ANÁLISIS SECTORIAL DE RIESGO

FINANCIACIÓN DE LA PROLIFERACIÓN

2025

MINISTERIO
DE ECONOMÍA, COMERCIO
Y EMPRESA

COMISIÓN DE PREVENCIÓN DEL
BLANQUEO DE CAPITALES E
INFRACCIONES MONETARIAS

Contenido

1. Resumen Ejecutivo 4
2. Introducción 7
2.1 Presentación 7
2.2 Objetivos 8
3. Metodología 10G
3.1. Instituciones Participantes 10
3.2. Fuentes de información 11
3.3. Definiciones y metodología 11
4. Arquitectura institucional sobre proliferación 14
4.1. Instrumentos internacionales 14
4.1.1 Instrumentos internacionales con competencias en materia de financiación de la proliferación con participación de España 14
4.1.2. Organismos internacionales con competencias en materia de proliferación con participación de España 15
4.1.3. Tratados y compromisos internacionales suscritos por España en materia de proliferación 17
4.2. Estructura nacional 17
4.3. Relaciones diplomáticas de España con la RPDC e Irán 19
5. Principales amenazas en materia de financiación de la proliferación 20
5.1. Amenazas a nivel internacional 20
5.2. Amenazas detectadas en el marco nacional 23
5.3. Amenazas emergentes 27
6. Principales Vulnerabilidades 29
6.1. Vulnerabilidades estructurales 29
6.1.1. Derivadas del marco normativo 29
6.1.2. Derivadas de la implementación de las sanciones del CSNU 29
6.1.3. Derivadas de la ausencia de una Autoridad Nacional de Coordinación en materia de Financiación de la Proliferación 30
6.1.4. Derivadas del cumplimiento por parte del sector privado 30
6.2. Vulnerabilidades contextuales o geográficas 31
6.3. Vulnerabilidades Sectoriales 31
6. 3.1. Derivadas del comercio internacional 31

6. 3.2. Derivadas del sector financiero 33
6. 3.3. Derivadas de actividades y profesiones no financieras 34
6.4. Vulnerabilidades específicas de productos y servicios comercializados... 34
6.5. Resumen de vulnerabilidades 37
7. Riesgos 42
7.1. Riesgos inherentes 42
7.2. Medidas mitigadoras 44
7.2.1. Medidas mitigadoras Institucionales 44
7.2.2. Medidas mitigadoras comerciales 46
7.2.3. Mecanismos de control de la titularidad real para evitar la puesta a disposición de personas sancionadas 47
7.2.4. Medidas aplicadas por el sector financiero. 48
7.3. Riesgo residual 49
ANEXO 1- Estadísticas de controles a la exportación 51
ANEXO 2. Régimen jurídico en materia de comercialización de bienes de doble uso. 56
ACRÓNIMOS 57

1. Resumen Ejecutivo

La financiación de la proliferación (en adelante, FP) de armas de destrucción masiva (en adelante, ADM) cobra importancia por la movilización de fondos monetarios y su introducción en sistema financiero internacional de fondos ilícitos que se utilizan para la fabricación, adquisición o transporte de productos sancionados o el desarrollo de armas nucleares.

FP de ADM es un reto de calado internacional en continua evolución frente al que se establecen medidas desde diversas organizaciones. Por un lado, Naciones Unidas, a través de las resoluciones emitidas por el Consejo de Seguridad (en adelante, CSNU) y, por otro, el Grupo de Acción Financiera Internacional (en adelante, GAFI) al configurar la FP de ADM como tercer pilar al que hay que hacer frente desde una perspectiva preventiva. Las obligaciones en esta materia se recogen dentro de la Recomendación 7 de los estándares de GAFI principalmente, sin olvidar que en la Recomendación 1 se determina la necesidad de analizar el riesgo en FP y se enfatiza la cooperación internacional en esta materia en la Recomendación 2. La eficacia del cumplimiento de las obligaciones en materia de FP se evalúa en el Resultado Inmediato 11.

El objetivo general de este análisis sectorial de riesgos es identificar y entender las amenazas, vulnerabilidades y riesgos de FP en España. En este análisis han participado todos los actores relevantes, tanto en el ámbito del sector público como en el sector privado.

El análisis se basa en información cuantitativa y cualitativa, a partir del estudio de documentos estratégicos, informes y estadísticas oficiales. Asimismo, se ha creado un grupo de trabajo con las principales entidades bancarias de España, con las cuales se ha interaccionado en fase de elaboración de este informe y se ha discutido los principales temas tratados. A raíz de este grupo de trabajo, se remitió un cuestionario para determinar las amenazas, vulnerabilidades y principales medidas de mitigación que actualmente están implantadas en nuestro sistema financiero.

Con el fin de determinar la exposición al riesgo, se han analizado las evidencias que entrañan las jurisdicciones vinculadas directamente con la FP (República Democrática de Corea del Norte e Irán), así como las que se derivan de la interacción con otras jurisdicciones intermedias. Teniendo en cuenta estos factores, en el marco nacional, las amenazas se centran en los ciberdelitos ejecutados por organizaciones que actúan de forma globalizada, las transferencias internacionales en las que intervienen jurisdicciones intermedias consideradas de riesgo, la actividad comercial internacional en la que se han detectado amenazas de desvío de material de defensa y sustancias

químicas prohibidas hacia jurisdicciones de riesgo intermedias a través de sociedades pantalla y la actividades de compensación de pagos por cuenta de empresas iraníes susceptibles de estar vinculadas a los programas nucleares o de misiles de Irán.

La actividad patrimonial que se genera a través de la proliferación cobra importancia en la movilización de fondos cuyo origen o destino es la FP. En este sentido, el uso de empresas pantallas y la interconexión con jurisdicciones intermedias son las principales amenazas detectadas.

Las vulnerabilidades que pueden ser aprovechadas por estas amenazas son principalmente las derivadas de la posición geoestratégica de España como punto de encuentro de los 3 continentes y su situación en una de las principales rutas marítimas del mundo como es el estrecho de Gibraltar.

Por otro lado, la detección de operativa sospechosa indirectamente vinculada a la FP entraña dificultades dada la interconexión con otras actividades delictivas de blanqueo de capitales y financiación del terrorismo (en adelante, BC/FT).

Los sectores que están expuestos a un mayor riesgo son aquellos vinculados la banca corresponsal, las entidades de crédito y dinero electrónico y los proveedores de servicios de criptoactivos. No hay evidencias en España que determinen la existencia de canales naturales de exposición a la FP en sectores no financieros, por lo que el riesgo en este sector se configura como bajo de forma inicial.

Tras el análisis de las amenazas y vulnerabilidades que afectan al contexto nacional en materia de FP de ADM se ha concluido que el riesgo inherente es medio-bajo.

Las medidas de mitigación existentes minoran el riesgo inicial. Entre ellas se destacan: la ausencia de proyectos de cooperación entre España y la República Democrática de Corea del Norte (en adelante, RPDC o Corea del Norte), la base jurídica para la ejecución de las sanciones financieras a través de Reglamentos de la Unión Europea (UE), tanto el régimen de RPDC como como la aplicación de la modificación del Reglamento (UE)

267/2012 con el reforzamiento de las medidas contra el programa nuclear iranís tras el "*snap-back*" de sanciones en 2025. Asimismo, también destacan como medidas de mitigación la normativa sectorial española en función de la naturaleza de fabricación de cada tipología de material de doble uso, la regulación existente en materia de comercio internacional, los mecanismos de control de la titularidad real y los sistemas de alertas y detección de operaciones del sistema financiero, así como los procedimientos automatizados implantados para la ejecución de sanciones.

En conclusión, una vez corregido el nivel de riesgo inherente a partir de las medidas de mitigación existentes, se ha concluido que el riesgo residual en materia de FP de ADM es bajo.

2. Introducción

2.1 Presentación

La FP de ADM abarca el dinero o los recursos financieros que se utilizan para apoyar la fabricación, adquisición, transporte o desarrollo de armas nucleares, químicas y biológicas, así como los medios para entregarlas.

Por un lado, las Naciones Unidas pretenden hacer frente a la proliferación de ADM a través de las Resoluciones emitidas por el CSNU. Por otro, desde una perspectiva financiera, el GAFI ha reforzado las ya existentes exigencias en materia de FP, convirtiéndolas en el tercer pilar de sus objetivos preventivos, junto a la prevención del blanqueo de capitales y la financiación del terrorismo (en adelante, PBC/FT).

Las obligaciones del GAFI relativas a la no proliferación se encuentran recogidas en la Recomendación 7, que exige a los países que:

- Congelen sin demora los fondos u otros activos y aseguren que ningún fondo u otro activo se ponga a disposición, directa o indirectamente.

- Cuenten con mecanismos para comunicar las designaciones a las instituciones financieras y a las actividades y profesiones no financieras designadas (en adelante, APNFD).

- Exijan a las instituciones financieras y a las APNFD que reporten a las autoridades competentes los activos congelados o las acciones tomadas en cumplimiento de los requisitos de prohibición de las resoluciones pertinentes del Consejo de Seguridad, incluyendo las transacciones intentadas.

- Adopten medidas apropiadas para monitorear y asegurar el cumplimiento de las obligaciones de la Recomendación 7 por instituciones financieras y las APNFD.

Ninguno de los requisitos de la Recomendación 7 persigue sustituir otras medidas u obligaciones que pudieran estar ya establecidas para manejar fondos u otros activos en el contexto de una investigación o proceso penal, civil o administrativa.

El énfasis de la Recomendación 7 está en las medidas preventivas. Éstas son necesarias y únicas en el contexto de la detención y el uso del flujo de fondos u otros activos hacia los proliferadores o hacia la proliferación.

La Recomendación 7 es aplicable a todas las resoluciones actuales del CSNU que imponen sanciones financieras dirigidas en el contexto de la FP de ADM, así como a cualquier resolución sucesora futura que establezca sanciones financieras dirigidas.

Por un lado, respecto a la RPDC, son aplicables la Resolución 1718 (2006) y sus posteriores: 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) y 2356 (2017).

Por otro lado, con respecto a Irán, son aplicables las Resoluciones 1737 (2006), 1747 (2007), 1803 (2008) y 1929 (2010), que impusieron sanciones relacionadas con su programa nuclear. Estas sanciones fueron levantadas, en gran parte, tras la adhesión de Irán al Plan de Acción Integral Conjunto en 2015 (en adelante JCPOA) y la posterior adopción de la Resolución 2231 (2015), que avaló el acuerdo. Esta Resolución estableció un mecanismo de "*snap-back*" para reimponer sanciones en caso de incumplimiento. En septiembre de 2025 el CSNU no aprobó una Resolución que prolongara el alivio de sanciones bajo el JCPOA, de modo que las sanciones levantadas vuelven a aplicarse automáticamente si no se adopta una nueva resolución dentro del mecanismo previsto.

Cabe destacar que recientemente se han producido cambios en los estándares del GAFI relacionados con la FP para la Quinta Ronda de evaluaciones, buscando una mejor comprensión de los riesgos y una mejora en la coordinación. En particular, la Recomendación 1 se actualizó para exigir que los países y las entidades del sector privado identifiquen, evalúen, comprendan y mitiguen los riesgos de financiación de la proliferación, enfatizándose la necesidad de implementar medidas basadas en el riesgo para prevenir posibles incumplimientos o evasiones de las sanciones financieras dirigidas. Por otro lado, se fortaleció la Recomendación 2, para mejorar la cooperación y coordinación nacional en la lucha contra la FP de ADM.

2.2 Objetivos

En 2020 se elaboró en España un Análisis Nacional de Riesgos (en adelante, ANR) en el cual se analizaban las amenazas y vulnerabilidades en materia de BC/FT, incluyéndose un apartado específico de riesgos relativos a vulneración de las sanciones financieras internacionales, tanto las relacionadas con FT como de FP.

El ANR fue objeto de revisión y actualización en el año 2024, mediante la publicación de una adenda que incluía una revisión de este análisis. No obstante lo anterior, se ha considerado necesario profundizar en las amenazas y vulnerabilidades existentes en el país en relación con el riesgo de evasiones e incumplimientos de la implementación de sanciones financieras referidas a la FP.

Por lo tanto, el objetivo general de este documento es identificar y entender las amenazas, vulnerabilidades y riesgos en materia de evasión de las sanciones financieras en materia de FP. Dicho objetivo general se acompaña de otros objetivos específicos como:

- Diseño de una infografía que ayude a los sujetos obligados en la evaluación, análisis y determinación de los riesgos en materia de no proliferación, así como facilitar el cumplimiento de sus obligaciones en esta materia.
- Creación de programas de divulgación de los riesgos asociados a la proliferación en nuestro país que generen conciencia social sobre el impacto potencial que conllevaría la evasión de sanciones.
- Cumplimiento del Plan de Acción en materia de FP que prevé la existencia de un análisis de FP ad hoc.

3. Metodología

3.1. Instituciones Participantes

Las instituciones públicas con participación en la elaboración de este análisis han sido:

- Agencia Española de Administración Tributaria (AEAT).
- Banco de España.
- Centro Nacional de Inteligencia.
- Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO).
- Comisaría General de Información de la Policía Nacional.
- Consejo General del Poder Judicial.
- Departamento de Seguridad Nacional.
- Dirección General de Política Exterior y Seguridad.
- Fiscalía General del Estado.
- Fiscalía de la Audiencia Nacional.
- Fiscalía Especial contra la Corrupción y la Criminalidad Organizada.
- Jefatura de Información de la Guardia Civil (JI).
- Secretaría de Estado de Seguridad.
- Secretaría General del Tesoro y Financiación Internacional.
- Servicio Ejecutivo de Prevención de Blanqueo de Capitales (Sepblac).
- Subdirección General de Comercio Internacional de Material de Defensa y Doble Uso.

Además, se creó un grupo de trabajo con participantes del sector privado donde estuvieron presentes las siguientes instituciones:

- Asociación Española de Banca (AEB).
- Banco Bilbao Vizcaya, S.A.
- Banco Santander, S.A.
- Banco de Crédito Social Cooperativo, S.A.
- CaixaBank, S.A.
- CecaBank, S.A.
- Confederación Española de Cajas de Ahorros (CECA)
- Deustche Bank, S.A.
- Unión Nacional de Cooperativas de Crédito (UNACC).

3.2. Fuentes de información

Se han tenido en consideración los siguientes documentos:

- Análisis Nacional de Riesgos de España de 2020 así como la Adenda de 2024.
- Guía Ejecutiva de No Proliferación y Desarme de 2022.
- Estrategia de Seguridad Nacional de 2021.
- CCN-CERT. Ciberamenazas y Tendencias. Edición 2024.
- Money Laundering National Risk Assessment Guidance 2024 del GAFI.
- Guidance on Proliferation Financing Risk Assessment and Mitigation de 2021 del GAFI.
- Complex Proliferation Financing and Sanctions Evasion Schemes, GAFI, 2025.
- Informes de Grupos de Expertos establecidos en virtud de las Resoluciones.
- Consultas efectuadas a las distintas autoridades competentes en cada uno de los ámbitos de actuación y documentos elaborados por las mismas, en algún caso, de naturaleza clasificada.

3.3. Definiciones y metodología

A continuación, se detallan las definiciones de los principales conceptos que van a ser utilizados a lo largo de este análisis:

- **Financiación de la Proliferación**[1] es todo acto que **provea fondos o utilice servicios financieros**, en todo o en parte, para la fabricación, adquisición, posesión, desarrollo, exportación, trasiego de material, fraccionamiento, transporte, transferencia, depósito o uso de armas nucleares, químicas o biológicas, sus medios de lanzamiento y otros materiales relacionados (incluyendo tecnologías y bienes de uso dual para propósitos ilegítimos) en **contravención de las leyes nacionales u obligaciones** internacionales, cuando esto último sea aplicable.

En este concepto hay que distinguir entre:

a) **Financiación directa:** implica el uso de fondos para **apoyar explícitamente actividades de proliferación**.

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Status-report-proliferation-financing.pdf

b) Financiación indirecta: es el **apoyo financiero no intencionado o disimulado** que facilita actividades de proliferación.

Atendiendo a estas definiciones se ha utilizado la metodología establecida en la "*Guía para la evaluación y mitigación de riesgos de financiación de la proliferación de GAFI*". Esta guía propone la combinación de la identificación de los siguientes factores:

(i) de las amenazas existentes en España,
(ii) de las vulnerabilidades del sistema y el contexto del país que permiten a esas amenazas desarrollar sus actividades y
(iii) de los sectores (económicos y no económicos) y los tipos de entidades y estructuras jurídicas que pueden ser utilizados o explotados por esas amenazas para perpetrar actividades de FP aprovechando las vulnerabilidades existentes respecto de la evasión de sanciones financieras.

Según GAFI, cuando define "**amenazas**" de FP se refiere a las "*personas y entidades designadas que han causado previamente o con potencial para evadir, incumplir o explotar un fallo en la aplicación de PF-TFS en el pasado, presente o futuro. Dicha amenaza también puede ser causada por aquellas personas o entidades que actúen para o en nombre de personas o entidades designadas. Puede tratarse de una amenaza real o potencial. No todas las amenazas presentan el mismo nivel de riesgo para todos los países y empresas del sector privado."*

Teniendo en cuenta que las amenazas tienen propósitos delictivos y de carácter desestabilizador, su análisis debe tener principalmente un enfoque desde el punto de vista represivo, a partir de su evaluación por parte de las autoridades competentes en la investigación y procesamiento de las actividades delictivas, como son las autoridades policiales (Guardia Civil, Dirección General de la Policía Nacional o policías autonómicas), el CITCO, el CNI, la Fiscalía General del Estado, los jueces y tribunales o la Agencia Estatal de Administración Tributaria en materia aduanera y fiscal.

Por su parte, las "**vulnerabilidades**" son aquellas situaciones y circunstancias *"que pueden ser explotadas por la amenaza o que pueden apoyar o facilitar la violación la no aplicación o la evasión de la FP"*.

El análisis individualizado del impacto que esas vulnerabilidades suponen un estudio en cada uno de los diferentes sectores financieros y no financieros: sus actividades, los tipos societarios y otros elementos y operaciones susceptibles de ser utilizados por las distintas amenazas para fines de FP, que conducen a una valoración del nivel de riesgo de cada uno de ellos.

Siguiendo el sistema de calificación establecido en el artículo 12.3 del Reglamento (UE) 2024/1620 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, por el que se crea la Autoridad de Lucha contra el Blanqueo de Capitales y la Terrorismo, los niveles de riesgo inherente y residual tendrán la siguiente calificación:

- Bajo
- Medio
- Sustancial
- Alto

4. Arquitectura institucional sobre proliferación

4.1. Instrumentos internacionales

4.1.1 Instrumentos internacionales con competencias en materia de financiación de la proliferación con participación de España.

Naciones Unidas

El CSNU tiene un enfoque de dos niveles para contrarrestar la FP a través de resoluciones adoptadas en virtud del Capítulo VII de la Carta de las Naciones Unidas y que, por tanto, imponen obligaciones a los Estados Miembros de la ONU:

(i) **Enfoque global en virtud de la RCSNU 1540 (2004) y sus resoluciones sucesoras:**

Esta Resolución y sus posteriores prohíben la financiación de actividades relacionadas con la proliferación por parte de agentes no estatales y exigen a los países que establezcan, desarrollen, revisen y mantengan controles adecuados sobre el suministro de fondos y servicios, como la financiación, relacionados con la exportación y el transbordo de artículos que puedan contribuir a la proliferación de ADM.

El objetivo de esta Resolución es que se tomen medidas efectivas para evitar la proliferación y el uso de ADM por parte de agentes no estatales, especialmente grupos terroristas.

A raíz de esta Resolución se creó, en 2004, el **Comité de la Resolución 1540**, compuesto por los 15 Estados que formen el CSNU. Su finalidad es comprobar que los Estados se abstienen de prestar cualquier tipo de apoyo a los agentes no estatales que traten de desarrollar, adquirir, fabricar, poseer, transportar, transferir o emplear armas nucleares, químicas o biológicas y sus sistemas vectores.

(ii) **Enfoque específico por país:**

Actualmente existen dos regímenes de sanciones del CSNU con enfoque específico por país: el primero es el establecido mediante la **Resolución 1718 (2006) y sus sucesivas, dirigidas contra Corea del Norte**, en respuesta a sus ensayos nucleares y de misiles balísticos, que imponen un amplio embargo de armas, restricciones financieras, comerciales y de transporte.

El segundo corresponde a la **Resolución 1737 (2006) y sucesoras, dirigidas contra Irán.** Si bien la Resolución 2231 (2015), relativa al refrendo por parte de Irán del JCPOA suspendió las sanciones financieras del CSNU impuestas por las Resoluciones 1737 (2006), 1747 (2007), 1803 (2008) y 1929 (2010), manteniendo ciertas restricciones específicas, el 27 de septiembre de 2025 el CSNU decidió reinstaurar sanciones dirigidas. Ello en aplicación del llamado mecanismo "*snap-back"*, previsto en la propia Resolución 2231 y que implica que se vuelvan a imponer la prohibición de transferencias de armas y materiales relacionados con programas nucleares y de misiles balísticos, la congelación de activos y restricciones de viaje a personas y entidades vinculadas al régimen, así como limitaciones financieras y comerciales destinadas a impedir el apoyo directo o indirecto a sus programas de proliferación.

4.1.2. Organismos internacionales con competencias en materia de proliferación con participación de España

(i) Organización de las Naciones Unidas.

Además de las resoluciones mencionadas, la ONU cuenta con diferentes instituciones cuya misión es garantizar el desarme a nivel global:

- Oficina de Asuntos de Desarme (UNODA)
- Conferencia de Desarme
- Comisión de Desarme
- Instituto de Naciones Unidas para la Investigación en materia de Desarme (UNIDIR)

(ii) Unión Europea

La Unión Europea (en adelante, UE) cuenta con la "*Estrategia de la UE contra la proliferación de ADM*", de 2003, en la que se propone integrar todos los instrumentos disponibles dentro de la UE para prevenir y detener la proliferación de ADM. Las medidas de no proliferación se aplican principalmente a través de dos regímenes específicos:

- **El Reglamento (UE) 267/2012 del Consejo, de 23 de marzo de 2012, relativo a medidas restrictivas contra Irán**, con mención especial a la Decisión (PESC) 2025/1978, que modifica la Decisión 2010/413/PESC cuyo objetivo es la reintroducción en la UE sin demora de todas las sanciones nucleares suspendidas

ante incumplimientos del PAIC, así como los demás instrumentos jurídicos aprobados el 29 de septiembre de 2025 y que modifican el Reglamento (UE) 267/2012.

- **El Reglamento (UE) 2017/1509 del Consejo, de 30 de agosto de 2017, relativo a medidas restrictivas contra la República Popular Democrática de Corea**, que consolida las sanciones a este país imponiendo un embargo total de armas, restricciones de exportación e importación, limitaciones financieras, prohibiciones de viaje y congelación de activos.

(iii) OTAN

La OTAN no posee competencias jurídicas directas para regular o sancionar la Financiación de la Proliferación, ya que el Tratado del Atlántico Norte no contempla funciones en materia financiera o sancionadora. Sin embargo, su actuación se fundamenta indirectamente en los artículos 4 y 5 del Tratado, que le permiten abordar cualquier amenaza a la seguridad de los Estados miembros, incluida la proliferación de armas de destrucción masiva y las redes que la financian.

(iv) Organización para la Seguridad y Cooperación Europea (OSCE)

No existe un tratado específico que confiera a la OSCE competencias en financiación de la proliferación. Su papel deriva de compromisos políticos que le permiten apoyar la implementación de resoluciones de la ONU y fortalecer capacidades de los Estados participantes, sin funciones regulatorias ni sancionadoras propias. Entre estos compromisos destaca la firma en Maastricht (2003) de la Estrategia de la OSCE para Enfrentar las Amenazas a la Seguridad y la Estabilidad del Siglo XXI donde se reconoce la proliferación de ADM y las redes que la financian como amenazas y compromete a los Estados a cooperar para impedirlas.

(v) Iniciativa de Seguridad contra la Proliferación (PSI)

Lanzada en 2003, busca prevenir el tráfico ilícito de ADM, sus vectores de lanzamiento y materiales relacionados, hacia y desde Estados y actores no estatales, poniendo énfasis

en la interceptación del tráfico ilícito. Cuenta con un núcleo de 23 países participantes que se reúnen anualmente en el llamado Grupo de Expertos Operacionales y sirve como foro para discutir y desarrollar conceptos para mejorar las capacidades de los Estados miembros en los ámbitos legales y operativos.

4.1.3. Tratados y compromisos internacionales suscritos por España en materia de proliferación

España ha ratificado diversos tratados y compromisos internacionales en materia de armas nucleares, armas químicas y armas biológicas:

(i) Tratado de No Proliferación de las Armas Nucleares (TNP).
(ii) Tratado de Prohibición de las Armas Nucleares (TPAN).
(iii) Tratado de Prohibición Completa de Ensayos Nucleares (TPCEN).
(iv) Tratado de Prohibición de Producción de Material Fisible (FMCT).
(v) Iniciativa de Estocolmo para el Desarme Nuclear.
(vi) Iniciativa Global contra el Terrorismo Nuclear (IGTN).
(vii) Grupo de Suministradores Nucleares (GSN).
(viii) Convención sobre las Armas Químicas (CAQ).
(ix) Organización para la Prohibición de las Armas Químicas (OPAQ) Partenariado Internacional contra la Impunidad por el Uso de Armas Químicas.
(x) Convención de Armas Bacteriológicas y Toxínicas (CABT).
(xi) Mecanismo del Secretario General para la Investigación del Presunto Empleo de Armas Químicas, Biológicas o Toxínicas (UNSGM).

4.2. Estructura nacional

4.2.1 Arquitectura institucional en materia de No Proliferación

En materia de No Proliferación, destacan dos órganos importantes con competencias a nivel nacional:

Por un lado, **el Comité Especializado de No Proliferación,** creado por Orden PRA/29/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se crea y regula el Comité Especializado de no proliferación de armas de destrucción masiva. Es un órgano de apoyo al Consejo de Seguridad Nacional, de los

previstos en el artículo 20.3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, al que le corresponde ejercer las funciones asignadas por aquel en el ámbito de la no proliferación de ADM y en el marco del Sistema de Seguridad Nacional.

Por otro lado, la **Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Doble Uso (JIMDDU)**[2]. Es el máximo órgano nacional de evaluación de las operaciones relativas al comercio exterior del material de defensa y doble uso, cuya presidencia recae en la Secretaría de Estado de Comercio. La JIMDDU tiene un papel esencial en la materia, por cuanto es la encargada de informar, con carácter preceptivo y vinculante, las autorizaciones administrativas para transferencias de material de defensa, de otro material[3] y de productos y tecnologías de doble uso.

4.2.2 Arquitectura institucional y marco normativo en materia de financiación de la proliferación

El Comité Especializado de No Proliferación de ADM, en su reunión de 20 de julio de 2022, aprobó la creación del **Grupo de Trabajo de Financiación de la Proliferación,** sobre las nuevas obligaciones impuestas por el GAFI sobre FP.

En julio de 2024, presentó un proyecto de Plan Nacional contra la Financiación de la Proliferación de ADM. Éste fue elevado al Comité de No Proliferación para su valoración y aprobación, en sesión de 23 de abril de 2025. Posteriormente, el Consejo de Seguridad Nacional hizo lo propio con fecha 14 de julio de 2025, y se elevó al Consejo de Ministros. Finalmente, el Plan fue publicado en el BOE como Orden PJC/1028/2025, de 10 de septiembre por la que se publica el Acuerdo del Consejo de Ministros de 26 de agosto de 2025, por el que se aprueba el Plan Nacional contra la Financiación de la Proliferación de Armas de Destrucción Masiva.

Por lo que al marco normativo de la financiación de la proliferación respecta, el artículo 42 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, incluye provisiones específicas para garantizar la aplicación de sanciones financieras internacionales. Éstas se complementan con el desarrollo

[2] Creada por la Ley 53/2007, de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso. En la sección 3 de esta Ley se regula su estructura y funciones.
[3] Armas de caza y deportivas, equipamiento policial y antidisturbios e instrumentos destinados a tortura y pena de muerte

contenido en los artículos 47 a 49 del Reglamento de la Ley 10/2010, de 28 de abril, aprobado por Real Decreto 304/2014, de 5 de mayo.

Este marco se ve complementado a nivel europeo por lo establecido en el Reglamento (UE) 2024/1624 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.

4.3. Relaciones diplomáticas de España con la RPDC e Irán

El 15 de diciembre del 2000, el Consejo de Ministros dio luz verde al establecimiento de relaciones diplomáticas con la RPDC. España mantiene formalmente relaciones diplomáticas con Pyongyang desde el 7 de febrero de 2001, una decisión adoptada juntamente con el resto de los Estados Miembros de la UE, excepto Francia.

Las relaciones se canalizan desde 2006 en régimen de acreditación múltiple desde la Embajada de España en Seúl. Corea del Norte abrió embajada residente en Madrid en octubre de 2013 y la cerró en octubre de 2023. En la actualidad, es la Embajada de la RPDC en Roma la acreditada para llevar los asuntos de España.

En el caso iraní, España mantiene relaciones diplomáticas con Irán desde 1950. La Embajada de España en Teherán abrió en 1951, consolidando los canales diplomáticos y consulares bilaterales. Por parte iraní, la Embajada de Irán en Madrid funciona desde 1956, manteniendo actividad diplomática permanente.

Durante las últimas décadas, la relación se ha desarrollado dentro del marco general de la política exterior de la Unión Europea hacia Irán, especialmente en ámbitos como el diálogo político, la cooperación económica y la aplicación del régimen de sanciones de la UE y Naciones Unidas.

En la actualidad, las relaciones se canalizan a través de ambas embajadas (España en Teherán e Irán en Madrid), así como mediante la coordinación diplomática y consular dentro de la UE. Aunque la relación bilateral ha experimentado diferentes fases de intensidad debido al contexto regional e internacional, los canales diplomáticos permanecen abiertos y operativos con restricciones.

5. Principales amenazas en materia de financiación de la proliferación

5.1. Amenazas a nivel internacional

Según la Guía del GAFI sobre Evaluación y Mitigación del Riesgo de FP, los factores que se deben analizar dentro de las amenazas se agrupan en torno a la identificación de personas o entidades designadas, las actividades que realizan y las formas en que intentan evadir las sanciones financieras dirigidas**.**

El documento *Complex Proliferation Financing and Sanctions Evasion Schemes* (GAFI, junio 2025)[4] menciona los principales **factores agravantes para la FP de la RPDC** y su programa de ADM: la creciente conectividad financiera de la RPDC y la diversidad de sus fuentes de generación de ingresos.

En cuento al primer factor, Rusia es uno de los principales actores relevantes. En concreto, Rusia firmó en 2024 el Tratado de Asociación Estratégica Integral con la RPDC[5].

Por lo que respecta al segundo factor, en cuanto a la diversificación de fuentes para generar ingresos, han cobrado importancia los ciberataques y robos de criptoactivos.

Las amenazas internacionales identificadas con Irán se centran en el uso de redes de evasión de sanciones que incluyen el contrabando de petróleo, la utilización de casas de cambio y bancos extranjeros, así como complejas tramas de empresas pantalla y proveedores de servicios fiduciarios que facilitan la ocultación de la titularidad real y la adquisición de bienes de doble uso.

[4] www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf
[5] http://en.kremlin.ru/acts/news/75534

Cuadro 1. Amenazas internacionales FP de ADM

TIPO DE AMENAZA	DESARROLLO	EVIDENCIA
Representantes del sistema	Habitualmente representantes del sector bancario que actúan a través de aliados financieros en jurisdicciones intermedias para movilizar fondos. Uso de casas de cambio en Emiratos Árabes Unidos y Turquía, con utilización de esquemas tipo *hawala.*	*RPDC: Sim Hyon Sop*, representante de la *Korea Kwangson Banking Corporation* (KKBC), recibió más de 24 millones de dólares en criptoactivos, de los cuales la mitad procedía de trabajadores de tecnología norcoreanos que, utilizando identidades falsas, obtuvieron empleos en empresas tecnológicas (incluidas de EE. UU.) y exigieron pagos en monedas virtuales. *Irán:* de red de casas de cambio en Dubái que, actuando en nombre del Banco Central de Irán y del IRGC-*Qods Force*, procesaba los ingresos derivados de exportaciones de petróleo y los transfería a través de bancos corresponsales extranjeros, ocultando así su verdadero origen y destino.
Empresas pantalla y estructuras societarias opacas	Falta de transparencia de la titularidad real, carácter transnacional que permite la operativa en diferentes divisas y ocultación de la naturaleza real de la operativa. Triangulación en la operativa de compra de material de doble uso por empresa pantalla en un tercer país intermediario y pago desde una entidad financiera ubicada en otro tercer país. Países intermediarios identificados de	*RPDC*: *Glocom* (Malasia) empresa fachada de la RPDC dedicada a la venta encubierta de equipos de comunicaciones militares. *Stroytreyd LLC* (Moscú) identificada en 2023–2024 como pantalla para recuperar fondos de bancos rusos en quiebra y transferirlos a la RPDC, con apoyo de la *Russian Financial Corporation* y *Timer Bank*. *Irán*: *Shiraz Electronics Industries* (SEI) y *Rayan Roshd Afzar* son empresas iraníes identificadas por el desarrollo de misiles

	riesgo: Rusia, Hong Kong y Emiratos Árabe	y drones. Están vinculadas la a operativa de 4 ciudadanos chinos que utilizaron empresas pantalla en China para canalizar artículos de doble uso de origen estadounidense hacia estas entidades sancionadas.
Ciberataques	Uso de criptoactivos y plataformas de finanzas descentralizadas (DeFi), como mixers, exchanges no regulados y tokens de anonimato.	Lazarous Group. Uso de ransomware como Maui[6] y H0lyGh0st[7].
Manipulación del transporte marítimo	Operativa de proliferación con impacto patrimonial. Transbordos barco a barco en alta mar y la falsificación de documentación de carga. Importación de productos petroleros que generan ingresos mediante exportación ilegal de carbón.	*RPDC*: Investigaciones independientes de C4ADS[8] y reportes del Departamento del Tesoro de EE.UU. *Irán*: en 2021 una empresa estadounidense falsificó documentos de exportación para desviar componentes clasificados como bienes de doble uso hacia un país de alto riesgo vinculado al programa nuclear iraní. Uso de empresas pantalla, documentación adulterada y estructuras fraudulentas de importación/exportación para ocultar la titularidad real y el destino final de los productos.
Contrabando y el tráfico de bienes de gran valor	Actividades asociadas a organizaciones criminales.	*RPDC*: el Panel de Expertos de Naciones Unidas (2024[9]) documentó operaciones de contrabando de marfil y cuerno de rinoceronte procedentes de África; tráfico de metanfetaminas y armas

[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a
[7] https://www.microsoft.com/en-us/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/
[8] C4ADS, Risky Business: A System-Level Examination of North Korea's Proliferation Financing and Sanctions Evasion Networks, 2019, https://c4ads.org/s/RiskyBusiness.pdf
[9] https://docs.un.org/en/S/2024/215

		ligeras coordinadas por representantes en el extranjero, cuyos ingresos fueron canalizados hacia el programa nuclear y de misiles. Irán: contrabando de petróleo, oro y bienes de lujo a través de intermediarios en Emiratos Árabes Unidos, Turquía y Asia Oriental (Departamento del Tesoro de EE. UU[10]).

5.2. Amenazas detectadas en el marco nacional

En el caso de España, de la información proporcionada por el sector público y privado en cuanto a amenazas relacionadas con la FP de ADM, se desprende que las tipologías de evasión mencionadas en el punto anterior son difíciles de identificar de forma directa.

En el caso español debe mencionarse a jurisdicciones intermedias que generan amenazas en relación con la FP debido la canalización de fondos o la realización de operaciones internacionales con empresas exportadoras de materiales de estas jurisdicciones. Esta última operativa se va a analizar dentro del impacto patrimonial que tienen las operativas sospechosas sobre proliferación, ilustrando especialmente aquellas que han terminado en investigación con una posible resolución de sentencia.

[10] https://home.treasury.gov/news/press-releases/sb0082?utm_source=chatgpt.com

Cuadro 2. Amenazas nacionales FP de ADM vinculadas a RPDC

TIPO DE AMENAZA	DESARROLLO	EVIDENCIA
Actores designados	Son representantes o facilitador de actividades vinculadas a RPDC. Intermediación en contactos o negocios que faciliten los flujos monetarios. Captación de seguidores.	No hay evidencias de actividad en España. No hay censo de norcoreanos en España.
Cibercriminalidad	Canalización de fondos para FP a través de ciberataques y ciberestafas. Ciberespionaje.	Grupo Lazarus: - WannaCry 2017. Estimación de 600 compañías españolas que pudieron haber sido afectadas por el ataque. - Ciberespionaje a empresa aeroespacial española (2021-2022).

Cuadro 2. Amenazas nacionales FP de ADM vinculadas a Irán

TIPO DE AMENAZA	DESARROLLO	EVIDENCIA
Creación de cuentas en países intermediarios	Canalización de fondos mediante la implicación de otros países.	Cuentas creadas con intereses iraníes en Suiza, Hong Kong, Turquía o Emiratos Árabes Unidos.

Uso de sociedades pantalla	BC con figuras empresariales ficticias. Evasión fiscal. Daños en la economía nacional.	Gestión de cuentas en el extranjero por casas de cambio (a nombre de sociedades pantallas que realizan la venta por cuenta de sociedades sancionadas) o profesionales iraníes.
Uso de testaferros en cobro/pagos	Evasión de controles por sanciones financieras. Daño reputacional en el caso de uso de profesionales independientes. (Especialmente aquellos que son sujetos obligados).	Compensaciones directas con cuentas bancarias específicas mediante la intermediación de profesionales que coordinan los cobros/pagos de las mercancías sin que exista una transferencia directa desde o hacia Irán.
Compra de inmuebles por iraníes	Posibilidad de encubrir actores que movilicen fondos con fines de FP.	En España, se han comunicado operaciones, pero las unidades policiales encargadas de la investigación para BC/FT no han encontrado indicios.

Las operativas vinculadas a la proliferación de ADM tienen asociado un flujo monetario que hace que se vincule indirectamente con la FP, es por ello que las FCSE realizan una investigación patrimonial asociada a la operativa.

Cuadro 3. Amenazas nacionales de proliferación con vínculos en FP.

TIPO DE AMENAZA	DESARROLLO	EVIDENCIA
Utilización de países intermediarios	Comercio de bienes de doble uso.	Operativas de cobro y pago desde/hacia España con sociedades de China, Hong Kong, Turquía.
Uso de sociedades pantalla para el desvío de material de defensa y sustancias químicas prohibidas	Operaciones de BC asociadas a la operativa y posibilidad de vulneración de controles aduaneros.	Desvió material aeronáutico y de doble uso antes de su exportación a Rusia. Volumen inusual de ventas y transferencias financieras irregulares.
Organización criminal	Operativa de comercio de doble uso, conexión con narcotráfico e intermediación de personas jurídicas europeas.	Empresa española que, entre 2013 y 2018, en colaboración con otra empresa alemana, importó e introdujo ilegalmente en España equipos de visión nocturna y térmica siendo una parte de los mismos posteriormente vendidos a organizaciones de narcotráfico en Andalucía.
Exportaciones a Irak	Operativa de comercio de doble uso, vínculos con BC e intermediación de terceros países de riesgo.	Empresa española que exportó ilegalmente a Irak equipos de radio con capacidad criptográfica..

En la Memoria de Información Estadística de la Comisión de Prevención de BC/FT[11] se publica el dato de las investigaciones sobre contra- proliferación que nacen de informes de inteligencia remitidos por el Sepblac y a iniciativa propia.

Cuadro 5. Investigaciones policiales sobre contra proliferación con informes Sepblac

	2020	2021	2022	2023	2024
Investigaciones policiales sobre contra-prolif. con informes SEPBLAC	5	10	4	15	14

Fuente: Policía y Guardia Civil

En este cuadro, las investigaciones estaban relacionadas con Rusia, Irán y Venezuela.

Cuadro 6. Investigaciones policiales sobre contra- proliferación propias

	2020	2021	2022	2023	2024
Investigaciones por propia iniciativa	70	21	30	45	40
Detenidos	37	3	3	8	11
Incautaciones (€)	3.520.882	7.000	5.405.514	1.444.263	7.430

Fuente: Policía y Guardia Civil

Las investigaciones por iniciativa propia giraban sobre operativa con Rusia, China, Pakistán e Irán.

5.3. Amenazas emergentes

En el contexto actual de creciente tensión geopolítica y rápida evolución tecnológica los mecanismos de prevención de FP deben adaptarse. Las respuestas recabadas por los distintos actores del sector privado revelan un panorama muy diverso, en el que convergen amenazas tradicionales (evasión de sanciones, uso de efectivo, empresas pantalla) y factores propios de la innovación digital y financiera (criptomonedas, ciberataques, IA, impresión 3D).

[11] https://www.tesoro.es/prevencion-del-blanqueo-y-movimiento-de-efectivo/comision-de-prevencion-del-blanqueo-de-capitales-e-infracciones-monetarias/estadisticas-e-informes/estadisticas

Cuadro 7. Amenazas emergentes identificadas por el sector privado

TIPO DE AMENAZA	HERRAMIENTAS	CARACTERÍSTICAS
Canales financieros ilícitos e innovaciones tecnológicas	Canales financieros ilícitos e innovaciones tecnológicas Sistemas de pago digitales no regulados. Inteligencia Artificial y fabricación aditiva	Hackeo de *exchanges* Pasarelas de pago alternativo y *fintech* que permiten movimientos hacia destinatarios sancionados. IA, impresión 3D o biotecnología que para eludir controles de exportación o acelerar la producción de componentes sensibles.
Ciberfraude	*Phishing/*uso de *malware*	Fraude hacia *wallets* de criptoactivos
Comercio ilícito y manipulación logística	Falsificación documental Triangulación y rutas alternativas	Facturas y licencias falsificadas para ocultar destino o titular real de los bienes exportados Uso de países intermediarios aliados de regímenes sancionados
Uso de tecnologías de bajo coste	Uso ilícito de drones	En España se han identificado riesgos específicos: presencia de drones en las inmediaciones de bases aéreas, centrales nucleares o prisiones, pero sin poder identificar su una clara vinculación con la FP de ADM.

6. Principales Vulnerabilidades

6.1. Vulnerabilidades estructurales

6.1.1. Derivadas del marco normativo

Las sanciones internacionales aprobadas por el CSNU no son directamente aplicables en España, sino que requieren de su previa adopción por la Unión Europea.

Actualmente, España no cuenta con legislación específica en materia penal sobre FP de ADM. Sin embargo, la Unión Europea ha aprobado la Directiva (UE) 2024/1226 del Parlamento Europeo y del Consejo, de 24 de abril de 2024, relativa a la definición de los delitos y las sanciones por la vulneración de las medidas restrictivas de la Unión. Esta Directiva se encuentra en fase de trasposición al ordenamiento español .

6.1.2. Derivadas de la implementación de las sanciones del CSNU

La mayor vulnerabilidad en España evidenciada en el Informe de Evaluación Mutua de 2014 es la falta de aplicación “sin demora” de las sanciones establecidas por el CSNU. Aunque esta obligación se cumple en la práctica por la existencia de procedimientos automatizados en los sistemas preventivos de los sujetos obligados, normativamente no existe tal obligatoriedad, pues la UE tarda más de 24 horas, normalmente, en transponer las RCSNU al ordenamiento comunitario.

En el año 2019, España fue sometida a un informe de recalificación de la efectividad de GAFI por la que el Resultado Inmediato 11 subió su calificación de moderada a significativa. Entre las mejoras identificadas, a pesar de que sigue detectándose la vulnerabilidad mencionada en el párrafo anterior, se incrementó la capacidad para identificar y perseguir la evasión de sanciones financieras relacionadas con la FP a través de las investigaciones de las FCSE y la supervisión del Sepblac.

Por otro lado, en la actualidad, el Mandato del Panel de expertos sobre Corea del Norte no fue renovado, por lo que permanece inactivo desde abril de 2024[12]. La disolución de este Panel de Expertos representa un desafío importante para el monitoreo de las

[12] https://press.un.org/en/2024/sc15648.doc.htm

violaciones de sanciones relativas a la RPDC, por cuanto sus informes se utilizan para elaborar estrategias de seguridad nacional y directrices o emitir instrucciones.

El Panel de Expertos sobre Irán se estableció en 2010 por la Resolución 1929 para apoyar al Comité 1737 y monitorear sanciones. Su mandato terminó en 2016, con la implementación del JCPOA y la disolución del régimen de sanciones del Consejo de Seguridad sobre Irán. Tras la reactivación de las sanciones contra Irán, la Resolución del CSNU 1929 (S/RES/1929 (2010) | Consejo de Seguridad) preveía la reactivación de este Panel si se volvían a poner en marcha las sanciones contra este país.

6.1.3. Derivadas de la ausencia de una Autoridad Nacional de Coordinación en materia de Financiación de la Proliferación

Si bien España no ha designado una única autoridad nacional de coordinación en materia de FP en los términos de la Recomendación 2 del GAFI, las competencias se vienen ejerciendo por el Comité Especializado de No Proliferación y su grupo sobre Financiación, así como por la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y sus órganos de apoyo.

6.1.4. Derivadas del cumplimiento por parte del sector privado

De la experiencia del sector privado se extrae que cada vez visualizan una mayor conexión entre las actividades de BC/FT, por lo que esta conexión persiste igualmente en la identificación de las operativas vinculadas a la FP. Aun así, es compleja la identificación de operativas vinculadas directamente con la FP, debido a la complejidad que entrañan y el nivel de sofisticación de algunos entramados empresariales que podrían tener vínculos con esta actividad.

Una de las debilidades más extendidas es la **menor concienciación y formación específica** sobre los riesgos del FP.

6.2. Vulnerabilidades contextuales o geográficas

La ubicación de España como punto de conexión entre Europa, África y América Latina constituye una ventaja comercial, pero también supone una exposición al uso potencial del territorio como plataforma logística para actividades ilícitas. Los principales puntos vulnerables de la geografía española son:

- Estrecho de Gibraltar y aduana de Algeciras, punto estratégico para el comercio internacional y para el transporte encubierto de materiales sensibles.
- Puertos de Valencia, Barcelona y Bilbao por su gran capacidad y alto volumen de tránsito. Esto plantea un desafío operativo en cuanto a la capacidad de inspección y control de mercancías.
- Ceuta, Melilla y Canarias por su proximidad a territorios con menor control aduanero.

En conclusión, la posición geográfica de España, su infraestructura logística y portuaria, su entorno regional y su papel en el comercio internacional aumentan su vulnerabilidad. Ello no implica necesariamente un riesgo alto en términos absolutos, pero exigen una vigilancia continua, una aplicación rigurosa de los controles de exportación y un refuerzo de la capacidad de detección y análisis por parte de autoridades competentes y del sector privado.

6.3. Vulnerabilidades Sectoriales

6. 3.1. Derivadas del comercio internacional

España se configura como como importante centro portuario internacional[13] debido al importante sector comercial internacional que posee. España es el cuarto país de Unión Europea con mayor volumen de tráfico marítimo de mercancías, principalmente a través del puerto marítimo de Algeciras. Los puertos de Valencia y Algeciras están dentro de los cinco puertos europeos más grandes de tráfico de grandes contenedores[14].

[13] Fuente: Anuario Estadístico del Sistema Portuario de Titularidad Estatal 2023.
[14] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Maritime_transport_of_goods_at_port_level_-_quarterly_data

En líneas generales, a Europa se exportan los volúmenes más altos, seguidos de Estados Unidos, China y Rusia. Sin embargo, a pesar del contexto geográfico de España, regiones como África, América del Sur y Oceanía presentan volúmenes considerablemente más bajos.

En términos de productos comercializados, la mercancía general continúa siendo la categoría predominante en términos de volumen, representando el 48 % del total transportado. Entre los principales bienes movilizados destacan los productos alimenticios, los químicos, los materiales de construcción, los productos siderúrgicos, además de maquinaria, herramientas y repuestos, así como frutas, hortalizas, legumbres, papel y pasta de papel.

El alto volumen de mercancías puede suponer por lo tanto una vulnerabilidad a la hora de detectar el tráfico de mercancías y, en última instancia, posibles vulneraciones de sanciones internacionales, en particular con jurisdicciones que tienen relaciones directas con la RPDC e Irán.

A continuación, se muestran los datos de comercio exterior de España con la RPDC e Irán, totales y, las partidas consideradas con un posible doble uso[15] para el periodo 2020-2024[16]:

Cuadro 8: Estadísticas comercio internacional con RPDC e Irán

	Exportaciones		Importaciones	
	Valor (miles de €)	**%**	**Valor (miles de €)**	**%**
RPDC	922,44	0,0001%	10,66	0,000001%
Irán	1.079.340,68	0,06%	523.384,74	0,03%
TOTAL ESPAÑA	1.734.649.078,98	100%	1.930.875.347,71	100%

Fuente: Datos de comercio exterior de España https://datacomex.comercio.es/Metadata/Index

[15] Se han tenido en cuenta las siguientes partidas que se publican en las estadísticas de comercio internacional: 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 59, 72, 73, 74, 75, 76, 78, 79, 80, 81, 82, 84, 85, 86, 87, 88, 89, 90, 93.

[16] En relación de partidas identificadas como potencialmente vinculadas a material de doble uso se ha realizado con carácter orientativo. Es importante destacar que la inclusión de estas categorías no implica que todos los productos comprendidos en ellas sean considerados de doble uso, sino únicamente determinados bienes, componentes o sustancias específicas conforme a la normativa aplicable. Asimismo, la cifra incorporada constituye una estimación sobrevalorada, elaborada con el objetivo de garantizar un margen de seguridad en la evaluación.

Cuadro 9: Estadísticas comercio internacional con RPDC e Irán de productos vinculados al doble uso

	Exportaciones doble uso		Importaciones doble uso	
	Valor (miles de €)	%	Valor (miles de €)	%
RPDC	425,03	0,00003%	8,15	0,000001%
Irán	850.291,17	0,06%	171.840,89	0,02%
TOTAL ESPAÑA	1.366.436.637,32	100%	1.078.776.052,21	100%

Fuente: Datos de comercio exterior de España https://datacomex.comercio.es/Metadata/Index

En cuanto a las relaciones comerciales internacionales de España con Irán y la RPDC, en los cuadros 8 y 9 anteriores se observa la escasa relevancia que tiene el comercio internacional español con estos dos países.

6. 3.2. Derivadas del sector financiero

El sector financiero español, aunque cuenta con un marco regulatorio sólido y una supervisión eficaz, enfrenta diversas vulnerabilidades en relación con la FP, derivadas de la complejidad de las operaciones financieras y de la sofisticación de las redes que buscan eludir los controles establecidos.

Por un lado, se identifica como vulnerabilidad la complejidad en la identificación de operaciones sospechosas. Además, hay actividades con productos como los criptoactivos y las transferencias internacionales mediante SWIFT en múltiples etapas, que dificultan la trazabilidad de los fondos.

Por otro lado, se han identificado como productos de riesgo las cuentas de corresponsalía bancaria con bancos extranjeros ubicados en jurisdicciones de riesgo o con controles laxos o las transferencias internacionales mediante SWIFT en múltiples etapas.

Finalmente, la menor formación y concienciación en materia de FP constituye un factor agravante generando mayores dificultades que en BC/FT para identificar y reportar operaciones sospechosas relacionadas con la proliferación.

6. 3.3. Derivadas de actividades y profesiones no financieras

En el caso de este tipo de sujetos obligados, las dificultades en cuanto a la implantación de sistemas automatizados de alertas y la detección de operativas vinculadas con la evasión de sanciones es mayor, principalmente en negocios minoristas.

Hay sectores que no perciben el riesgo de FP y pueden desconocer la regulación para determinar las listas de personas y entidades designadas vinculadas con programas de proliferación, lo que limita su capacidad para actuar como primera línea de defensa.

Asimismo, ciertas profesiones, en especial abogados, notarios o asesores fiscales, son más vulnerables a las operativas con sociedades pantallas o estructuras complejas que buscan ocultar al titular real**.** Es precisamente esta opacidad la que buscan muchas redes de proliferación para eludir controles financieros y evadir sanciones internacionales.

Otro foco de vulnerabilidad se encuentra en el comercio de bienes de alto valor y fácil movilidad, como ocurre en el sector de los joyeros o comerciantes de metales y piedras preciosas. Estos bienes pueden ser utilizados como instrumentos de pago en operaciones internacionales, sin requerir necesariamente el uso del sistema financiero tradicional. Esta característica los convierte en una posible vía para movilizar fondos relacionados con el valor de los bienes sin ser detectados.

6.4. Vulnerabilidades específicas de productos y servicios comercializados

España es el noveno país en exportaciones de armamento a nivel mundial[17] en exportación de materiales de defensa y bienes de doble uso.

En el año 2024 destaca un aumento en los valores autorizados y una baja tasa de realización (o ejecución) en comparación con otros años. En resumen, en el 2024 se tramitaron un total de 5.257 licencias de exportación entre las cuales 4.154 resultaron aprobadas, 111 denegadas y el resto desistidas, caducadas o renunciadas. Los productos que se comercian son[18]:

[17] Fuente: Banco Mundial. Según el SIPRI (Stockholm International Peace Research Institute), España sería el noveno exportador mundial en el periodo 20-24 y undécimo en el año 2024.
[18] Fuente: Ministerio de Economía, Comercio y Empresa

Material de defensa

El valor total de material autorizado fue de 17.395 millones de €, lo que representa un incremento del 11% con respecto al año anterior. Se expidieron 2.439 licencias, con un aumento respecto al año anterior del 23%. El valor total de las exportaciones realizadas en 2024 sumó 3.491 millones de € (un 7% menos respecto a 2023). La categoría de "aeronaves" fue la más destacada en términos de valor, tanto en autorizaciones como en exportaciones. Geográficamente, la Unión Europea y la OTAN fueron los principales destinos, abarcando el 64,6% del total. Alemania y Gran Bretaña fueron los mayores receptores, enfocándose en aeronaves munición y transferencia de tecnología. Se observa una creciente tendencia en la transferencia intangible de tecnología, software y formación técnica, lo que consolida a España como un actor clave en proyectos de I+D en defensa europea.

Material policial y de seguridad

Las autorizaciones disminuyeron su valor drásticamente de 4,2 millones de € en 2023 a 1,5 millones de € en 2024, reflejando una menor demanda. A pesar de esto, las exportaciones realizadas aumentaron a 2,2 millones de €, superando el valor autorizado en 2024 debido a licencias del año anterior, alcanzando una excepcional tasa de realización del 147% (debido a las licencias vigentes expedidas el año anterior).

Armas de caza y deportivas

Las autorizaciones casi se duplicaron, pasando de 354 millones de € a 695 millones de €, lo que sugiere una mayor demanda potencial y agilidad en la expedición de licencias. No obstante, las exportaciones realizadas se mantuvieron estables en 137 millones de €, con una tasa de realización de aproximadamente el 20%.

Productos y tecnologías de doble uso

Las exportaciones realizadas de productos y tecnologías de Doble Uso se redujeron un 26% respecto al año anterior, alcanzando los 293 millones de €. Por otro lado, el número de licencias autorizadas aumentó un 50%, llegando a 1.249, aunque el valor autorizado total disminuyó un 60% a 1.315 millones de €. La tasa de realización o ejecución fue del 22%. Además, se aprecia una tendencia creciente en el número de licencias autorizadas en los últimos 8 años. Los principales destinos por valor exportado fueron Arabia Saudí (63,6 millones de €), Francia (31,5 millones de €), China (39,8 millones de €) y Estados Unidos (16,7 millones de €). Los productos más exportados abarcan una gran diversidad, desde reactivos de laboratorio y explosivos hasta componentes aeroespaciales, software

de simulación y sistemas anti-drones, mostrando una estrategia exportadora orientada a diversos sectores tecnológicos e industriales.

Uso de drones[19]

El uso de drones genera vulnerabilidades en la seguridad nacional, con posibles efectos que incluyen la alteración de operaciones militares, el espionaje o la utilización de drones como medio para sortear controles de exportación y financiar actividades proliferadoras.

En resumen, 2024 se caracterizó por un incremento notable en las autorizaciones de licencias en Material de Defensa y Doble Uso y la baja tasa de realización en general, aunque la mayoría de las licencias solicitadas puedan ejecutarse en años posteriores.

[19] Informe Anual de Seguridad Nacional 2024

6.5. Resumen de vulnerabilidades

Cuadro 10. Vulnerabilidades

Vulnerabilidad		Variables	Consecuencias
Vulnerabilidad principal	**Tipología**		
Vulnerabilidades estructurales	Derivadas del marco normativo	Normativa Europea de trasposición directa a España. Sanciones por no congelación de fondos. Carencia de legislación penal.	La dependencia de la normativa europea puede producir lapsos en la adopción de la normativa internacional a nivel nacional; la ausencia de un régimen sancionador penal específico reduce el efecto disuasorio y dificulta investigar violaciones graves de sanciones; y el régimen sancionador actual centrado en la no congelación de fondos como infracción administrativa, limita en procedimiento sancionador en materia de sanciones financieras internacionales.
	Derivadas de la implementación de las sanciones del CSNU	Ausencia de marco normativo nacional que establezca regulatoriamente la aplicación "sin demora".	Aunque se cumple en la práctica por la existencia de procedimientos automatizados en los sistemas preventivos de los sujetos obligados, no está establecida de forma literal tal y como se exige en el Resultado Inmediato 11.

	Derivadas de la ausencia de una Autoridad Nacional de Coordinación	No hay una autoridad designada por regulación.	Se están ejerciendo todas las competencias exigidas por la metodología de GAFI a este respecto por la S.G. de Inspección y Control de Movimientos de Capitales del Tesoro Público.
	Derivadas del cumplimiento por parte del sector privado	Dificultad de identificación de operativas directamente relacionadas con la FP. Menor concienciación sobre los riesgos del FP, especialmente en sectores no financieros que cuentan con sistemas de monitoreo menos sofisticados.	Incremento de gasto preventivo de los sujetos obligados en identificar este tipo de operativa. Vulneración de los controles implantados por los sujetos obligados.
Vulnerabilidades contextuales o geográficas		Posición geográfica de España ligada a su infraestructura logística y portuaria: • Estrecho de Gibraltar y aduana de	Desafío operativo en cuanto a la capacidad de inspección y control de mercancías y, por lo tanto, en el análisis patrimonial que conlleva esta operativa.

		Algeciras, punto estratégico para el comercio internacional y para el transporte encubierto de materiales sensibles. • Puertos de Valencia, Barcelona y Bilbao por su gran capacidad y alto volumen de tránsito. • Ceuta, Melilla y Canarias por su proximidad a territorios con menor control aduanero.	
Vulnerabilidades Sectoriales	Derivadas del comercio internacional	Algeciras y Valencia puerto importantes en el tráfico de grandes contenedores. Algeciras cuarto puesto en importancia respecto al volumen de mercancía.	Ocultación de mercancías ilícitas dentro de grandes volúmenes de importaciones/exportaciones cuya finalidad sea la FP.

	Derivadas del sector financiero	Complejidad en la identificación de operaciones sospechosas por la vinculación de operativas de BC/FT con FP. Productos de riesgo como las cuentas de corresponsalía bancaria con bancos extranjeros ubicados en jurisdicciones de riesgo o con controles laxos o las transferencias internacionales mediante SWIFT en múltiples etapas. Operativa con cripto ligada a la evasión de sanciones.	Uso de criptoactivos para movilizar fondos, especialmente las plataformas de finanzas descentralizadas. Ocultación del delito subyacente para evadir sanciones. Operativas y productos que dificultan la transparencia de los intervinientes y de la naturaleza de las operaciones.
	Derivadas de APNFD	Profesionales que actúan como intermediarios de estructuras accionariales o que intervienen en operativas vinculadas a actos societarios, especialmente	Dificultad en la identificación del titular real Utilización de profesionales como instrumentos para la evasión de sanciones.

		cuando el interviniente no se ha constituido en España o es parte de una estructura compleja. Comercio de bienes de alto valor y fácil movilidad usados como pago en transacciones comerciales internacionales.	Facilidad de movimientos de fondos cuando se emplean bienes de lujo.
Vulnerabilidades específicas de productos y servicios comercializados		Los productos comercializados vulnerables son: material de defensa, material policial y de seguridad, armas de caza y deportivas, productos y tecnologías considerados de doble uso y uso de drones.	Dado los volúmenes comercializados pueden encubrir amenazas ligadas a la FP. El uso de drones ocasiona vulnerabilidades en la seguridad nacional además de tener una operativa económica ligada a la FP.

7. Riesgos

7.1. Riesgos inherentes

El análisis de las amenazas y vulnerabilidades y las escasas evidencias vinculadas a la FP determina una calificación del **riesgo inherente en España para la FP medio-bajo.**

Se ha realizado una matriz de riesgo con el objetivo de identificar que sujetos obligados están sometidos a un mayor riesgo de FP.

El artículo 10.3 del Reglamento (UE) 2024/1624 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, establece que *"A excepción de las entidades de crédito, las entidades financieras, los proveedores de servicios de financiación participativa y los intermediarios de financiación participativa, los supervisores podrán decidir que no se requieren evaluaciones de riesgos documentadas de toda la actividad de negocio de cada una de las entidades obligadas si los riesgos específicos inherentes al sector están claros y se han comprendido"*

El riesgo inherente por sector se puede visualizar en la siguiente tabla:

Cuadro 11. Riesgo inherente sectorial

Letra	Sujeto Obligado	Riesgo Inherente
a	Entidades de crédito	
b	Entidades aseguradoras ramo vida / inversiones y corredores de seguros	
c	Empresas de servicios de inversión	
d	Sociedades gestoras de IIC y sociedades de inversión sin gestora	
e	Entidades gestoras de fondos de pensiones	
f	Sociedades gestoras de ECR y sociedades de capital-riesgo sin gestora	
g	Sociedades de garantía recíproca	
h	Entidades de dinero electrónico y entidades de pago	
i	Personas que ejerzan profesionalmente actividades de cambio de moneda	
j	Servicios postales en actividades de giro o transferencia	
k	Intermediarios en concesión de préstamos o créditos	
l	Promotores inmobiliarios y agentes en compraventa/arrendamientos ≥120.000€/10.000€ mes	
m	Auditores, contables externos, asesores fiscales y quienes presten asistencia fiscal	
n	Notarios y registradores	
ñ	Abogados, procuradores y profesionales en operaciones financieras/inmobiliarias	
o	Prestadores de servicios a terceros	
p	Casinos de juego	
q	Comercio profesional de joyas, piedras o metales preciosos	
r	Comercio profesional de arte/antigüedades e intermediarios, incluidos puertos francos	
s	Actividades Ley 43/2007 (bienes con oferta de restitución del precio)	
t	Depósito, custodia o transporte profesional de fondos o medios de pago	
u	Gestión/explotación/comercialización de loterías y juegos de azar	
y	Gestores de sistemas de pago y compensación/liquidación, gestores de tarjetas	
z	Proveedores de cambio de moneda virtual por fiduciaria y custodia de monederos	
-	Resto de proveedores de servicios de criptoactivos	

Leyenda

Alto	Alto/ Sustancial	Sustancial	Sutancial/ Medio	Medio	Medio/ Bajo	Bajo

7.2. Medidas mitigadoras

7.2.1. Medidas mitigadoras Institucionales

En el caso de la UE, la política en relación con la RPDC se articula bajo el principio de *critical engagement*, que combina sanciones multilaterales y autónomas con disposición al diálogo, siempre con el objetivo de la desnuclearización verificable y la preservación del régimen internacional de no proliferación. España se alinea con este enfoque, limitándose al cumplimiento del marco sancionador y de control establecido en la UE.

En relación con Irán, el control en la UE se ha reforzado tras el "*snap-back*" de sanciones en 2025, traducido en la modificación del Reglamento (UE) 267/2012. Esto implica la reintroducción de restricciones financieras, la inmovilización de fondos y la prohibición de transferencias a entidades designadas, junto con un refuerzo de los mecanismos de supervisión y transparencia. España ejecuta y controla estas disposiciones, garantizando la congelación efectiva de fondos y el bloqueo de transferencias de tecnología sensible, lo que constituye la principal medida mitigadora normativa actual frente a la FP iraní.

Respecto a los posibles acuerdos de cooperación, la UE mantiene un marco de diálogo limitado tanto con RPDC como con Irán, pero siempre sujeto a estrictas salvaguardas. En el caso norcoreano, no existen proyectos de cooperación bilaterales con España y el comercio es prácticamente inexistente debido a sanciones y restricciones. En el caso iraní, los canales diplomáticos permanecen abiertos en la UE y en España, aunque con un alcance muy restringido. La cooperación se limita a intercambios diplomáticos.

A nivel nacional, España cuenta con grupos especializados dependientes de Seguridad Nacional, como se ha podido ver en el apartado 4.

En materia específica de financiación de la proliferación, el Tesoro Público, en calidad de regulador, publica varios documentos en relación con la aplicabilidad de las sanciones recogidas en las resoluciones del CSNU[20], siendo además el encargado de autorizar las transferencias de fondos sometidas a contramedidas. Por último, el Sepblac combina sus funciones de análisis de inteligencia financiera y supervisión con un enfoque basado en riesgo, lo que le permite identificar vulnerabilidades y supervisar a las entidades obligadas.

[20] https://www.tesoro.es/prevencion-del-blanqueo-y-movimiento-de-efectivo/sanciones-financieras

En el caso del comercio de material de material de defensa, de otro material y de productos y tecnologías de doble uso, la exportación de estos productos sin su correspondiente licencia supone una infracción de la legislación en virtud de lo establecido en el Código Penal y en la Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando.

7.2.1.1. JIMDDU: Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Doble Uso.

El régimen de control de exportaciones de España está supervisado por la JJIMDDU, que se encarga de registrar todas las empresas que fabrican o comercian con material de defensa, otro material, así como de aprobar cualquier transacción relacionada con la exportación de estos productos desde España.

La JIMDDU revisa cada solicitud de licencia de exportación y solo autoriza aquellas operaciones en las que no exista riesgo de que los productos exportados sean desviados para uso militar o para la fabricación de ADM.

La JIMDDU examina la empresa española exportadora, el producto exportado y el receptor y usuario final del producto.

Además, España participa en acuerdos multilaterales de control de exportaciones. Policía Nacional y la Guardia Civil, que son responsables de investigar posibles infracciones en el control de exportaciones., forman parte tanto de la JIMDDU. El Sepblac participa en las reuniones del grupo de trabajo preparatorio a las reuniones de la JIMDDU, colaborando en el intercambio de información de inteligencia.

7.2.1.2. Registro Especial de Operadores de Comercio Exterior (REOCE)

Su propósito es recopilar e inscribir la información de los operadores dedicados al comercio exterior de material de defensa, armas de caza y deportivas, equipamiento policial y antidisturbios, así como productos y tecnología de doble uso. Estas actividades están sujetas a control y regulación bajo el Real Decreto 679/2014, de 1 de agosto.

7.2.1.3. Sistema Integral de Guerra Electrónica Contra UAS y programa SUCCAUL[21]

Como consecuencia de la creciente amenaza que representa el uso ilícito de drones, España ha reforzado sus capacidades con sistemas de detección y neutralización específicos, como el Sistema Integral de Guerra Electrónica Contra UAS (SIGLO-CD) y el programa SUCCAUL, orientados a la vigilancia, identificación y neutralización de aeronaves no tripuladas en espacios sensibles.

Dentro de esta estrategia se encuentra la identificación de las tramas económicas que facilitan la adquisición de estas plataformas mediante empresas pantalla, operaciones trianguladas o pagos encubiertos.

7.2.2. Medidas mitigadoras comerciales

Si bien existen vulnerabilidades comerciales ligadas al importante volumen de exportaciones en España, el marco regulatorio existente posibilita el control de mercancías en ciertos casos, lo cual mitiga el riesgo:

- En el caso de los productos agroalimentarios o fitosanitarios, se exige certificación sanitaria.

- El material de defensa, otro material y productos y tecnologías de doble uso está sometido a exigencia de licencia de exportación. El régimen jurídico en materia de comercialización de bienes de doble uso es prolífico en España se incluye en el Anexo 2

- Las mercancías peligrosas o restringidas, por su parte, requieren la verificación de documentos.

- En aquellos casos que proceden de países con sanciones o restricciones comerciales, se aplica vigilancia especial.

[21] Informe de Seguridad Nacional 2024

- Por último, siempre que haya sospechas de fraude, contrabando o evasión fiscal, Aduanas tiene la potestad de realizar controles aleatorios en base a su normativa específica[22].

Además, el Departamento de Aduanas e Impuestos Especiales de la Agencia Estatal de Administración Tributaria aplica un procedimiento de control de exportaciones en España, en virtud del artículo 46 del Código Aduanero de la Unión- Reglamento (UE) 952/2013 basado en análisis de riesgos. En base a este marco regulatorio, existe la posibilidad de establecer excepciones por certificación y procedimientos simplificados, que eviten a ciertos exportadores inspecciones rutinarias.

Estos procedimientos generales se unen a aquellos controles adicionales para bienes caracterizados por su peligrosidad y su vinculación con regímenes de sanciones, lo cual limita la posibilidad de violar sanciones internacionales a través del sistema aduanero español.

7.2.3. Mecanismos de control de la titularidad real para evitar la puesta a disposición de personas sancionadas [23]

España no es un centro de formación de empresas a nivel mundial donde se hayan dado caso en los que los titulares reales de personas jurídicas pudiesen estar relacionadas con la evasión de sanciones o la creación de sociedades.

Además, los notarios han desarrollado en España un sistema de detección de operativas y estructuras jurídicas complejas como consecuencia de la implantación del Órgano Centralizado de Prevención en el Consejo General del Notariado, que aplica herramientas como el Índice Único Informatizado Notarial, que cruza información de millones de operaciones notarizadas en todo el territorio nacional que son debidamente analizadas por el equipo especializado del OCP, o como la Base de Datos de Titularidad Real que permite consultar a los notarios, autoridades y sujetos obligados la veracidad de las declaraciones de los beneficiarios finales de las personas jurídicas que realizan operaciones sometidas a escritura pública.

[22] Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando, La Ley 58/2003, de 17 de diciembre, General Tributaria (LGT) y el Real Decreto 335/2010, de 19 de marzo, por el que se regula el control de los servicios de vigilancia aduanera.
[23] Fuente: Adenda del Análisis Nacional de Riesgos, 2024

Como medida adicional, y en el marco europeo, en el año 2021, el Real Decreto-ley 7 de 2021, de 27 de abril, introdujo la Disposición Adicional Tercera de la Ley 10/2010, de 28 de abril, para la creación de un Registro Central de Titularidades Reales (en adelante,

Además, España forma parte del proyecto europeo BORIS que consiste en la interconexión de registros centrales de titulares reales de la Unión Europea.

7.2.4. Medidas aplicadas por el sector financiero.

Las instituciones financieras han desarrollado un marco integral de políticas y procedimientos orientados a prevenir y detectar operaciones vinculadas a la proliferación de ADM. A continuación, se exponen las medidas aplicadas.

- Enfoque de gestión de clientes basado en el riesgo: todos los clientes son sometidos a medidas de diligencia debida y a los de "alto riesgo" les es de aplicación un procedimiento reforzado.
- Uso de algoritmos capaces de detectar coincidencias parciales y seudónimos potenciales que detectan en tiempo real coincidencias con las listas proporcionadas por CSNU y UE, entre otras.
- Límites a ingresos en efectivo en términos de lo establecido en la Ley 10/2010, de 28 de abril.
- Petición de soporte documental pertinente en caso de transacciones inusuales o no coherentes con la actividad del cliente.
- Sistemas de monitoreo transaccional automatizados que funcionan las 24 horas.
- Mejora de medidas de ciberseguridad específicas: detección de intrusiones, protección del sistema bancario y monitoreo colaborativo entre las unidades de fraude, ciberseguridad y prevención de blanqueo, con el fin de identificar y bloquear ingresos derivados de actividades maliciosas en la red.
- Auditorías internas y se colaboran con organismos públicos y privados para ajustar continuamente los procedimientos a las nuevas amenazas y tendencias.

El Reglamento (UE) 2024/1624 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, exigir medidas específicas frente al riesgo de FP y la elusión de sanciones.

7.3. Riesgo residual

Teniendo en cuenta las medidas mitigadoras existentes, su grado de implementación, y la eficacia demostrada en sectores clave, se concluye que **el riesgo residual de España respecto a la FP para todos los sectores se reduce a bajo.**

Atendiendo al 10.3 del Reglamento (UE) 2024/1624 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024 y en base al análisis realizado los sujetos obligados no financieros bajo la ley 10/2010, de 28 de abril con un riesgo residual inferior medio o alto no estarían obligados a la realización de un análisis de autoevaluación de la FP, ya que basándonos en la calificación del riesgo obtenida.

El riesgo residual para cada sector una vez aplicadas las medidas mitigadoras pueden verse en el siguiente cuadro:

Cuadro 11. Riesgo residual sectorial

Letra	Sujeto Obligado	Riesgo Residual
a	Entidades de crédito	
b	Entidades aseguradoras ramo vida / inversiones y corredores de seguros	
c	Empresas de servicios de inversión	
d	Sociedades gestoras de IIC y sociedades de inversión sin gestora	
e	Entidades gestoras de fondos de pensiones	
f	Sociedades gestoras de ECR y sociedades de capital-riesgo sin gestora	
g	Sociedades de garantía recíproca	
h	Entidades de dinero electrónico y entidades de pago	
i	Personas que ejerzan profesionalmente actividades de cambio de moneda	
j	Servicios postales en actividades de giro o transferencia	
k	Intermediarios en concesión de préstamos o créditos y actividades	
l	Promotores inmobiliarios y agentes en compraventa/arrendamientos ≥120.000€/10.000€ mes	
m	Auditores, contables externos, asesores fiscales y quienes presten asistencia fiscal	
n	Notarios y registradores	
ñ	Abogados, procuradores y profesionales en operaciones financieras/inmobiliarias	
o	Prestadores de servicios a terceros	
p	Casinos de juego	
q	Comercio profesional de joyas, piedras o metales preciosos	
r	Comercio profesional de arte/antigüedades e intermediarios, incluidos puertos francos	
s	Actividades Ley 43/2007 (bienes con oferta de restitución del precio)	
t	Depósito, custodia o transporte profesional de fondos o medios de pago	
u	Gestión/explotación/comercialización de loterías y juegos de azar	
y	Gestores de sistemas de pago y compensación/liquidación, gestores de tarjetas	
z	Proveedores de cambio de moneda virtual por fiduciaria y custodia de monederos	
-	Resto de proveedores de servicios de criptoactivos	

Leyenda

Alto	Alto/ Sustancial	Sustancial	Sutancial/ Medio	Medio	Medio/ Bajo	Bajo

ANEXO 1- Estadísticas de controles a la exportación[24]

Año	Destino	Contenido	Valor (€)	Motivo
2024	Emiratos Árabes Unidos	3 Vectores autopiloto, unidades de software para UAV y reactivos de laboratorio para diagnóstico in vitro		Riesgo de desvío a país con sanciones de la UE y existencia de denegaciones
2024	India	2 Vectores autopiloto		Riesgo de desvío a país con sanciones de la UE y existencia de denegaciones
2024	Kazajstán	1 Convertidores de Frecuencia Variable (VFD)		Riesgo de desvío a país con sanciones de la UE y existencia de denegaciones
2024	Nigeria	1 Vehículos aéreos no tripulados UAV y sus componentes		Riesgo de desvío a país con sanciones de la UE y existencia de denegaciones
2024	R.P.China	1 Máquina taladro		Riesgo de desvío a país con sanciones de la UE y existencia de denegaciones

[24] Estadísticas españolas de exportación de material de defensa, de otro material y de productos y tecnologías de doble uso. Ministerio del Interior de Economía, Comercio y Empresa https://comercio.gob.es/ImportacionExportacion/Informes_Estadisticas/Paginas/Hitorico_Material_Defensa.aspx

2024	Rusia	3 Analizador automático y Equipo de procesado de alimentos por alta presión		Sanciones de la UE
2024	Cuba	7 Cartuchos diferentes calibres, Escopetas de caza de diferentes calibres y Rifles de caza de diferentes calibres		Artículo 8.d) de la Ley 53/2007. Limitaciones derivadas del Derecho Internacional (Embargo)
2024	Guinea Bissau	Un cartucho de escopeta, calibre 12, munición no metálica.		Situación interna y riesgo de uso en represión interna
2024	Venezuela	Escopeta Perazzi calibre 12		Artículo 8.d) de la Ley 53/2007. Limitaciones derivadas del Derecho Internacional (Embargo)
2023	Serbia	12 Tn. de trinitrotolueno	160.000	Denegada la ampliación de productos en el REOCE
2023	Bangladesh	5,5 millones de cartuchos de caza con bolas de goma de calibre 12	2.700.000	Criterios 2 y 3[25] de la Posición Común 2008/944/PESC

[25] Criterio 2: Respeto de los derechos humanos en el país de destino final
Un Estado miembro debe denegar una exportación de armas si existe un riesgo claro de que el material pueda utilizarse:

- Para represión interna (por ejemplo, represión de manifestaciones pacíficas, torturas o violaciones de derechos humanos).
- Para facilitar violaciones graves del derecho internacional humanitario.

Criterio 3: Un Estado miembro debe denegar una exportación si el material contribuye a:

- Agravamiento de tensiones o conflictos armados internos.
- Inestabilidad interna que pueda derivar en guerras civiles, golpes de Estado o violencia étnica o religiosa.

2023	Guinea Bissau	2,9 millones de cartuchos de caza de calibre 12	1.700.000	Criterios 4[26] y 7[27] de la Posición Común 2008/944/PESC
2023	India	Autopilotos y software de control para UAV	1.300.000	Riesgo de desvío a país sancionado por la UE
2023	China	Equipos lógicos de software para simulación de datos, cámaras no refrigeradas, polvo metálico base níquel	444.473	Riesgo de transferencia de tecnología para uso militar
2023	Rusia	Reactivos, analizadores automáticos, tarjetas de análisis de sangre, liofilizador	417.873	Aplicación de sanciones UE a Rusia
2022	Pakistán	670 pistolas de uso deportivo con cargadores	175.175	Falta de información sobre el destinatario y riesgo de desvío a país sancionado

[26] Criterio 4: Mantenimiento de la paz, la seguridad y la estabilidad regionales
Los Estados miembros denegarán la licencia de exportación cuando exista un riesgo manifiesto de que el receptor previsto pueda utilizar la tecnología o los equipos militares cuya exportación se propone para agredir a otro país o para imponer por la fuerza una reivindicación territorial. Al estudiar dichos riesgos, los Estados miembros tendrán en cuenta, entre otras cosas:

a) la existencia o la probabilidad de un conflicto armado entre el país receptor y otro país;
b) la reivindicación de territorio de un país vecino que el receptor haya intentado imponer o haya amenazado con obtener por la fuerza en el pasado;
c) la probabilidad de que la tecnología o los equipos militares sean utilizados con fines distintos de la seguridad nacional y la legítima defensa del receptor;
d) la necesidad de no perjudicar de forma importante la estabilidad regional.

[27] Criterio 7: Riesgo de desvío del material exportado
Un Estado miembro debe denegar una exportación si existe un riesgo claro de que:

- El material exportado pueda ser reexportado sin autorización a otro país o grupo no autorizado.
- La exportación pueda caer en manos de grupos terroristas o criminales.
- No hay garantías suficientes sobre el control del material en el país de destino.

2022	Burkina Faso	5,5 millones de cartuchos de caza	1.600.000	Criterio 7 de la Posición Común 2008/944/PESC
2022	Guinea Bissau	13,5 millones de cartuchos de caza	5.400.000	Criterios 4 y 7 de la Posición Común 2008/944/PESC
2022	Cuba	2.500 cartuchos lacrimógenos y fumígenos, 40 artificios de luz, sonido y lacrimógenos	350.000	Criterio 2 de la Posición Común 2008/944/PESC
2022	República Centroafricana	50.000 cartuchos lacrimógenos	2.100.000	Criterio 2 de la Posición Común 2008/944/PESC
2022	China	9 cámaras de infrarrojos no refrigeradas, 2 cámaras de escaneo, 1 sistema de control de potencia	77.000	Riesgo de desvío a programa de proliferación
2022	Rusia	153 válvulas de globo en acero inoxidable y bronce aluminio, 26 válvulas de compuerta y repuestos	1.400.000	Sanciones UE y riesgo de desvío a la industria militar
2022	Israel	418 sistemas de referencia y navegación inercial para UAV, 2 placas de evaluación, 18 vectores autopiloto	700.000	Riesgo de desvío en uso y destino

2022	Turquía	1 centro de mecanizado	115.000	Riesgo de desvío a un país objeto de sanciones
2022	Egipto	5 vectores autopilotos de UAV	40.344	Riesgo de desvío al no tener información sobre el destinatario
2021	Burkina Faso	11,4 millones de cartuchos de caza	1.200.000	Criterio 7 de la Posición Común 2008/944/PESC
2021	China	996 convertidores digitales, software para simulación, 200 kgs. de polvo de base níquel	343.252	Riesgo de desvío a uso militar y existencia de denegaciones de otros países
2021	Rusia	1 módulo de frecuencia, 2 cámaras no refrigeradas	288.424	Sanciones UE y riesgo de desvío a uso militar
2020	Ucrania	1 centro de mecanizado	846.597	Riesgo de desvío a fabricación de equipos militares para reexportación a un tercer país sancionado
2020	China	30 sensores de imagen	128.250	Riesgo de desvío a uso militar y existencia de denegaciones de otros países

ANEXO 2. Régimen jurídico en materia de comercialización de bienes de doble uso.

- Ley 53/2007, de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso.

- Real Decreto 679/2014, de 1 de agosto, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.

- Real Decreto 494/2020, de 28 de abril por el que se modifica el Real Decreto 679/2014, de 1 de agosto, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.

- Real Decreto 414/2022, de 31 de mayo, por el que se modifica el 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.

- 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.[28]

- Reglamento (UE) 2021/821 del Consejo, de 20 de mayo, por el que se establece un régimen de la Unión de control de las exportaciones, el corretaje, la asistencia técnica, el tránsito y la transferencia de productos de doble uso, actualizado por el Reglamento Delegado (UE) Nº 2022/1 de la Comisión, de 20 de octubre.

[28] En virtud de los compromisos de España en los diferentes foros internacionales de lucha contra la proliferación, la colaboración con los EEMM de la UE y las propias necesidades de seguridad nacional, anualmente se publica una actualización de los productos cuya exportación está controlada. Se cita el último. Será necesario actualizar a lo largo de 2026 con la nueva orden ministerial.

ACRÓNIMOS

ADM Armas de destrucción masiva

AEAT Agencia Española de Administración Tributaria

APNFD Actividades y profesiones no financieras designadas

BC Blanqueo de Capitales

BC/FT El Blanqueo de Capitales y la Financiación del Terrorismo

CITCO Centro de Inteligencia contra el Terrorismo y el Crimen Organizado

CSNU Consejo de Seguridad de Naciones Unidas

FP Financiación de la proliferación

FT Financiación del terrorismo

FCSE Fuerzas y Cuerpos de Seguridad del Estado

GAFI Grupo de Acción Financiera Internacional

JCPOA Plan de Acción Integral Conjunto

ONU Organización de Naciones Unidas

PBC/FT Prevención del blanqueo de capitales y de la financiación del terrorismo

RCTIR Registro Central de Titularidades Reales

RPDC República Democrática de Corea del Norte

SEPBLAC Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias

UE Unión Europea