figura 13.4)



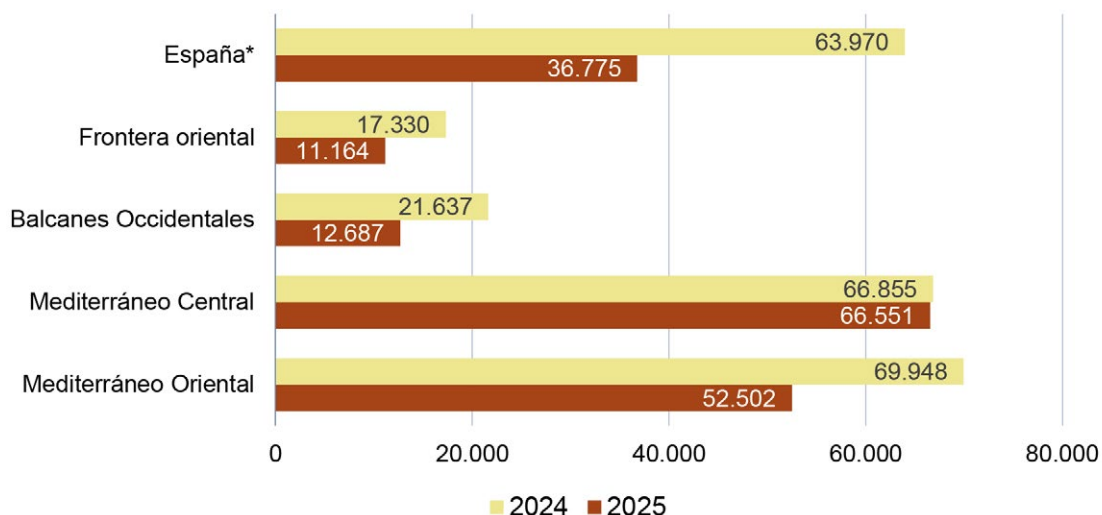
Fuente: Elaboración DSN con datos del Ministerio del Interior

Figura 13.4: Llegadas irregulares a España por zonas 2025

Por su parte, las Fuerzas Armadas han proporcionado en 2025 apoyo a otros Ministerios, especialmente, a los de Inclusión, Seguridad Social y Migraciones, del Interior y de Sanidad, en materia de Atención Humanitaria y apoyo a la gestión de la recepción y acogida de inmigrantes, con ocasión de las crisis provocadas por los flujos migratorios irregulares desde el Norte de África, o los desplazados temporales por la guerra en Ucrania. En particular, se apoyó al Centro de Estancia Temporal de Inmigrantes (CETI) de Ceuta con capacidades de material de alojamiento proporcionada por el Ejército de Tierra.

Visión general en el plano de la Unión Europea

La frontera sur de la Unión Europea sigue afectada por los flujos migratorios irregulares que llegan por vía marítima a través de las rutas Atlántica, Mediterráneo Occidental, Mediterráneo Central y Mediterráneo Oriental. No obstante, en 2025 se ha observado una reducción general de la presión migratoria, con un descenso del 25% en los cruces irregulares hacia las fronteras exteriores europeas respecto a 2024. Cabe comentar que, en lo referente a España, durante 2025, la suma de las llegadas por las dos rutas que afectan a España (rutas Atlántica y del Mediterráneo Occidental) es menor que las llegadas registradas en la ruta del Mediterráneo Central, seguidas por la ruta del Mediterráneo Oriental. En relación con el resto de rutas, la ruta de los Balcanes Occidentales continuó su tendencia a la baja con un descenso del 41%; las fronteras orientales de la UE redujeron las llegadas en un 35%. En el ámbito nacional, En 2025, el número de llegadas irregulares se redujo en un 42,6% en comparación con 2024. (Figura 13.5)



*España incluye datos integrados de las rutas del Mediterráneo Occidental y Atlántica

Fuente: Elaboración propia con información de la UE y Ministerio del Interior

Figura 13.5: Llegadas irregulares a través de las fronteras exteriores de la UE

En 2025, la política migratoria de la Unión Europea continúa desarrollándose en un contexto de transición institucional hacia la entrada en vigor del Pacto Europeo de Migración y Asilo, prevista para junio de 2026.

Durante el mismo año se han negociado y propuesto distintos instrumentos normativos vinculados a la implementación del nuevo marco europeo de migración y asilo. Entre ellos se encuentra la reforma del marco de retornos de la Unión, que revisa la *Directiva 2008/115/CE* con el objetivo de armonizar determinados procedimientos y prever, entre otras medidas, la posible creación de centros de retorno (medida esta última a la que se opone España). Asimismo, la Comisión Europea presentó propuestas para modificar el Reglamento de Procedimiento de Asilo (UE) 2024/1348, incluyendo el establecimiento de una lista común de países de origen seguros a escala de la Unión y la aplicación anticipada de determinados elementos del procedimiento fronterizo acelerado. Posteriormente, se presentó otra propuesta de modificación del mismo reglamento relativa a la aplicación del concepto de “tercer país seguro”, que permite declarar inadmisibles determinadas solicitudes de protección internacional cuando el solicitante pueda acceder a protección en un tercer Estado considerado seguro.

En diciembre de 2025 se ha aprobado igualmente el contingente anual del mecanismo de solidaridad previsto en el nuevo marco europeo, que contempla contribuciones de los Estados miembros en apoyo de aquellos países clasificados como sometidos a presión migratoria, situación migratoria significativa o riesgo de presión. España ha sido identificada como uno de los Estados miembros con presión migratoria, lo que la sitúa entre los potenciales beneficiarios de dicho mecanismo.

Inestabilidad en el Sahel

En el Sahel, la inestabilidad política y la proliferación de grupos yihadistas es cada vez más preocupante desde la perspectiva de gestión de las fronteras y control de los flujos migratorios. Estos factores se suman a los factores de empuje socio económico que están fomentando la salida constante de migrantes del continente hacia Europa.

La dinámica migratoria irregular hacia España se encuentra intrínsecamente ligada a la inestabilidad en la franja del Sahel y el Golfo de Guinea, siendo este el factor principal que determina su evolución. Con excepción de los inmigrantes magrebíes (argelinos y marroquíes), la mayoría de los flujos pasan a través de Mali y Níger en sus trayectos hacia los principales países de salida (Mauritania, Senegal, Gambia, Marruecos o Argelia). Incluso migrantes provenientes de Asia o África Oriental suelen utilizar rutas mixtas que incluyen un trayecto terrestre a través de Mali y Níger.

En este contexto regional, la actual inestabilidad en Mali es esencial, ya que las rutas terrestres que atraviesan el país son centrales en las vías migratorias con destino a España. El escenario más probable, que contempla una relativa estabilización en la capital, implicaría un incremento progresivo y significativo de los flujos migratorios procedentes de este país.

Esta crisis de seguridad genera un desplazamiento masivo de refugiados, predominantemente malienses y de otros Estados afectados, lo que ejerce una creciente presión sobre la vecina Mauritania, que se ha convertido en el vector más complejo. De acuerdo con los datos que se manejan por parte del Ministerio del Interior, aproximadamente 380.000 personas originarias del Sahel se encuentran ya en territorio mauritano.

En respuesta a este compromiso regional, Mauritania acoge el campamento de M'Berra desde 1991, que alberga a más de 153.000 refugiados malienses, ubicados en gran medida en las proximidades de las ciudades de M'Bera y Fassala, en la región de Hodh Chargui, cercana a la frontera con Mali.

Para gestionar esta presión, el gobierno mauritano intensifica su lucha contra la inmigración irregular con medidas legislativas, estratégicas y operativas. Estas acciones se centran en impedir las salidas por vía marítima, detener a los organizadores y llevar a cabo la expulsión de inmigrantes en situación irregular.

En el caso de Níger, el año 2025 ha venido marcado por una profunda reconfiguración del sistema de tránsito migratorio a través del país. La nueva legislación culmina el cambio de enfoque de la política migratoria nigerina desde una perspectiva orientada al control de flujos migratorios hacia una óptica centrada puramente en la seguridad nacional frente a los riesgos de infiltración y desestabilización. Con estos cambios, el repunte significativo de los flujos migratorios que hubo en 2024 se ha consolidado durante el 2025, aunque sin regresar a los niveles previos a 2015. A pesar de que la ruta hacia Libia sigue siendo preponderante, han repuntado los flujos hacia Argelia.

A un nivel más específico, existe la preocupación por la posible filtración de antiguos combatientes dentro de estos flujos masivos de refugiados con destino a las costas españolas. No obstante, la pertenencia temporal a grupos yihadistas en el Sahel, aspecto detectado de manera testimonial hasta el momento, suele obedecer a la necesidad de subsistencia o a criterios forzosos, más que a un marcado componente ideológico.

Como viene produciéndose desde 2023, aumentan las llegadas de personas inmigrantes procedentes del Sahel. En el caso de Baleares, además del aumento de llegadas irregulares, se ha producido un cambio en los perfiles de estas, con cada vez menos personas que provienen de países del Magreb, a favor de las procedencias del África subsahariana y el Sahel, con una mayor presencia de mujeres y familias completas. Estas personas, por lo general, cuentan con menos redes familiares o de apoyo, a lo que se suma una travesía mucho más larga, lo que ha obligado a adaptar el sistema de acogida en las Islas Baleares.

Gestión de flujos migratorios irregulares

La gestión de los flujos migratorios irregulares, la cooperación con los países de origen y tránsito, el control fronterizo y el resguardo fiscal constituyen líneas de actuación prioritarias para las autoridades encargadas de la gestión integral de las fronteras, dado que estos flujos representan un desafío de naturaleza transnacional.

Un elemento central es el análisis de los riesgos aparejados y la potencial incidencia de los grupos criminales que operan en este ámbito para la Seguridad Nacional. Se destaca la posibilidad de instrumentalización por parte de amenazas exteriores de gran entidad, tanto por parte de terceros Estados como por actores no estatales, como elementos vinculados al terrorismo yihadista o crimen organizado, bien en los flujos irregulares o en otros fenómenos transnacionales derivados de conflictos o desastres.

Además del desafío que supone la ordenación de los flujos, la inmigración por vía marítima incorpora el riesgo derivado de la precariedad de las embarcaciones utilizadas. Esta circunstancia constituye un serio peligro para la vida humana en el mar, lo que demanda un gran esfuerzo de salvamento y rescate de estas personas, así como la subsiguiente atención sanitaria y ayuda humanitaria al llegar a puerto, especialmente en el caso de personas vulnerables.

Programa de atención humanitaria. Protección internacional y asilo

La gestión de los flujos migratorios irregulares distingue entre las personas inmigrantes que presentan una solicitud de protección internacional, y que, en caso de carecer de recursos económicos, pasan a integrarse en el sistema de acogida de protección internacional, de aquellas que no formalizan dicha solicitud las cuales son atendidas en el marco del programa de atención humanitaria.

El sistema de acogida de protección internacional es el conjunto de recursos, prestaciones y actuaciones dirigidos a las personas solicitantes y beneficiarias de protección internacional que carecen de medios económicos, con el fin de garantizar su atención básica de acogida temporal en su proceso de integración conforme a lo previsto en la normativa española y europea.

Desde hace ya unos años la ingente cantidad de extranjeros que solicitan Protección Internacional, tanto en nuestras fronteras como dentro de nuestro territorio, ha favorecido la proliferación de redes que persiguen el lucro económico a costa de esas personas.

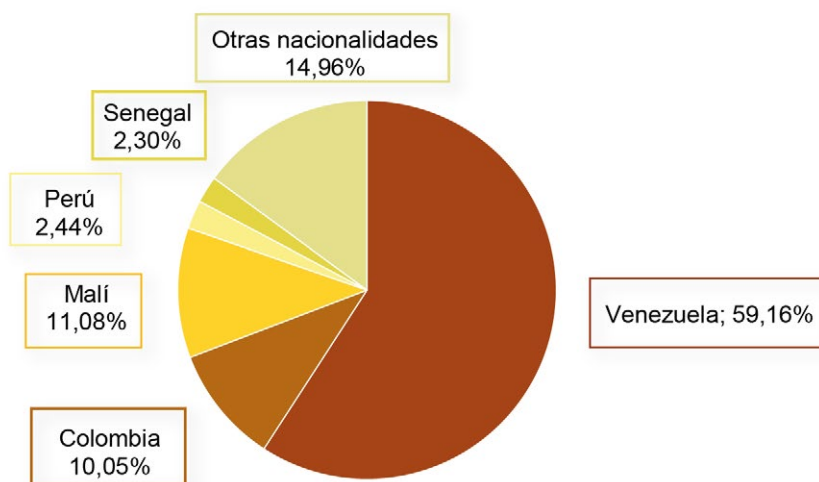
En 2025, se registraron en España 144.693 solicitudes de protección internacional, lo que supone una disminución del 13,55% respecto a las solicitudes registradas en 2024. (Figuras 13.6 y 13.7)



Fuente: Ministerio del Interior

Figura 13.6: Evolución de las solicitudes de protección internacional 2021-2025

PAÍSES DE PROCEDENCIA DE LOS PETICIONARIOS DE PROTECCIÓN INTERNACIONAL Total de peticiones en 2025: **144.693**



Fuente: Ministerio del Interior

Figura 13.7: Países de procedencia de los peticionarios de protección internacional

A la vista de los datos, a lo largo del 2025 se produjo un gran aumento de solicitudes de nacionales de Venezuela (cerca de 85.600 frente a 66.700 en 2024), que constituyen casi el 60% de todas las solicitudes, a gran distancia del segundo país, Mali. Sin embargo, Colombia, registra una reducción en su porcentaje de solicitudes: de representar el 25% en 2024 ha pasado al 10% en 2025.

Se ha observado que la concesión generalizada por España de la residencia por razones humanitarias a los venezolanos, junto con el cambio de la política migratoria de la Administración de EEUU, han actuado como factores de atracción de esta población hacia España.

Por su parte, el programa de atención humanitaria se orienta a inmigrantes en situación de vulnerabilidad que no solicitan protección internacional y ofrece intervenciones de carácter básico y urgente como alojamiento temporal, manutención o atención social básica, destinadas a cubrir necesidades esenciales y a proporcionar una respuesta inmediata ante situaciones de desprotección.

El número de plazas de acogida con las que cuentan ambas redes (protección internacional y atención humanitaria) por provincias es: [\(Figuras 12.8\)](#)

Figura 13.8: Capacidad y ocupación de las redes de protección internacional y atención humanitaria por provincias

Capacidad y ocupación de las redes de protección internacional y atención humanitaria por provincias						
	Atención humanitaria		Protección Internacional		Total	
	Capacidad	Ocupación	Capacidad	Ocupación	Capacidad	Ocupación
Albacete	0	0	193	163	193	163
Alicante/Alacant	310	233	1.367	1.201	1.677	1.434
Almería	980	853	559	532	1.539	1.385
Araba/Álava	0	0	336	323	336	323
Asturias	176	131	532	481	708	612
Ávila	0	0	172	148	172	148
Badajoz	894	470	258	225	1.152	695
Balears, Illes	378	42	116	111	494	153
Barcelona	425	245	3.081	2.624	3.506	2.869
Bizkaia	15	5	621	501	636	506
Burgos	0	0	256	241	256	241
Cáceres	0	0	213	192	213	192
Cádiz	904	626	1.514	1.202	2.418	1.828
Cantabria	0	0	460	432	460	432
Castellón/Castelló	0	0	343	323	343	323
Ceuta	512	625	0	0	512	625
Ciudad Real	0	0	340	319	340	319
Córdoba	314	206	608	558	922	764
Coruña, A	117	41	288	275	405	316
Cuenca	54	45	61	50	115	95
Gipuzkoa	0	0	214	205	214	205
Girona	752	603	573	487	1.325	1.090
Granada	580	450	591	548	1.171	998
Guadalajara	108	92	501	470	609	562
Huelva	236	167	366	336	602	503
Huesca	225	183	361	351	586	534
Jaén	0	0	252	227	252	227
León	50	40	411	374	461	414
Lleida	0	0	347	297	347	297
Lugo	0	0	469	442	469	442
Madrid	3.449	1.993	4.275	3.414	7.724	5.407
Málaga	777	647	1.801	1.493	2.578	2.140
Melilla	686	76	0	0	686	76
Murcia	1.218	569	1.587	1.484	2.805	2.053
Navarra	0	0	564	525	564	525
Ourense	60	49	128	110	188	159
Palencia	0	0	174	157	174	157
Palmas, Las	2.213	870	229	155	2.442	1.025
Pontevedra	349	260	521	485	870	745
Rioja, La	0	0	149	146	149	146
Salamanca	0	0	491	466	491	466
Sta Cruz de Tenerife	4.513	1.206	171	157	4.684	1.363
Segovia	0	0	420	389	420	389
Sevilla	671	497	2.286	2.020	2.957	2.517
Soria	94	85	339	320	433	405
Tarragona	0	0	753	590	753	590
Teruel	177	159	375	327	552	486
Toledo	0	0	540	504	540	504
Valencia/València	361	325	1.714	1.536	2.075	1.861
Valladolid	8	7	619	546	627	553
Zamora	0	0	53	53	53	53
Zaragoza	517	438	1.406	1.300	1.923	1.738
TOTAL	22.123	12.238	33.998	29.815	56.121	42.053

Fuente: Ministerio de Inclusión, Seguridad Social y Migraciones

Vigilancia y control de fronteras

En el Sahel, la inestabilidad política y la proliferación de grupos yihadistas es cada vez más preocupante desde la perspectiva de gestión de las fronteras. Estos parámetros se suman a los factores de empuje socio económico que están fomentando un flujo constante de migrantes del continente.

Además, España gestiona 81 pasos fronterizos, lo que está expuesta a retos muy complejos desde el punto de vista del control de la migración irregular. Asimismo, se continúa trabajando en la mejora del sistema de control de fronteras, con el fin de facilitar el paso legítimo de éstas a los millones de pasajeros que las cruzan anualmente, al tiempo que se previene el tránsito no autorizado y se lucha contra la delincuencia grave transfronteriza. El Ministerio del Interior continúa invirtiendo en innovación en el control de fronteras y en la mejora de las capacidades para afrontar este reto.

El Pacto Europeo de Migración y Asilo refuerza aún más el sistema común de gestión de fronteras, mediante la introducción de controles en frontera obligatorios (*screening*) para las personas que lleguen de forma irregular, incluyendo comprobaciones de identidad, seguridad y salud.

Dentro de estos mecanismos europeos, destaca el sistema *Entry-Exit* (EES), aplicado en los controles fronterizos de la UE, especialmente en aeropuertos y otros puntos de entrada y salida del espacio Schengen, con el objetivo principal de mejorar la gestión de los flujos migratorios y fortalecer la seguridad fronteriza en puntos habilitados.

El Sistema de Entradas y Salidas (EES) entró en funcionamiento con éxito el 12 de octubre de 2025, marcando un hito en la modernización del control fronterizo en el espacio Schengen. Su despliegue será gradual a lo largo del 2026, permitiendo la transición completa desde el sellado manual de pasaportes a un sistema digital basado en datos biométricos y registros electrónicos.

Además, las Fuerzas Armadas (FAS) colaboran con las FCSE contribuyendo a la detección de migrantes por vía marítima. Esta colaboración se materializa proporcionando información de las diferentes detecciones que se realizan por parte de los efectivos y medios militares durante el desarrollo de las misiones propias de FAS.

Cooperación con países de origen y tránsito

España impulsa una política migratoria integral y equilibrada, basada en el tratamiento de las causas profundas de la migración, el impulso de la migración legal y la lucha contra la inmigración irregular.

La colaboración con los países de origen y tránsito es fundamental. Por ello, España ha desarrollado desde hace casi veinte años una política de cooperación con los países africanos de origen y tránsito de la inmigración irregular, basada en la prevención de las salidas irregulares y la lucha contra las redes del tráfico de personas.

Esta estrategia se fundamenta en la confianza mutua y la conciencia de una responsabilidad compartida entre esos países; la colaboración operativa sostenida y previsible, basada en la escucha activa de las necesidades de los países socios; el desarrollo de operaciones conjuntas, con el objetivo de apoyar los esfuerzos de las fuerzas de seguridad de los terceros países en la desarticulación de dichas redes; y el apoyo presupuestario directo para sufragar parte de los gastos en los que se incurren los países socios en sus labores de control fronterizo y gestión migratoria, la provisión del equipo técnico necesario para desarticular redes y la capacitación de efectivos.

En el ámbito de la cooperación con los países de origen y tránsito, la red de Representaciones (Embajadas y consulados) de España desempeña un papel esencial como instrumento de interlocución permanente y estructurada. A través de consultas políticas, diálogos migratorios y contactos técnicos regulares, las representaciones diplomáticas facilitan la coordinación con las autoridades nacionales y locales en materia de prevención de salidas irregulares, lucha contra las redes de tráfico y gestión de retornos. Asimismo, actúan como canal de enlace con las instituciones y agencias de la Unión Europea sobre el terreno, contribuyendo a alinear posiciones, reforzar la coherencia de la acción exterior y apoyar la implementación de los partenariados y proyectos europeos en materia migratoria.

Con el impulso de nuestra red de Embajadas, se está realizando un esfuerzo conjunto que implica a las autoridades y a las fuerzas de seguridad de los países socios en el ámbito de la prevención, orientado a evitar las salidas irregulares, así como en la lucha contra la inmigración irregular, que es decisivo para reducir la presión migratoria sobre España.

Esta cooperación ha permitido evitar un gran número de salidas irregulares. La mejora del control fronterizo en Mauritania y Senegal ha provocado que las rutas migratorias se desplacen más al sur, aumentando las salidas desde Gambia, Guinea Bissau y Guinea Conakry.

Del mismo modo, es importante destacar el papel de España en impulsar, desde las instituciones europeas y sus agencias, especialmente Frontex, un enfoque conjunto del fenómeno migratorio, promoviendo, conforme al Pacto Europeo de Migración y Asilo, partenariados estables y de largo plazo, así como otros instrumentos de cooperación con los países de origen y tránsito africanos. España apoya una mayor presencia de Frontex sobre el terreno en terceros países para apoyar los esfuerzos en prevención.

Por otro lado, con el fin de 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, el Ministerio del Interior participa en diferentes proyectos financiados por la Unión Europea dirigidos a la lucha contra las redes de inmigración y el tráfico ilícito de personas en los países de origen y tránsito, entre los que se incluyen, los Equipos Conjuntos de Investigación (ECIs) y los Partenariados Operativos Conjuntos (POCs).

La Policía Nacional cuenta con un ECI y un POC, ambos desplegados en Mauritania. El POC está desplegado en Nuakchot y es financiado con fondos de la UE, mientras el ECI se localiza en Nuadibú, financiado con fondos propios. Este Cuerpo policial ha tenido desplegados funcionarios en POCs en Senegal y Gambia, así como en el proyecto NETCOP, con base en Senegal, que tiene como fin la coordinación y puesta en común de la información obtenida por los diferentes POCs y ECIs. También participa en el proyecto liderado por ONUDD “Apoyo a la gestión de la migración en Nigeria”, cuyo objetivo es la lucha contra la trata de seres humanos y las redes de favorecimiento de la inmigración irregular”, contado con un funcionario desplegado sobre el terreno.

En otras latitudes, la Policía Nacional también lidera el proyecto de la UE “Apoyo a la Gestión Integral de fronteras en América Latina” (EUROFRONT), que tiene como objeto el fortalecer las capacidades operativas de las fuerzas policiales que se ocupan de la gestión de las fronteras, prestando especial atención al control de los flujos migratorios y al delito transfronterizo en cuatro fronteras piloto de 7 países: Argentina, Bolivia, Brasil, Colombia, Ecuador, Paraguay y Perú.

Por su parte, la Guardia Civil sigue impulsando la cooperación bilateral y multilateral con numerosos países de origen y tránsito de los flujos migratorios. Son de especial relevancia los intercambios de información con Marruecos, Argelia, Mauritania, Senegal y Mali para conocer las tendencias migratorias y los modos de operar. En los países de origen, tránsito y salida mantiene un despliegue permanente de medios aéreos, navales y terrestres para la realización de patrullas conjuntas para mejorar el control fronterizo, lo que contribuye a evitar la pérdida de vidas en el mar.

Con relación al despliegue de la Guardia Civil para reforzar las capacidades policiales de los países vecinos del Magreb y del Sahel en materia de control de la migración irregular, cabe señalar los despliegues que mantiene en Mauritania; los destacamentos en Nouadhibou y Nouakchott; en Senegal (Dakar, Saint Louis y en Mbour /Kaolack); en Gambia (Banjul) y en otros países, como Cabo Verde, Guinea Bissau, Guinea Conakry y Mali.

Expertos policiales de este Cuerpo también participan con Marruecos en el marco del proyecto de “Apoyo a la gestión integrada de las fronteras y la migración”, con financiación de la Unión Europea”. En el ámbito de las relaciones entre la Guardia Civil y la Gendarmería Real Marroquí, son destacables las patrullas mixtas entre ambos Cuerpos.

El desarrollo de la Guardia Europea de Fronteras y Costas ha permitido en estos últimos años trabajar en conjunto y de manera más coordinada con los socios europeos, alineando estrategias, planes operativos y desarrollos de capacidades, compartiendo datos, análisis de riesgos, actividades formativas, lecciones aprendidas. Esto se ha manifestado en un mayor esfuerzo operativo con el despliegue de más personal y medios que en ningún otro momento en las fronteras exteriores europeas y países del África occidental.

Además de la cooperación que se desarrolla en el marco de la gestión integrada de las fronteras, en el ámbito del Ministerio de Inclusión, Seguridad Social y Migraciones, se están implementando los programas de migración segura, ordenada y regular en base a los memorándums de entendimiento firmados en 2024 con varios países, entre los cuales destacan: Mauritania, Gambia, Senegal y Egipto.

Por su parte, el Ministerio de Defensa, realiza actividades periódicas de Seguridad Cooperativa y actividades bilaterales de formación y capacitación de las Fuerzas Armadas de los Estados de estas regiones, con el objeto de dotarlos de las herramientas que les permitan hacer frente a riesgos y amenazas emergentes y, por extensión, combatir los flujos migratorios irregulares, en el marco establecido en el Plan Estratégico de Proyección de Estabilidad.

Asimismo, el CNI, en sus labores de frontera avanzada, lidera los proyectos financiados por la Unión Europea, dirigidos al fortalecimiento de Células de Cooperación de Inteligencia en materia migratoria (CCIs) junto a los Servicios de Inteligencia de los principales países de origen, tránsito y salida. La buena acogida de los proyectos y los excelentes resultados obtenidos sugieren extender este mecanismo de colaboración a otros países a partir de 2026, ampliando de este modo la visión regional del proyecto.

Dimensión europea: nuevo pacto migración y asilo

La aprobación del Pacto Europeo de Migración y Asilo, adoptado en mayo de 2024, ha consolidado un nuevo marco jurídico para la política migratoria y de asilo de la Unión Europea, que ya está en fase de implementación. El plazo para la plena aplicación de estos instrumentos se mantiene, salvo el del Reglamento de Reasentamiento, que ya está en vigor desde junio de 2024. Durante 2025, la Unión y los Estados miembros han avanzado en la fase preparatoria.

De esta forma, España presentó en plazo su Plan Nacional de Implementación a la Comisión Europea el 11 de diciembre de 2024, estructurado en los 10 bloques de trabajo definidos en el Plan Común de Implementación. Este plan prevé reformas legislativas, el refuerzo de capacidades operativas, así como el desarrollo de sistemas interoperables, como Eurodac.

Asimismo, en abril de 2025, España remitió a la Agencia de Asilo de la Unión Europea (AAUE) su Plan de Contingencia de Asilo y Acogida, orientado a garantizar la respuesta ante situaciones de presión migratoria y, en junio de 2025, presentó a la Comisión Europea la Estrategia Nacional de Gestión del Asilo y la Migración. Este documento se articula en 18 objetivos estratégicos agrupados en 6 ejes e incluye medidas destinadas a reducir la presión migratoria, reforzar la gestión fronteriza y garantizar el respeto a los derechos fundamentales.

En noviembre de 2025, la Comisión ha puesto en marcha en primer ciclo anual de gestión de la migración, con la publicación del Informe Europeo Anual sobre Asilo y Migración. Este informe constata una reducción del 35% en los cruces irregulares en la Unión e identifica como Estados miembros bajo presión migratoria, y por tanto beneficiarios del contingente anual europeo de solidaridad, a España, Italia, Grecia y Chipre. Este mecanismo de solidaridad será clave para la aplicación efectiva del Pacto a partir de junio de 2026.

Visión general sobre los desplazados ucranianos

España es el 4º país de la UE en concesión de protección temporal a desplazados debido a la crisis de Ucrania (unas 262.500 personas a 31 de diciembre, de las que 1.582 son menores no acompañados) de un total de 5.310.800 en la UE (para una mejor comprensión de esta afirmación, hay que tener en cuenta que el 4 de marzo de 2022 se activó el régimen de protección temporal para aquellos ciudadanos desplazados por el conflicto de Ucrania).

Así, durante el 2025 se ha atendido a un total de 9.982 personas beneficiarias de protección temporal en el Sistema de acogida español. A fecha de diciembre de 2025 permanecían 4.666 acogidas dentro del mencionado sistema.

VULNERABILIDAD ENERGÉTICA

- La caída del sistema eléctrico en todo el territorio peninsular del 28 de abril de 2025 ha motivado la adopción de numerosas medidas para mejorar la resiliencia de la red eléctrica frente a eventuales cortes de suministro.
- La diversificación continua siendo una de las principales medidas para la seguridad del suministro energético, tanto de fuentes de energía como en sentido geográfico. Así, las llegadas a España de petróleo y de gas natural proceden de más de veinte países de todo el mundo.
- En España, el principal indicador de la seguridad energética, que es la dependencia del exterior, marca una senda decreciente, con un valor del 68,4% en 2024, hacia el objetivo marcado en 2030, que es del 50%.

VULNERABILIDAD ENERGÉTICA

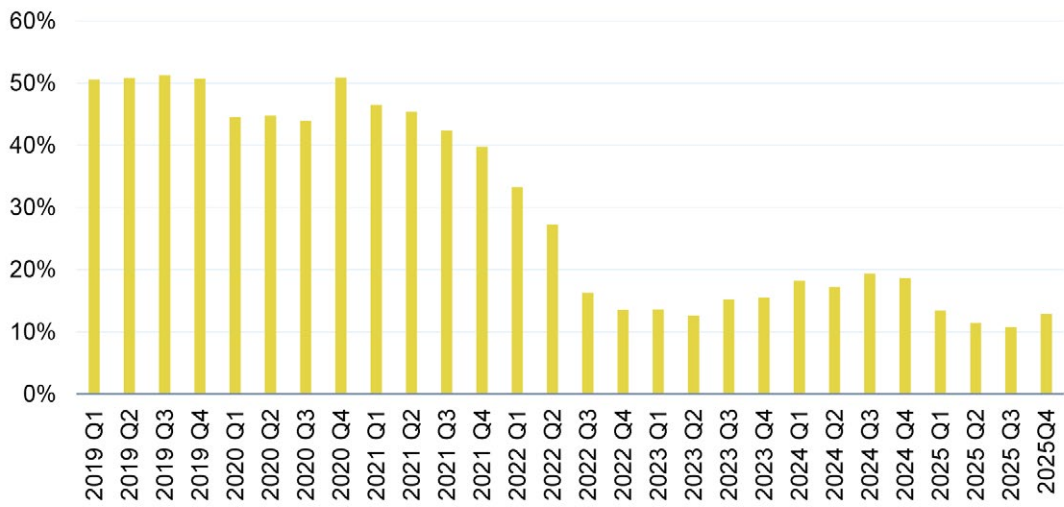
A nivel mundial, según el *World Energy Outlook 2025* de la Agencia Internacional de la Energía, se ha superado por primera vez el 40% de generación eléctrica a partir de fuentes de baja emisión. Esta transición hacia un modelo energético que contempla una mayor presencia de energías renovables convive con un panorama geopolítico marcado por la incertidumbre. En este contexto, además de los escenarios focos de tensión y de volatilidad, el control de las cadenas de suministro de tecnologías limpias es tan crítico como el acceso a los hidrocarburos.

El sistema energético europeo muestra interdependencias críticas (gas, electricidad e infraestructuras de interconexión) que lo hacen vulnerable a interrupciones externas y oscilaciones de precios; la UE refuerza la resiliencia mediante normas comunes y coordinadas para reforzar la seguridad del suministro, obligaciones de almacenamiento de gas natural y diversificación de suministros.

En esta línea, la dependencia europea de materias críticas (litio, cobalto, tierras raras) introduce riesgos de abastecimiento y presión geopolítica suministro y presión geopolítica; la UE y España promueven reciclaje, diversificación de importaciones y fomento de la extracción/transformación local para reducir vulnerabilidades.

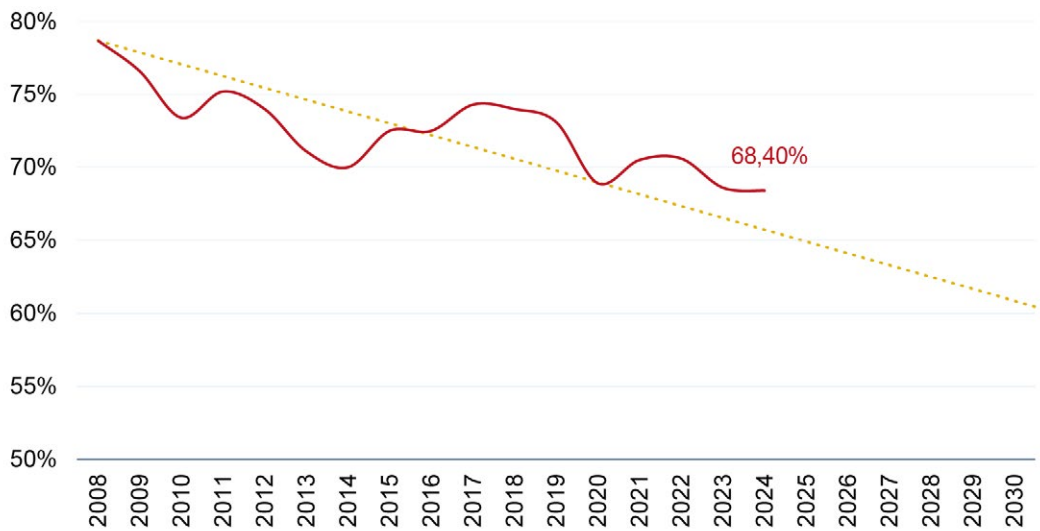
En dimensión europea, la UE ha reducido en 2025 su dependencia respecto a los combustibles fósiles rusos, acelerando los objetivos de su plan *REPowerEU*. La Unión Europea aprobó el 19º paquete de sanciones con prohibición de importar GNL procedente de Rusia. Además de ello, el *Reglamento (UE) 2025/2600 del Consejo, de 12 de diciembre de 2025, sobre medidas de emergencia ante las graves dificultades económicas causadas por las acciones de Rusia en el contexto de la guerra de agresión contra Ucrania* formalizan la prohibición de nuevos contratos de gas natural ruso y establece un calendario hasta llegar al cese total de las importaciones, incluido el GNL, para 2027. Las importaciones rusas representaban en 2019, antes de la invasión de Ucrania, el 45% del gas consumido en la UE y se han reducido a niveles inferiores al 15% en 2025. (Figura 14.1)

En España, el principal indicador de la seguridad energética, que es la dependencia del exterior, marca una senda decreciente, con un valor del 68,4% en 2024, hacia el objetivo marcado en 2030, que es del 50%. (Figura 14.2)



Fuente: Gráfico elaborado por el DSN con la base de datos de Bruegel (2022) - European natural gas imports- (versión de 9 de enero de 2026)

Figura 14.1: Dependencia media de los 27 países de la Unión Europea del gas ruso



Fuente: Ministerio para la Transición Energética y el Reto Demográfico

Figura 14.2: Dependencia energética del exterior de España

Diversificación: importaciones de crudo y gas natural

En 2025, el panorama energético de España se consolidó bajo una estrategia de diversificación y seguridad de suministro, marcada por una ligera caída en el consumo de crudo y un repunte en el de gas natural.

Las importaciones de crudo cerraron el año con aproximadamente 61,42 millones de toneladas, lo que supone un descenso del 4,9% respecto al año anterior. Por el contrario, el gas natural experimentó un incremento en la demanda de importación cercano al 9,6%, impulsado en parte por la necesidad de respaldo en la generación eléctrica y la recuperación del sector industrial, con un papel predominante del Gas Natural Licuado (GNL), que ya representa más del 70% del total frente al gas por gasoducto.

Los tres mayores exportadores de crudo a España en 2025 mantuvieron un equilibrio geográfico notable. En el sector del petróleo, los líderes fueron Estados Unidos (15,2%), Brasil (13,6%) y México (12,3%), consolidando a América (tanto del Norte como del Sur) como el principal bloque de suministro. (Figura 14.3)

En cuanto al gas natural, los protagonistas fueron Argelia (34,6%), que reforzó su posición gracias a la conexión por gasoducto y GNL, seguida muy de cerca por Estados Unidos (30,0%) y, en tercer lugar, Rusia (11,5%). Geográficamente, África y América del Norte dominaron el mix, suministrando conjuntamente casi el 80% de la energía importada por el país. (Figura 14.4)

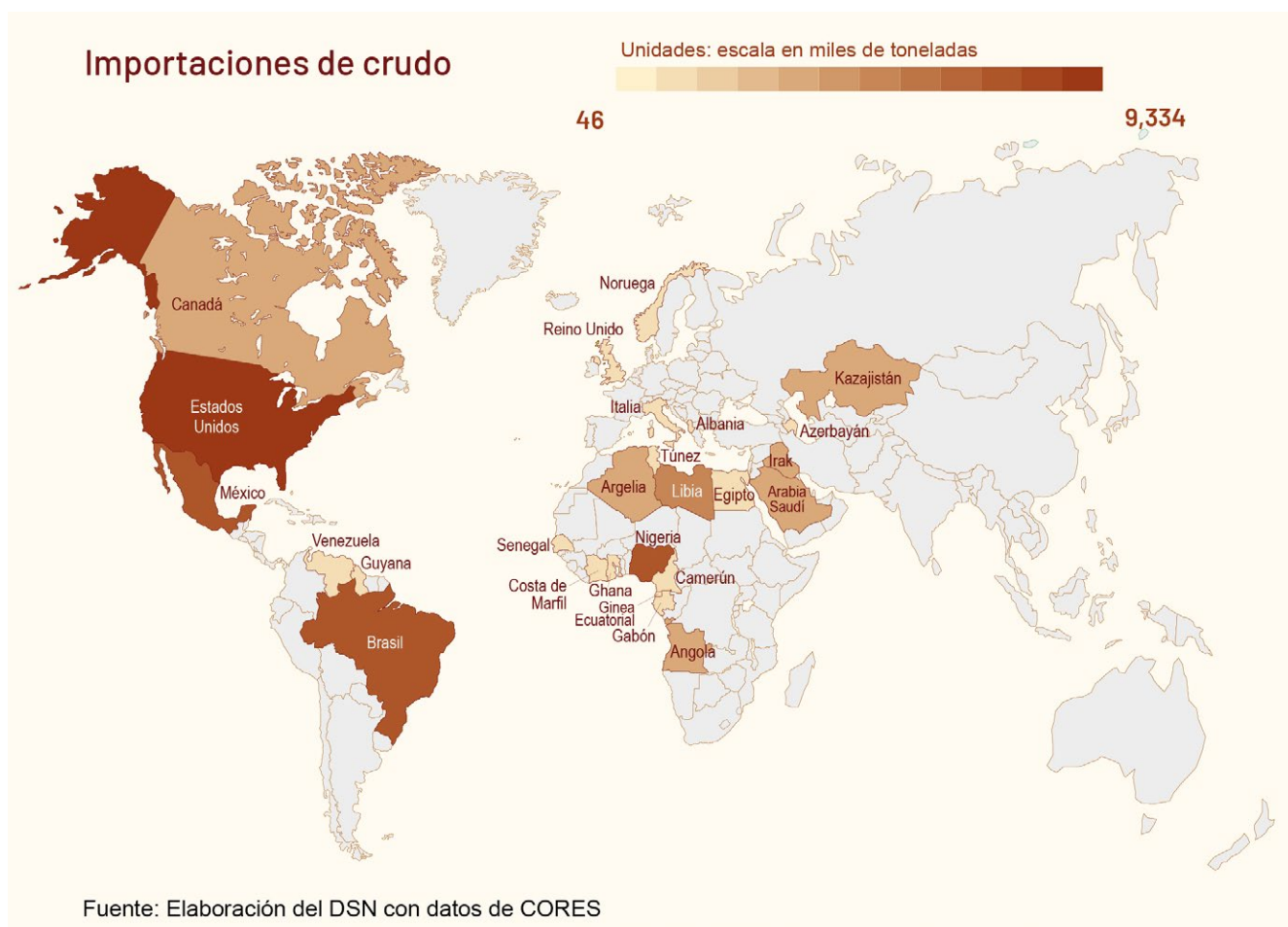


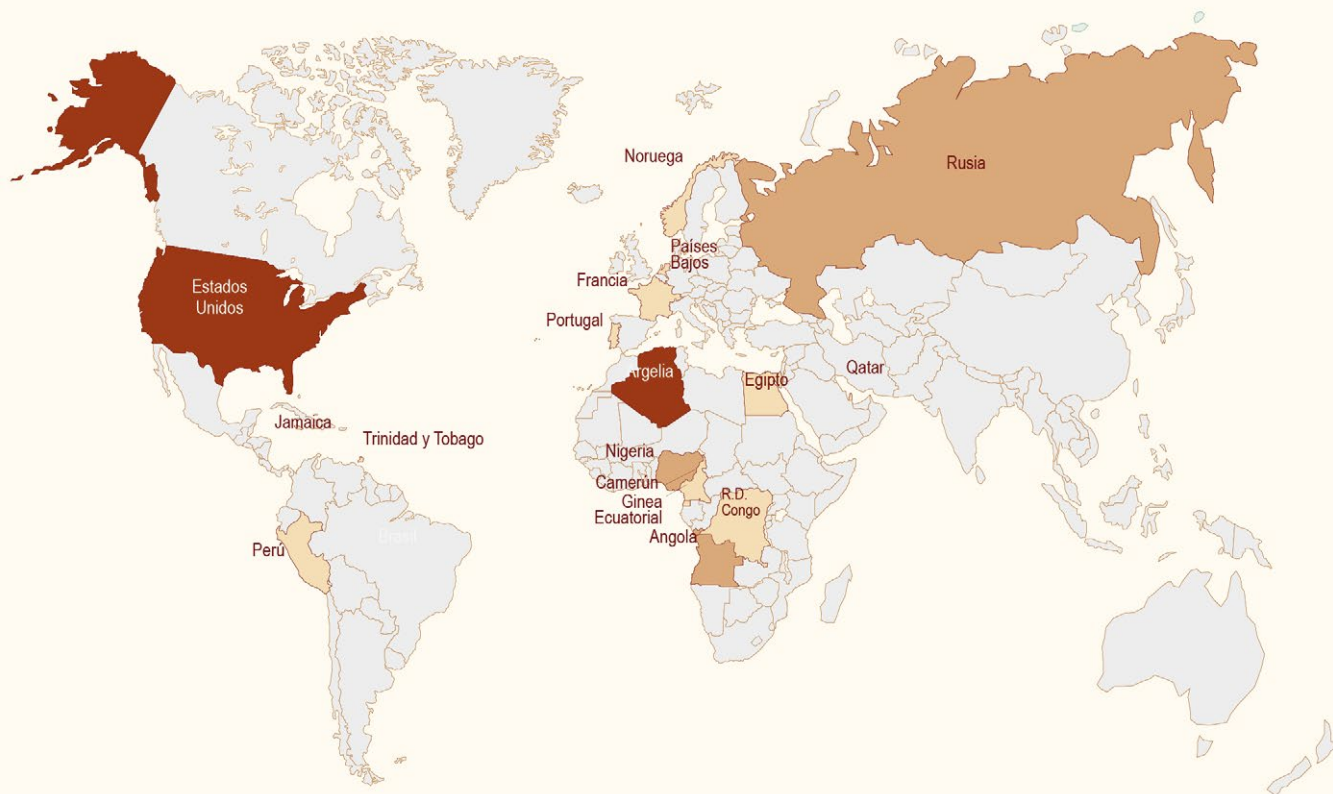
Figura 14.3: Importaciones de crudo en España en 2025

Importaciones de gas natural

Unidades: escala en gigawatios - hora

10

128,502



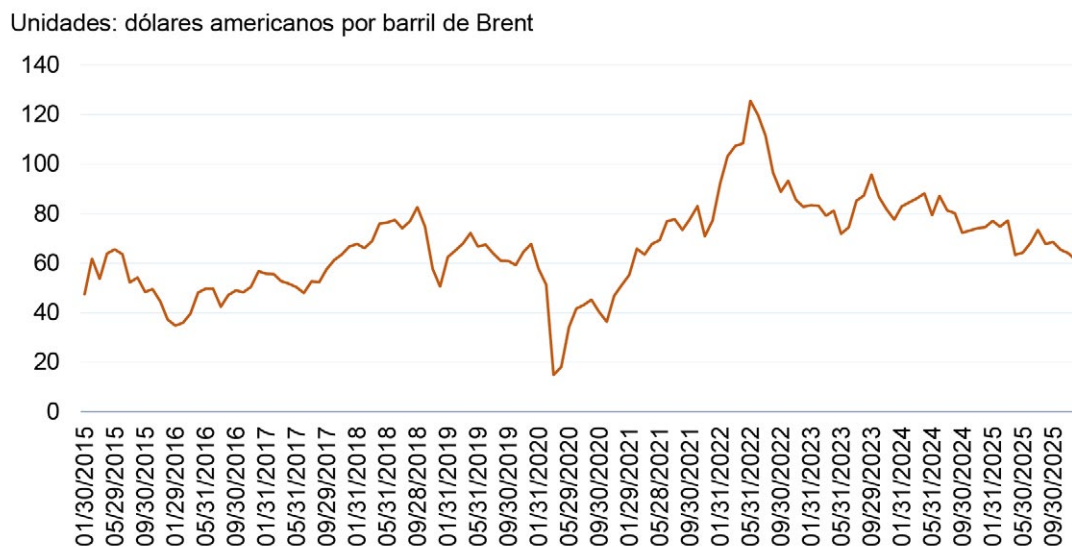
Fuente: Elaboración del DSN con datos de CORES

Figura 14.4: Importaciones de gas natural en España en 2025

La evolución en los últimos cinco años (2021-2025) muestra una transformación significativa. Si en 2021 España aún dependía de un equilibrio más tradicional entre el Magreb y el Golfo Pérsico, la invasión de Ucrania en 2022 aceleró un giro drástico hacia el atlántico. Las importaciones desde Estados Unidos se dispararon, pasando de ser un proveedor secundario a liderar ambos sectores (crudo y gas) en varios periodos del lustro.

Precios de los recursos energéticos

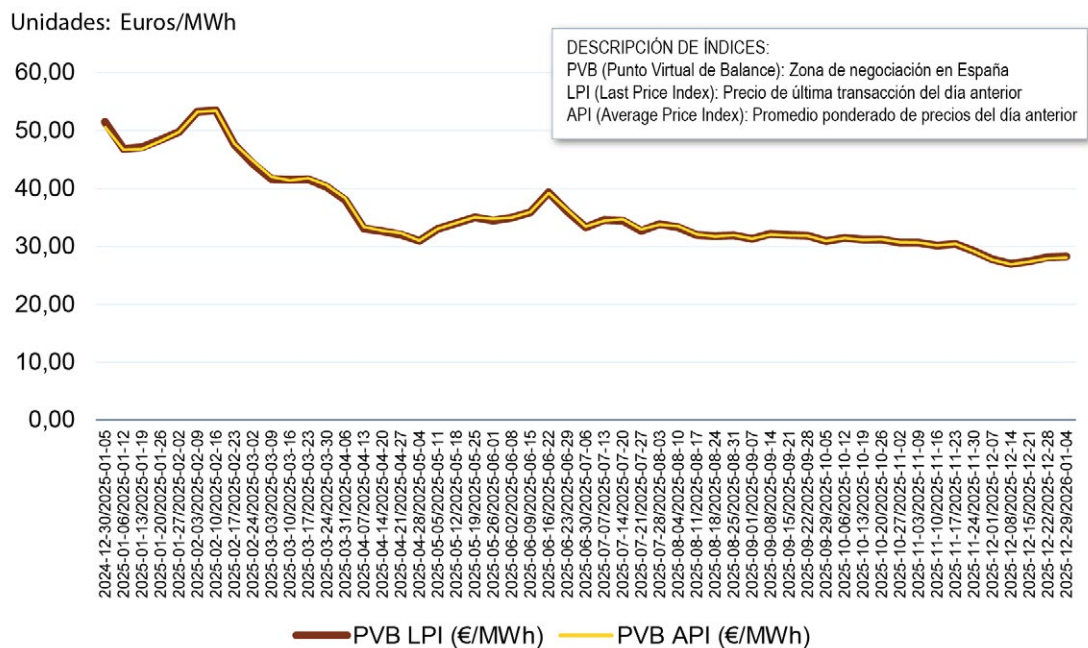
El precio del petróleo Brent se mantuvo a lo largo de 2025 en una franja relativamente contenida, de entre 60 y 80 dólares por barril. El año arrancó en torno a los 77 dólares, para caer bruscamente en abril hasta los 63 dólares, mínimo del ejercicio, coincidiendo con la incertidumbre global sobre la demanda. Una ligera recuperación llevó el barril a los 73 dólares en julio, aunque la tendencia fue de nuevo descendente durante el segundo semestre, cerrando el año en 61 dólares. El principal factor de volatilidad fue la situación geopolítica, con especial incidencia de la guerra de los Doce Días entre Israel e Irán en junio, que provocó tensiones puntuales en los mercados antes de ceder terreno. En conjunto, pese a los sobresaltos, el crudo mantuvo un comportamiento más estable que en ejercicios anteriores, sin los picos extremos registrados en 2022. (Figura 14.5)



Fuente: Elaboración del DSN con datos de la U.S. Energy Information Administration

Figura 14.5: Evolución del precio del petróleo 2015-2025

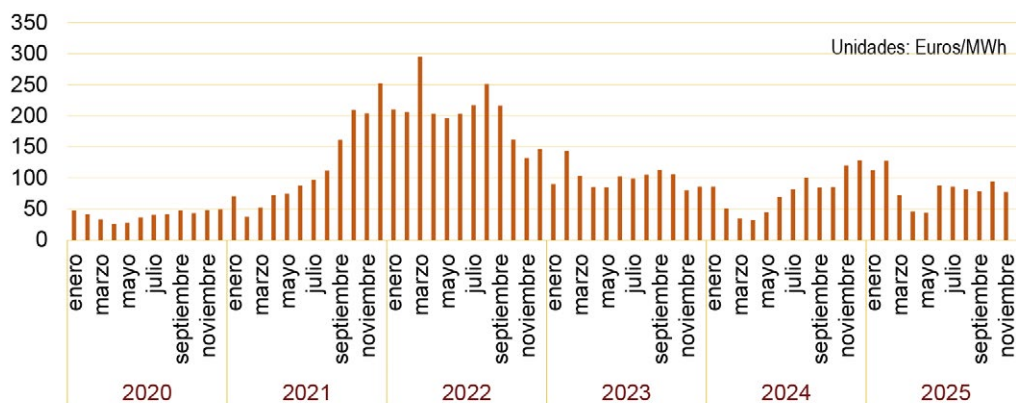
El gas natural, por su parte, experimentó en 2025 una caída sostenida e intensa. Según los datos del MIBGAS, el precio de referencia en España pasó de cerca de 51 €/MWh en la primera semana de enero hasta aproximadamente 28 €/MWh a finales de diciembre, lo que supone un descenso de casi el 45% en el año. Esta tendencia respondió a causas principalmente estructurales: con una demanda asiática relativamente débil y una fuerte capacidad exportadora de Estados Unidos, Europa se convirtió en el principal destino del GNL estadounidense, ejerciendo una presión constante a la baja sobre los precios. A ello se sumaron unos buenos niveles de almacenamiento en el continente y una demanda europea estructuralmente contenida, marcada por el despliegue de energías renovables y la mejora de la eficiencia energética. El único repunte relevante registrado en la semana del 16 al 22 de junio, cuando el precio rozó los 39 €/MWh, se motiva en el cierre temporal del estrecho de Ormuz durante la guerra de los Doce Días, aunque el efecto fue breve y los precios retomaron la senda bajista desde julio. (Figura 14.6)



Fuente: Elaborado por el DSN con datos de MIBGAS

Figura 14.6: Evolución de los precios del gas en España en 2025 (Media semanal del mercado ibérico MIBGAS)

En cuanto a la electricidad, España cerró 2025 con un récord histórico de generación renovable, con el 55,5%, donde la energía eólica y la solar fotovoltaica destacaron, liderando el mix con el 21,6% y el 18,4% del total respectivamente. Los precios fueron muy irregulares: arrancaron en niveles elevados, más de 127 €/MWh en febrero, para desplomarse en primavera hasta los 43-45 €/MWh, impulsados por la alta producción renovable y la bajada del gas, y recuperarse después. El precio final medio anual de la demanda nacional (que se componen del precio del mercado diario e intradiario, más los servicios de ajuste y los pagos por capacidad) fue de 83,45 €/MWh, un 9,4% más que en 2024, según información de Red Eléctrica. (Figura 14.7)

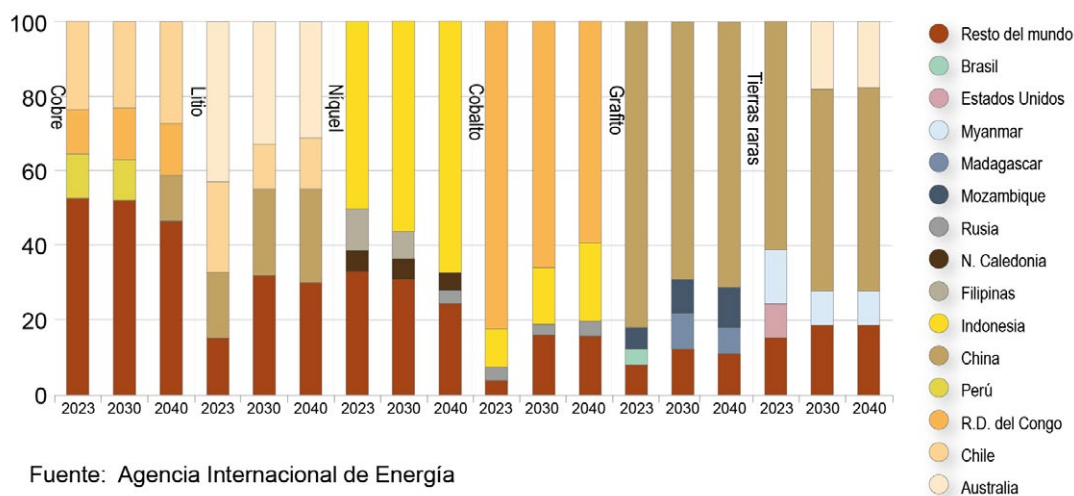


Fuente: Red Eléctrica Española

Figura 14.7: Evolución del componente del precio final medio de la energía. (Media mensual)

Materias primas fundamentales

El acceso a las materias primas es esencial para la economía de la Unión Europea y para el funcionamiento del mercado interior. Existe un conjunto de materias primas no agrícolas ni energéticas que se consideran fundamentales debido a su gran importancia económica y a su elevado riesgo para el suministro, a menudo por tener su origen en un reducido número de terceros países. La demanda de muchas de estas materias primas fundamentales es susceptible de aumentar exponencialmente en las próximas décadas, dado su papel clave en la realización de las transiciones ecológica y digital. (Figura 14.8)



Fuente: Agencia Internacional de Energía

Figura 14.8 Distribución geográfica de la producción de minerales clave para la transición energética, ya sea extraídos o en materia prima 2023-2040

Para hacer frente a esta situación, los legisladores de la UE (Consejo y Parlamento Europeo) aprobaron en 2024 el Reglamento 2024/1252 sobre materias primas fundamentales (CRMA, por sus siglas en inglés), por el que se estableció un marco para garantizar un suministro seguro y sostenible de materias primas fundamentales.

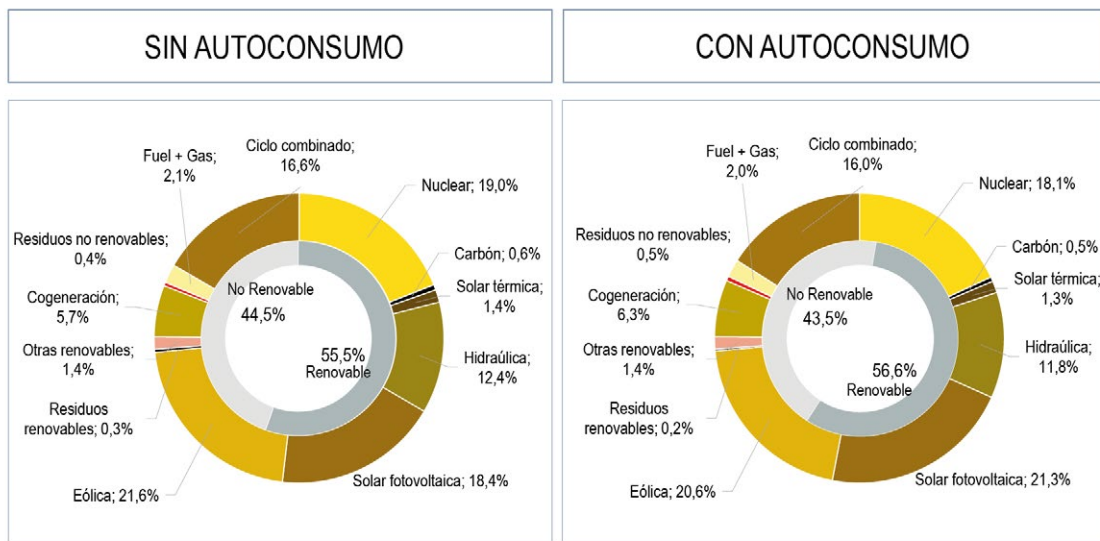
Nuevamente, a finales de 2025, la Comisión Europea adoptó el Plan de Acción *RESourceEU*, para responder al aumento de riesgos geopolíticos, la concentración de cadenas de suministro y la creciente demanda de materias primas críticas esenciales para la competitividad de la UE, la doble transición verde y digital, la preparación para la defensa y la seguridad alimentaria. Basándose en la Ley de Materias Primas Críticas, el Plan de Acción *RESourceEU*, pretende acelerar el avance hacia los objetivos de seguridad del suministro, reducir la dependencia excesiva de proveedores individuales y fortalecer la resiliencia de la economía de la UE.

Un pilar clave de dicho Plan de Acción es el uso de la Ley de Emergencias y Resiliencia del Mercado Interior (IMERA) para monitorizar las cadenas de suministro, coordinar respuestas y garantizar la continuidad durante las interrupciones, con relevancia directa para la resiliencia del comercio minorista y la continuidad del negocio en todo el Mercado Único.

Producción de energía eléctrica

El entorno energético en España en el año 2025 ha experimentado un incremento de generación de energía eléctrica del 3,7% respecto al año anterior. En particular la generación renovable en el sistema eléctrico nacional en 2025 ha aumentado un 1,3% registrando así el máximo histórico de producción con 150.988 GWh. Este incremento se concentra en la producción solar fotovoltaica y otras renovables que han crecido un 12,5% y un 5,6%, respecto a 2024 respectivamente.

Durante el ejercicio 2025 la participación de la producción renovable en el mix nacional ha sido de un 55,5%. (Figura 14.9)



Fuente: Red Eléctrica de España

Figura 14.9: Estructura de generación de energía eléctrica nacional en 2025 (%)

En cuanto a las diferentes tecnologías, la energía eólica lidera, por tercer año consecutivo, el mix con una cuota del 21,6% y una generación de 58.801 GWh. Mientras, la nuclear se mantiene en el segundo puesto con una aportación del 19% y, la energía solar fotovoltaica, ocupa la tercera posición, superando de nuevo los máximos tanto de participación en el mix nacional con el 18,4% como de producción con 50.188 GWh. Los ciclos combinados de gas natural se mantienen en el cuarto lugar con un 16,8%, aunque se ha incrementado su producción un 27,9%. Finalmente, en quinta posición, se sitúa la energía hidráulica con un 12,4 %, que alcanza los 33.685 GWh. Mientras, el carbón cierra el año con la menor producción de su historia, con una reducción de un 50 % respecto al año anterior y con la participación en el mix más baja aportando el 0,6% del total. Este hecho se debe, fundamentalmente, a la reconversión de la central térmica de Aboño II (en Asturias) a turbina de vapor, que tuvo lugar a mediados de julio.

Si se tiene en cuenta la estimación de la energía producida por las instalaciones de autoconsumo en 2025, la participación de la producción renovable en el mix nacional se incrementa en 1,1 puntos porcentuales, llegando al 56,6%. Considerando dicha estimación de la energía producida por las instalaciones de autoconsumo el mix nacional estaría liderado por la solar fotovoltaica (21,3%), seguida de la eólica (20,6%) y la nuclear (18,1 %).

Por otra parte, los programas de intercambio de energía eléctrica de España con países vecinos (UE y extra UE) cierran el 2025 con saldo exportador por cuarto año consecutivo y acumulando 50 meses seguidos de saldo exportador. Se programaron 26.206 GWh en sentido exportador, un 1,5% más que el año anterior y 13.202 GWh de importación, valor inferior en un 15,5% al del año 2024. El saldo neto resulta exportador, con un valor de 13.004 GWh, valor superior al del año anterior en un 27,8%.

El desglose por cada una de las interconexiones con otros países del saldo neto anual de intercambios de energía eléctrica programados es el siguiente:

- Con Francia resulta un saldo importador por segundo año consecutivo, en 138 GWh, frente a los 2.795 GWh del año anterior.
- En la interconexión con Portugal el saldo neto anual ha sido exportador, por séptimo año consecutivo, con un valor de 9.184 GWh, valor inferior en un 10% al del año anterior.
- Con Andorra el saldo ha sido exportador, con un valor de 215 GWh, que supone un descenso de casi un 9% respecto al año 2024.
- Con Marruecos vuelve a ser un saldo exportador, por cuarto año consecutivo, con un valor de 3.743 GWh, el valor más alto desde el año 2017, superando en casi un 48% al del pasado año.

Dimensión nacional: cero energético de 28 de abril de 2025

A las 12:33 horas del 28 de abril de 2025 se produjo un cero de tensión en la península ibérica y la desconexión del sistema eléctrico de España y Portugal del sistema interconectado europeo. Se trató de un evento sin precedentes. En el mismo momento del incidente, se realizó la declaración de una crisis de electricidad de acuerdo con el Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la *Directiva 2005/89/CE*, y con el Plan de preparación frente a los riesgos en el sector eléctrico en España, por haberse superado los umbrales de pérdida de carga y de energía no suministrada previstos en dicho plan. El Gobierno de España, a través del Ministerio para la Transición Ecológica y el Reto Demográfico, comunicó a la Comisión Europea y a las autoridades francesas y portuguesas dicha declaración de crisis de electricidad.

Como consecuencia de este evento, durante el 28 de abril, se interrumpió el normal funcionamiento de infraestructuras, comunicaciones, carreteras, trenes, aeropuertos, colegios y hospitales. Algunas de estas instalaciones y centros, especialmente los hospitalarios, continuaron prestando los servicios más urgentes respaldados por grupos electrógenos. Con relación a los transportes, el tráfico ferroviario fue el más afectado. Más de treinta estaciones de tren en diversas ciudades del país permanecieron abiertas toda la noche para que unos 35 mil viajeros afectados pudiesen ser atendidos e incluso pernoctar en sus instalaciones.

Las centrales nucleares españolas que estaban en situación operativa (Almaraz II, Ascó I y II, Vandellós II) notificaron al Consejo de Seguridad Nuclear (CSN) la declaración de situación de “prealerta de emergencia” debido a la pérdida de suministro eléctrico exterior, siendo necesario que sus generadores diésel de respaldo mantuvieran su funcionamiento en condición segura mientras se recuperaba la normalidad.

Las Fuerzas Armadas y, en particular, la Unidad Militar de Emergencias, proporcionaron numerosos apoyos a organismos civiles, tanto públicos como privados, fundamentalmente mediante la instalación de grupos electrógenos y suministro de combustible para mantener el funcionamiento de organismos e instalaciones esenciales.

El ministro del Interior procedió a la declaración de la emergencia de interés nacional mediante la aprobación de la Orden INT/399/2025, de 28 de abril. La participación de las Fuerzas y Cuerpos de Seguridad del Estado durante el cero energético fue determinante para asegurar los suministros críticos, y para garantizar la seguridad ciudadana en condiciones tan adversas.

La reposición se llevó a cabo de acuerdo con los Planes de Reposición y en tiempo récord, como se ha reconocido a nivel internacional por ENTSO-E. Según datos de Red Eléctrica de España, el propio día 28 ya se había restablecido el suministro al 50%. Prácticamente todas las Comunidades Autónomas mejoraban, si bien con cierta asimetría (ocho están en nivel 3 de Protección Civil: Andalucía, Castilla y León, Comunidad de Madrid, Comunitat Valenciana, Extremadura, Galicia, La Rioja y Murcia). El día 29 de abril, a las 07:00h, ya se había recuperado el 99,95% de la demanda peninsular.

En el marco de la seguridad nacional fueron seis las reuniones del Consejo de Seguridad Nacional celebradas entre los días 28 y 30 de abril para el seguimiento de la situación y la coordinación de las posibles consecuencias del corte de suministro eléctrico para la seguridad. Con posterioridad, fueron dos las reuniones del Comité de Situación para continuar con el seguimiento de la situación.

En el seno del Consejo de Seguridad Nacional se adoptó la decisión de crear un Comité para el análisis de las circunstancias que concurrieron en la crisis de electricidad del 28 de abril de 2025 (Comité 28A). Este comité fue creado formalmente mediante una orden comunicada el 30 de abril de 2025, bajo la presidencia de la Vicepresidenta Tercera del Gobierno y Ministra para la Transición Ecológica y el Reto Demográfico.

El informe del Comité 28A fue presentado en el Consejo de Seguridad Nacional de 17 de junio y posteriormente publicado. Adicionalmente, ENTSO-E elaboró su informe sobre el evento de acuerdo con la normativa UE. Las conclusiones del Informe del Comité 28A y del Comité ENTSO-E coinciden en que se trató de un incidente multifactorial, provocado por causas diversas combinadas entre sí.

Medidas para reforzar el sistema eléctrico

En el Informe del Comité 28A se identificaron medidas para reforzar el sistema, que se han articulado con carácter inmediato a lo largo de 2025 con el objetivo de mejorar la resiliencia del sistema eléctrico y a responder a los riesgos y oportunidades de la transición ecológica.

1. Medidas urgentes para el refuerzo de la planificación de la infraestructura eléctrica

El 8 de julio, el Consejo de Ministros, a petición del Ministerio para la Transición Ecológica y el Reto Demográfico, aprobó un listado de actuaciones específicas para aumentar la resiliencia de la red eléctrica, para incorporar como modificación puntual al *Plan de Desarrollo de la Red de Transporte de Energía Eléctrica 2021-2026*. El listado fue publicado mediante Resolución de 10 de julio de 2025, de la Secretaría de Estado de Energía e incluye 65 actuaciones destinadas a incorporar herramientas adicionales a las redes que faciliten el control de tensión, la estabilidad ante oscilaciones y en general, el refuerzo del sistema eléctrico, tanto en la Península como en Canarias y Baleares.

2. Medidas regulatorias y normativas

- a. *Real Decreto 997/2025, de 5 de noviembre, por el que se aprueban medidas urgentes para el refuerzo del sistema eléctrico.* Esta norma refuerza la resiliencia, robustez y estabilidad del sistema eléctrico. Mejora la supervisión, el control y la transparencia para el cumplimiento de las obligaciones por parte del conjunto de agentes del sector eléctrico, con mandatos a la Comisión Nacional de los Mercados y la Competencia (CNMC) para realizar informes de seguimiento y un plan de inspección extraordinario, e impulsa el almacenamiento de energía y la electrificación de la economía.
- b. *Resolución de 12 de junio de 2025, de la CNMC, por la que se modifican los procedimientos de operación para el desarrollo de un servicio de control de tensión en el sistema eléctrico peninsular español.* Implementa un nuevo procedimiento operativo 7.4 (P.O. 7.4). Con este procedimiento, las renovables (y no sólo las energías “convencionales”) están obligadas a participar en el servicio de control dinámico de tensión.
- c. *Resolución de 20 de octubre de 2025, de la CNMC, por la que se modifican temporalmente varios procedimientos de operación eléctricos para la introducción de medidas urgentes para la estabilización de la tensión en el sistema eléctrico peninsular español.* Esta Resolución introduce la aplicación temporal (desde el 20 de octubre 2025 hasta el 19 de enero de 2026) de los procedimientos operativos 3.1 y 3.2 (relativos a la resolución de restricciones técnicas con mayor antelación, antes de la primera subasta intradiaria,) para asegurar la reserva de banda de regulación necesaria; y 7.2., de control de rampas (se establecen límites a la velocidad de variación de potencia (rampas) para evitar que la entrada o salida brusca de generación renovable desestabilice la tensión de la red). Además, se aumentó la exigencia a las centrales eléctricas para el cumplimiento de consigna de tensión al 90% de las muestras (anteriormente era menos estricto). También se aumentó el muestreo a 60 valores por periodo para detectar con mayor precisión si una central se desviaba de la tensión ordenada, penalizando a las que no ayudaban a estabilizar la red.

3. Medidas de seguimiento y adaptación a las necesidades de cobertura oferta-demanda del sistema eléctrico

La CNMC aprobó el 20 de octubre de 2025 modificar determinados procedimientos de operación del sistema por razones operativas. Dichos cambios tuvieron una vigencia temporal con el objetivo de incrementar las herramientas del operador del sistema para reforzar la seguridad del suministro en caso de producirse variaciones bruscas de tensión.

Las modificaciones afectaban a los procedimientos de operación del sistema eléctrico: P.O. 3.1 Proceso de Programación, P.O. 3.2 Restricciones Técnicas y P.O. 7.2 Regulación Secundaria.

Estas medidas perdieron vigencia el 19 de enero de 2026, y se convirtieron en estructurales a partir del acuerdo de la CNMC, que entró en vigor el día 20 de enero de 2026.

4. Hoja de ruta de resiliencia

El Consejo de Seguridad Nacional aprobó, el 16 de diciembre de 2025, la *Hoja de Ruta de Resiliencia*. Contiene objetivos específicos, como el de la creación de centros de situación para crisis en todos los ministerios y organismos que forman parte del Sistema, o nombrar un centro en aquellos organismos en los que ya exista, que operen 24/7/365 y bajo cualquier circunstancia.

PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA

- El 16 de diciembre de 2025, el Consejo de Seguridad Nacional aprobó la primera Estrategia Nacional contra la Proliferación de Armas de Destrucción Masiva.
- Durante 2025, el régimen internacional de no proliferación continuó enfrentándose al actual escenario geopolítico global donde impera el uso de la fuerza frente al multilateralismo y el orden basado en reglas.
- España participa activamente con la Organización para la Prohibición de las Armas Químicas a través de la Autoridad Nacional para la Prohibición de las Armas Químicas.

PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA

Arquitectura internacional de la no proliferación

El régimen internacional de no proliferación se encuentra en un momento muy complicado, debido tanto a factores derivados de la situación política internacional, como por la propia falta de avances en los elementos de dicha estructura.

En el ámbito nuclear, la retórica y las posturas estratégicas de Rusia, junto con el incremento y modernización de los arsenales nucleares por parte de China, representan factores que complican los avances hacia el desarme nuclear. A su vez, la falta de resolución de los expedientes nucleares de Irán y Corea del Norte contribuye a generar tensiones en torno al Tratado de No Proliferación Nuclear (TNP).

En cuanto a las armas químicas, la situación se mantiene compleja. Por un lado, el uso de agentes químicos prohibidos en conflictos bélicos por parte de Rusia constituye un desarrollo contrario a la Convención sobre Armas Químicas. Al mismo tiempo, el compromiso de las nuevas autoridades sirias con la resolución de las cuestiones pendientes del programa de armas químicas clandestino del anterior régimen, en colaboración con la Organización para la Prohibición de las Armas Químicas (OPAQ), podría conducir a la resolución de una de las crisis de proliferación más significativas de los últimos años.

Por último, a pesar de la percepción de que tecnologías como la IA pueden suponer un incremento de la amenaza de desarrollo de armas biológicas, se está dando un renovado impulso al desarrollo de un sistema de verificación de la Convención de Armas Biológicas.

En este contexto, la falta de avances del TNP, cuyo último documento de consenso data de 2010, la no entrada en vigor del Tratado de Prohibición Completa de los Ensayos Nucleares (TPCEN) y las dudas sobre el futuro del control de armamentos nucleares, una vez expire el nuevo START en febrero de 2026, suponen elementos de incertidumbre sobre el futuro de la arquitectura internacional de no proliferación.

Por ello, los esfuerzos han de ir dirigidos a reforzar esos instrumentos y las organizaciones internacionales como el OIEA, la OPAQ o la OTPCE (Comisión Preparatoria de la Organización del Tratado de Prohibición Completa de los Ensayos Nucleares) que los sustentan.

En líneas generales, se ha producido un deterioro del entorno de seguridad global, con avances limitados y desafíos en los principales tratados. Los organismos, foros y regímenes de control de no proliferación continúan sufriendo las consecuencias de la falta de acuerdo entre sus miembros, lo que impide que tomen medidas y avancen en sus objetivos, llegando, en algunos casos, a causar la suspensión de las reuniones.

Además, durante 2025, el régimen internacional de no proliferación continuó enfrentándose al actual escenario geopolítico global donde impera el uso de la fuerza frente al multilateralismo y el orden basado en reglas, lo que sigue mermando su eficacia en la medida que los principales actores, no confían en las instituciones para resolver sus conflictos.

En cuanto a las negociaciones nucleares, la paralización de las conversaciones de estabilidad estratégica entre Washington y Moscú, dirigidas a desarrollar un nuevo marco de control de armamentos que sustituya al Nuevo Tratado de Reducción de Armas Estratégicas (Nuevo START), que expira en febrero de 2026, pone en peligro la estabilidad estratégica.

La Tercera Sesión del Comité Preparatorio de la Conferencia de Revisión del TNP, que tuvo lugar en mayo de 2025, sirvió para seguir trabajando en la preparación de la Conferencia de Revisión del 2026, si bien las perspectivas de que la Conferencia de Revisión llegue a un documento de consenso siguen siendo muy escasas.

Por otra parte, en relación con las armas químicas, la valoración es mixta. Cabe destacar el compromiso de las autoridades sirias por aclarar todas las cuestiones pendientes del programa clandestino de armas químicas desarrollado por el anterior régimen. El trabajo de la OPAQ, apoyado por España será fundamental. En el lado negativo, el uso por Rusia de agentes antidisturbios prohibidos en contextos bélicos, así como los indicios sobre el uso de armas químicas en otros conflictos como Sudán, ponen de manifiesto que la proliferación de armas químicas y la detección de programas clandestinos siguen siendo retos pendientes. Desde una presencia institucional, el próximo mes de junio acabará el mandato del actual Director General de la OPAQ, el español Fernando Arias, que será sustituido por Sabrina Dallafor, designada por la reciente Conferencia de Estados Partes.

En relación con las armas biológicas, los trabajos de los grupos de trabajo creados en la última conferencia de revisión de la Convención de armas biológicas, especialmente el de verificación, han recibido un inesperado impulso por parte de Estados Unidos que ha anunciado la creación de nuevos instrumentos de verificación.

Además, la agresión de Rusia contra Ucrania se ha convertido en el principal factor de desgaste de la arquitectura internacional de no proliferación. Desde la violación de las garantías de seguridad dadas por un país dotado de armas nucleares (Rusia) a uno no nuclear, como Ucrania, pasando por la retórica nuclear rusa o el uso sistemático por la propia Rusia de agentes químicos prohibidos por la Convención de Armas Químicas, no cabe duda de que la agresión rusa está teniendo implicaciones muy negativas para la no proliferación de Armas de Destrucción Masiva (ADM).

A lo anterior cabe añadir, como factor negativo, el bloqueo al que Rusia está sometiendo numerosos foros internacionales de no proliferación y desarme, para evitar rendir cuentas por sus acciones. Como ejemplo, cabe destacar el bloqueo de participación de distintas organizaciones internacionales y regionales (UE / AIEA / INTERPOL / FAO / OEA / OMS) y de la sociedad civil, en el contexto de los trabajos que la Convención para la Prohibición de las Armas Biológicas está realizando durante los últimos años.

Mecanismos de prevención, detección y control

En cuanto a los mecanismos de prevención, detección y control de las armas de destrucción masiva y la tecnología de doble uso, cabe destacar que España participa activamente con la Organización para la Prohibición de las Armas Químicas (OPAQ) a través de la Autoridad Nacional para la Prohibición de las Armas Químicas (ANPAQ). En este sentido, el Ministerio de Defensa mantiene su contribución a organismos e instalaciones y con expertos a diferentes iniciativas internacionales, como son: las capacidades ofertadas a la OPAQ para respuesta ante incidentes, los expertos que participan en el Mecanismo del Secretario General de Naciones Unidas para investigar el posible uso de armas químicas (UNSGM); la organización de cursos para el Grupo de países de Latinoamérica y Caribe (GRULAC), y la disponibilidad del Laboratorio de Verificación de Armas Químicas (LAVEMA), que es el laboratorio de referencia de la OPAQ con capacidad para analizar agentes de guerra química en muestras medioambientales.

Además, el Ministerio de Defensa continúa participando a través del Departamento de Sistemas de Defensa Nuclear, Biológica y Química (NBQ) del Instituto Nacional de Técnica Aeroespacial (INTA) en varios proyectos de investigación internacionales que afectan, entre otras, al Área de Defensa Biológica: SAFE STADIUM para prevención de la amenaza NBQ en grandes estadios de fútbol, y HOTHREAT para gestión de la amenaza NBQ en hoteles y salas de convención.

Por otra parte, el Ministerio de Defensa participa como laboratorio de referencia, junto con otros laboratorios nacionales, en la Red de Laboratorios de Alerta Biológica (RE-LAB), regulada por la Orden PCI/1381/2018 y coordinada por el Instituto de Salud Carlos III (ISCIII).

Además, cabe reseñar el desarrollo de las actividades rutinarias derivadas del cumplimiento del Tratado sobre la No Proliferación de las armas nucleares (TNP), dentro de las competencias de la Subdirección General de Energía Nuclear (SGEN) de la Dirección General de Planificación y Coordinación Energética (DGPLACE), en el ámbito de aplicación de este, y cumplimiento del Protocolo Adicional al Acuerdo de Salvaguardias establecido entre España y el Organismo Internacional de Energía Atómica (OIEA).

A su vez, en el ámbito de competencias de la DGPLACE, se ha continuado con la tramitación de los expedientes de autorización de protección física y de aprobación de los Planes de Protección Física de las instalaciones nucleares y radiactivas y sus transportes. El objetivo de dichas autorizaciones es aprobar el sistema de protección física de las instalaciones y las actividades mencionadas, que se define como el conjunto integrado de organización, personal, procedimientos y equipos previstos para evitar que un potencial adversario pueda completar con éxito un acto malintencionado contra la instalación, los materiales nucleares o las fuentes radiactivas.

Mientras, en el ámbito de la lucha contra la proliferación de armas de destrucción masiva, las Aduanas españolas refuerzan sus protocolos de prevención, detección y control de armas químicas, nucleares, agentes biológicos y sus precursores, así como de la tecnología de doble uso.

Asimismo, el transporte marítimo y la utilización de pabellones de conveniencia, transferencias buque a buque o manipulación de sistemas de identificación automática (AIS) constituyen vectores potenciales de ocultación de materiales sensibles, lo que refuerza la necesidad de vigilancia reforzada en los nodos logísticos estratégicos. La creciente disponibilidad de tecnologías emergentes de uso dual, incluidas capacidades digitales avanzadas y desarrollos en el ámbito biotecnológico, amplía el espectro de riesgos asociados a la proliferación y exige la actualización constante de los mecanismos de control y de los sistemas de análisis de riesgo.

Dentro de este ámbito, a nivel internacional, destaca la participación de la AEAT en el Grupo de Suministradores Nucleares (GSN) y en el programa de control estratégico de mercancías de la Organización Mundial de Aduanas (OMA) para prevenir el tráfico transfronterizo de sustancias NRBQ y productos de doble uso. En el ámbito europeo, la AEAT forma parte del *Customs Threat Assessment Trust* (CTA) del *Law Enforcement Working Party (Customs)* (LEWP-C) del Consejo de la UE, que coordina la cooperación entre autoridades aduaneras de los Estados miembros para el control exhaustivo de mercancías estratégicas. Además, colabora en el *Forum of Strategic Trade Enforcement* (STENFOR) para identificar buenas prácticas y armonizar enfoques de control comercial estratégico.

Igualmente, a nivel nacional, la AEAT ha contribuido a la elaboración y aprobación del “Protocolo para la Interceptación de Actividades de Proliferación” en el seno del Comité especializado de no proliferación de armas de destrucción masiva. Esta intensificación de la transmisión de información responde al incremento del riesgo de desvío de material de doble uso y de defensa en Europa, en el contexto de tensiones geopolíticas y conflictos activos o latentes, como la guerra en Ucrania, y otros latentes alrededor del Mediterráneo.

Concretamente, en 2025 ha concluido la actualización tecnológica del sistema MEGAPORT, un sistema integral de gestión de alarmas para material radiactivo basado en herramientas no intrusivas y técnicas de Inteligencia Artificial, y se han desplegado tres unidades móviles de retro dispersión localizadas en Vigo, Bilbao y Las Palmas.

Además, hasta octubre de 2025 se han registrado cuatro detecciones de material radiactivo (tres en el puerto de Valencia y una en el de Barcelona), todas clasificadas como de riesgo bajo.

Asimismo, se han incorporado 27 nuevos escáneres de equipaje.

Por su parte, el Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT) colabora en este ámbito con el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación aportando expertos técnicos en la delegación española del grupo de trabajo B de la Organización del Tratado para la Prohibición Completa de Ensayos Nucleares (OTPCE).

Este organismo contribuye también con inspectores *in situ* y en el grupo de trabajo sobre la mejora en la formación de inspectores *in situ* en temas de evaluación y gestión de datos y muestras. Por otro lado, participó con expertos en el equipo de evaluación del experimento 2024 que organizó el Centro Nacional de Datos (CND) de la OTPCE.

En el plano internacional, los informes de la OPAQ señalan que Rusia empleó armas químicas en Ucrania, lo que parece indicar que los mecanismos de verificación de la convención funcionan correctamente. A estos informes se unen las medidas diplomáticas con Siria para la destrucción de las armas químicas no declaradas anteriormente.

Por su parte, a raíz del conflicto ruso-ucraniano, tanto Rusia como Ucrania se han denunciado mutuamente por el incumplimiento de la Convención sobre las Armas Químicas por el empleo de sustancias prohibidas por esta.

En cuanto a Irán, por el momento, las negociaciones continúan estancadas. A su vez, se han restaurado las sanciones del Consejo de Seguridad de la Organización de las Naciones Unidas por este programa nuclear de uso militar de Irán.

La situación del expediente nuclear iraní no ha tenido una evolución positiva en 2025. Por un lado, tras la activación por parte del E3 (Alemania, Francia y Reino Unido) del mecanismo de reimposición automática de sanciones han vuelto a entrar en vigor las resoluciones del Consejo de Seguridad de Naciones Unidas 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), y 1929 (2010).

Por otra parte, resoluciones de la Junta de Gobernadores del OIEA de junio y noviembre de 2025 exigen a Irán que colabore con el propio OIEA para aclarar cuestiones pasadas pendientes de ser resueltas, así como la ubicación de las existencias de uranio enriquecido, tras los ataques contra Irán del pasado mes de junio.

A pesar de la situación, la diplomacia es más necesaria que nunca y ninguna de las partes parece haber cerrado la vía a una solución diplomática. Más allá de EEUU e Irán será necesaria la implicación de numerosos actores, desde la UE y el E3 hasta actores regionales, para poder alcanzar un nuevo acuerdo. También será fundamental que Irán vuelva a colaborar activamente con el OIEA.

Como consecuencia de los ataques de Israel y EE UU a sus instalaciones del programa nuclear, Irán sigue sin colaborar con el OIEA y no facilita información respecto a la cantidad y porcentaje de enriquecimiento del uranio almacenado, ni permite las inspecciones sensibles desde el punto de vista de la proliferación nuclear, aunque según la propia OIEA, Irán contaba con 400 kg de uranio enriquecido al 60% antes de los ataques aéreos contra Irán, de junio de 2025.

Los ataques con misiles balísticos y drones sobre Israel han permitido que iraníes y hutíes puedan probar sus capacidades para evitar las defensas israelíes, a pesar del desgaste de su arsenal.

En cuanto a Corea del Norte, a pesar de que desde 2009 los inspectores del OIEA no han tenido acceso al país, la información disponible sigue siendo extremadamente preocupante. Por un lado, las actividades nucleares no sólo no han disminuido, sino que se habrían intensificado, habiéndose detectado una mayor operación de las instalaciones de enriquecimiento de uranio en Kangson y Yongbyon y la posible construcción de una instalación adicional de enriquecimiento de uranio en Yongbyon. Por otra parte, se mantendría el estado de preparación para realizar un nuevo ensayo nuclear (el último tuvo lugar en septiembre de 2017). Por último, a lo largo de 2025 han seguido los ensayos de diversos tipos de misiles, llegando Corea del Norte a anunciar el desarrollo de misiles hipersónicos.

En este contexto, y dada además la creciente colaboración militar entre Corea del Norte y Rusia, la perspectiva de reanudar las negociaciones para la desnuclearización completa, verificable e irreversible de Corea del Norte, parece todavía lejana.

Mientras, la República Popular de China dispone del tercer mayor arsenal nuclear del mundo y está dedicando esfuerzos notables a su ampliación, modernización y diversificación, a fin de fortalecer su disuasión estratégica. (Figura 15.1)

Figura 15.1: Inventario estimado de cabezas nucleares en el mundo 2024-2025

Inventario de ojivas nucleares 2024-2025								
Estado	Desplegadas	Almacenadas	Desplegadas + Almacenadas		Retiradas		TOTAL	
	2025	2025	2024	2025	2024	2025	2024	2025
EE.UU.	1.770	1.930	3.708	3.700	1.620	1.477	5.328	5.177
Rusia	1.718	2.591	4.380	4.309	1.200	1.150	5.580	5.459
Reino Unido	120	105	225	225	-	-	225	225
Francia	280	10	290	290	-	-	290	290
China	24	576	500	600	-	-	500	600
India	-	180	172	180	-	-	172	180
Pakistán	-	170	170	170	-	-	170	170
Corea del Norte	-	50	50	50	-	-	50	50
Israel	-	90	90	90	-	-	90	90
TOTAL	3.912	5.702	9.585	9.614	2.820	2.627	12.405	12.241
CAMBIO PORCENTUAL DE INVENTARIO			+0,30%		+6,84%		-1,32%	

Fuente: Instituto Internacional de Estudios para la Paz de Estocolmo (SIPRI) Yearbook 2025

Para ello, está ampliando sus silos de misiles balísticos intercontinentales (ICBM) y busca consolidar la tríada nuclear con el concurso de bombarderos estratégicos como el H-6N, submarinos de propulsión nuclear y misiles balísticos (SSBN) como de clase Jin (tipo 094).

España continúa su compromiso firme con la No Proliferación de Armas de Destrucción Masiva, siendo parte del Tratado sobre la No Proliferación de las armas nucleares (TNP), Tratado Euratom (Capítulo 7-Control de Seguridad) y la Convención sobre la Protección Física de los Materiales Nucleares y su Enmienda (CPFMN).

Además, entre la normativa en materia de No Proliferación Nuclear y de protección física de los materiales nucleares y de fuentes radiactivas, destaca el **Nuevo Reglamento (Euratom) 2025/974 de la Comisión, de 26 de mayo de 2025, relativo a la aplicación del control de seguridad de Euratom**, que se une a la legislación ya existente en esta materia, entre las que destaca:

- INFCIRC/193, de 14 de septiembre de 1973, texto del acuerdo concertado entre Bélgica, Dinamarca, la República Federal de Alemania, Irlanda, Italia, Luxemburgo, Países Bajos, la Comunidad Europea de Energía Atómica (Euratom) y el OIEA en relación con el Tratado sobre la No Proliferación de las armas nucleares.
- *Real Decreto 1206/2003, de 19 de septiembre, para la aplicación de los compromisos contraídos por el Estado español en el Protocolo adicional al Acuerdo de salvaguardias derivado del Tratado sobre la no proliferación de las armas nucleares.*
- Orden ITC/2637/2004, de 21 de julio, relativa a la aplicación de determinadas disposiciones del Real Decreto 1206/2003, de 19 de septiembre, para la aplicación de los compromisos contraídos por el Estado Español en el Protocolo Adicional al Acuerdo de Salvaguardias derivado del Tratado sobre la no Proliferación de las Armas Nucleares, por su encomienda a la Comisión Europea.
- *Real Decreto 1308/2011, de 26 de septiembre, sobre protección física de las instalaciones y los materiales nucleares, y de las fuentes radiactivas.* Se ha creado un grupo de trabajo interministerial, entre Consejo de Seguridad Nuclear, MITECO y Ministerio del Interior, con el fin de acordar un texto revisado de este Real Decreto que se materializará en un Reglamento sobre la materia.
- Instrucción IS-41, de 26 de julio de 2016, del Consejo de Seguridad Nuclear, por la que se aprueban los requisitos sobre protección física de fuentes radiactivas.
- Instrucción IS-43 del CSN, de 20 de marzo de 2019, por la que se establecen los criterios de notificación de sucesos relativos a la seguridad física por parte de las centrales nucleares.
- Instrucción IS-46, de 14 de mayo de 2024, del Consejo de Seguridad Nuclear, sobre seguridad física durante el transporte de materiales nucleares y fuentes radiactivas.

Asimismo, España continúa trabajando en el marco de las salvaguardias nucleares, participando en reuniones nacionales e internacionales.

- Número total de instalaciones sometidas al control del uso del material nuclear según el TNP del OIEA y según el Tratado Euratom: 34, distribuidas de la siguiente forma:
 - 8 reactores nucleares
 - 1 fábrica de elementos combustibles
 - 6 almacenes temporales de combustible nuclear gastado (ATIs)
 - 2 almacenes de residuos radiactivos
 - 17 instalaciones industriales (con uranio empobrecido en blindaje de fuentes).

- Número de inspecciones realizadas por inspectores del OIEA y/o Euratom en dichas instalaciones, hasta diciembre de 2025: 90.
- Remisión a la Comisión Europea de la declaración anual y de las declaraciones trimestrales de exportaciones, en cumplimiento de las obligaciones establecidas en el Protocolo Adicional al Acuerdo de Salvaguardias.
- Celebración en Madrid de la Reunión Trilateral (OIEA-Euratom-España) sobre la aplicación de las salvaguardias nucleares en España.
- Participación en la reunión anual del Programa Español de Apoyo a las Salvaguardias Nucleares del OIEA.
- Participación de la SGEN en la reunión organizada por la Comisión Europea, en Luxemburgo: “*Meeting with Member States on Implementing EURATOM Treaty Safeguards*”.
- Participación en las dos reuniones anuales del Grupo de trabajo de Implementación de Salvaguardias, creado en el seno de la “*European Safeguards Research & Development Association*” (ESARDA).
- Participación en las reuniones del Grupo Nacional de Salvaguardias Nucleares, a las que asisten también los responsables de salvaguardias de todas las instalaciones nucleares sometidas al control del material nuclear en España.
- Participación en las reuniones del Grupo de Trabajo de Indicadores de No Proliferación de ADM en el seno del Comité Especializado de No Proliferación de Armas de Destrucción Masiva (CENP).

Finalmente, cabe destacar igualmente el trabajo de España en el marco de la protección física de los materiales nucleares y las fuentes radiactivas y reuniones nacionales e internacionales en las que se ha participado, dentro del que ha llevado a cabo las siguientes actividades:

- Coordinación y cooperación entre la DGPLACE, el Consejo de Seguridad Nuclear y la Secretaría de Estado de Seguridad del Ministerio del Interior en materia de protección física de los materiales nucleares, de las instalaciones nucleares y de las fuentes radiactivas y sus transportes.
- Participación de la SGEN en el Grupo de trabajo para la optimización de revisiones de planes de protección física de centrales nucleares.
- Número de instalaciones nucleares y radiactivas cuya aprobación de Planes de Protección Física es competencia de la : 41, distribuidas de la siguiente forma:
 - 10 instalaciones nucleares.
 - 31 instalaciones radiactivas.

- Número de Resoluciones emitidas, hasta diciembre de 2025, de aprobación de revisiones de Planes de Protección Física de las instalaciones nucleares: 5.
- Número de solicitudes de protección física de transporte de material nuclear de categoría III hasta diciembre de 2025: 3.
- Número de transportistas registrados en el Registro de entidades que llevan a cabo transportes de material nuclear y fuentes radiactivas que requieren medidas de protección física: 3.

Avances regulatorios y estratégicos

Estrategia Nacional contra la Proliferación de Armas de Destrucción Masiva

A nivel nacional, el impacto del contexto internacional, marcado por la guerra de Rusia contra Ucrania, el deterioro del sistema de control de armamentos, el aumento de las tensiones geopolíticas o el cuestionamiento por diversos actores de las bases del sistema de no proliferación ha acelerado la necesidad de una respuesta coordinada del Estado.

Así, el 16 de diciembre de 2025, el Consejo de Seguridad Nacional aprobó la primera Estrategia Nacional contra la Proliferación de Armas de Destrucción Masiva. Este documento refleja los cambios en el panorama geopolítico y geoestratégico mundial y nace con la aspiración de integrarse en la arquitectura del régimen internacional de no proliferación y de alinearse con la Estrategia Española de Acción Exterior y la Directiva de Defensa Nacional. Además, la estrategia persigue un doble objetivo: por un lado, proyectar el compromiso de España con la seguridad global y, al mismo tiempo, blindar el territorio nacional frente a amenazas emergentes, incluidas las procedentes de actores no estatales.

Para ello, sitúa la lucha contra la proliferación en el nivel político-estratégico y busca articular una actuación conjunta de todos los organismos de la Administración, así como reforzar la preparación institucional y social ante posibles intentos de desarrollo, adquisición o uso de materiales nucleares, radiológicos, químicos o biológicos.

Plan Estratégico Nacional contra la Financiación de la Proliferación de Armas de Destrucción Masiva

La financiación de la proliferación de armas de destrucción masiva se ha convertido en un reto de calado internacional en los últimos años, debido en gran medida a las políticas armamentísticas que al respecto se han llevado a cabo por los principales actores internacionales en la materia.

El Plan Estratégico Nacional contra la Financiación de la Proliferación de Armas de Destrucción Masiva, aprobado el 26 de agosto de 2025, que tiene por objeto la implementación de medidas que impidan se proporcionen fondos para el desarrollo, adquisición y uso de armas de destrucción masiva, nucleares, químicas y biológicas, así como de los materiales y tecnología relacionados. El desarrollo y cumplimiento del Plan será coordinado y supervisado por parte del Comité Especializado de No Proliferación, como órgano de apoyo al Consejo de Seguridad Nacional.

EFECTOS DEL CAMBIO CLIMÁTICO Y DE LA DEGRADACIÓN DEL MEDIO NATURAL

- Según el Informe sobre la Brecha de Emisiones 2025 del Programa de las Naciones Unidas para el Medio Ambiente, las emisiones mundiales de gases de efecto invernadero batieron un récord en 2024: 57,7 GtCO₂e, un 2,3 % más que la cifra de 2023.
- El año 2025 ha tenido carácter extremadamente cálido, con una temperatura media en la España peninsular de 15,0°C, siendo destacable el calor registrado durante la época estival, que ha situado el verano de 2025 como el más cálido desde 1961.
- En las últimas décadas, los inventarios forestales reflejan una expansión sostenida de la superficie arbolada en España, lo que refuerza el papel de los bosques como sumideros de carbono, reguladores del ciclo hidrológico y barreras frente a la erosión.

EFECTOS DEL CAMBIO CLIMÁTICO Y DE LA DEGRADACIÓN DEL MEDIO NATURAL

En las últimas décadas, los mares que rodean la Península Ibérica muestran un marcado calentamiento, especialmente en superficie, donde las temperaturas aumentan más rápido que el promedio global y han alcanzado valores récord entre 2022 y 2024, mientras que en zonas de afloramiento costero persisten aguas frías que actúan como refugios climáticos; en profundidad el calentamiento también progresa, aunque con un ligero enfriamiento reciente en aguas intermedias del Atlántico por la llegada de masas del norte, todo ello acompañado de una subida del nivel del mar que agrava riesgos costeros.

Este calentamiento repercute profundamente en los ecosistemas marinos, favoreciendo la expansión de especies de afinidad cálida —incluidas algas tóxicas—, el retroceso de especies boreales de interés pesquero y la proliferación de invasoras, incrementando el estrés en sistemas ya sobreexplotados, mientras la mayor temperatura superficial intensifica la evaporación y contribuye a fenómenos meteorológicos más extremos y, a largo plazo, a posibles alteraciones de la circulación oceánica global, incluido el riesgo de debilitamiento del AMOC (Circulación de Retorno Meridional del Atlántico).

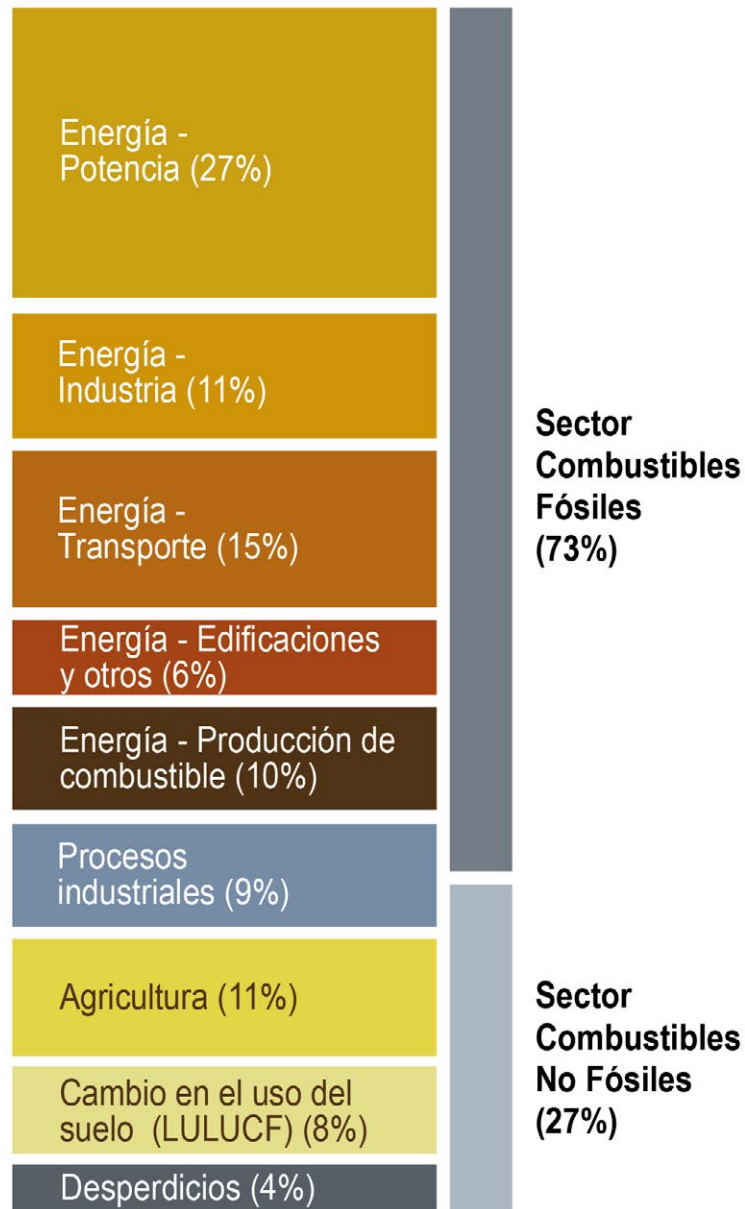
Paralelamente, el aumento del CO₂ antropogénico está acidificando el océano, comprometiendo a organismos calcificantes como corales, moluscos o parte del plancton. En este contexto, España ha encadenado a lo largo del año diversos episodios meteorológicos extremos: sequías intermitentes en distintas regiones, una de las olas de calor más intensas y prolongadas registradas, episodios notables de frío en invierno y múltiples lluvias torrenciales que causaron inundaciones graves en zonas mediterráneas y otras áreas del país.

Gases de efecto invernadero

El Informe sobre la Brecha de Emisiones 2025 del Programa de las Naciones Unidas para el Medio Ambiente refleja que las emisiones mundiales de Gases de Efecto Invernadero (GEI) batieron un récord en 2024: 57,7 GtCO_{2e}, un 2,3 % más que la cifra de 2023. Ese repunte en las emisiones mundiales totales de GEI es más de cuatro veces superior que la tasa promedio de crecimiento durante la década de 2010 a 2019 (0,6% al año de media), y comparable a la década de los años 2000 (2,2% anual de media).

El incremento se ha registrado en todas las fuentes principales de GEI y en todos los sectores. A pesar del papel clave que desempeñan los combustibles fósiles en el aumento de las emisiones totales, la deforestación y el cambio en el uso del suelo fueron factores decisivos para el rápido aumento de las emisiones en 2024. Las emisiones netas mundiales de CO₂ derivadas del uso del suelo, el cambio en el

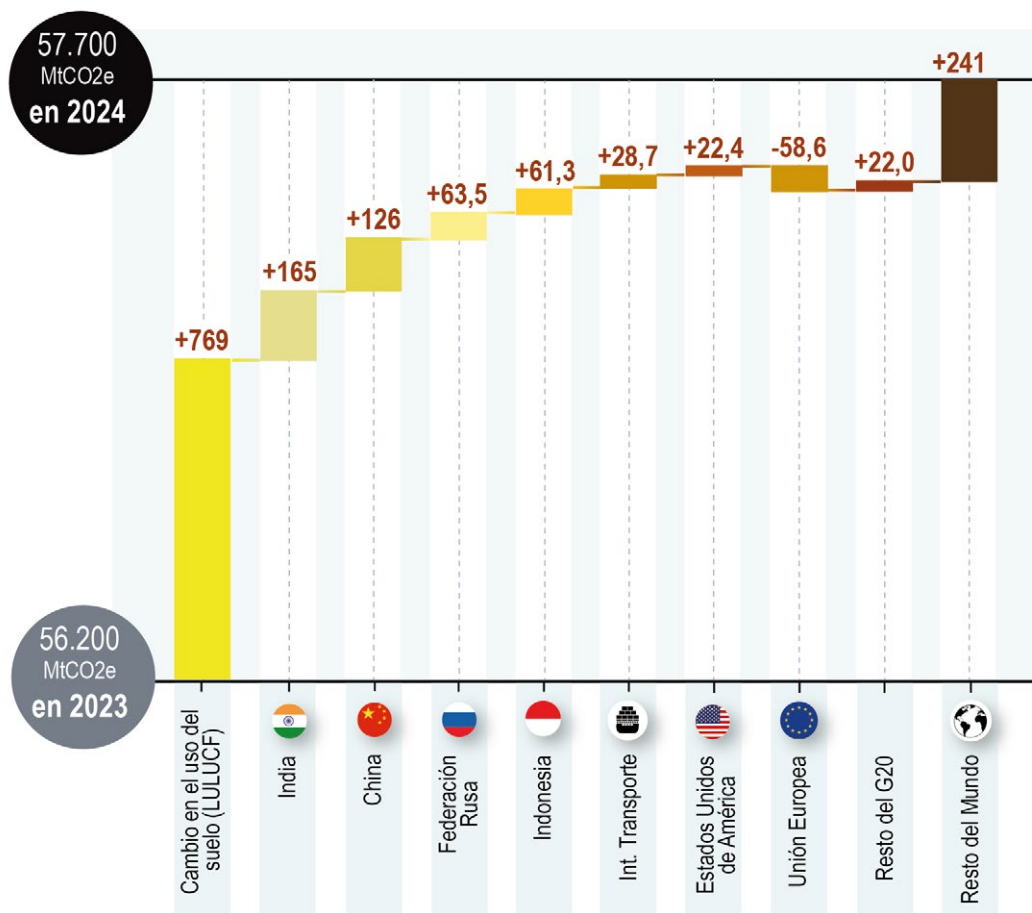
uso del suelo y la silvicultura (LULUCF) aumentaron un 21% en 2024 y fueron responsables del 53% del aumento total de las emisiones mundiales de GEI. En 2023, el sector energético (concretamente, la producción de electricidad) generó el 27% de las emisiones y mantuvo su puesto como principal emisor a escala global, seguido del transporte (15% de las emisiones), la agricultura (11%) y la industria (11%). (Figura 16.1)



Fuente: Informe sobre la Brecha de Emisiones 2025, PNUMA

Figura 16.1: Emisiones globales de GEI en 2024

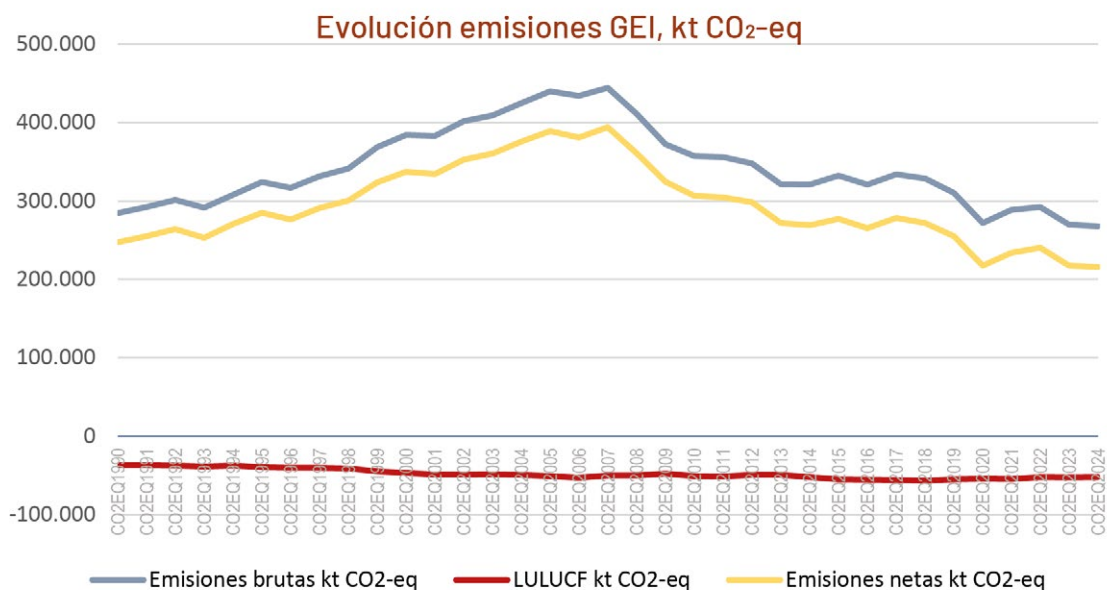
Las emisiones de GEI de los miembros del G20, excluyendo a la Unión Africana, también fueron a más en 2024 y representaron el 77% de las emisiones de todo el planeta. De los seis mayores emisores de GEI, la Unión Europea fue el único que redujo sus emisiones en 2024. El mayor aumento absoluto de las emisiones totales de GEI, excluido el sector LULUCF, se observó en la India y China, mientras que Indonesia registró el crecimiento relativo más rápido de las emisiones. (Figura 16.2)



Fuente: Informe sobre la Brecha de Emisiones 2025, PNUMA

Figura 16.2: Contribuciones al aumento de las emisiones de GEI en 2024 con respecto a los niveles de 2023 de los seis mayores emisores, el resto de los miembros del G20, el resto del mundo, el transporte internacional y el sector LULUCF

La situación de las emisiones en España la presenta el Inventario de Emisiones de Gases de Efecto Invernadero (GEI) correspondientes a la serie 1990-2024, publicada en enero de 2026. Dicho Inventario estima unas emisiones brutas de 267,71 millones de toneladas de CO₂ equivalente para el año 2024, lo que supone una disminución de emisiones de CO₂-eq, en 2024 del -0,8%, respecto al año anterior. El nivel de emisiones brutas se sitúa en un -5,9% respecto a 1990 y un -39,1% respecto a 2005. (Figura 16.3)



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

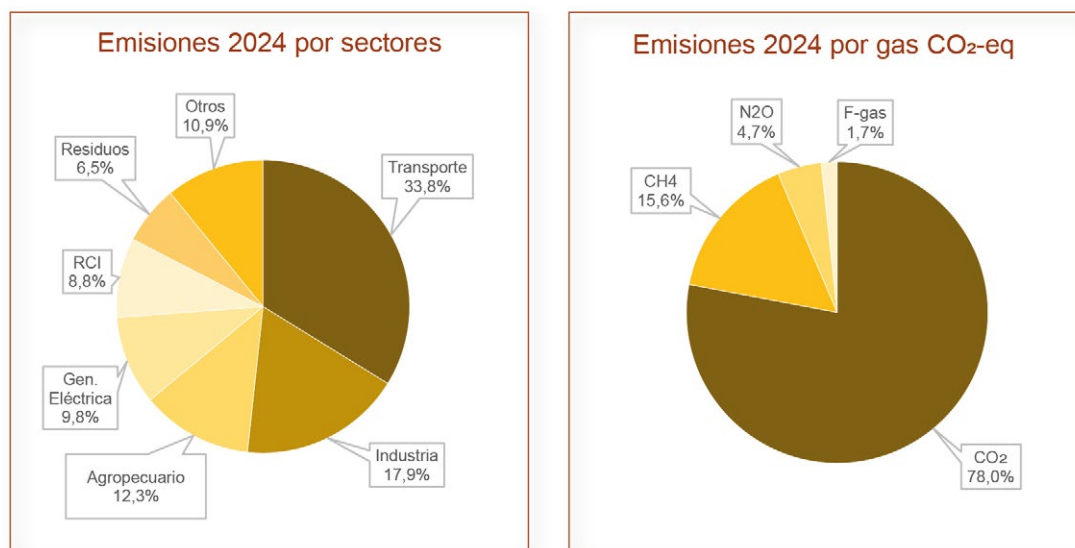
Figura 16.3: Histórico de las emisiones brutas de Gases de Efecto Invernadero

Las emisiones de CO₂-equivalente han registrado un descenso global del 0,8% en 2024 respecto a 2023. Esta reducción está determinada por la caída del 14,6% en las emisiones procedentes de la generación de energía eléctrica. Este descenso se debe a la senda de la transición energética, en la que ha disminuido el uso de fuentes fósiles y se ha incrementado el uso de fuentes renovables: en 2024, el 56,8% de la generación eléctrica nacional provino de estas últimas. La producción no renovable en el sistema eléctrico español se redujo un 11,9% en 2024, mientras que la generación renovable aumentó un 10,3%, registrando el máximo histórico de producción. Este incremento se debió principalmente al aumento de la producción hidráulica (35,6%) y de la solar fotovoltaica (19,1%). La generación eólica sigue siendo la mayoritaria en el mix nacional.

Así pues, este Inventario estima un descenso en las emisiones de GEI de 2,26 millones de toneladas CO₂-eq, en 2024 con respecto a 2023, que son debidas a:

- Las emisiones de gases de efecto invernadero procedentes de la generación eléctrica han disminuido -14,6% respecto a 2023.
- Las emisiones de GEI de los combustibles en el sector de la Energía (que incluye generación eléctrica, transportes y combustión en industrias, entre otros) registra una disminución de emisiones de GEI de -1,7% respecto al año anterior.
- Las emisiones de los procesos industriales y uso de productos han aumentado un 5,1% respecto al año anterior.
- El sector Agropecuario muestra un ligero aumento interanual de las emisiones de GEI de 0,6%, y el sector de Residuos muestra un leve descenso de emisiones de GEI del 0,2% respecto al año anterior.
- El sector de Usos de la Tierra, Cambios de Uso de la Tierra y Selvicultura (LULUCF) es el único con efecto sumidero de CO₂. Las absorciones de LULUCF se han estimado para 2024 en -51,9 millones de toneladas de CO₂-eq (lo que equivale a un 19,4% del total de emisiones brutas del Inventario en 2023), con un ligero descenso del -1,2% respecto al año anterior. Las emisiones netas (descontando el sector LULUCF) en el año 2024 se estiman en 215,79 millones de toneladas de CO₂-eq (lo que supone una disminución del -0,75% respecto a 2023).

El subsector de actividad con más peso en el total de emisiones brutas de GEI continúa siendo el transporte (33,8% del total), seguido de la industria (17,9%, incluyendo tanto las procedentes del consumo de combustibles como las de los propios procesos industriales), el sector agropecuario en su conjunto (12,4%), la generación de electricidad (9,8% del total), el consumo de combustibles en los sectores Residencial, Comercial e Institucional (8,8%), y la gestión de residuos (6,5% del total de emisiones brutas). (Figura 16.4)



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 16.4: Reparto de las emisiones brutas de GEI, por sectores y gases

Las altas cifras de emisiones brutas de GEI hacen cada vez más necesario implementar políticas de movilidad y logística basadas en la transferencia de los modos de transporte dependientes del petróleo hacia los modos eficientes energéticamente y descarbonizados, como establece el Plan Nacional Integrado de Energía y Clima.

Por parte de ENAIRE, durante 2025 se ha continuado la mejora de la eficiencia de las rutas aéreas de cara a reducir el impacto sobre el cambio climático del transporte aéreo y en potenciar la transición hacia una energía sostenible, como proporcionar vuelos directos al 70% de los vuelos (durante la primera parte del año) que operaron en el espacio aéreo nacional o la realización de descensos continuos (CDO) conocidos como aproximación “verde” en un 38% de los vuelos (hasta octubre), contribuyendo así al ahorro de combustible de las aeronaves y a la reducción de las emisiones a la atmósfera procedentes del tráfico aéreo. Además, la eficiencia de las rutas aéreas, en 2025 (enero-octubre) es superior a 96,7%, lo que supone unos ahorros, con respecto a 2024 de 702.000 km y más de 13.000 T de CO₂, logrados incluso con un incremento de tráfico del 4,75% por encima de 2024.

La actividad de Renfe contribuye a frenar el incremento de GEI, gracias a que el 81,1% de la energía primaria que consume es energía eléctrica con garantía de origen renovable certificada CERO CO₂ por AENOR. El Plan Nacional Integrado de Energía y Clima (PNIEC) 2021-2030 ya contempla una importante

transferencia desde los modos dependientes del petróleo hacia el ferrocarril, con el objetivo de multiplicar en 2,5 veces la demanda en 2030 respecto a la existente en 2015. Esta transferencia modal, tanto en viajeros como en mercancías, es clave para que las emisiones GEI del sector transporte se reduzcan significativamente, motivo por el que el fomento de las soluciones de movilidad y logísticas basadas en el transporte ferroviario son el núcleo de las políticas públicas de Transporte Sostenible.

Durante 2025 por parte de la Guardia Civil, a través del Servicio de Protección de la Naturaleza (SEPRONA), se han llevado a cabo investigaciones sobre gestión ilegal de vehículos al final de su vida útil (residuos) en Centros Autorizados de Tratamiento de Vehículos (CATV). En concreto, la problemática consiste en que los desguaces no retiran el gas refrigerante (potente gas de efecto invernadero) de los vehículos durante su descontaminación, operación de tratamiento de residuos a la que están obligados para evitar su emisión incontrolada. La finalidad de tal práctica ilegal reside en ahorros económicos para las empresas explotadoras de los desguaces. En consecuencia, grandes cantidades de estos gases de efecto invernadero, con alto potencial de calentamiento atmosférico, son emitidos a la atmósfera.

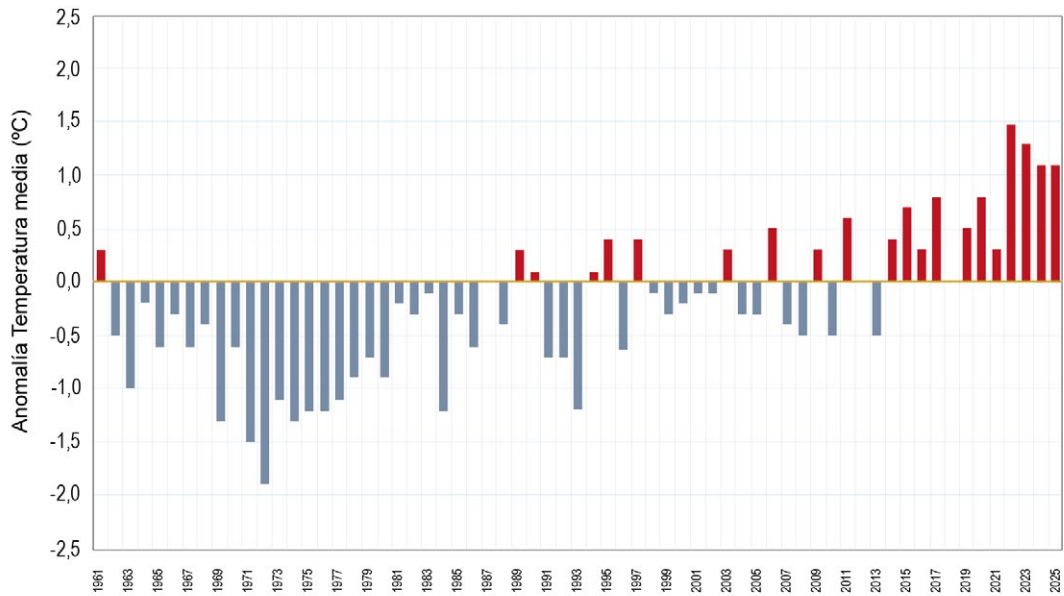
A tal respecto, merece también citar el tráfico ilegal de gases refrigerantes, muchos de ellos prohibidos o altamente regulados por su contribución al calentamiento global supone un desafío importante para el cumplimiento de acuerdos internacionales. Se trata de un fenómeno delictivo en incremento, no solo en España, sino en toda la Unión Europea. El sistema de reducción gradual a través de las cuotas de importación/fabricación (*Reglamento (UE) 2024/573*) es cada vez más restrictivo (las cuotas otorgadas por la Comisión Europea son cada vez menores), ya que se pretende prohibir la comercialización de estas sustancias en 2050. Por ello, se está observando, y se prevé, que el tráfico ilícito de gases refrigerantes aumente considerablemente hasta entonces (sigue existiendo demanda y, en consecuencia, mercado negro). El tráfico fraudulento de estos productos elude los controles aduaneros, fomenta mercados paralelos y rompe la trazabilidad, lo que debilita las políticas ambientales del país. Además, genera beneficios económicos que pueden alimentar estructuras criminales organizadas, lo que transforma un delito ambiental en una amenaza para la seguridad nacional.

Estas acciones pueden desestabilizar sectores estratégicos de la economía verde, afectando a empresas que cumplen con la legislación y desincentivando la inversión tecnológica y ambiental. Por ello, su combate requiere un enfoque integral que combine cooperación internacional, inteligencia económica, fortalecimiento de las agencias de control y un marco penal capaz de tratar estos delitos no solo como infracciones administrativas, sino como amenazas reales para la seguridad y el desarrollo sostenible del país.

Calentamiento global

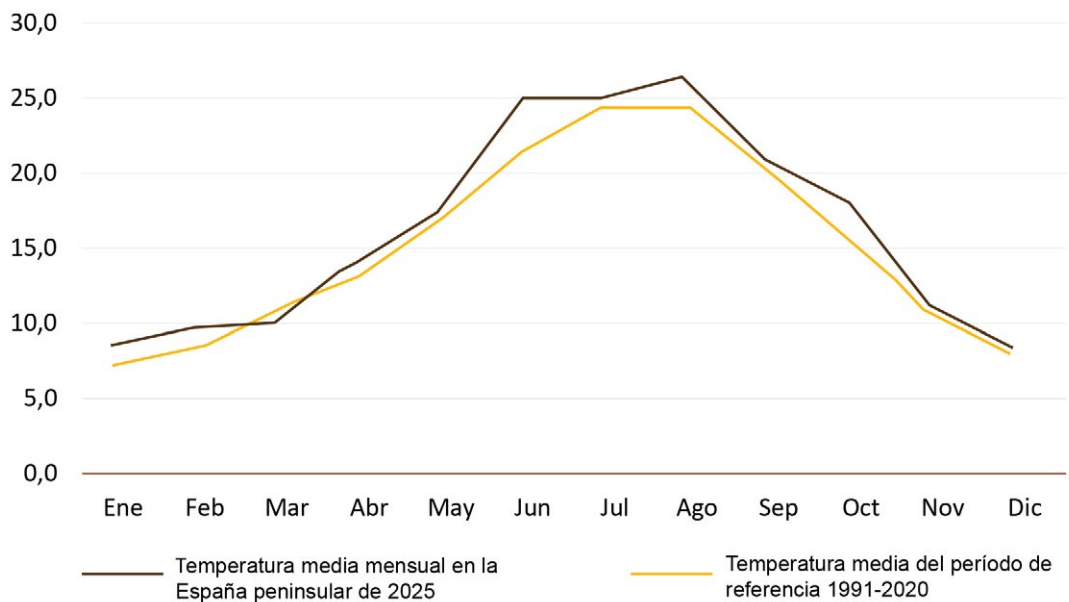
De acuerdo con datos oficiales de AEMET, el año 2025 ha tenido carácter extremadamente cálido, con una temperatura media en la España peninsular de 15,0°C, esto es +1,1°C por encima del valor medio en el periodo de referencia 1991-2020. Ha sido el tercer año más cálido desde el comienzo de la serie en 1961, empatado con el año 2024, y por detrás del 2022 y del 2023. Los once años más cálidos de la serie corresponden todos al siglo XXI. En Baleares, la temperatura media ha sido de 18,2°C, con un valor de anomalía de +1,1°C y un carácter extremadamente cálido, que convierte a 2025 en el segundo año más cálido de la serie en este archipiélago, detrás de 2022. Finalmente, en Canarias, la temperatura media ha sido de 18,8°C, con un valor de anomalía de +0,4°C y carácter muy cálido.

La temperatura promedio del agua del mar de las zonas circundantes a España alcanzó los 20°C, convirtiéndose en el segundo año con las aguas más cálidas. Tan solo 2023, 2024 y 2025 han alcanzado o superado esa temperatura media anual, en una serie histórica que empieza en 1940. Además, se batieron récords de temperatura diaria en zonas del Mediterráneo y de Canarias. (*Figuras 16.5 a 16.7*)



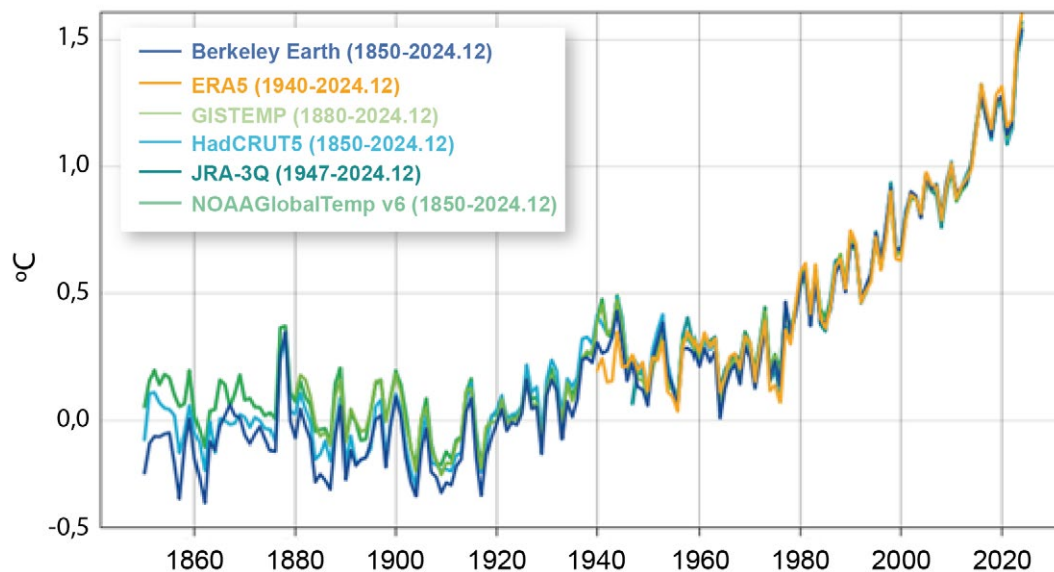
Fuente: Agencia Estatal de Meteorología

Figura 16.5: Anomalías de temperatura de 2025 en la España peninsular desde 1961 con respecto al periodo de referencia 1991-2020



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 16.6: Temperatura media mensual en la España peninsular de 2025 y temperatura media del periodo de referencia 1991-2020



Fuente: Datos procedentes de los seis conjuntos de datos indicados en la leyenda, gráfica extraída de WMO (2025). State of the Global Climate 2024

Figura 16.7: Anomalías de la temperatura media anual a escala mundial respecto al valor de referencia de la era preindustrial (1850-1900) desde 1850 hasta 2024

Por su parte, el CIEMAT investiga en la eficacia de medidas de mitigación a través de su colaboración con MITECO en el II Programa Nacional de Control de la Contaminación Atmosférica y en medidas de adaptación en zonas urbanas y periurbanas así como en la búsqueda de especies agrícolas resilientes al cambio climático.

En las ciudades, el futuro crecimiento urbano supondrá un incremento aún mayor de las temperaturas, lo que significa que el número de personas que tendrán que hacer frente a los riesgos por el sobrecalentamiento urbano sea mayor. Madrid es la ciudad de estudio del proyecto MULTIURBAN, cuyo principal objetivo es comprender cuáles son los mecanismos responsables del impacto de la estructura urbana sobre las circulaciones regionales y el microclima urbano de Madrid, desde un punto de vista multiescalar y en un contexto del cambio climático.

Desertificación

Según la Evaluación de Riesgos e Impactos derivados del Cambio Climático en España (ERICC 2025), la desertificación constituye uno de los riesgos clave para el país. Actualmente, el 74% del territorio nacional presenta vulnerabilidad a este proceso, una vulnerabilidad que se ve intensificada por la aridificación progresiva del clima y el aumento de la torrencialidad en amplias zonas del país. En particular, el riesgo se relaciona con el agravamiento de las condiciones de aridez derivado del incremento de las temperaturas, la mayor frecuencia e intensidad de las sequías, el aumento de episodios de lluvias torrenciales y el crecimiento del riesgo de incendios forestales. En conjunto, estos procesos pueden alterar la composición y estructura de las masas forestales, reducir su productividad y comprometer su persistencia a largo plazo.

El calentamiento global, acompañado de ligeras reducciones en las precipitaciones, aunque no son estadísticamente significativas, es el principal motor de la evolución de los climas en España. Este incremento térmico ha intensificado la aridez y disminuido la disponibilidad hídrica, con implicaciones críticas para la vegetación, el agua disponible para todos sus usos, y la biodiversidad en España.

De acuerdo con estudios publicados por el CSIC en la España peninsular y las Islas Baleares, se ha experimentado una transición hacia categorías más áridas en un 12% de sus territorios entre 1961-1990 y 1991-2020, mientras que casi ninguna zona ha experimentado una transición hacia categorías más húmedas.

En las Islas Canarias, la transición hacia clases más áridas afectó a un 16% de su territorio.

Así, para hacer frente a esta problemática, en 2025 se ha aprobado la Orden TED/776/2025, de 8 de julio, por la que se actualiza la Estrategia Nacional de Lucha Contra la Desertificación y se aprueba su Plan de Implementación para el periodo comprendido entre 2025 y 2027. En el Plan de Implementación se detallan las acciones de la Estrategia que se pondrán en marcha en este periodo. Estas acciones se centran en la gobernanza y la coordinación; la cooperación y la investigación; el seguimiento y evaluación de la desertificación; la difusión de buenas prácticas de gestión sostenible de las tierras; la planificación y ejecución de acciones y proyectos; y la comunicación y sensibilización.

Por otra parte, para reforzar la gobernanza de la lucha contra la desertificación en España, se ha adoptado el Real Decreto 105/2025, de 18 de febrero, creándose un nuevo Comité de Lucha Contra la Desertificación, de coordinación entre las administraciones públicas para la aplicación coherente en el territorio nacional de las políticas de lucha contra la desertificación y la degradación de las tierras, así como del intercambio de buenas prácticas

A nivel internacional, España ha continuado impulsando, en 2025, la Alianza Internacional para la Resiliencia a la Sequía, iniciativa liderada por los gobiernos de España y Senegal y apoyada por la Secretaría de la Convención de las Naciones Unidas de Lucha contra la Desertificación (CNULD).

Igualmente, la conservación de los suelos y la prevención de la desertificación es uno de los objetivos del primer Programa de Trabajo (2021-2025) del Plan Nacional de Adaptación al Cambio Climático (PNACC).

Biodiversidad

La ciencia ha mostrado claramente que, a nivel mundial, la pérdida de biodiversidad y la degradación de los ecosistemas marinos y terrestres, la contaminación, el agotamiento de los recursos y el cambio climático se están acelerando a un ritmo sin precedentes; que el riesgo de aparición y propagación de enfermedades infecciosas aumenta a medida que se destruye la naturaleza; que más del 65% del área oceánica está experimentando un aumento de los impactos acumulativos y que los ecosistemas marinos y costeros están mostrando grandes pérdidas de extensión y condición así como un rápido declive; y que la naturaleza desempeña un papel fundamental en la provisión de bienes y servicios básicos para el bienestar y la salud de la humanidad.

Las especies marinas tienen cada vez mayor dificultad para adaptarse a los diversos impactos del cambio climático que son cada vez más abundantes. Por ejemplo, las especies de peces, muchos de ellos de importancia comercial, están cambiando su distribución en busca de nuevos hábitats óptimos a través de fronteras geopolíticas. Sin embargo, en mares semicerrados como el Mar Mediterráneo, donde las especies no tienen opciones de grandes desplazamientos latitudinales, otras respuestas

como contracción, expansión, atomización de las poblaciones o desplazamientos batimétricos se han observado en varias especies.

Así, es destacable el sexto informe de evaluación del Grupo Intergubernamental de Expertos sobre Cambio Climático (IPCC, por sus siglas en inglés) que aporta una mayor comprensión en relación con la manifestación del cambio climático, sobre todo en sus extremos, y cómo éstos están afectados a los sistemas naturales.

Además, el nitrógeno reactivo (N) es un elemento esencial para la vida que forma parte de un complejo ciclo biogeoquímico que conecta la atmósfera, la vegetación, el suelo y los sistemas acuáticos. Las concentraciones de N en la atmósfera se han incrementado en el último siglo debido a las actividades humanas asociadas a la quema de combustibles fósiles y la intensificación de la agricultura y la ganadería. Una vez emitidos a la atmósfera, estos compuestos pueden ser transportados a grandes distancias y depositarse en lugares remotos alejados de fuentes de contaminación. Este depósito de compuestos nitrogenados puede suponer una amenaza para la conservación de los ecosistemas, debido a que puede alterar el ciclo natural del nitrógeno ocasionando procesos de acidificación, eutrofización, daños directos a la vegetación, formación de ozono troposférico y partículas, y pérdida de biodiversidad.

El CIEMAT ha investigado cómo las entradas de N en un bosque mediterráneo, tanto por vía húmeda como seca, interactúan con el dosel forestal, los microorganismos y el suelo, y cómo estas interacciones influyen en el funcionamiento del ecosistema. Para ello se han monitorizado tres encinares en España, ecosistemas representativos de la cuenca mediterránea, expuestos a diferentes condiciones climáticas y niveles de concentración y depósito de compuestos nitrogenados. Los resultados han permitido demostrar que el dosel forestal actúa como un filtro activo para el depósito atmosférico de N, pudiendo funcionar el bosque como fuente o sumidero de N, dependiendo de factores estacionales y atmosféricos, y participando activamente en el ciclo del nitrógeno. Comprender esta dinámica es esencial para predecir las respuestas de los ecosistemas al aumento del depósito de N atmosférico y poder desarrollar metodologías que permitan realizar análisis de riesgo de efectos de los contaminantes atmosféricos para proteger los ecosistemas vulnerables.

Esta investigación se ha realizado en el marco de los proyectos EDEN (Efectos del depósito de nitrógeno atmosférico en los ecosistemas mediterráneos) y REMEDAP (Respuesta de la vegetación mediterránea a los efectos de la contaminación atmosférica).

Asimismo, como resultado del Plan General de Actuaciones (PGA) firmado con la Secretaría de Estado de Medio Ambiente, y el Organismo Autónomo Parques Nacionales, el CIEMAT ha realizado el diseño de un programa de seguimiento de la calidad del aire y sus efectos en la red de parques nacionales.

Por otra parte, también es de interés mencionar el PGA con la Dirección General de Calidad y Evaluación Ambiental y el CIEMAT en materia de contaminación atmosférica y contaminantes orgánicos persistentes, y cómo del resultado de estos proyectos y acuerdos se obtienen los conocimientos científicos que sientan las bases para desarrollar herramientas de ayuda a la toma de decisiones para la mejora de la calidad del aire en entornos naturales.

Gestión forestal sostenible y reforestación y actuaciones frente al riesgo de incendios forestales

En las últimas décadas, los inventarios forestales reflejan una expansión sostenida de la superficie arbolada en España, lo que refuerza el papel de los bosques como sumideros de carbono, reguladores del ciclo hidrológico y barreras frente a la erosión.

No obstante, este avance convive con amenazas crecientes que comprometen su estabilidad. Por un lado, los incendios forestales se han vuelto más intensos y extensos, con más de 353.000 hectáreas quemadas hasta octubre de 2025 y episodios especialmente virulentos en Galicia y Castilla y León, debido al abandono rural, la acumulación de combustible, la limitada gestión forestal y olas de calor cada vez más frecuentes y prolongadas. Por el otro, el incremento térmico y la prolongación de los periodos secos están provocando un debilitamiento fisiológico y episodios de mortandad en el arbolado, como el decaimiento del pino resinero en Castilla y León, con impactos ecológicos, económicos y riesgos añadidos en cabeceras de cuenca, donde los bosques son clave para la regulación hídrica. A todo ello se suma la expansión de plagas y enfermedades favorecida por el cambio climático y el comercio internacional.

En conjunto, la combinación de incendios más destructivos, debilitamiento forestal y plagas emergentes subraya la urgencia de reforzar la gestión forestal sostenible, mejorar la prevención y fortalecer los sistemas de vigilancia y respuesta para proteger el patrimonio forestal nacional.

En este contexto, es conveniente plantear una gestión forestal sostenible adaptada a la realidad y condiciones geográficas y climáticas del país. En España, se mantiene la tendencia creciente de superficie forestal ordenada, en línea con una de las metas de la Estrategia Forestal Española horizonte 2050, de extender la superficie forestal sujeta a instrumentos de gestión forestal sostenible tarea especialmente importante en el caso de montes de titularidad privada, cuya superficie ordenada es sensiblemente inferior a la de los montes de titularidad pública.

La gestión forestal sostenible requiere, por definición, integrar criterios que aseguren la viabilidad ecológica y climática de los bosques a largo plazo. Esto implica planificar la reforestación con especies y modelos de restauración adecuados a las condiciones locales y futuras, promover estructuras forestales resilientes y garantizar la conservación del suelo y de los recursos hídricos. Asimismo, una gestión sostenible debe incluir actuaciones específicas en zonas estratégicas para la prevención del riesgo de incendios forestales.

Gestión del agua

Las proyecciones para España muestran un aumento de las temperaturas y una reducción de las precipitaciones anuales acumuladas, con una importante variabilidad en el patrón de distribución de las precipitaciones. Esto se traduce en una menor disponibilidad de recursos hídricos para diferentes usos, así como para el sostenimiento de los ecosistemas acuáticos.

La gestión del agua en España se desarrolla bajo los principios establecidos por la Directiva Marco del Agua de la Unión Europea, otras Directivas relacionadas con el agua y su transposición a la normativa estatal. Las Orientaciones Estratégicas sobre agua y cambio climático, aprobadas en julio de 2022, marcan estos principios orientadores y las herramientas para llevarlos a cabo. Estos principios se basan, entre otras cuestiones, en la seguridad hídrica para las personas, la biodiversidad y las actividades socioeconómicas. Como principales herramientas de desarrollo pueden mencionarse: los

Planes Hidrológicos de cuenca, los Planes de Gestión del Riesgo de Inundación, los Planes Especiales de Sequía, la Estrategia Nacional de Restauración de Ríos, el Plan de Acción de Aguas Subterráneas, la gestión de seguridad de presas y embalses, el PERTE de digitalización del ciclo del agua o las modificaciones normativas. Estas herramientas que se han ido desarrollando, afrontan, cada una en su ámbito, la adaptación del sector del agua a los efectos del cambio climático, el riesgo de degradación del medio natural, o el mantenimiento y seguridad del importantísimo patrimonio hidráulico español.

La gestión del riesgo de sequía y escasez parte del análisis general de riesgos realizado en los planes hidrológicos de cuenca, que establecen una asignación de recursos a los diferentes usos compatible con los objetivos ambientales y con los criterios de garantía para los diferentes usos. La herramienta fundamental de la gestión de episodios coyunturales de sequía y escasez son los Planes Especiales de Sequía. Permiten gestionar estas secuencias secas, estableciendo actuaciones graduales a medida que se avanza en la situación de sequía, mitigando su impacto y retrasando o evitando llegar a las fases más severas de la escasez. Gracias a estos Planes Especiales de Sequía, el abastecimiento urbano ha podido ser prácticamente garantizado, salvo casos aislados de pequeñas poblaciones no conectadas a las grandes redes que pueden requerir actuaciones o medidas más puntuales.

Además, AEMET mantiene el sistema de monitorización de sequías meteorológicas, diseñado para el seguimiento, alerta temprana y evaluación de la sequía meteorológica, para lo que utiliza en tiempo real la información climática disponible que muestra el desarrollo de las condiciones de sequía meteorológica.

Por otra parte, la producción de agua desalada en cuencas deficitarias del mediterráneo español (Júcar, Segura y Mediterránea Andaluza), continúa siendo un elemento fundamental para proporcionar garantía de suministro de agua de calidad tanto para el abastecimiento como, en la medida de lo posible, el regadío, mitigando el impacto del cambio climático en cuanto a la escasez del recurso y reduciendo la sobreexplotación de las acuíferos al sustituir el consumo de agua subterránea por agua procedente de la desalación.

España está desarrollando un ambicioso plan de inversiones a favor de los regadíos sostenibles con fondos propios y europeos (principalmente, del Mecanismo de Recuperación y Resiliencia del PRTR) y la colaboración público-privada de las Comunidades de Regantes Españolas. Este plan busca promover un uso eficiente del agua y la energía en los regadíos españoles, apostando por la innovación y la digitalización de estos sistemas de producción. El volumen total de inversión previsto con este plan de inversiones es superior a los 2.500 millones de euros y se extiende hasta el año 2027. Con esta alta inversión de más de 2.500 M€ durante el período 2021-2027 se pretende:

- La modernización y mejora de la eficiencia hídrica y energética en 500.000 has.
- Beneficiar a más de 20.000 regantes.
- Garantizar un ahorro de agua para el regadío del 10 % respecto a la situación de partida
- Un uso más eficaz de la energía, gracias al uso de energías renovables o mediante el uso de la gravedad con balsas.

Además, y debido a los hechos acontecidos entre el 28 de octubre y 4 de noviembre de 2024 en España, sufriendo la peor Depresión Aislada en Niveles Altos (DANA) en lo que va de siglo en diversas comunidades autónomas, con consecuencias especialmente graves y trágicas en determinados municipios y zonas de la provincia de Valencia, el Gobierno de España dispuso, a través del Real Decreto-ley 7/2024, de 11 de noviembre, por el que se adoptan medidas urgentes para el impulso del Plan de respuesta inmediata, reconstrucción y relanzamiento frente a los daños causados por la DANA en diferentes municipios entre el 28 de octubre y el 4 de noviembre de 2024, una serie de medidas en diferentes ámbitos, con el fin de subvertir y mitigar los severos impactos que esta catástrofe natural

ha tenido en el ámbito socioeconómico y que tiene por objeto la adopción de medidas urgentes para el impulso del Plan de Respuesta Inmediata, Reconstrucción y Relanzamiento frente los daños causados por la DANA en diferentes municipios. Estas actuaciones se han centrado fundamentalmente en la recuperación de los caminos agrarios afectados, las infraestructuras de riego de las Comunidades de Regantes Afectadas y las infraestructuras deterioradas o perdidas en las explotaciones agrarias. Actualmente se lleva ejecutado una inversión de 140 M€ del total previsto de 193 M€ invertidos a la finalización del PRTR en junio de 2026.

Asimismo, en 2025 se aprobaron las órdenes TED/225/2025 y TED/934/2025 en relación con la seguridad de presas y embalses. Junto a ello, es conveniente reseñar las acciones realizadas en esta materia, entre las que destacan:

- los trabajos en la presa de Buseo en Chera (Valencia), para recuperar su seguridad tras el desbordamiento durante las avenidas de la DANA en Valencia en 2024; y, en la presa del río Agrio en Aznalcollar (Sevilla), que soportó importantes avenidas en marzo de 2025, cuando registró un caudal punta 702,6 m³/s.
- la gestión de un importante episodio de avenidas, a raíz de la borrasca Martinho, en marzo de 2025, por dieciocho presas de la Confederación del Tajo y las del Canal de Isabel II. Asimismo, destacaron los alivios de las presas de Cedillo, Alcántara y el Alcorlo. Hubo afectaciones en las Comunidades de Madrid, Castilla la Mancha y Castilla León.
- La gestión, en octubre de 2025, durante la DANA Alice que afectó a Murcia y sur de la Comunidad Valenciana, aunque las presas absorbieron bien sus efectos, hubo importantes daños en los canales de la Mancomunidad del Taibilla y de la Confederación del Segura, que supusieron la interrupción durante 4 días del abastecimiento a 100.000 habitantes de la comarca del Mar Menor.

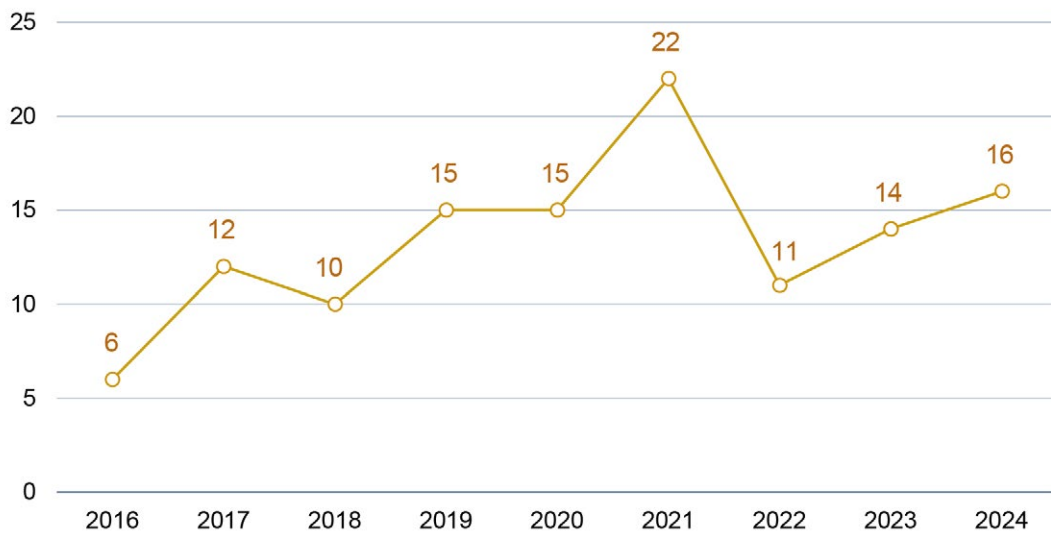
Asimismo, se han establecido las siguientes ayudas económicas frente a situaciones de emergencia:

- Se ha continuado con la aplicación de las ayudas promovidas por el Ministerio para la Transición Ecológica y el Reto Demográfico (MITECO), para la adaptación al riesgo de inundación (Real Decreto 1158/2020, Real Decreto 731/2022 y Real Decreto 786/2022).
- Se ha iniciado la tramitación de un real decreto por el que se establece una subvención directa a los municipios afectados por la DANA para la adaptación al riesgo de inundación y de un real decreto por el que se adoptan medidas de gestión de los riesgos de inundación.

Mientras, en materia de inundaciones, se han llevado a cabo numerosas actuaciones orientadas a la reducción del riesgo y a la mejora del estado de las masas de agua y los ecosistemas fluviales, que contribuyen a la reducción de la vulnerabilidad frente a los impactos del cambio climático. Especialmente, para la gestión del riesgo de inundación se han realizado importantes acciones, tales como:

- La continuación con la implantación de las medidas contempladas en los Planes de Gestión del Riesgo de Inundación (PGRI) de 2º ciclo;
- La consulta pública de los mapas de peligrosidad y riesgo de las Áreas de Riesgo Potencial Significativo de Inundación (ARPSI) de tercer ciclo.
- El desarrollo la primera versión beta del Observatorio de la Gestión del Agua que permite, entre otras cosas, la integración en una única plataforma de toda la información disponible en los SAIH y AEMET relevante para la gestión del riesgo de inundación. Esto permitirá también facilitar la comunicación con la RAN.

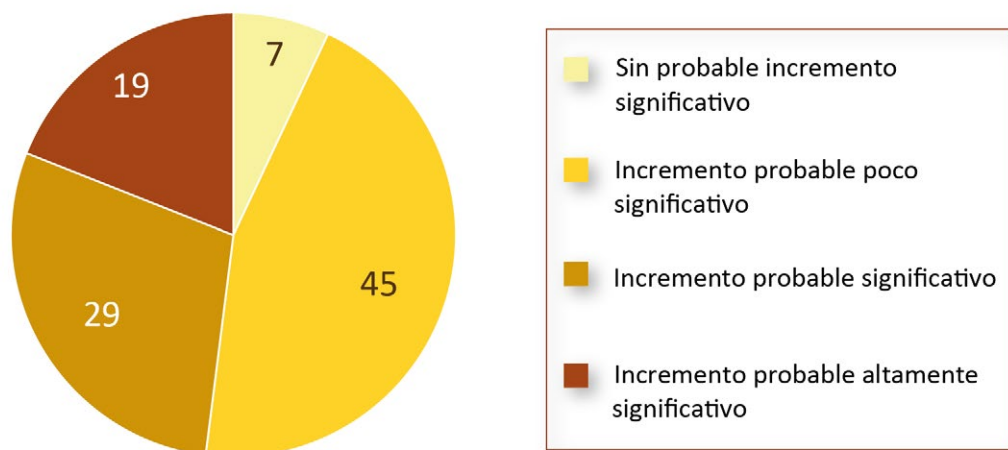
(Figura 16.8 y 16.9)



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 16.8: Episodios calificados como “graves inundaciones” en las cuencas de gestión estatal

ARPSI en riesgo (% ARPSI intercomunitarias)
Escenario de cambio climático RCP 8.5 T 500 años



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 16.9: Porcentaje de ARPSI en las que es esperable un cambio en el nivel de riesgo para el escenario de emisión RCP 8.5 y el periodo de retorno de 500 años

Finalmente, para la revisión y actualización de la evaluación preliminar del riesgo de inundación que se ha aprobado en 2025 en casi todas las demarcaciones, se han realizado nuevos estudios que continúan con la línea iniciada en los Planes de gestión del riesgo de inundación (PGRI) para la estimación de frecuencias y magnitudes de las avenidas y en el análisis de los efectos del cambio climático a partir de episodios climáticos singulares del pasado. En estos trabajos se ha efectuado también un análisis de las tasas de cambio en cuantil de caudal en función de los escenarios de cambio climático y su potencial efecto en las Áreas de Riesgo Potencial Significativo de Inundaciones (ARPSI).

En relación con la situación de las costas, el cambio climático, lleva aparejada la subida del nivel del mar y el aumento de efectos climáticos extremos, así como la acidificación. A nivel global, según el sexto informe IPCC, el nivel del mar en el Mediterráneo ha aumentado 1,4 mm anuales durante el siglo XX, y más recientemente $2,4 \pm 0,5$ mm anuales entre 1993 y 2012 y es probable que siga subiendo en el futuro, lo que requerirá inversiones importantes. En España, el ascenso del nivel del mar ha sido especialmente notable desde el año 1993 en el área del Estrecho, en el archipiélago canario y la costa atlántica.

Con el objetivo general de proporcionar un enfoque coherente en la protección del litoral, se ha presentado el Plan Estratégico Nacional para la Protección de la Costa considerando los efectos del cambio climático, financiado con cargo al Programa de Apoyo a las Reformas Estructurales de la Comisión Europea.

Finalmente, es necesario mencionar también que, desde el punto de vista ambiental, las construcciones ilegales multiplican la presión sobre recursos y servicios que no estaban preparados para soportar esa carga. Suelen carecer de sistemas adecuados de saneamiento y gestión de residuos, lo que deriva en vertidos directos a ríos, acuíferos o suelos. Estas edificaciones suelen levantarse al margen de la legalidad urbanística y, en muchos casos, en zonas vulnerables o de alto valor ecológico. Como resultado, se ocupan áreas protegidas, cauces fluviales, laderas inestables o espacios costeros, lo que provoca la degradación de hábitats, la pérdida de biodiversidad y un mayor riesgo ante fenómenos naturales como inundaciones, deslizamientos o erosión acelerada.

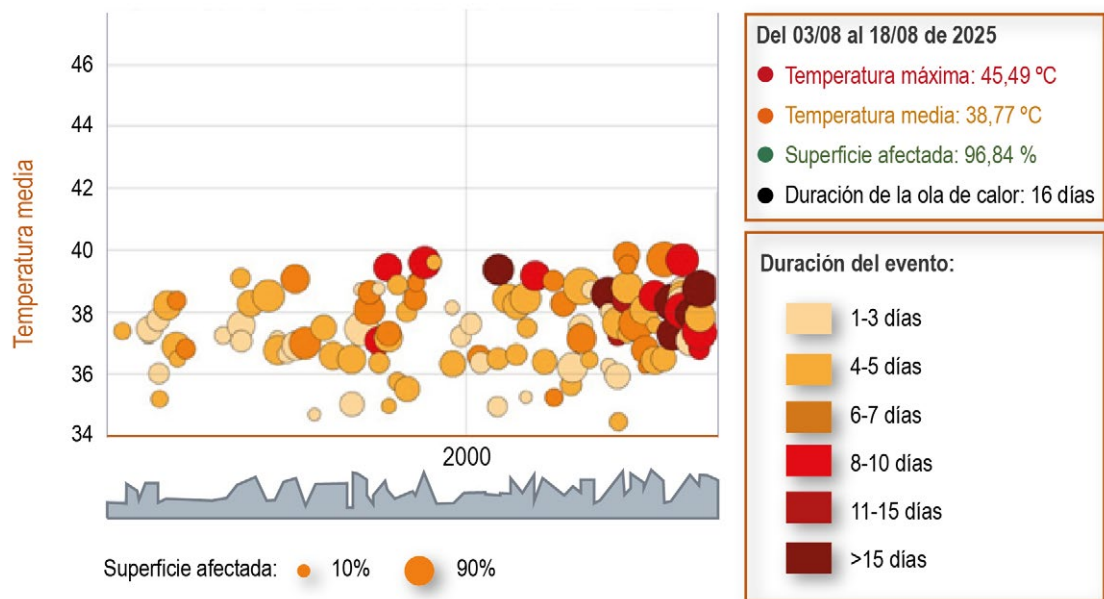
Fenómenos meteorológicos adversos

En cuanto a los fenómenos meteorológicos adversos, en 2025 se pueden destacar los siguientes episodios:

- Las borrascas Garoe, Herminia e Ivo, que afectaron a amplias zonas del oeste y norte peninsular. En particular, la borrasca Herminia, ocurrida entre los días 26 y 28 de enero, generó un intenso temporal de viento, lluvia, oleaje y nieve que afectó a gran parte de la Península, especialmente a Galicia y Castilla y León. Las rachas superaron los 160 km/h en zonas de montaña y las lluvias dejaron más de 150 mm en puntos de Ourense. El fuerte viento causó numerosos daños materiales e interrupciones en el transporte.
- Las borrascas Jana, Konrad, Laurence y Martinho, registradas entre el 6 y el 20 de marzo, que afectaron especialmente al noroeste y centro peninsular. De ellas, Laurence fue la más significativa, con un temporal de lluvia, viento y tormentas que afectó a amplias zonas del sur y suroeste peninsular, especialmente a Andalucía, donde se produjeron inundaciones, evacuaciones y rescates. Se registraron acumulaciones de precipitación de más de 100 mm en 24 horas en puntos de Sevilla y rachas de viento superiores a 100 km/h en puntos de Sierra Nevada y del Sistema Central. El temporal causó tres fallecidos en accidentes de tráfico y la formación de un tornado en la provincia de Huelva.

- Las borrascas Nuria y Oliver de 3 y 4 de abril, de las cuales Nuria fue la más y afectó tanto a Canarias como al suroeste peninsular, dejando rachas huracanadas en las islas occidentales y lluvias localmente intensas en Andalucía y Extremadura. Se observaron pequeños tornados en Huelva y Sevilla, acompañados de inundaciones y daños estructurales. En Coria del Río (Sevilla) el derrumbe de una nave agrícola a causa del viento y la lluvia provocó el fallecimiento de tres trabajadores.
- Dos olas de calor en la España peninsular y Baleares. La primera, entre el 18 de junio y el 4 de julio, fue la tercera ola de calor más larga y extensa de la serie (al menos desde 1975), además de muy temprana. Afectó a 40 provincias y tuvo una anomalía de 2,8°C, con temperaturas que alcanzaron los 40°C en muchas regiones y que superaron los 43°C en zonas del sur peninsular. La segunda ola de calor, entre el 3 y 18 de agosto, fue la segunda ola de calor más intensa y extensa de la serie, y la cuarta más larga. Afectó a 42 provincias y presentó una anomalía de 4,2°C, registrándose las temperaturas más altas del verano, con valores que superaron los 45°C en puntos del sur peninsular. La temperatura más alta correspondió a Jerez de la Frontera/aeropuerto (Cádiz), con 45,8°C el 17 de agosto, que constituye el registro más alto en esta estación desde el comienzo de su serie. En total, con 33 días, se trató del verano con mayor número de días de ola de calor en Península y Baleares, tras el verano de 2022, y fueron claves de cara a los graves incendios forestales de agosto.
- La dana Alice octubre fue el primer episodio de gran impacto de la temporada 2025-2026. Entre los días 8 y 14 de octubre provocó un extenso temporal de lluvias muy fuertes y persistentes en el este peninsular y Baleares. Se registraron acumulaciones superiores a 250 mm en 48 horas en puntos de Valencia, Alicante y Murcia, y máximos de 190 mm en Tortosa (Tarragona). Las precipitaciones torrenciales ocasionaron inundaciones urbanas y cortes de carreteras en la Comunidad Valenciana y la Región de Murcia, así como incidencias en aeropuertos y balsas de agua en Ibiza y Mallorca.
- La borrasca Claudia afectó entre los días 11 y 15 de noviembre a la Península y Canarias con precipitaciones persistentes y localmente muy intensas, rachas huracanadas que superaron los 180 km/h en zonas de montaña y fenómenos costeros adversos. Las lluvias dejaron acumulados superiores a 150 mm en puntos del centro y oeste peninsular y provocaron inundaciones, cortes de vías y numerosos daños, especialmente en Andalucía occidental y en el archipiélago canario.
- Las borrascas Davide y Emilia, en diciembre, dieron lugar a episodios de gran adversidad. En especial Emilia, que provocó lluvias torrenciales en el litoral mediterráneo, con acumulados superiores a 120 mm en el sureste, así como un intenso temporal en Canarias con nevadas excepcionales en el Teide y rachas cercanas a 160 km/h, lo que ocasionó caídas de árboles, cortes de carreteras y episodios de interrupciones del suministro eléctrico.

El seguimiento sistemático de las olas de calor ocurridas en España confirma el incremento en su frecuencia, intensidad, duración y extensión geográfica, así como su antelación, lo que hace que la estación cálida se prolongue. De acuerdo con los datos proporcionados por AEMET, en el periodo 1975-2021 se ha triplicado el número de días en que se superan los umbrales de temperatura de ola de calor en la España peninsular. Además, las olas de calor registradas en junio, cuando tienen más consecuencias sobre la salud, son ahora 10 veces más frecuentes que en los años 1980 y 1990 del siglo XX. (Figura 16.10)



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 16.10: Características de las olas de calor observadas en España

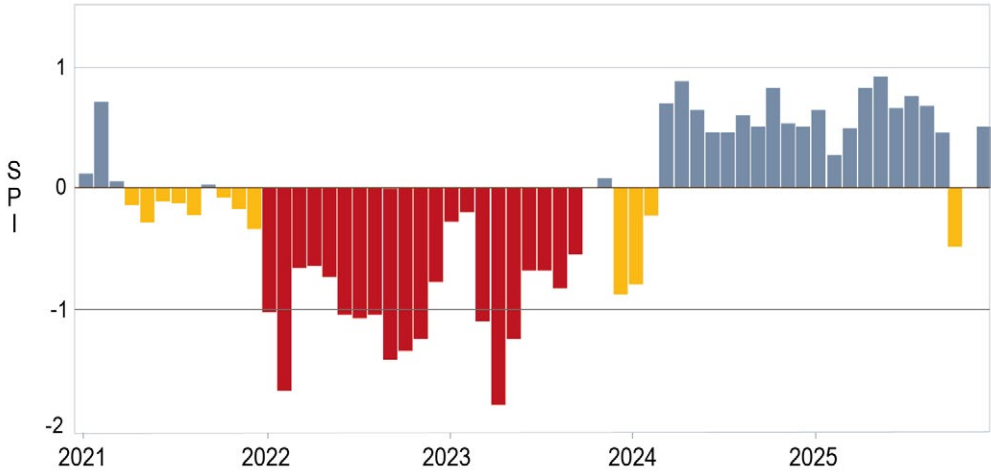
Las proyecciones climáticas en España indican que las temperaturas aumentarán 1,6 veces más rápido que la media mundial, posicionando a nuestro país como una de las regiones más vulnerables frente al cambio climático. Se prevé un incremento considerable en la frecuencia e intensidad de las olas de calor, con especial incidencia en el sur peninsular.

En cuanto a las precipitaciones acumuladas anuales se observan cambios en los patrones de distribución. Así, la intensidad de los eventos extremos de precipitación ha aumentado, especialmente en el este peninsular, donde se observa en la región mediterránea un aumento de los eventos de precipitación torrencial extrema, con más de 200 mm en un día, tanto en magnitud como en frecuencia.

A nivel del conjunto de la España peninsular, el índice de precipitación estandarizado (SPI) acumulado de 1 año se ha encontrado en valores positivos desde principios de 2024, sin sequía meteorológica en esta acumulación temporal. Sin embargo, en el mes de octubre de 2025 pasó a un valor negativo, aunque sin llegar al valor de -1 a partir del que se considera sequía meteorológica. Este índice se recuperó en los últimos dos meses del año, pasando de nuevo a ser positivo. En cuanto a cuencas hidrológicas, el SPI acumulado de 1 año es positivo en todas las cuencas salvo en las del Ebro y del Norte y Noroeste. (Figura 16.11)

En cuanto al SPI a 3 años, indica que la sequía meteorológica para este rango temporal que se venía arrastrando para el conjunto de la España peninsular desde principios de 2023 se ha dado por finalizada en marzo de 2025 y el índice continúa en valores positivos en estos momentos. (Figura 16.12)

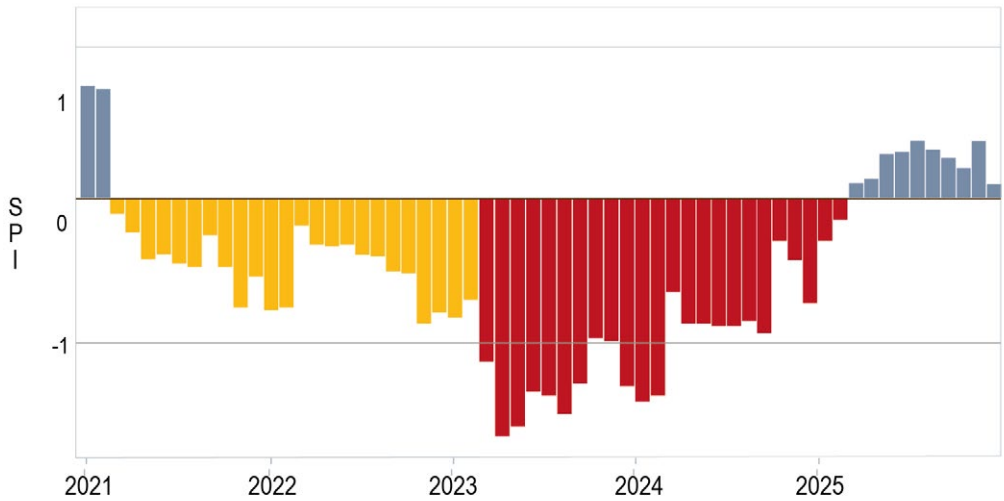
SPI 12 meses. ESPAÑA PENINSULAR



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 16.11: Evolución temporal del índice de precipitación estandarizado (SPI) acumulado de 1 año para la España peninsular

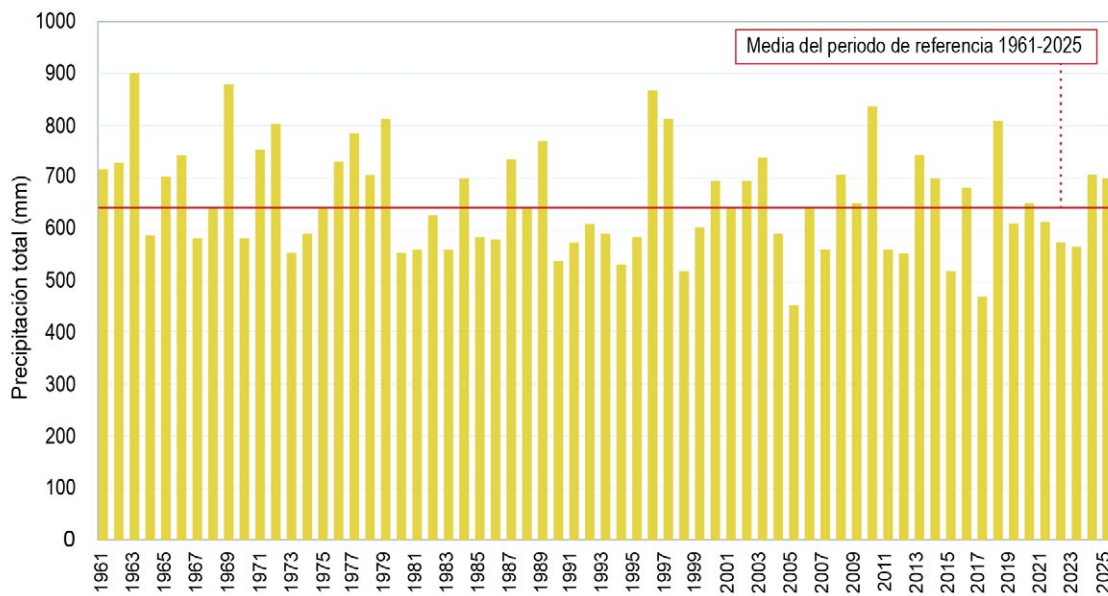
SPI 36 meses. ESPAÑA PENINSULAR



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 16.12: Evolución temporal del índice de precipitación estandarizado (SPI) acumulado de 3 años para la España peninsular

El año 2025 ha sido en su conjunto húmedo en cuanto a precipitaciones, con un valor de precipitación media sobre España peninsular de 696,1 mm, valor que representa el 109% del valor normal en el periodo de referencia 1991-2020. Se ha tratado del vigésimo quinto año más húmedo desde el comienzo de la serie en 1961, y el octavo del siglo XXI. En Baleares, el valor de precipitación ha sido de 559,9 mm, que supone un 97% del valor medio del periodo de referencia y una caracterización de normal. Finalmente, en Canarias, la precipitación ha sido de 282,2 mm, un 106% del valor promedio y una caracterización de húmedo. (Figura 16.13)



Fuente: Ministerio para la Transición Ecológica y el Reto Demográfico

Figura 16.13: Serie de precipitación media en España peninsular desde 1961

Al mismo tiempo, el siglo XXI ha experimentado la mayor frecuencia de sequías graves de los últimos 150 años. A pesar de que las precipitaciones totales se han situado en torno a los valores promedio, las altas temperaturas han aumentado la evaporación, agravando las condiciones de sequía. En el futuro, se prevén sequías más frecuentes y severas, especialmente bajo escenarios de altas emisiones (CEDEX, 2017).

Marco estratégico y normativo nacional de adaptación y mitigación del cambio climático

El Plan Nacional Integrado de Energía y Clima (PNIEC) 2023-2030 y el Plan Nacional de Adaptación al Cambio Climático (PNACC) 2021-2030 son las principales herramientas de planificación estratégica nacional que integran la política de energía y clima, y reflejan la contribución de España a la consecución de los objetivos establecidos en el seno de la Unión Europea en materia de energía y clima.

Por su parte, el PNACC constituye el marco estratégico fundamental de la Administración General del Estado para fortalecer la resiliencia y la capacidad de adaptación ante los impactos del cambio climático. Durante el periodo 2021-2025 se ha puesto en marcha el primer programa de trabajo de este Plan y se han desarrollado múltiples acciones y políticas que se traducen en una mejora sustancial de la transversalización de la adaptación y de su gobernanza.

Entre los hitos alcanzados, destaca la Evaluación de Riesgos e Impactos derivados del Cambio Climático en España (ERICC-2025), desarrollada entre 2023 y 2025 y que responde al artículo 18 de la *Ley 7/2021, de cambio climático y transición energética*, y se alinea con los enfoques del IPCC y la Evaluación Europea de Riesgos Climáticos (EUCRA), adaptados al contexto español. Este trabajo constituye el primer ejercicio integral a escala nacional orientado a identificar y caracterizar los riesgos asociados al cambio climático en España. Su objetivo es facilitar la definición y priorización de medidas de adaptación, considerando sus implicaciones sociales, económicas y ambientales. Además, la evaluación identifica y analiza riesgos e impactos derivados del cambio climático en 14 campos sectoriales, analiza sus interrelaciones y ofrece una estimación de la urgencia para abordarlos.

Los resultados de la ERICC servirán para orientar el nuevo programa de trabajo 2026-2030 del PNACC, así como para orientar otras políticas y medidas en materia de adaptación, e identificar lagunas de conocimiento y áreas prioritarias de investigación.

A su vez, el Sistema Portuario de interés general dispone de un Marco Estratégico que de forma expresa establece objetivos relativos a adaptación y mitigación frente al cambio climático en el marco del PNACC (2021-2030). Se contempla que para 2030 las Autoridades Portuarias tengan planes de adaptación aprobados para todos los puertos de interés general, así como el establecimiento de un observatorio portuario de cambio climático. Los puertos, especialmente expuestos a efectos del cambio climático como el aumento del nivel del mar o de la intensidad y frecuencia de los temporales, entre otros, deben anticiparse y responder a los riesgos asociados, tanto en activos físicos como en operaciones, adoptando las medidas oportunas.

Por otra parte, AEMET ha elaborado el Informe sobre el estado del Clima de España 2024 que pretende dar a conocer los aspectos más significativos del tiempo y el clima en nuestro país con periodicidad anual e indagar en las tendencias climáticas a largo plazo.

Asimismo, el CIEMAT ha contribuido en la elaboración de la última actualización del Programa Nacional de Control de la Contaminación Atmosférica 2023-2030 (PNCCA) y ha realizado también el estudio que contiene el Programa sobre evaluación del impacto en la calidad del aire de las medidas existentes (CM) y adicionales (CMA) incluidas en el PNCCA-2023 para los años 2025 y 2030.

Además, el CIEMAT ha realizado el estudio sobre el transporte transfronterizo de las emisiones nacionales de España, centrándose en el impacto en los países vecinos incluido en el PNCCA-2023.

En el marco de la UE, en 2025 se ha completado el primer ciclo de cumplimiento de la directiva europea de comercio de derechos de emisiones. España, como Autoridad Administrativa, ha aprobado los planes de seguimiento de 4.500 buques, mientras que las empresas navieras han presentado informes verificados de las emisiones de 3.094 buques. Sobre la base de dichos informes, se han elaborado y presentado 732 informes agregados a nivel de empresa, que representan un volumen total de 13 millones de toneladas de CO₂ de las cuales debe entregarse un 40% de derechos este primer año.

Además, se está implantando el Reglamento FuelEU Marítimo en el que España gestionará el cumplimiento de una flota de las mismas dimensiones que la de la directiva de comercio de derechos de emisiones.

A su vez, a nivel nacional, se ha aprobado en el consejo de ministros el Plan de Acción Nacional para la descarbonización del Transporte Marítimo.

Autoabastecimiento alimentario

El sector agrario, como suministrador de alimentos y como medio de fijación de población en las zonas rurales, es un sector estratégico en el conjunto de la economía nacional. Al desarrollar su actividad productiva mayoritariamente al aire libre, los riesgos a la exposición y dependencia a la variabilidad climática y la aparición de plagas y enfermedades, si no se manejan adecuadamente, puede suponer una importante merma de renta e incluso, la desaparición de muchas de ellas.

Por otra parte, la cadena alimentaria, en gran medida gracias a su intensa y cada vez mayor presencia en los mercados internacionales, se ha convertido en un sector estratégico de la economía nacional con una participación en el PIB cercana al 12%. Es este crecimiento económico el que de verdad permite la existencia de un sector fuerte y resiliente que nos asegura el abastecimiento. Esa exposición cada vez mayor a los mercados internacionales también nos hace más sensibles a cualquier disrupción de estos y por tanto nos obliga a estar más atentos a esta realidad.

El Sistema de Seguros Agrarios Combinados en España representa un instrumento fundamental para la gestión de los riesgos mencionados, contribuyendo a la resiliencia de las explotaciones agrarias y al mantenimiento de su renta, y por tanto, garantizando la robustez del sector primario español. El Ministerio de Agricultura, Pesca y Alimentación (MAPA), a través de la Entidad Estatal de Seguros Agrarios O.A. (ENESA), subvenciona hasta el 70% del coste de las pólizas para facilitar su contratación.

Por su parte, el Gobierno aprobó el 47º plan de seguros agrarios para el ejercicio 2026 con un presupuesto inicial de 315 millones de euros destinados a ayudar a la contratación de pólizas. Este plan incluye medidas para ajustar el apoyo en pólizas que presentan una elevada siniestralidad en sus resultados del seguro, fomentando de esta manera la adopción de medidas de adaptación por parte de los productores, en sintonía con las necesidades que impone el nuevo contexto climático.

Durante 2025, son varios los eventos climáticos que han afectado de manera negativa al sector agrícola y ganadero, con una superficie agrícola siniestrada de 1,46 millones de hectáreas y una previsión de indemnizaciones de 737,97 millones de euros.

Finalmente, es destacable el marco estratégico y normativo nacional de adaptación y mitigación del cambio climático desarrollado durante 2025:

- Orden HAC/408/2025, de 28 de abril, por la que se modifican para el período impositivo 2024 los índices de rendimiento neto aplicables en el método de estimación objetiva del Impuesto sobre la Renta de las Personas Físicas para las actividades agrícolas y ganaderas afectadas por diversas circunstancias excepcionales.
- Ley 1/2025, de 1 de abril, de prevención de las pérdidas y el desperdicio alimentario.
- Real Decreto 347/2025, de 22 de abril, por el que se aprueba una ayuda de concesión directa para compensar los efectos de la sequía sobre la producción agraria en determinadas provincias del arco mediterráneo español.
- Real Decreto 683/2025, de 29 de julio, por el que se disponen determinadas excepciones temporales relativas al cumplimiento de la normativa básica que regula los regímenes de ayudas a los sectores de frutas y hortalizas y vitivinicultura de la Política Agrícola Común, y se modifican diversos reales decretos relativos al sector de frutas y hortalizas y vitivinicultura en el marco del Plan Estratégico para la PAC 2023-2027 en el Reino de España. (como consecuencia de la DANA de octubre de 2024).
- Real Decreto 684/2025, de 29 de julio, por el que se regula la concesión directa de una ayuda para compensar el daño no indemnizado a los titulares de pólizas del seguro agrario combinado afectados por la Depresión Aislada en Niveles Altos (DANA) ocurrida en diferentes municipios entre el 28 de octubre y el 4 de noviembre de 2024 sobre la producción agraria, establece una ayuda directa extraordinaria para compensar los daños no cubiertos por el seguro agrario en las explotaciones afectadas por la DANA.
- Real Decreto 939/2025, de 21 de octubre, por el que se regula la concesión directa de ayudas para compensar los daños producidos sobre la actividad agraria por los grandes incendios acaecidos en 2025.

Igualmente, destacan las medidas adoptadas en los siguientes acuerdos del Consejo de Ministros, de:

- 1 de abril de 2025: Acuerdo por el que se declara “Zona afectada gravemente por una emergencia de protección civil” el territorio afectado como consecuencia de las inundaciones y otros fenómenos de distinta naturaleza acaecidos entre el 16 de septiembre de 2024 y el 24 de marzo de 2025.
- 24 de junio de 2025: Acuerdo por el que se declara “Zona afectada gravemente por una emergencia de protección civil” diferentes comarcas de las comunidades autónomas de Illes Balears, Castilla y León, Canarias, Cataluña, La Rioja, Comunidad Valenciana, Galicia, Andalucía, Aragón y Castilla-La Mancha que sufrieron 26 emergencias de distinta naturaleza entre el 25 de marzo y el 22 de junio de 2025.
- 26 de agosto de 2025: Acuerdo por el que se declara “Zona afectada gravemente por una emergencia de protección civil el territorio afectado por los incendios forestales y otras emergencias de protección civil que se produjeron entre el 23 de junio y el 25 de agosto de 2025.



ANÁLISIS DE RIESGOS
2025/26

2022/23

Vulnerabilidad energética

Vulnerabilidad del ciberespacio
Inestabilidad económica y financiera
Campañas de desinformación
Tensión estratégica y regional

2023/24

Campañas de desinformación

Vulnerabilidad del ciberespacio
Flujos migratorios irregulares
Tensión estratégica y regional
Terrorismo y radicalización violenta

2024/25

Vulnerabilidad del ciberespacio

Campañas de desinformación

Flujos migratorios irregulares
Tensión estratégica y regional
Inestabilidad económica y financiera

2025/26

Vulnerabilidad del ciberespacio

Campañas de desinformación

Vulnerabilidad energética
Emergencias y catástrofes
Espionaje e injerencias desde el exterior

INTRODUCCIÓN

Este informe presenta los resultados de la encuesta de percepción de riesgos a la Seguridad Nacional, elaborada en el transcurso de los meses de febrero y marzo de 2026. Se trata del séptimo informe de riesgos que aprueba el Consejo de Seguridad Nacional, práctica que se inauguró en el año 2019 y que tiene como objetivo ofrecer un panorama integral de los dieciséis riesgos y amenazas para la Seguridad Nacional. Los aspectos más destacables de esta edición son los siguientes:

En lo que respecta al proceso de elaboración:

cabe destacar el significativo aumento del número de participantes en la encuesta de percepción de riesgos para la Seguridad Nacional con respecto a ediciones anteriores. Este aumento es debido a la participación, por segundo año consecutivo, de expertos del ámbito científico a este proyecto, gracias a la contribución de la Oficina Nacional de Asesoramiento Científico (ONAC), órgano directivo del Gobierno de España encargado de establecer mecanismos institucionales para reforzar el papel de conocimiento científico en la toma de decisiones del Gobierno de España.

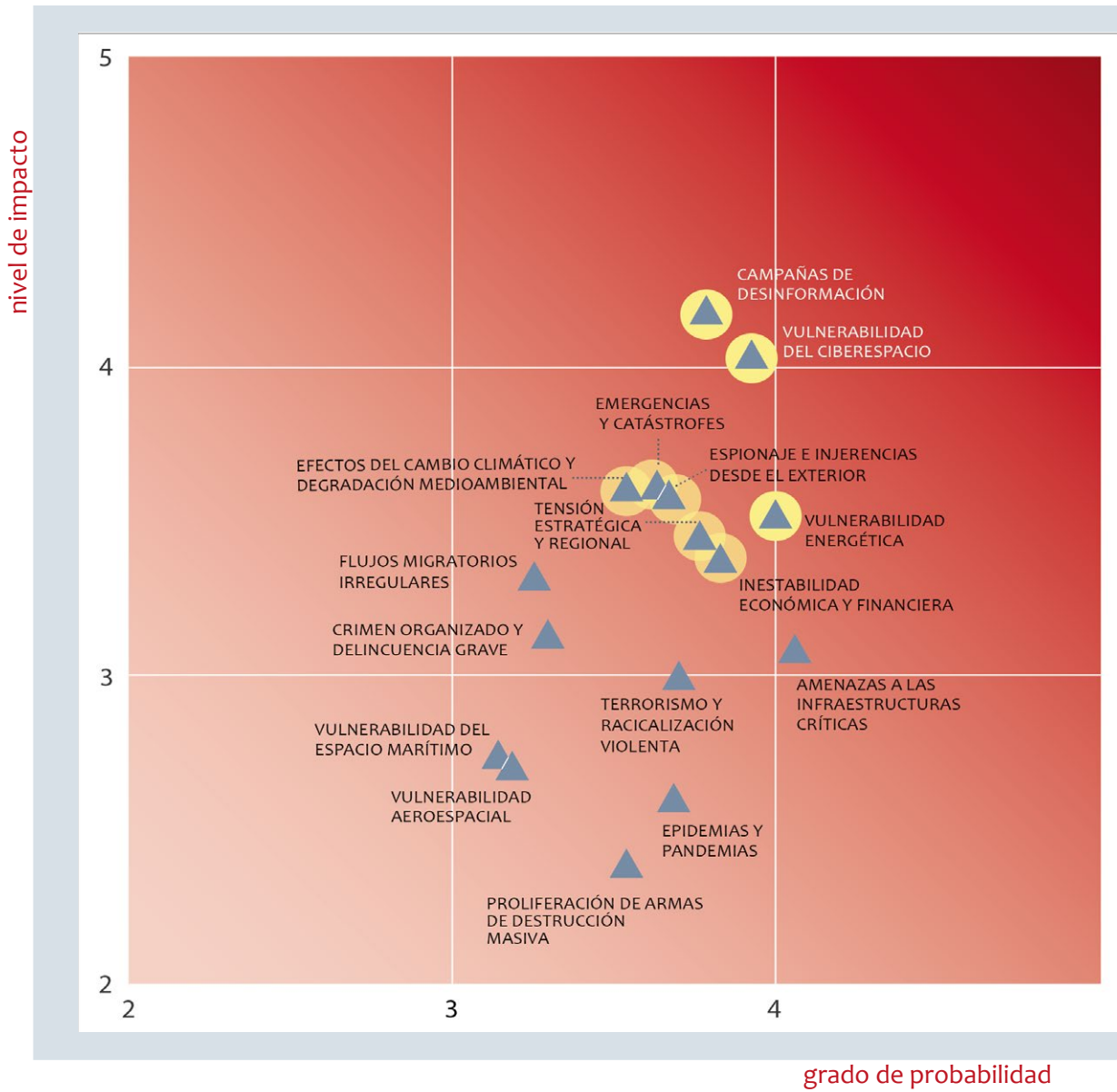
En lo relativo a los resultados:

una mirada retrospectiva cinco años atrás permite afirmar el predominio de la preocupación para la sociedad del empleo del ciberespacio para fines irregulares y las campañas de desinformación. Son dos amenazas para la seguridad nacional que, al margen de la situación coyuntural de cada año, siempre han ocupado los puestos más altos en el *ranking* del mapa de riesgos. Como rasgo más distintivo de lo acontecido a lo largo de 2025, cabría identificar el cero energético de 28 de abril, evento que ha vuelto a poner de manifiesto la importancia de la seguridad energética.

Figura A-1

Evolución de los cinco riesgos y amenazas de mayor nivel de intensidad

Figura A-2
Mapa de Riesgos para la Seguridad Nacional 2025



MAPA DE RIESGOS

El mapa de riesgos representa de forma gráfica los 16 riesgos y amenazas para la Seguridad Nacional según su nivel de impacto (eje vertical) y su grado de probabilidad (eje horizontal) en una escala de 0 a 5. En el gráfico ampliado se representan las zonas de riesgos que se corresponden con las áreas de puntuaciones más altas en cuanto a las variables de nivel de impacto y grado de probabilidad (escala de 2 a 5). De los resultados obtenidos este año, caben destacar las siguientes consideraciones:

■ **Los riesgos de naturaleza más tecnológica ocupan los dos primeros puestos**

- La vulnerabilidad del ciberespacio y las campañas de desinformación aparecen en posición destacada en el área correspondiente a valoraciones en cuanto a nivel de impacto superior a 4 y grado de probabilidad cercana a 4.

■ **La vulnerabilidad energética sube en el escalafón**

- En 2022, la vulnerabilidad energética fue percibida como la principal amenaza para la Seguridad Nacional con motivo de la crisis causada por la invasión de Ucrania en 2022. Este año, la vulnerabilidad energética escala puestos, año en el que se produjo el cero energético de 28 de abril.

■ **Emergencias y catástrofes, efectos del cambio climático y degradación medioambiental**

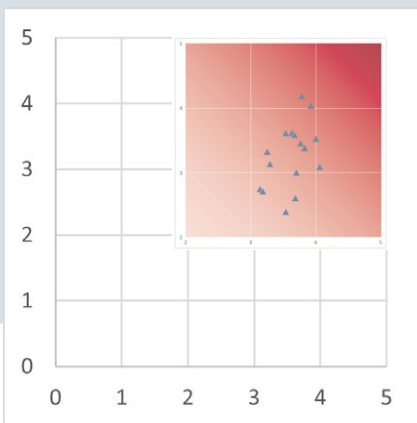
- La sucesión de emergencias climáticas y de eventos meteorológicos graves producidos en España recientemente tiene reflejo en el mapa de riesgos de este año, al situar en la zona alta del gráfico ambas amenazas para la Seguridad Nacional.

■ **Co-existencia de amenazas más tradicionales con las denominadas “estrategias híbridas”**

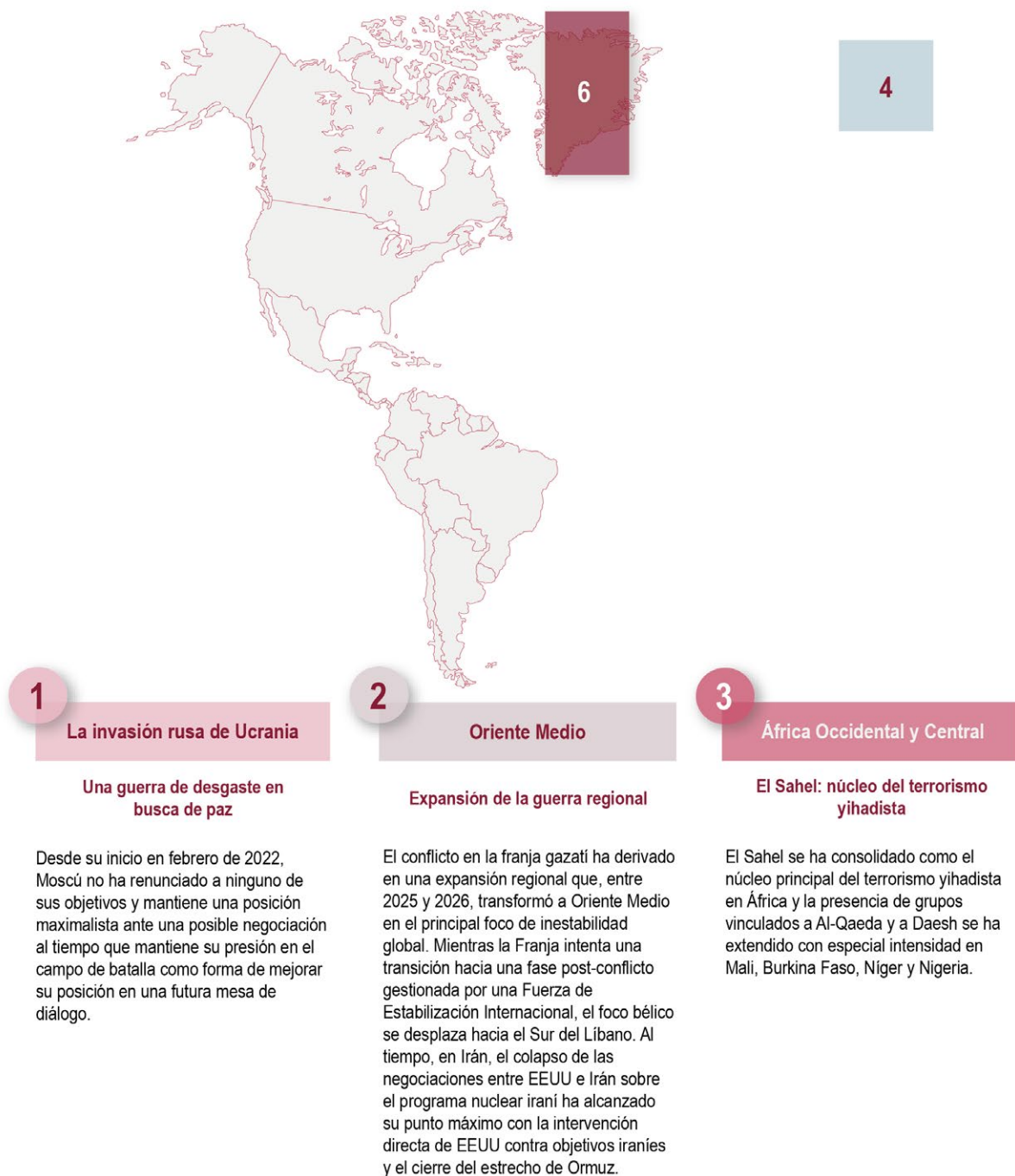
- A las amenazas consideradas más “tradicionales” como son el terrorismo, el crimen organizado, los flujos migratorios irregulares, o la inestabilidad económica y financiera, se les unen otras como pueden ser las amenazas a las infraestructuras críticas, el espionaje y las injerencias desde el exterior, asociadas a las denominadas “estrategias híbridas”.

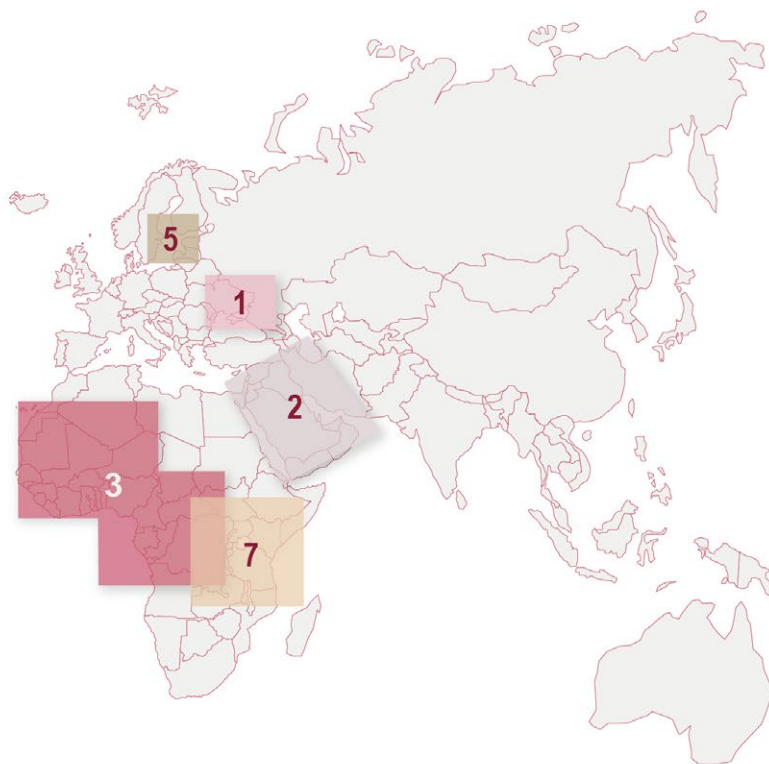
■ **Vulnerabilidad del espacio marítimo, vulnerabilidad aeroespacial y proliferación de armas de destrucción masiva**

- Pese a no ser valoradas con tanta intensidad, estas tres amenazas mantienen su relevancia en el mapa de riesgos de 2025.



ESCENARIOS DE TENSIÓN ESTRATÉGICA Y REGIONAL 2025-2026





- 4** **Espacio aéreo y ultraterrestre**
 Nuevo tablero de la guerra híbrida y el control tecnológico
- 5** **Ciberseguridad y guerra híbrida**
 La ofensiva digital y el sabotaje se consolidan como el primer frente de batalla
- 6** **Groenlandia**
 El epicentro de la nueva competencia por el control del Ártico
- 7** **La competición por los recursos naturales**
 Las materias primas: el primer motor de la geopolítica actual

El ámbito aeroespacial se consolida como un terreno cada vez más disputado entre grandes potencias, organizaciones y actores no estatales, con un aumento del riesgo de incidentes, provocaciones o ataques relacionados con satélites.

El aumento de los ataques híbridos y cibernéticos para desestabilizar a los países y afectar a su infraestructura crítica, hacen de la ciberseguridad un ámbito de atención prioritaria. En especial, las infraestructuras marítimas se consolidan como un foco estratégico. Puertos, terminales energéticas, cables submarinos, gasoductos e interconexiones eléctricas concentran una parte significativa del tráfico de datos, energía y mercancías, lo que incrementa el impacto potencial de cualquier incidente que afecte a su funcionamiento.

El Ártico está pasando de ser una zona de cooperación a un escenario clave de rivalidad global. El panorama geopolítico de Groenlandia atraviesa una importante crisis diplomática ante el riesgo de escalada de tensiones.

La alta demanda de recursos naturales, necesarios para la transición ecológica y digital, aumentan las tensiones económicas entre los principales poderes globales, que intensifican su presencia en regiones clave como LATAM, el Ártico y África para asegurar su suministro.

Figura A-3
Escenarios de tensión estratégica y regional 2025

TENDENCIAS A CINCO AÑOS

Por sexto año consecutivo, la percepción de la previsible evolución del contexto de Seguridad Nacional con un horizonte temporal de cinco años es de deterioro.

Los resultados de la encuesta sitúan a dos elementos en el rango de los riesgos y las amenazas que muestran un fuerte deterioro. Son la vulnerabilidad del ciberespacio y las campañas de desinformación.

El bloque mayoritario es aquel que se corresponde con los riesgos y amenazas que se perciben con una tendencia a empeorar. En esta categoría se encuentran el terrorismo y la radicalización violenta; el crimen organizado y la delincuencia grave; las amenazas para las infraestructuras críticas; los flujos migratorios irregulares; la vulnerabilidad energética; el espionaje y las injerencias desde el exterior; la inestabilidad económica y financiera; las emergencias y catástrofes; los efectos del cambio climático y la degradación del medio natural; y la tensión estratégica y regional.

Dentro del tercer bloque se encuentran la vulnerabilidad del espacio marítimo; la proliferación de armas de destrucción masiva; las epidemias y pandemias; y la vulnerabilidad aeroespacial.

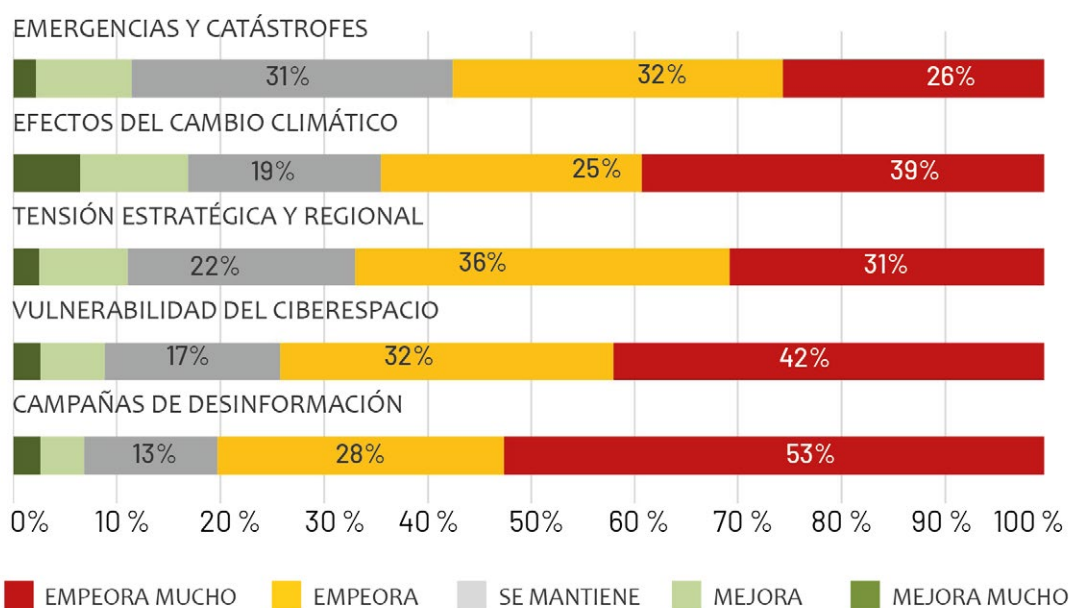


Figura A-4
Los cinco riesgos y amenazas para la Seguridad Nacional que presentan una tendencia más negativa a cinco años

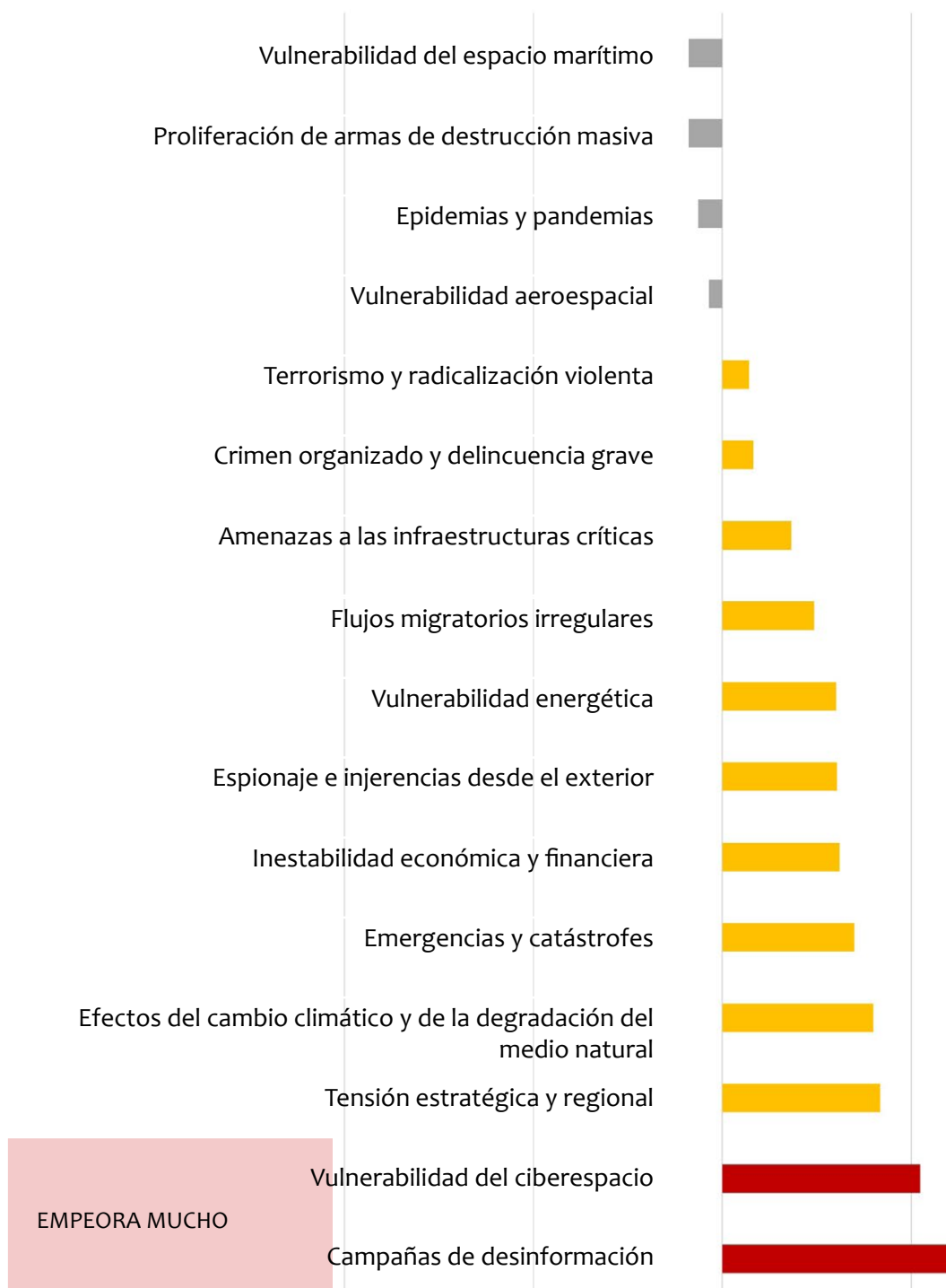
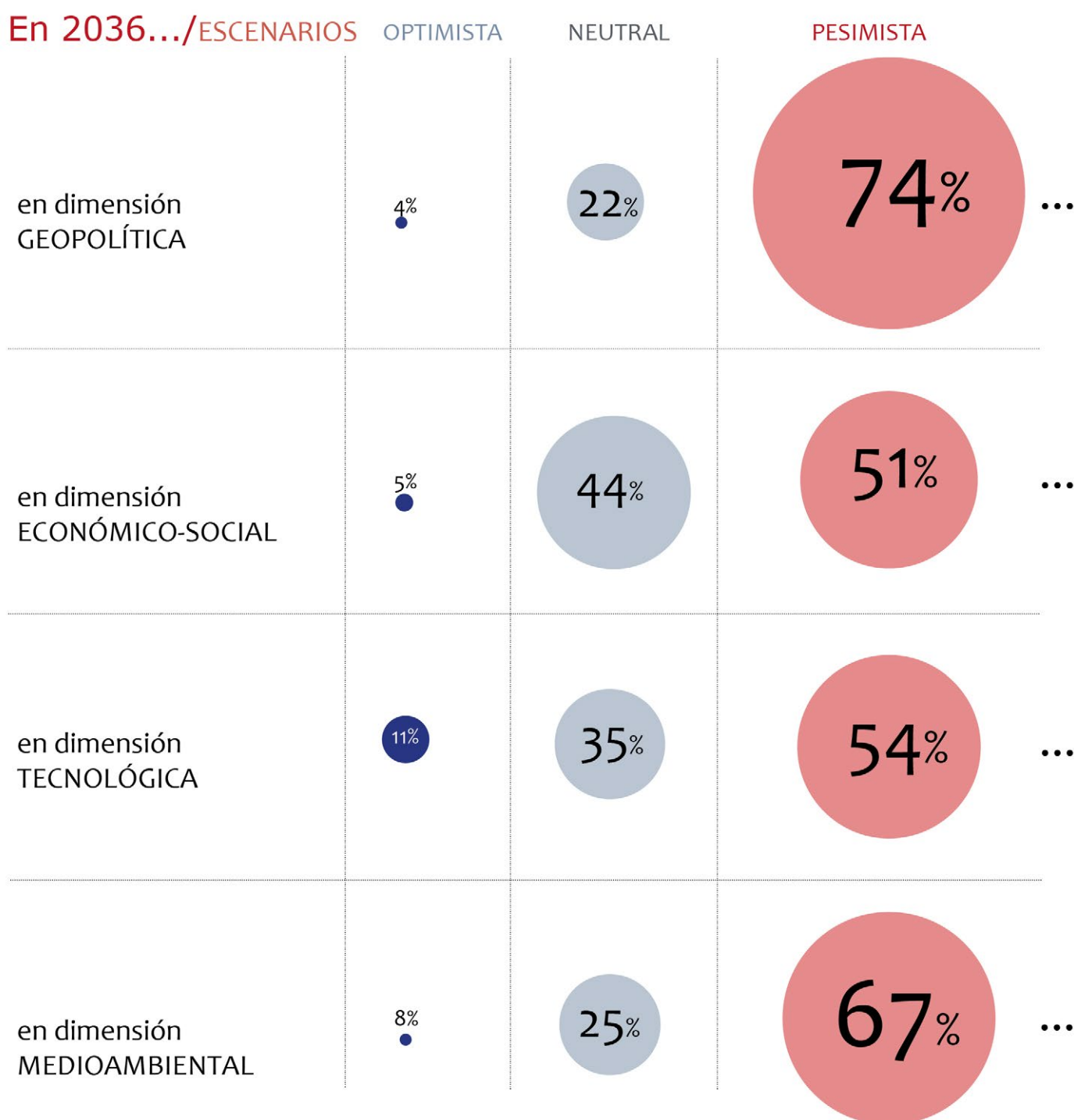


Figura A-5
Resultados de la encuesta de percepción de riesgos para la Seguridad Nacional (tendencias a cinco años)

ESCENARIOS 2036

En esta sección, se presentan los resultados del bloque final de la encuesta de percepción de riesgos, donde se solicitaba a los expertos que valoraran el grado de probabilidad de tres posibles escenarios (que se podrían calificar como escenarios optimista, central y pesimista) para cada una de las cuatro dinámicas de transformación global identificadas en la *Estrategia de Seguridad Nacional 2021 (ESN 2021)* en dimensión geopolítica, económico-social, tecnológica y medioambiental.



Leyenda

% de respuestas que cada corresponsal ha seleccionado en primer lugar de las tres alternativas posibles

Figura A-6

Resultados de la encuesta de percepción de riesgos para la Seguridad Nacional (Escenarios 2036)

Las cifras muestran el porcentaje de respuestas de la primera opción que cada corresponsal ha seleccionado en primer lugar de las tres alternativas posibles

Dinámicas de transformación global (ESN 2021)

El contexto geopolítico en 2036 se caracterizará por ser un **escenario de mayor fragmentación y complejidad**. El desenlace de los actuales conflictos en Ucrania y en la franja de Gaza será determinante para el panorama de seguridad internacional en los próximos años.

Tras la crisis socioeconómica de la pandemia, parece consolidarse una tendencia hacia la regionalización geográfica de las cadenas de suministro. El **equilibrio entre un adecuado nivel de autonomía y una aproximación aperturista** y cooperativa será clave en la próxima década.

Tecnologías como los **semiconductores y la inteligencia artificial generativa** plantean serios desafíos para la seguridad. Pese a las ventajas del avance tecnológico, sofisticadas tecnologías pueden ser empleadas por actores tanto Estatales como no estatales, como vector de influencia para defender sus intereses estratégicos.

Los objetivos para hacer frente a los efectos del cambio climático se ven cada vez más inalcanzables. Como consecuencia, **la degradación medioambiental en determinadas zonas del planeta aumentará significativamente**, incrementando la inestabilidad y la inseguridad.

RADIOGRAFÍA DE LA MASA CRÍTICA

El presente análisis ha sido acometido gracias a la participación de 806 personas, pertenecientes a los distintos órganos y grupos del trabajo del Sistema de Seguridad Nacional.



Figura A-7

Distribución por ámbitos de especial interés para la seguridad nacional

CONCLUSIONES

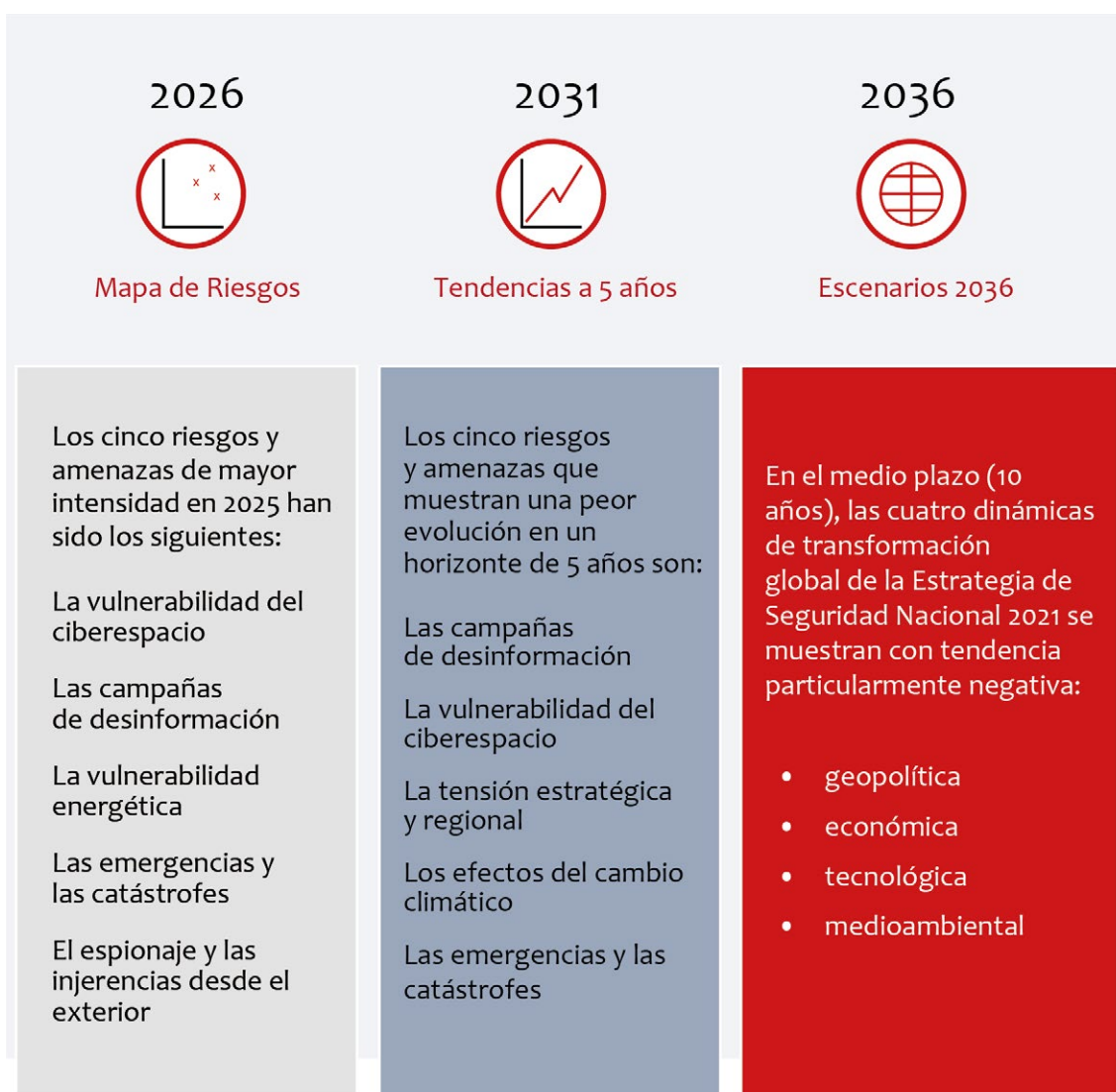


Figura A-8

Elementos de mayor preocupación como resultado de la encuesta de percepción de riesgos para la Seguridad Nacional (Mapa de riesgos, tendencias a 5 años y escenarios 2036)



CULTURA DE SEGURIDAD
NACIONAL

CULTURA DE SEGURIDAD NACIONAL

En los capítulos previos se han analizado los principales riesgos y amenazas que afectan al conjunto del Estado, tensión estratégica y regional; terrorismo y radicalización violenta; emergencias y catástrofes; campañas de desinformación; vulnerabilidad del ciberespacio; inestabilidad económica y financiera; flujos migratorios irregulares; efectos del cambio climático. La persistencia de este entorno dinámico y, al mismo tiempo, convulso, refuerza la necesidad de intensificar el trabajo de las administraciones para garantizar una divulgación adecuada de la Cultura de Seguridad Nacional.

Con este objetivo nació el **Plan Integral de Cultura de Seguridad Nacional** (aprobado en 2021). Su principio rector afirma que «lograr una sociedad más sensibilizada, más fuerte y más resiliente ante cualquier adversidad requiere favorecer la concienciación sobre todos los esfuerzos que exige la garantía de la Seguridad Nacional». En este cometido participan todos los ministerios, la Secretaría de Estado de Comunicación (SEC) y el Centro Nacional de Inteligencia (CNI), junto con representantes de la sociedad civil y del sector privado, coordinados por el Departamento de Seguridad Nacional (DSN). La labor conjunta de estos actores persigue promover esta cultura como condición indispensable para el disfrute de la libertad, la justicia, el bienestar, el progreso y los derechos de la ciudadanía.

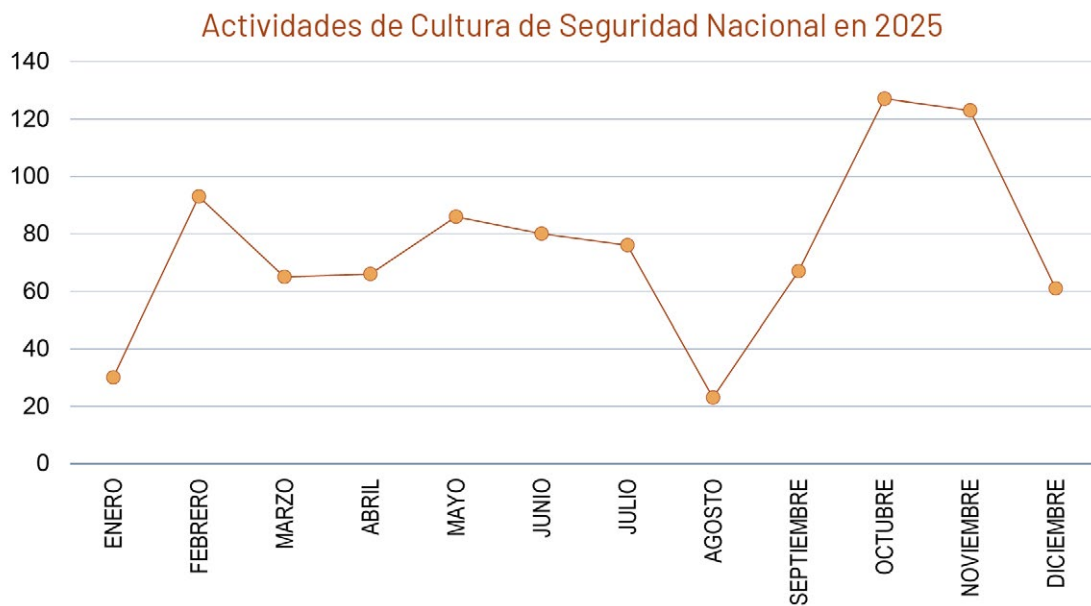
Durante 2025 se ha consolidado el respaldo del Grupo Interministerial de Cultura de Seguridad Nacional y del Foro Integral de Cultura de Seguridad Nacional a las actividades de concienciación, con especial impulso a la colaboración público-privada. Este esfuerzo reafirma la importancia de las sinergias para alcanzar al conjunto de la sociedad y asegurar un nivel adecuado de preparación y compromiso.

El Plan define cuatro ámbitos de acción, formación, comunicación pública y divulgación, proyección exterior y participación, a partir de los cuales se impulsa la cooperación entre las comunidades implicadas. Su objetivo es fortalecer la conciencia social sobre la importancia de la Seguridad Nacional y sobre la corresponsabilidad de toda la ciudadanía en las tareas de anticipación, prevención, análisis, respuesta, resistencia y recuperación ante desafíos, riesgos y amenazas.

Como en años anteriores, una vez concluido 2025 se solicitó a los miembros del Grupo Interministerial, integrado por representantes de todos los ministerios, la SEC, el CNI y el DSN, un listado de actividades relacionadas con la Cultura de Seguridad Nacional. A partir de sus aportaciones, junto con las acciones realizadas por los miembros del Foro, se han elaborado los gráficos incluidos en este capítulo, con el fin de evaluar el impacto de esta política y mejorar su alcance y sus propuestas de futuro.

Iniciativas de impulso de la cultura de Seguridad Nacional en 2025

En 2025 se perfeccionó el análisis de los datos mensuales, especialmente respecto a cursos de carácter continuado. En comparación con el ejercicio anterior, el número total de actividades registradas por las administraciones públicas experimentó un incremento aproximado del 175%. (Figura 1)



Fuente: Elaboración del DSN

Figura 1: Actividades de Cultura

El año se inició con un crecimiento significativo entre los meses de enero y febrero, coincidiendo con el comienzo del ejercicio administrativo y la puesta en marcha de las planificaciones anuales.

Entre marzo y julio, la actividad se mantuvo estable y sostenida, sin variaciones acusadas, consolidándose como el periodo más regular del año.

En agosto se registró un descenso notable, asociado al periodo vacacional y a la consiguiente reducción de la capacidad operativa de las administraciones públicas.

En la fase final del año, entre octubre y noviembre, se produjo un nuevo incremento de actividad, resultado de los esfuerzos institucionales vinculados al cierre de las campañas anuales y a las planificaciones internas de cada administración. El mes de diciembre concluyó con un volumen moderado de actuaciones.

En resumen, la evolución de 2025 refleja un impulso inicial marcado, un tramo central estable, una ralentización estival y un repunte significativo durante el otoño, periodo que concentra la mayor parte de la actividad anual en materia de Cultura de Seguridad Nacional.

Principales actividades desarrolladas en 2025

Durante el segundo trimestre del año, el Ministerio de Política Territorial y Memoria Democrática y el Departamento de Seguridad Nacional llevaron a cabo el II Curso de Cultura de Seguridad Nacional para Delegaciones y Subdelegaciones del Gobierno. En esta edición participaron expertos procedentes de diversos organismos y ministerios, entre ellos:

- Ministerio de Asuntos Exteriores, Unión Europea y Cooperación
- Ministerio de Defensa
- Ministerio del Interior
- Ministerio de Agricultura, Pesca y Alimentación
- Ministerio de Educación, Formación Profesional y Deportes
- Ministerio de Sanidad
- Ministerio de Inclusión, Seguridad Social y Migraciones
- Ministerio de Juventud e Infancia
- Ministerio para la Transición Ecológica y el Reto Demográfico
- Ministerio para la Transformación Digital y de la Función Pública - INCIBE
- CNI - CCN
- Secretaría de Estado de Comunicación
- Federación Española de Municipios y Provincias
- Departamento de Seguridad Nacional

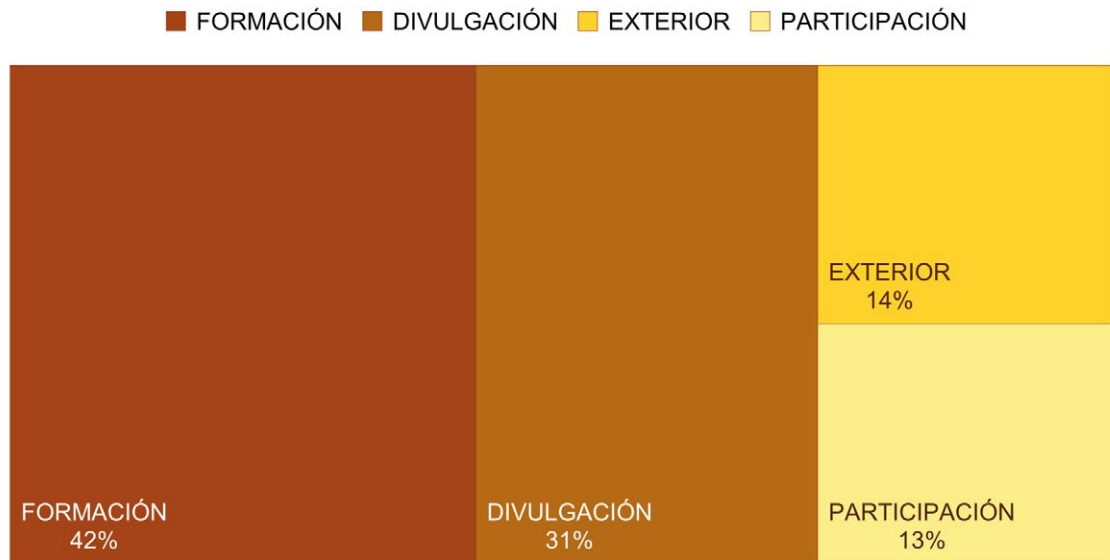
En noviembre, la Directora del Departamento de Seguridad Nacional impartió la conferencia «Los retos actuales de la Seguridad Nacional» en el Ministerio de Industria y Turismo.

A lo largo del año se llevaron a cabo diversas actividades formativas, entre las que destacan las dirigidas a funcionarios con responsabilidades de seguridad en el Ministerio de Industria y Turismo, el curso de «Planificación estratégica como herramienta de gestión pública», así como las incorporaciones a través del ICEX en el Ministerio de Economía, Comercio y Empresa. Entre estas formaciones se encuentran el Curso Selectivo de Nuevos Funcionarios de Cuerpos Superiores de TCEE y DCE, y las acciones destinadas al Cuerpo de Inspectores e Ingenieros Técnicos del SOIVRE.

En línea con las prioridades del Plan, se confirma la tendencia observada en años anteriores: la formación continúa siendo el ámbito que concentra el mayor esfuerzo institucional, reafirmando la capacitación como eje fundamental para fortalecer la preparación y concienciación de la ciudadanía. (Figura 2)

Como continuación a los análisis realizados en años anteriores, se han plasmado los resultados de las actuaciones relacionadas con la cultura de Seguridad Nacional. (Figura 3)

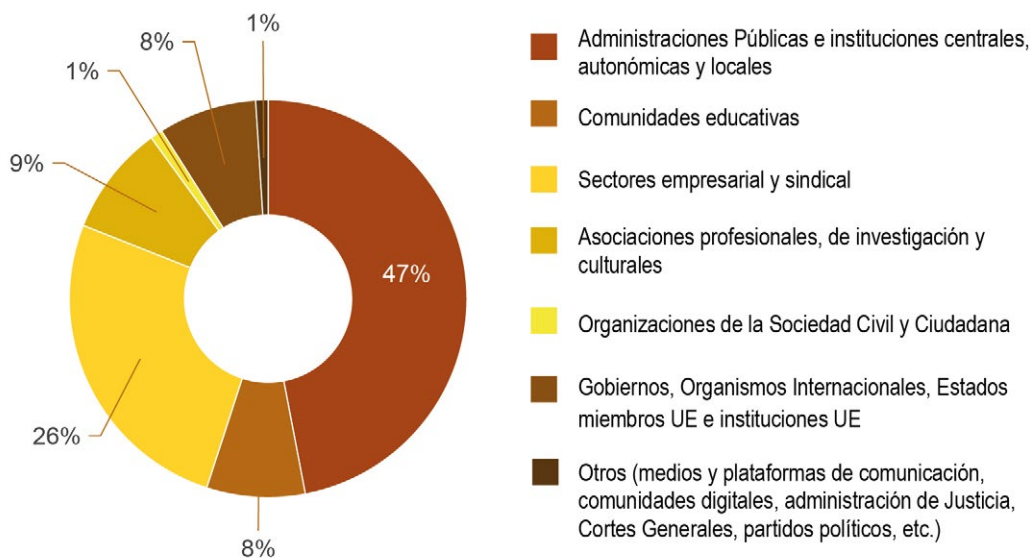
Líneas de actuación de Cultura de Seguridad Nacional



Fuente: Elaboración del DSN

Figura 2: Líneas de actuación de Cultura de Seguridad Nacional

Cultura de Seguridad Nacional y comunidades de referencia



Fuente: Elaboración del DSN

Figura 3: Cultura de Seguridad Nacional y comunidades de referencia

El Plan, como eje vertebrador, identifica diez comunidades de referencia, junto con el conjunto de la ciudadanía, que actúan como principales receptores:

1. Cortes Generales
2. Administraciones públicas e instituciones de los ámbitos estatal, autonómico y local
3. Administración de Justicia
4. Partidos políticos
5. Comunidades educativas
6. Organizaciones de la sociedad civil
7. Sectores empresarial y sindical
8. Asociaciones profesionales, de investigación y culturales
9. Medios y plataformas de comunicación
10. Comunidades digitales

En 2025, las administraciones públicas se consolidan como principales receptoras de la Cultura de Seguridad Nacional, lo que avala su mantenimiento como eje central en la difusión de mensajes y actividades. Les sigue el sector empresarial y sindical, lo que subraya la necesidad de acompañar estas acciones con el sector privado como parte imprescindible del tejido social. Las asociaciones profesionales, de investigación y culturales, junto con las comunidades educativas, refuerzan la llegada a un público referenciado con capacidad de evolución y proyección futura.

Formación para una comprensión fundamentada de la Seguridad Nacional

Tal y como se desprende de los datos correspondientes a las actividades vinculadas a la Cultura de Seguridad Nacional, la formación representa el 42% del total. El principal público destinatario lo conforman las Administraciones Públicas y las Instituciones de los ámbitos estatal, autonómico y local. El propósito fundamental es ofrecer una visión plural, global y objetiva que contribuya a fortalecer el conjunto del sector público, en beneficio último de la sociedad.

A lo largo de 2025 se han desarrollado líneas formativas dirigidas a funcionarios, como el «Curso de formación en emergencias con afectación al patrimonio cultural» del Ministerio de Cultura; el curso «Rehabilitación energética: novedades en la generación de energía de los edificios, climatización e iluminación» del Ministerio de Vivienda y Agenda Urbana; el «Plan de formación ante emergencias de protección civil en centros educativos no universitarios» del Ministerio de Educación, Formación Profesional y Deportes; y los «Planes de formación en seguridad y de concienciación en seguridad» del Ministerio de Ciencia, Innovación y Universidades. Todas estas iniciativas tienen como objetivo proporcionar a los funcionarios una base sólida en Cultura de Seguridad Nacional que facilite el desempeño de sus funciones.

Respecto al Ministerio para la Transformación Digital y de la Función Pública, sigue dando continuidad a actividades consolidadas y ampliamente respaldadas como la 10ª edición del *Cybersecurity Summer BootCamp*, el 19º ENISE (Encuentro Internacional de Seguridad de la Información) y la 8ª edición de los International CYBEREX25.

Por parte del Centro Nacional de Inteligencia se ha llevado a cabo numerosas conferencias de sensibilización en materia de contrainteligencia para distintos organismos públicos y empresas estratégicas así como la realización de las Jornadas del XIX STIC CCN-CERT, las jornadas de VII Ciberdefensa ESPDEF-CERT y el Congreso RootedCON.

De igual modo, se ha mantenido un número elevado de actividades orientadas a ámbitos prioritarios de la Seguridad Nacional, tales como la lucha contra el terrorismo, el crimen organizado, la seguridad sanitaria, la seguridad fronteriza, la igualdad, el tratamiento de información clasificada, las ciberamenazas y la desinformación.

Comunicación estratégica para una sociedad informada y comprometida

La segunda línea de acción del Plan, la divulgación y comunicación pública orientada a fortalecer una opinión pública consciente del carácter imprescindible e irrenunciable de nuestra seguridad, concentra el 31% del total de actividades previstas para 2025. (Figura 2)

La ciudadanía se configura como una audiencia prioritaria. A través de eventos, publicaciones, folletos, campañas institucionales, notas de prensa y contenidos en redes sociales, se persigue generar un impacto social amplio. Una población adecuadamente informada sobre las amenazas y desafíos en materia de seguridad es, en consecuencia, más segura y resiliente. Por ello, la divulgación en Seguridad Nacional debe promover la concienciación y la corresponsabilidad de todos los ciudadanos.

Entre las iniciativas más destacadas se encuentran el *Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos*, el *Plan Mayor Seguridad* y el *Plan Turismo Seguro*, todos ellos impulsados por el Ministerio del Interior.

En el ámbito del Ministerio de Transportes y Movilidad Sostenible, sobresalen el *Plan de Cultura de Seguridad de Renfe 2026–2028*, la celebración del *XII Congreso Internacional de la Asociación de Ingenieros de Protección Contra Incendios*, las *jornadas de Protección de Puertos y Aeropuertos*, mientras que, desde el Ministerio de Hacienda, destacan los *Foros de Relación Cooperativa* de la Agencia Estatal de Administración Tributaria (AEAT).

Finalmente, el Ministerio de Sanidad mantiene una página web específica para la difusión de alertas vigentes en materia de salud pública, constituyendo un referente informativo para la ciudadanía.

Durante 2025 se aprobaron dos nuevas estrategias sectoriales que orientarán las líneas de acción en los próximos años:

- *Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2025*, orientada a reforzar la protección de los ciudadanos ante amenazas que buscan socavar el libre ejercicio de sus derechos y libertades.
- *Estrategia de Seguridad Aeroespacial 2025*, centrada en la actualización del análisis de las amenazas presentes y futuras en el ámbito aeroespacial, en un contexto marcado por nuevas dinámicas geopolíticas, la irrupción de tecnologías emergentes y los desafíos medioambientales, que exigen una adaptación global por parte de la sociedad.

La proyección de España en el exterior

El año 2025 se ha desarrollado en un contexto de especial volatilidad, marcado por numerosos conflictos internacionales que afectan no solo a la seguridad de las personas, sino también en ámbitos esenciales como la seguridad energética, alimentaria, sanitaria, climática, de abastecimiento y de libertad de movimientos.

En este escenario, la labor de España como impulsora de la seguridad y la paz internacionales adquiere una relevancia aún mayor. El objetivo es proyectar al exterior la imagen de España como un país fiable y seguro, comprometido con la paz, la seguridad y el derecho internacional, y firmemente alineado con una Unión Europea resiliente, proveedora de seguridad y decidida a reforzar su base tecnológica e industrial en el nuevo ciclo legislativo. Gracias al trabajo desarrollado en esta línea, España continúa situándose entre los países más seguros del mundo, tal y como refleja el *Global Peace Index 2025*.

El 14% de las actividades vinculadas a la Cultura de Seguridad Nacional realizadas por las distintas administraciones se han orientado a esta dimensión exterior. Entre las iniciativas más destacadas desarrolladas por el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación figuran la participación en la *Conferencia de Seguridad de Múnich 2025*, en la que se abordaron, entre otros asuntos, la cooperación económica y el papel de Europa en un mundo multipolar, en el *Foro de Doha* sobre mediación en tiempos de conflicto y la situación en Gaza, o la campaña «*Viaja Seguro*», que recuerda la importancia de consultar las recomendaciones de viaje antes de desplazarse al extranjero.

En el ámbito del Ministerio de Defensa, destaca la participación en la *Annual Baltic Conference on Defence*, un espacio de referencia para el diálogo estratégico en materia de seguridad y defensa.

Por su parte, el Ministerio de Agricultura, Pesca y Alimentación ha intervenido en la 44ª Conferencia de la FAO y en la VI Conferencia de ministros de Agricultura entre la Unión Europea (UE) y la Unión Africana (UA), y en la 92ª Asamblea de la OMSA reafirmando el compromiso de España con los desafíos globales vinculados a la alimentación, la sanidad animal bajo el enfoque de *One Health* y la sostenibilidad.

En referencia al Ministerio para la Transición Ecológica y el Reto Demográfico, ha tenido una presencia relevante en la 30ª Conferencia de las Naciones Unidas sobre el Cambio Climático (COP 30), contribuyendo activamente al debate internacional sobre políticas climáticas y transición energética.

Asimismo, se mantiene el apoyo a la organización de cursos de formación tanto dentro como fuera de España, que, junto con las escalas de buques militares en puertos extranjeros, continúan siendo canales prioritarios para la proyección y difusión de la Cultura de Seguridad Nacional en el ámbito internacional.

Promoción de la participación social

La participación ciudadana constituye un pilar esencial de la implicación social en la Seguridad Nacional, alcanzando en 2025 el 13% del total de actividades desarrolladas. (Figura 2)

El principal órgano dinamizador de iniciativas y eventos público-privados es el *Foro Integral de Cultura de Seguridad Nacional*, que actúa como espacio de encuentro entre la sociedad civil y la administración. Gracias a este foro, se generan sinergias que facilitan el intercambio de información y conocimientos, reforzando el papel de la ciudadanía como elemento fundamental en la consolidación de la Cultura de Seguridad Nacional.

Entre las iniciativas más relevantes destaca la celebración del *Día Internacional de la Convivencia en Paz*, impulsada por la Conferencia de Rectores y Rectoras de las Universidades Españolas (CRUE). Asimismo, el Ministerio de Igualdad subraya la labor de la *Red Iberoamericana de Mujeres Mediatoras*, centrada en la promoción de los derechos de las mujeres. A ello se suma la presentación del *Youth Test*, una herramienta desarrollada por el Consejo de la Juventud de España para evaluar el impacto de las políticas públicas en la población joven.

La participación social busca integrar tanto a asociaciones civiles, con fines culturales, educativos, divulgativos, deportivos, de defensa de la igualdad o de lucha contra la discriminación, como a la ciudadanía, de forma individual o colectiva, en actividades vinculadas a la Seguridad Nacional. Con ello, se fomenta una implicación más amplia y representativa en los asuntos que afectan al bienestar y la protección de la sociedad en su conjunto.

Visión de futuro

Después de cuatro años desde la aprobación del Plan Integral de Cultura de Seguridad Nacional, ha llegado el momento de que el Grupo y el Foro analicen hasta qué punto las líneas de acción desarrolladas han logrado incorporarse a la percepción de la sociedad como una necesidad de adaptación ante las vicisitudes que están por venir. Los resultados obtenidos son claramente favorables en comparación con etapas previas a la implantación del plan. Este avance ha sido posible gracias al trabajo coordinado de administraciones, empresas, asociaciones y de la sociedad civil, que han sabido generar nuevas sinergias impulsadas desde el Grupo y el Foro.

Resulta esencial construir una sociedad plenamente concienciada, informada sobre las amenazas y riesgos que afectan a la seguridad, capaz de avanzar hacia un modelo más preparado, seguro y resiliente.

Si bien no podemos prever los acontecimientos futuros, los cambios sociales o las amenazas a las que nos enfrentaremos como comunidad, nuestra labor ha sido, es y será velar por la cohesión social, fortalecer la seguridad y preparar a la ciudadanía para los retos venideros.

El Plan Integral de Cultura de Seguridad Nacional debe consolidarse como marco de referencia para la implantación progresiva y efectiva de la Cultura de Seguridad Nacional.

GLOSARIO

A

AAAVF	Asistencia a las Víctimas de Accidentes de Aviación y sus Familiares
ACNUR	Agencia de la ONU para los Refugiados
ADM	Armas de Destrucción Masiva
AEAD	Agencia Estatal de Administración Digital
AEAT	Agencia Estatal de Administración Tributaria
AECID	Agencia Española de Cooperación Internacional para el Desarrollo
AEE	Agencia Espacial Española
AEMET	Agencia Estatal de Meteorología
AESA	Agencia Estatal de Seguridad Aérea
AES	Alianza de Estados del Sahel
AESIA	Agencia Española de Supervisión de la Inteligencia Artificial
AIEA	Agencia Internacional de Energía Atómica
AIS	Sistemas de identificación automática (por sus siglas en inglés)
ANCC	Autoridad Nacional de Certificación de la Ciberseguridad
AOD	Ayuda Oficial al Desarrollo
APIs	Application Programming Interface
APT	Amenazas Persistentes Avanzadas
ARPSI	Áreas de Riesgo Potencial Significativo de Inundación
B	
BCE	Banco Central Europeo
BITD	Base Industrial y Tecnológica de Defensa
C	
CAP	Paquete de Asistencia Integral de la OTAN
CATV	Centros autorizados de tratamiento de vehículos
CCAES	Centro de Coordinación de Alertas y Emergencias Sanitarias
CCIs	Células de Cooperación de Inteligencia en materia migratoria
CCN	Centro Criptológico nacional
CCSE	Sistema de Conocimiento y Control de la Situación Espacial
CDTI	Centro para el Desarrollo Tecnológico y la Innovación
CEBAS	Centro de Edafología y Biología Aplicada del Segura
CECT	Comité Especializado contra el Terrorismo
CENEM	Centro Nacional de Seguimiento y Coordinación de Emergencias
CENP	Comité Especializado de No Proliferación de Armas de Destrucción Masiva
CETI	Centro de Estancia Temporal de Inmigrantes
CERT	Computer Emergency Response Team
CIAF	Comisión de Investigación de Accidentes Ferroviarios
CIAIAC	Comisión de Investigación de Accidentes e Incidentes de Aviación Civil
CIAIM	Comisión de Investigación de Accidentes e Incidentes Marítimos
CIEMAT	Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas
CIS	Centros de Sistemas y Tecnologías de la Información y las Comunicaciones
CISA	Centro de Investigación en Sanidad Animal
CITCO	Centro de Inteligencia contra el Terrorismo y el Crimen Organizado

CMCC	Centro de Coordinación Cívico Militar
CNA	Autoridad de Numeración de CVE –Common Vulnerabilities and Exposures
CND	Centro Nacional de Datos
CNI	Centro Nacional de Inteligencia
CNULD	Convención de las Naciones Unidas de Lucha contra la Desertificación
CPFMN	Convención sobre la Protección Física de los Materiales Nucleares
CPSTIC	Catálogo de Productos y Servicios de Tecnologías de la Información y las Comunicaciones
COCS	Centro de Operaciones de Ciberseguridad
COSI	Comité de Seguridad Interior
COCS-AGE	Centro de Operaciones de Ciberseguridad de la Administración General del Estado
COCS EELL	Centro de Operaciones de Ciberseguridad para Entidades Locales
COVE	Centro Español de Vigilancia y Seguimiento Espacial
CRA	Ciberer Resilient Act
CSIC	Consejo Superior de Investigaciones Científicas
CSIRTMIRPJ	Centro de Respuesta a Incidentes Cibernéticos del Ministerio del Interior en apoyo a la Policía Judicial
CSNU	Consejo de Seguridad de Naciones Unidas
CTE	Combatientes Terroristas Extranjeros
CVE	Common Vulnerabilities and Exposures
D	
DANA	Depresión Aislada en Niveles Altos
DDoS	Distributed Denial of Service
DGAVT	Dirección General de Apoyo a Víctimas del Terrorismo
DGPCE	Dirección General de Protección Civil de Emergencias
DGPLACE	Dirección General de Planificación y Coordinación Energética
E	
EAV	Embarcaciones de Alta Velocidad
ECCC	Centro Europeo de Competencias en Ciberseguridad
ECIs	Equipos Conjuntos de Investigación
EDIP	Programa Europeo de Industria de Defensa
EDMO	Observatorio Europeo de Medios Digitales (por sus siglas en inglés)
EES	Sistema de Entradas y Salidas (por sus siglas en inglés)
EMPACT	Plataforma Multidisciplinar Europea contra las Amenazas Delictivas
EMSA	Agencia Europea de Seguridad Marítima
ENAIRE	Entidad pública española responsable de la gestión y control del tráfico aéreo en España
ENESA	Entidad Estatal de Seguros Agrarios
ENIA	Estrategia Nacional de Inteligencia Artificial
ENFSI	Red Europea de Institutos Forenses
ENISA	Agencia Europea para la Ciberseguridad
ENS	Esquema Nacional de Seguridad
EPF	Fondo Europeo de Apoyo a la Paz
EPPO	Fiscalía Europea (por sus siglas en inglés)

ERICC	Evaluación de Riesgos e Impactos derivados del Cambio Climático en España
ESA	Agencia Espacial Europea (por sus siglas en inglés)
ESPDEF	Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa
EUAM Ukraine	Misión de Asesoramiento de la Unión Europea en Ucrania
EUCRA	Evaluación Europea de Riesgos Climáticos
EUDA	Agencia de la Unión Europea sobre Drogas
EUMAM-UA	Misión de Asistencia Militar a Ucrania
EUROPOL	Oficina de la Policía Europea
ESPII	Emergencia de Salud Pública de Importancia Internacional
EU SDI GoG	Iniciativa de la Unión Europea en materia de Seguridad y Defensa en apoyo a los Países de África Occidental del Golfo de Guinea
EUSPA	Agencia de la Unión Europea para el Programa Espacial
F	
FAO	Organización de las Naciones Unidas para la Alimentación y la Agricultura
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
FIES	Fuerza Internacional de Estabilización
FIMI	Manipulación e Injerencia Extranjera de la Información
FMA	Fenómenos Meteorológicos Adversos
FNO	Fiebre del Nilo Occidental
FRONTEX	La Agencia Europea de la Guardia de Fronteras y Costas
FUAES	Fuerza Unificada de la AES
G	
GADE	Grupo de Asesoramiento en Desastres y Emergencias
GEI	Gases de Efecto Invernadero
GIF	Grandes Incendios Forestales
GNL	Gas Natural Licuado
GRULAC	Grupo de países de Latinoamérica y Caribe
H	
HPS	Habilitaciones Personales de Seguridad
HSEM	Habilitación de Seguridad de Empresa
HTF	Homegrown Terrorist Fighter
I	
IA	Inteligencia Artificial
IC	Infraestructuras Críticas
ICC	International Maritime Bureau
ICS	Sistemas de Control Industrial (por sus siglas en inglés)
IDAEA	Instituto de Diagnóstico Ambiental y Estudios del Agua
I+D+i	Investigación + Desarrollo + innovación
IEO	Instituto Español de Oceanografía
IGAE	Intervención General de la Administración del Estado
IGME	Instituto Geológico y Minero de España
IGN	Instituto Geográfico Nacional
INAP	Instituto Nacional de Administración Pública
INCIBE	Instituto Nacional de Ciberseguridad de España

INTA	Instituto Nacional de Técnica Aeroespacial
INTERPOL	Organización Internacional de Policía
IPCC	Panel Intergubernamental sobre el Cambio Climático
ISAC	Centro de Intercambio y Análisis de Información
ISCIH	Instituto de Salud Carlos III
ISKP	Estado Islámico en la Provincia del Jorasán
IVA	Impuesto del Valor Añadido
J	
JAI	Justicia y Asuntos de Interior (del Consejo de la UE)
JCO	Joint Commercial Operations
JIMDDU	Junta Interministerial para el Comercio y Control del Material de Defensa y Tecnologías de Doble Uso
JNIM	Grupo de Apoyo al Islam y los Musulmanes
L	
LAVEMA	Laboratorio de Verificación de Armas Químicas
LULUCF	Uso de la tierra, Cambio de Uso de la Tierra y Silvicultura
M	
MAUEC	Ministerio de Asuntos Exteriores, Unión Europea y Cooperación
MCCE	Mando Conjunto del Ciberespacio
MENA	Menores Extranjeros No Acompañados
MITECO	Ministerio para la Transición Ecológica y el Reto Demográfico
MITMA	Ministerio de Transportes, Movilidad y Agenda Urbana
N	
NMCSUI	Centro Marítimo de la OTAN para la Seguridad de Infraestructuras Críticas y Subacuáticas
NPS	Nuevas Sustancias Psicoactivas
NRBQ	Nuclear, Radiológico, Biológico y Químico
O	
OACI	Organización de Aviación Civil Internacional
OAV	Oficina de Asistencia a Víctimas de Accidentes Aéreos
OCC	Oficina de Coordinación de Ciberseguridad
OCDE	Organización para la Cooperación y el Desarrollo Económico
OCHA	Oficina de las Naciones Unidas para la Coordinación de Asuntos Humanitarios
OEA	Organización de Estados Americanos
OEPM	Oficina Española de Patentes y Marcas
OIEA	Organismo Internacional de la Energía Atómica
OMM	Organización Meteorológica Mundial
OMS	Organización Mundial de la Salud
ONAC	Oficina Nacional de Asesoramiento Científico
ONDOD	Oficina Nacional contra los Delitos de Odio
ONG	Organización No Gubernamental
ONRED	Oficina Nacional de Recepción Electrónica de Denuncias
ONS	Oficina Nacional de Seguridad
ONUCT	Oficina de Naciones Unidas Contra el Terrorismo
ONUDD	Oficina de las Naciones Unidas contra la Droga y el Delito

OPAQ	Organización para la Prohibición de las Armas Químicas
OPE	Operación Paso del Estrecho
OTAN	Organización del Tratado del Atlántico Norte
OTPCE	Organización del Tratado para la Prohibición Completa de Ensayos Nucleares
P	
PAC	Paquete Integral de Asistencia a Ucrania
PACIAC	Plan Anual de Control Integral de Actividades Pesqueras
PAIC	Plan de Acción Integral Conjunto
PCM	Puestos de Control Manual
PADE	Protocolo de Asesoramiento en Desastres y Emergencias
PENTRA	Plan Estratégico Nacional de lucha contra la trata y explotación de seres humanos
PERTE	Proyecto Estratégico para la Recuperación y Transformación Económica Aeroespacial
PESCO	Cooperación Estructurada Permanente
PFNA	Punto Focal Nacional de Armas
PGA	Plan General de Actuaciones
PGRI	Planes de Gestión del Riesgo de Inundación
PLAEP	Plan de Acción de Ética Profesional
PLEGEM	Plan General de Emergencias del Estado
PNACC	Plan Nacional de Adaptación al Cambio Climático
PNIEC	Plan Nacional Integrado de Energía y Clima
PNNSC	Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes
POCs	Partenariados Operativos Conjuntos
PQC	Post-Quantum Cryptography
PRTR	Plan de Recuperación, Transformación y Resiliencia
PTA	Programa Tecnológico Aeronáutico
PTE	Programa Tecnológico Espacial
PURL	Prioritised Ukraine Requirements List
Q	
QRA	Quick Reaction Alert
R	
RAN	Red de Alerta Nacional de Protección Civil
RASVE	Red de alerta sanitaria veterinaria
RECAPI	Reserva Estratégica de Capacidades Nacionales de Producción Industrial
RE-LAB	Red de Laboratorios de Alerta Biológica
RENFE	Red Nacional de Ferrocarriles Españoles
RNB	Renta Nacional Bruta
RNS	Red Nacional de Centros de Operaciones de Ciberseguridad
RESI	Reglamento Sanitario Internacional
RSN	Red Sísmica Nacional
S	
S ₃ TOC	Spanish Space Surveillance and Tracking Operations Centre
SAIH	Sistemas Automáticos de Información Hidrológica

SASEMAR	Sociedad Española de Salvamento Marítimo
SAT	Sistema de Alerta Temprana
SEAE	Servicio Europeo de Acción Exterior
SCOMCE	Mando Conjunto del Ciberespacio para la obtención de un Sistema de Combate en el Ciberespacio
SDA	Sistemas Dinámicos de Adquisición
SGEN	Subdirección General de Energía Nuclear
SGSIC	Subsecretaría General de Sistemas de Información y Comunicaciones para la Seguridad
SGAD	Secretaría General de Administración Digital
SEPRONA	Servicio de Protección de la Naturaleza
SETELECO	Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
SI	Servicios de Inteligencia
SIGE	Sistema integrado de Gestión de Emergencias
SIVE	Sistema Integrado de Vigilancia Exterior
SNCA	Servicio Nacional de Coordinación Antifraude
SNCZI	Sistema Nacional de Cartografía de Zonas Inundables
SOC	Centros de Operaciones de Ciberseguridad
SST	Space Surveillance and Tracking
STENFOR	Forum of Strategic Trade Enforcement
STRA	Arquitectura de Respuesta a las Amenazas Espaciales (por sus siglas en inglés)
SVICA	Sistema de Vigilancia y Control Aeroespacial
T	
TIC	Tecnología de la Información y las Comunicaciones
TNP	Tratado de No Proliferación
TPCEN	Tratado de Prohibición Completa de los Ensayos Nucleares
TTP	Tácticas, Técnicas y Procedimientos
U	
UAS	Unmanned Aircraft Systems
UAV	Unmanned Aerial Vehicles
UDCG	Ukraine Defense Contact Group
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
UME	Unidad Militar de Emergencias
UNECI	Unidad Nacional de Retirada de Contenidos Ilícitos
UNIFIL	Fuerza Interina de Naciones Unidas en Líbano
UNRWA	Agencia de Naciones Unidas para la población refugiada de Palestina
UCPM	Mecanismo Europeo de Protección Civil (por sus siglas en inglés)
USI	Ukraine Support Instrument
UVR	Unidad de Valoración de Riesgo
Z	
ZEE	Zonas Económicas Exclusivas
V	
VoTAN	Red Global de Asociaciones de Víctimas de Terrorismo



DSN

www.dsn.gob.es