2024



Análisis Nacional de Riesgos

ADENDA 2024. VERSIÓN PÚBLICA

INDICE

1. INTRODUCCIÓN. 3
2. METODOLOGÍA. 4
2.1. Instituciones participantes. 4
2.2. Determinación de los riesgos, amenazas y vulnerabilidades. 5
3. MARCO NORMATIVO E INSTITUCIONAL. 7
3.1. Marco normativo: GAFI, Unión Europea y normas nacionales. 7
3.3. Marco preventivo: coordinación nacional. 8
3.4. Marco nacional de supervisión de BC/FT. 10
3.5. Marco de investigación y procesamiento. 11
4. ANÁLSIS DE HITOS: EL IMPACTO DE LA PANDEMIA COVID-19 Y DE LA GUERRA ENTRE RUSIA Y UCRANIA. 12
4.1. El impacto de la pandemia COVID-19. 12
4.2. El impacto de la guerra entre Rusia y Ucrania. 13
5. PRINCIPALES AMENAZAS DE BLANQUEO DE CAPITALES. 14
5.1. Crimen Organizado. 15
5.2. Tráfico de drogas. 20
5.3. Delitos económicos y financieros: fraudes, delito fiscal, y casos vinculados a la corrupción. 22
5.4. Blanqueo de capitales por terceros y por delitos cometidos en el extranjero. 24
6. PRINCIPALES AMENAZAS DE FINANCIACIÓN DEL TERRORISMO. 25
6.1. Terrorismo yihadista. 27
6.2. Financiación del terrorismo yihadista. 29
6.3. Terrorismo de ETA. 29
6.4. Otros grupos terroristas. 30
6.5. Estrategia Nacional Contra el Terrorismo. 30
7. PRINCIPALES VULNERABILIDADES EN BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO. 31
7.1. Vulnerabilidades derivadas de la población. 31
7.2. Vulnerabilidades derivadas de factores geográficos. 32
7.2.1 Realización de operaciones con territorios de riesgo o con ciudadanos/ entidades de esos territorios. 32
7.2.2. Operaciones con países de mayor riesgo de financiación del terrorismo. 33
7.2.3. Actividades en el área de Gibraltar. 33
7.3. Vulnerabilidades derivadas de la naturaleza de la entidad o actividad desarrollada. 35
7.4. Vulnerabilidades derivadas de los medios de pago, uso de efectivo y economía irregular. 36
7.5. Vulnerabilidades derivadas de innovaciones tecnológicas en operaciones financieras. 37
7.5.1. Vulnerabilidades por uso del ciberespacio. 37
7.4.2 Vulnerabilidades por el uso de monedas y activos virtuales. 37
8. RIESGOS SECTORIALES. 38
8.1. Riesgos sector financiero. 39
a) Servicios de inversión, instituciones de inversión colectiva y sociedades gestoras. 39

b) Envío de dinero por entidades de pago. 44
c) Otros servicios prestados por entidades de pago. 48
d) Operaciones con dinero electrónico. 51
e) Criptoactivos y Proveedores de Servicios de Criptoactivos. 53
f) Uso de dinero en efectivo, movimientos de efectivo y negocios con uso intensivo de efectivo. 58
8.2. Riesgo sectores no financieros. 64
a) Actividades realizadas por los notarios. 64
b) Actividades realizadas por registradores de la propiedad, mercantiles y de bienes muebles. 68
9. RIESGOS DE NO IMPLEMENTACIÓN O EVASIÓN DE LAS SANCIONES FINANCIERAS INTERNACIONALES. 73
9.1. Concepto de sanciones financieras internacionales. 73
9.2. Sanciones financieras internacionales relacionadas con el terrorismo y la financiación del terrorismo. 74
9.3. Sanciones financieras internacionales relacionadas con la proliferación de Armas de Destrucción Masiva (ADM). 74
9.4. Vulnerabilidades y riesgo sectorial. 76
9.5. Conclusiones. 78
10. MEDIDAS ADOPTADAS. 80
10.1. Medidas adoptadas de carácter general. 80
10.2. Otras medidas de mitigación de carácter específico. 82
11. CONCLUSIONES. 86
12. ESTADÍSTICAS. 88
Abreviaturas utilizadas 89
Lista de principales disposiciones normativas 91

1. INTRODUCCIÓN.

El artículo 7 de la Directiva la Directiva (UE) 2015/849[1] del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo (en adelante, IV Directiva) establece la obligación de elaborar y publicar un análisis nacional de riesgos. Igualmente, el Grupo de Acción Financiera Internacional (en adelante, GAFI) en su Recomendación 1 establece que los países tienen el deber de identificar, evaluar y entender los riesgos de blanqueo de capitales y de la financiación del terrorismo (en adelante, BC/FT respectivamente).

Estas premisas fueron mencionadas en el Análisis Nacional de Riesgos (en adelante, ANR) publicado en 2020 en su versión íntegra. En esta nueva publicación se va a llevar a cabo una actualización de las amenazas y vulnerabilidades existentes a nivel nacional, así como de los sectores que se enfrenten a riesgos que hayan emergido desde el anterior informe.

La actualización de este documento, en función de las nuevas variables que afectan a determinados sectores, se configura como estrategia nacional para identificar nuevas amenazas, vulnerabilidades y riesgos potenciales que les afecten a los mismos, con el fin de señalar las medidas mitigadoras que se han establecido o que se pueden establecer para hacer frente estos riesgos.

El objetivo de este análisis es por tanto proceder a una actualización parcial del ANR de 2020, puesto que hay determinados sectores que no han experimentado cambios sustanciales en los riesgos planteados en el anterior estudio, no se han visto afectados por actualizaciones normativas significativas o amenazados por recientes o nuevas actividades delictivas que puedan vulnerar sus sistemas preventivos. Desde 2020 sucesos como el COVID-19, la guerra de Rusia-Ucrania o la participación en el sistema financiero de nuevos agentes, tales como proveedores de servicios de criptoactivos (en adelante, PSCA), empresas *fintech* que actúan como intermediarias en servicios financieros o nuevos proveedores de servicios de pago, son hechos que impulsaron nuevos retos a los que se enfrentaron tanto instituciones y autoridades a nivel nacional como internacional en materia de BC/FT.

Estos hechos han provocado la evolución de las técnicas y métodos de BC/FT, que basan su éxito en explotar las vulnerabilidades de los sistemas nacionales. Esto requiere, como ya se puntualizó en el ANR de 2020, una continua actualización de los análisis y controles que permitan a las autoridades y sujetos obligados identificar los cambios en los modos de operar, las nuevas tipologías, las formas de utilización de los avances tecnológicos o la evolución en los tipos de jurisdicciones que suponen un riesgo en estas materias.

Como consecuencia de la actualización de este análisis, las autoridades tendrán herramientas actualizadas para adoptar nuevas medidas mitigadoras, adoptar el marco regulador a las necesidades identificadas, fortalecer los recursos empleados y mejorar la coordinación interna y la cooperación internacional, tanto en el ámbito preventivo como en el represivo. Finalmente, se procederá a realizar una evaluación de las medidas que se adoptaron en el ANR de 2020 y a realizar una evaluación de las que se han implementado con el objetivo de obtener un análisis de cumplimiento de estas propuestas.

[1] Los Estados Miembros deben: Poner a disposición del público un resumen de las evaluaciones nacionales de riesgos; poner los resultados de sus evaluaciones de riesgos a disposición de la Comisión Europea, autoridades supervisoras y demás estados miembros; elaborar su análisis nacional de riesgos teniendo en consideración el Informe de la Comisión Europea sobre la Evaluación Supranacional de Riesgos de Blanqueo de Capitales y Financiación del Terrorismo que afectan al mercado y que guardan relación con la actividad transfronteriza, publicado el 26 de junio de 2017 cuya segunda versión se ha publicado en julio de 2019. https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF .

2. METODOLOGÍA.

En la elaboración del presente documento, de conformidad con la Guía publicada por GAFI sobre la identificación y valoración de riesgos de BC/FT, y con la IV Directiva, se han tenido en consideración diferentes fuentes de información nacionales e internacionales, y se ha consultado con las autoridades públicas competentes de cada área y con representantes del sector privado. En concreto, este documento se fundamenta en:

a) El Análisis Nacional de Riesgos para España publicado en 2020.
b) El Análisis Sectorial de Riesgo de Criptoactivos y de Proveedores de Servicios de Criptoactivos de 2023.
c) La Estrategia de Seguridad Nacional 2022, coordinada por el Departamento de Seguridad Nacional y emitida por la Presidencia del Gobierno.
d) La Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave y la Estrategia Nacional contra el Terrorismo, coordinada por el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, CITCO.
e) Los distintos análisis sectoriales de riesgos ya existentes y que fueron objeto de evaluación por GAFI en 2014 y los informes de seguimiento de 2017 y 2019.
f) El Análisis de Riesgo Supranacional elaborado por la Unión Europea (en adelante, SNRA de la UE).
g) Las memorias anuales de instituciones públicas involucradas en la lucha contra BC/FT.
h) Los Informes Anuales del Consejo de Seguridad Nacional y presentados anualmente ante la Comisión Mixta Congreso-Senado.
i) Las estadísticas publicadas en estas materias, incluyendo las referentes al ámbito preventivo, supervisor, investigaciones policiales y procesamientos judiciales.
j) Las 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.
k) Las aportaciones de representantes de sujetos obligados y sector privado.

2.1. Instituciones participantes.

Las instituciones públicas con participación en la elaboración del ANR son:

- Agencia Estatal 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 Policía Judicial de la Policía Nacional.
- Comisaría General de Información de la Policía Nacional.
- Comisión Nacional del Mercado de Valores (CNMV).
- Consejo General del Poder Judicial.
- Delegación del Gobierno para el Plan Nacional sobre Drogas.
- Departamento de Seguridad Nacional.
- Dirección General de Ordenación del Juego.
- Dirección General de Política Exterior y Seguridad.
- Dirección General de Seguridad Jurídica y Fe Pública.
- Dirección General de Seguros y Fondos de Pensiones.
- Fiscalía General del Estado.
- Fiscalía Especial Antidroga.
- Fiscalía de la Audiencia Nacional.
- Fiscalía Especial contra la Corrupción y la Criminalidad Organizada.

- Jefatura de Información de la Guardia Civil (JI).
- Oficina de Gestión y Recuperación de Activos.
- Secretaría de Estado de Seguridad.
- Secretaría General del Tesoro y Financiación Internacional.
- Servicio Ejecutivo de Prevención de Blanqueo de Capitales (Sepblac).
- Unidad Técnica de Policía Judicial de la Guardia Civil (UTPJ).

2.2. Determinación de los riesgos, amenazas y vulnerabilidades.

Este análisis mantiene la metodología establecida en 2020 para determinar los riesgos, amenazas y vulnerabilidades a escala nacional. Tal y como se expuso en el anterior ANR, para establecer los riesgos de BC/FT se requiere identificar: (i) las amenazas existentes en España, (ii) las vulnerabilidades del sistema y el contexto del país que permiten a esas amenazas desarrollar sus actividades y (iii) 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 BC/FT aprovechando las vulnerabilidades existentes.

Además de estas variables, en esta adenda se ha tenido en cuenta factores endógenos que influyen en los riesgos derivados de las circunstancias económicas y sociales que han afectado al sistema durante estos años. Tal es el caso, de los efectos causados por el COVID-19 y la guerra de Ucrania en materia de BC/FT.

Se adoptan las definiciones establecidas en el anterior ANR, y que se fundamentan en los estándares internacionales impulsados por GAFI, para la identificación de las amenazas, vulnerabilidades y riesgos, así como los aspectos a tener en cuenta a la hora de determinar las vulnerabilidades y los factores de riesgos indicados para la definición del riesgo inherente y residual.

"Amenazas" son aquellas personas, grupos de personas o sus actividades que suponen un potencial peligro por su capacidad para causar daño al Estado, la sociedad, la economía u otros elementos fundamentales de la vida de un país.

Teniendo en cuenta que las amenazas tienen propósitos delictivos y de carácter desestabilizador, su análisis en materia de BC/FT debe tener principalmente un enfoque represivo, mediante su evaluación por parte de las autoridades competentes en la investigación y procesamiento de las actividades delictivas, como son las autoridades policiales (Dirección General de la Policía Nacional, Guardia Civil o policías autonómicas), Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (en adelante, CITCO), Centro Nacional de Inteligencia (en adelante, CNI), Fiscalía General del Estado, jueces y tribunales o la Agencia Estatal de Administración Tributaria (en adelante, AEAT) en materia de índole aduanera y fiscal.

"Vulnerabilidades" son aquellas situaciones y circunstancias que pueden ser aprovechadas o utilizadas por las organizaciones o personas que pretendan realizar actividades de blanqueo de capitales o financiación del terrorismo.

Para la determinación de estas vulnerabilidades inherentes del sistema se han analizado diferentes factores que pueden ser objeto de aprovechamiento para la comisión de actividades ilícitas. Dentro de las vulnerabilidades se han tenido en consideración aspectos:

- De carácter geográfico.
- De población.
- Tecnológicos.
- Derivados de la actividad desarrollada, su regulación y su supervisión prudencial y en materia de prevención de BC/FT.
- Derivados del tipo de persona jurídica: tamaño, modelo de negocio, presencia nacional/ internacional,

exposición a clientes de mayor riesgo, etc.

- Derivados de los medios de pago, uso de efectivo y economía irregular.

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

Por tanto, en cada capítulo se analizan los riesgos correspondientes a actividades, sectores y tipos de instituciones teniendo en consideración las amenazas detectadas, las características, contexto, volumen de negocio, principales vulnerabilidades y exposición al riesgo de cada uno de ellos. Para ello se tendrán en cuenta sus vulnerabilidades por la existencia de factores de riesgo endógenos y exógenos, así como sus riesgos inherentes y sus riesgos residuales:

a) Los factores de riesgo "endógenos" son aquellos intrínsecos, derivados de la naturaleza y características del sector, que pueden permitir o facilitar su acceso o control por delincuentes, por ejemplo, creando o adquiriendo una entidad con la finalidad de ser utilizada para BC/FT o bien captando a algún empleado o agente.
b) Los factores de riesgo "exógenos" son aquellos externos, asociados al posible uso indebido que se puede hacer de los servicios, canales o productos que ofrece el sector por parte de terceros, por ejemplo, mediante la utilización por el cliente, con fines BC/FT, de servicios comerciales o financieros legítimamente prestados.

<table>
<tr><th colspan="2">Factores de riesgo</th></tr>
<tr><th>Endógenos</th><th>Exógenos</th></tr>
<tr><td>Creación o control de entidad con fines de BC/FT.</td><td rowspan="2">Asociados al abuso de los servicios/ canales/ productos por parte de los clientes/intervinientes en las operaciones con fines de BC/FT.</td></tr>
<tr><td>Captación de agentes o empleados desleales.</td></tr>
</table>

El resultado de este análisis es la valoración de los distintos tipos de riesgos que afectan a cada sector de actividad, tomando en consideración el tipo de personas físicas o jurídicas que operan en ese sector, los productos que comercializa, los servicios que presta, las características de sus clientes y los países con los que opera. Además de la especial naturaleza de sus operaciones y servicios, se evalúan factores tales como la información recabada de la experiencia supervisora, el conocimiento de la actividad a través de las comunicaciones sistemáticas y comunicaciones por indicio y los informes de experto externo entre otras fuentes.

En concreto, para cada sector, tipo de institución o actividad, se determina cuál es el **riesgo inherente** de que sean utilizados con fines de BC/FT debido a sus vulnerabilidades y características propias. Este riesgo inherente es corregido en función de las medidas mitigadoras adoptadas a nivel nacional para ese sector, entre las que se tienen en cuenta su regulación prudencial, grado de supervisión, persecución penal, comprensión de riesgos por el sector, nivel de aplicación de medidas de prevención del BC/FT o la calidad de sus procedimientos de control interno.

Estas medidas de mitigación son las que permiten determinar cuál es el **riesgo residual** de que los sectores, entidades y actividades sean utilizados para fines relacionados con el BC/FT.

De conformidad con la clasificación de niveles de riesgos establecida por la Comisión de la Unión Europea en la **Evaluación Supranacional de Riesgos del Blanqueo de Capitales y de la Financiación del Terrorismo,** SNRA de la UE, los niveles de riesgo del presente análisis podrán clasificarse como:

- Bajo.
- Moderado.
- Significativo.
- Alto.

3. MARCO NORMATIVO E INSTITUCIONAL.

3.1. Marco normativo: GAFI, Unión Europea y normas nacionales.

El Grupo de Acción Financiera Internacional, GAFI, es un organismo intergubernamental creado en 1989 con el fin de combatir, a nivel mundial, el BC/FT. Establece los estándares internacionales, así como la efectiva implementación de las medidas legales, regulatorias y operativas para prevenir prácticas ilícitas que afecten al BC/FT en los países miembros y no miembros. Las Recomendaciones del GAFI, actualizadas varias veces, son la referencia para evaluar la efectividad de los sistemas nacionales de prevenir el BC/FT, así como la inspiración para las actualizaciones de la normativa europea y el principal motivo de las modificaciones de la normativa nacional.

La IV Directiva[2] recoge las novedades aprobadas por el GAFI en 2012, estableciendo un marco general que ha de ser, no sólo transpuesto, sino completado por los Estados miembros. La Directiva (UE) 2018/843, de 30 de mayo, (en adelante, V Directiva) modifica y actualiza este marco, ampliándolo a nuevos sectores como los proveedores de servicios de cambio de moneda virtual y los proveedores de servicios de custodia de monederos electrónicos, introduciendo medidas para aumentar la transparencia en la propiedad de las empresas y reforzar el sistema de identificación de los titulares reales, con nuevos activos objeto de comunicación al Fichero de Titularidades Financieras (en adelante FTF), y ampliando del concepto persona con responsabilidad pública, entre otros aspectos. El compromiso de España en la lucha contra el BC/FT ha llevado a la sucesiva adopción de diferentes iniciativas normativas y a la adaptación al marco legislativo español de las Directivas mencionadas en párrafos anteriores. En este sentido, la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, ha sido modificada en 2013[3], 2018[4], 2021[5], 2022[6] y 2023[7].

---

[2] Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.

[3] Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

[4] Real Decreto-ley 11/2018, de 31 de agosto, de transposición de directivas en materia de protección de los compromisos por pensiones con los trabajadores, prevención del BC y requisitos de entrada y residencia de nacionales de países terceros.

[5] Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del BC, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores.

[6] Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas y Ley Orgánica 9/2022, de 28 de julio por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales.

[7] Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
Real Decreto-ley 5/2023, de 28 de junio, por el que se adoptan y prorrogan determinadas medidas de respuesta a las consecuencias económicas y sociales de la Guerra de Ucrania, de apoyo a la reconstrucción de la isla de La Palma y a otras situaciones de vulnerabilidad; de transposición de Directivas de la Unión Europea en materia de modificaciones estructurales de sociedades mercantiles y conciliación de la vida familiar y la vida profesional de los progenitores y los cuidadores; y de ejecución y cumplimiento del Derecho de la Unión Europea.

Adicionalmente, el Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, procede a completar el enfoque basado en el riesgo de la normativa de prevención del BC/FT en España, incorporando las principales novedades de los estándares internacionales adoptados por el GAFI en 2013.

Junto a estas dos normas, que configuran el marco legal de prevención del BC/FT a nivel nacional, la principal regulación de carácter represivo viene establecida en el Código Penal, que fue objeto de sucesivas modificaciones en 2015, en 2019 y en 2022, tanto en lo relativo a la tipificación del delito de blanqueo de capitales como la de terrorismo y su financiación.

En desarrollo o directamente vinculadas con las anteriores normas existe un amplio número de disposiciones de aplicación a las materias de BC/FT, tanto en su faceta preventiva como represiva, con diferente rango, que se enumeran en el apartado titulado "Listado de principales disposiciones normativas".

3.3. Marco preventivo: coordinación nacional.

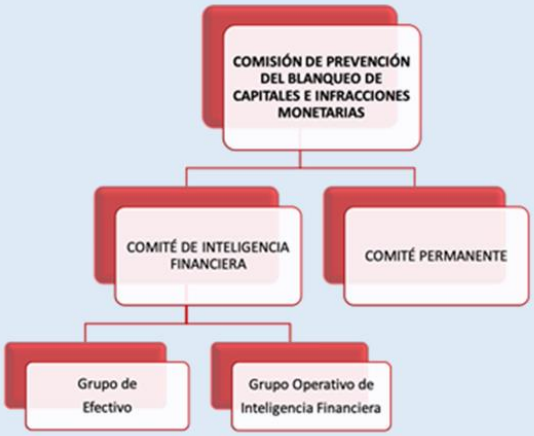
La Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (en adelante, la COPBLAC) es el órgano competente para el impulso, elaboración y coordinación de las políticas nacionales en materia de prevención del BC/FT e interviene en la imposición de sanciones por incumplimiento de las obligaciones de prevención del BC/FT establecidas en la Ley 10/2010, de 28 de abril. Está integrada por 26 miembros de las principales instituciones nacionales en materia de lucha contra el BC/FT.

PRESIDENCIA DE LA COMISIÓN Secretario/a de Estado de Economía y Apoyo a la Empresa.
VOCALES Director/a General del Tesoro y Política Financiera. Fiscal de Sala Jefe de la Audiencia Nacional. Fiscal de Sala Jefe de la Fiscalía Antidroga. Fiscal de Sala Jefe de la Fiscalía contra la Corrupción y la Criminalidad Organizada. Vocal del Consejo General del Poder Judicial. Secretario/a General del Banco de España. Director/a de Supervisión del Banco de España. Director/a General del Servicio Jurídico de la Comisión Nacional del Mercado de Valores. Director/a General de Seguros y Fondos de Pensiones. Director/a General de Comercio e Inversiones. Director/a General de Seguridad Jurídica y Fe Pública. Director/a General de Política Exterior y Asuntos Multilaterales, Globales y de Seguridad. Director/a de la Agencia Española de Protección de Datos. Director/a de Gabinete de la Secretaría de Estado de Seguridad. Comisario/a General de Policía Judicial de la Policía Nacional. General Jefe de Policía Judicial de la Guardia Civil. Director/a de Inteligencia del Centro Nacional de Inteligencia- CNI. Director/a de Aduanas e Impuestos Especiales de la Agencia Estatal de Administración Tributaria (AEAT). Director/a del Departamento de Inspección Financiera y Tributaria de la Agencia Estatal de Administración Tributaria (AEAT).

Director/a de la Policía Autónoma Vasca- Ertzaintza. Director/a de la Policía Foral de Navarra. Director/a General de la Policía de la Generalidad de Cataluña- Mossos d'Esquadra. Director/a del Servicio Ejecutivo de la Comisión - Sepblac.
SECRETARÍA DE LA COMISIÓN Subdirector/a General de Inspección y Control de Movimientos de Capitales. Dirección General del Tesoro y Política Financiera.

La COPBLAC se reúne al menos dos veces al año y actúa en Pleno o a través de sus Comités dependientes: el Comité Permanente y el Comité de Inteligencia Financiera.

CUADRO 1. Coordinación Nacional



El Comité Permanente se ocupa fundamentalmente de coordinar la acción supervisora. Recibe y analiza los informes de inspección elaborados por los supervisores, donde se desgrana el nivel de cumplimiento de la normativa de prevención del BC/FT por parte de los sujetos obligados. Es responsable de la incoación de procedimientos sancionadores por infracciones en esta materia y la realización de requerimientos de mejora a los sujetos obligados.

El Comité de Inteligencia Financiera se ocupa de los aspectos más operativos y de análisis de riesgos, tendencias y vulnerabilidades. Cuenta con un órgano técnico de apoyo, el Grupo Operativo de Inteligencia Financiera (GOIF) y con un grupo de trabajo especializado en riesgos y acciones en materia de movimientos de dinero en efectivo y medios de pago (Grupo de Efectivo).

La Comisión y sus Comités dependientes tienen como órganos de apoyo a la Secretaría de la Comisión y a el Servicio Ejecutivo de la Comisión, Sepblac.

La Secretaría de la Comisión corresponde a la Subdirección General de Inspección y Control de Movimientos de Capitales de la Dirección General del Tesoro y Política Financiera, que desempeña entre otras funciones las de instruir los expedientes sancionadores por infracción de las obligaciones en materia de prevención del BC/FT y formular

propuestas de resolución, así como proponer, elaborar y dar seguimiento a los requerimientos de mejora comunicados a los sujetos obligados.

El Servicio Ejecutivo de la Comisión (Sepblac) es la Unidad de Inteligencia Financiera en España y autoridad nacional de supervisión en materia de prevención BC/FT. Está encargado, entre otras funciones, de recibir las comunicaciones remitidas por los sujetos obligados, analizar la información recibida, auxiliar a los órganos judiciales, supervisar a los sujetos obligados y emitir los informes que se determinan normativamente.

3.4. Marco nacional de supervisión de BC/FT.

A nivel nacional, el Sepblac es responsable de supervisar el cumplimiento de las obligaciones de prevención del BC/FT de los sujetos obligados. En el caso de las entidades financieras, también los supervisores prudenciales de las entidades financieras, **Banco de España, Comisión Nacional del Mercado de Valores** (en adelante, CNMV) **y Dirección General de Seguros y Fondos de Pensiones** (en adelante, DGSFP) desarrollan funciones de supervisión e inspección en materia de BC/FT, teniendo en cuenta los convenios de cooperación suscritos.

La acción supervisora de la prevención del BC/FT sigue un enfoque basado en el riesgo. De hecho, el doble papel del Sepblac como unidad de inteligencia financiera y como autoridad supervisora ofrece sinergias entre ambas funciones, siendo este organismo en su doble vertiente una fuente fundamental de información utilizada en la evaluación de los riesgos a escala nacional, sectorial e institucional.

Los órganos supervisores examinan los riesgos, políticas, controles internos y los procedimientos en materia de BC/FT de las entidades. En el caso de las entidades financieras, se tienen en consideración las directrices aprobadas por las Autoridades Europeas sobre la supervisión basada en el riesgo y los factores de riesgo a tener en cuenta por los sujetos obligados en la aplicación de las medidas de diligencia debida.

El Sepblac, como supervisor general, efectúa evaluaciones de los riesgos específicos de cada sector y de cada entidad en particular, y esa información se usa como base para preparar el Plan Anual de Inspección. Las evaluaciones de riesgos se actualizan periódicamente o cuando así lo determine la información de inteligencia financiera, cuando se produce un cambio de titularidad, un incremento de la participación accionarial o cualquier información relevante.

Los supervisores prudenciales también realizan una supervisión de la prevención del BC/FT basada en el riesgo en la que los planes y recursos de supervisión se asignan a las entidades según su perfil de riesgo y su prioridad supervisora.

Además, cabe mencionar la coordinación entre supervisores a través de la elaboración de un Plan de Inspección Conjunto.

Junto a este marco nacional existe un marco institucional europeo de supervisión de entidades financieras, modificado a través del denominado paquete CRD-V[8], dirigido a reducir los riesgos del sistema financiero europeo y a mejorar la cooperación entre las autoridades competentes en prevención del BC/FT. En particular, incorpora medidas para promover la cooperación e intercambio de información entre supervisores prudenciales, autoridades competentes en prevención del BC/FT y las unidades de inteligencia financiera (UIF). Además, en el proceso de revisión y evaluación supervisora (denominado PRES), los asuntos de prevención del BC/FT deben ser considerados por los órganos supervisores en los análisis de riesgos de las entidades financieras debiendo notificarse a la Autoridad Bancaria Europea, EBA, y a las autoridades nacionales competentes en temas de prevención del BC/FT cuando se identifiquen debilidades en esta materia en el modelo de gobierno, actividades comerciales o modelo comercial de las entidades del sector. Este marco supervisor va a cambiar en los próximos años, pues en base al Reglamento AMLA pendiente de

[8] Capital Requirements Directive and Regulation.

publicación por parte de la UE, se creará un supervisor con competencias centralizadas a nivel de la UE, el cual coordinará a los supervisores nacionales de BC/FT.

3.5. Marco de investigación y procesamiento.

España cuenta con un amplio marco institucional de investigación y procesamiento integrado por: (i) las Fuerzas y Cuerpos de Seguridad del Estado (en adelante, FCSE) que gozan de la condición de policía judicial, y (ii) los fiscales y jueces a los que se les ha encomendado la responsabilidad de velar por que los delitos de BC/FT y los delitos precedentes de aquellos sean adecuadamente investigados.

Los dos principales cuerpos policiales, la Policía Nacional y la Guardia Civil, son responsables de luchar contra cualquier delito, incluidos el BC/FT bajo la dirección de la Secretaría de Estado de Seguridad (Ministerio del Interior). También el Servicio de Vigilancia Aduanera dependiente de la AEAT es responsable de la investigación y persecución de los delitos fiscales, de contrabando y de BC asociado a los mismos, y forma parte de la policía judicial. Además, Cataluña, País Vasco y Navarra tienen cuerpos policiales propios, que actúan bajo la dirección de las autoridades de las Comunidades Autónomas respectivas.

Todas las unidades y grupos de investigación de la policía judicial están facultados para realizar investigaciones financieras paralelas relacionadas con sus investigaciones penales bajo la supervisión de la Autoridad Judicial y de la Fiscal. También pueden remitir casos a otras autoridades para que continúen con investigaciones, cuando se considere necesario, con independencia de dónde se haya cometido el delito precedente. Las investigaciones de las FCSE son coordinadas por el CITCO, y cuentan con mecanismos de coordinación, como acuerdos de colaboración e intercambio de información y grupos o equipos conjuntos de trabajo, para facilitar las investigaciones de asuntos prioritarios.

Las unidades policiales especializadas en investigar delitos precedentes concretos y delitos relacionados de BC/FT son las siguientes:

- **Policía Nacional:** a la Comisaría General de Policía Judicial le corresponde la investigación y persecución de las infracciones supraterritoriales, especialmente de los delitos relacionados con las drogas, la delincuencia organizada, económica, financiera, tecnológica y el control de los juegos de azar, siendo la Unidad Central de Delincuencia Económica y Fiscal (en adelante, UDEF) la que asume la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y el apoyo técnico a las respectivas unidades territoriales; y la Comisaría General de Información (en adelante, CGI) encargada de investigar delitos relacionados con el terrorismo y su financiación, además de su coordinación, nacional e internacional, y recopilar información sobre dichas materias con fines de inteligencia.
- **Guardia Civil:** la Jefatura de Información (en adelante, JI) lucha contra el terrorismo y su financiación en las diferentes provincias del territorio nacional a través de Grupos de Información de Comandancia (GIC), y en todo el país a través del Servicio de Información, que tiene una Sección de Investigación Económica que realiza investigaciones complejas y asesora a los GIC en esta materia. La Jefatura de Policía Judicial, que persigue el BC, cuenta con la Unidad Técnica de Policía Judicial (en adelante, UTPJ) donde hay una unidad encargada de las labores de inteligencia financiera dentro de su ámbito competencial. En las diferentes provincias existen unidades de policía judicial territoriales. A nivel central, la Unidad Central Operativa, (en adelante, UCO), tiene un grupo de investigación especializado y se ocupa de las investigaciones de BC más complejas. La Guardia Civil en el ejercicio de sus misiones de Resguardo Fiscal del Estado, bajo la dependencia del Departamento de Aduanas e Impuestos Especiales, tanto en los recintos aduaneros, como en los puntos fronterizos habilitados y en el resto del territorio nacional, realiza a través del Servicio Fiscal misiones de control de movimiento de mercancías, incluidas las de movimiento de efectivo.

- **Agencia Estatal de Administración Tributaria (AEAT)**: el Servicio de Vigilancia Aduanera (en adelante, SVA), integrado como una Dirección Adjunta en el Departamento de Aduanas e Impuestos Especiales, tiene como misión la persecución e investigación de determinados delitos e infracciones relacionados con el fraude fiscal, el contrabando y el BC, actuando para ello como policía judicial. El Departamento de Aduanas e Impuestos Especiales, constituye la autoridad aduanera en España y es el único responsable de los controles relacionados con el comercio exterior, incluidos los relacionados con movimientos de medios de pago, contando para ello con los funcionarios del Servicio de Vigilancia Aduanera y con el apoyo de la Guardia Civil en el ejercicio de sus funciones como resguardo fiscal del Estado y las de prevención y represión del contrabando. El Área de Investigación Patrimonial de la Subdirección General de Operaciones dependiente de la Dirección Adjunta de Vigilancia Aduanera se ocupa, entre otras tareas, de coordinar las actuaciones del Servicio de Vigilancia Aduanera en materia de BC, incluidas las operaciones de control de efectivo.
- Por su parte, dentro de la **Fiscalía General del Estado**, las unidades fiscales especializadas en investigar delitos precedentes concretos y delitos relacionados de BC/FT son:
  - **Fiscalía Especial Antidroga**: para delitos de tráfico de drogas y el blanqueo relacionado con este delito.
  - **Fiscalía Especial contra la Corrupción y la Criminalidad Organizada:** para delitos relacionados con la corrupción (cohecho, prevaricación, malversación, etc.), la delincuencia organizada y el BC relacionado con estos delitos (se excluyen delitos de tráfico de drogas o de terrorismo).
  - **Fiscalía de la Audiencia Nacional**: para delitos de terrorismo y de financiación del terrorismo.
  - En el ámbito judicial, las causas por delitos de BC pueden ser juzgadas, dependiendo de las circunstancias y de la gravedad de los delitos, por las **Audiencias Provinciales, la Audiencia Nacional** y, en casos excepcionales, por los **Tribunales Superiores de Justicia** de las Comunidades Autónomas.

Por su parte, la Audiencia Nacional tiene competencia exclusiva para conocer de las causas por financiación del terrorismo y aquellas de BC relacionado con éste.

4. ANÁLSIS DE HITOS: EL IMPACTO DE LA PANDEMIA COVID-19 Y DE LA GUERRA ENTRE RUSIA Y UCRANIA.

4.1. El impacto de la pandemia COVID-19.

El COVID-19 fue una crisis internacional que afectó tanto al ámbito humanitario, como al económico y al social. Como respuesta a la declaración del COVID-19 como pandemia el 20 de marzo de 2020 por parte de la Organización Mundial de la Salud, se aprueba en España Real Decreto 463/2020, de 14 de marzo. Este Real Decreto declara el estado de alarma con el objetivo de gestionar y combatir la situación de crisis sanitaria ocasionada por el COVID-19.

En este contexto, se aprueban medidas de limitación de los movimientos nacionales a aquellos de primera necesidad, afectando al cierre, entre otros, de actividades económicas, colegios y fronteras, que requirieron de una acelerada adopción de nuevas tecnologías y digitalización de sectores, empresas e instituciones para el desarrollo de su actividad. La economía mundial se vio afectada por esta crisis y la delincuencia financiera se incrementó notablemente, tal y como reflejan las cifras de la Memoria Estadística de BC/FT, donde se muestra que las alertas por BC/FT se incrementaron en un 51%, las sentencias judiciales aumentaron un 19% y las sentencias condenatorias un 36% si comparamos los datos de 2021 respecto a 2019. En 2022 los datos de sentencias, tanto judiciales como condenatorias, se han situado en cifras similares a las que había en 2019.

Los datos de las comunicaciones por indicio realizados por el Sepblac muestran que, entre las actividades delictivas comunicadas por los sujetos obligados, los delitos contra el patrimonio fueron los que sufrieron un crecimiento

exponencial, pasando de 465 comunicaciones por indicio en 2019 a 3.044 en 2022, suponiendo un incremento del 555% en 2022 respecto de 2019.

En el estudio "Digitalización Financiera y COVID-19: Evidencia Empírica"[9] se analiza la digitalización financiera y las implicaciones derivadas de la pandemia de la COVID-19 y se corrobora el potencial uso por los ciudadanos de canales digitales a la hora de interactuar con las entidades financieras y la ejecución de pagos digitales, teniendo como principal causa las medidas de confinamiento y de distanciamiento social establecidas durante la crisis sanitaria.

En el ámbito del BC/FT, el resultado de la crisis sanitaria y la acelerada digitalización, tal y como se ha mencionado anteriormente, supone un aumento de los delitos del patrimonio especialmente los relacionados con las estafas, ciberdelitos, suplantaciones de identidad, falsificaciones de productos sanitarios, fraudes para la obtención de fondos públicos, evasión fiscal y estafas vinculadas a donaciones.

Por otro lado, las dificultades económicas que atravesó el tejido empresarial constituyeron un escenario ideal para introducir fondos de origen ilícito en la economía por grupos de delincuencia organizada. Además, se produjo una reducción del empleo de dinero físico efectivo entre particulares lo que incrementó los envíos camuflados en transacciones comerciales o de transportes de mercancías junto con el aumento de transferencias bancarias en la actividad del denominado "mulero" tradicional.

No obstante, la legalización del dinero obtenido por las organizaciones criminales sufrió una ralentización durante el estado de alarma debido a la limitación de movimientos nacionales que se dictó.

Una de las principales vulnerabilidades del sistema preventivo español fue la disminución de las inspecciones *in-situ* de los supervisores que obligaron adaptar el modelo supervisor a las necesidades del momento, afectando principalmente a las inspecciones que estaban en curso.

En el ámbito jurídico, la transposición de la V Directiva al ordenamiento jurídico español también sufrió retrasos ante la necesidad de emitir urgentemente medidas de contingencia sanitarias, económicas y sociales para combatir los efectos de la crisis. Sin embargo, el Real Decreto-ley 7/2021, de 27 de abril, y la Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas permitieron realizar dicha trasposición.

4.2. El impacto de la guerra entre Rusia y Ucrania.

En febrero de 2022, Rusia inició una guerra de agresión contra Ucrania que continúa en la actualidad. La existencia de una guerra en suelo europeo y sus consecuencias dibujan un escenario en el que surgen nuevos riesgos en relación con el BC/FT y sus delitos subyacentes.

En particular, existe el riesgo de que armas utilizadas en el conflicto se desvíen para su uso con fines delictivos en el resto de Europa. En consecuencia, la Unión Europea está ayudando a Ucrania a activar los controles necesarios para evitarlo.

Por otro lado, es necesario extremar los controles en el comercio de material de defensa y doble uso, con el objetivo de que Rusia y sus aliados no se abastezcan de productos que puedan destinar a su esfuerzo de guerra.

La invasión de Ucrania ha significado un importante movimiento de personas que huyen de la guerra. En situaciones así, aumentan los riesgos de que la población migrante sea objeto de delitos relacionados con el tráfico de seres humanos. Por ello, es necesario mantener la vigilancia sobre las operativas financieras que puedan estar relacionadas con su explotación.

[9] Funcas, 2021.

Los movimientos de personas conllevan movimientos de efectivo y estos movimientos también pueden ser aprovechados por el crimen organizado para trasladar dinero de origen ilegal.

Se han establecido sanciones internacionales contra Rusia y Bielorrusia con motivo de la invasión de Ucrania. Las medidas de la Unión Europea están concebidas para debilitar la base económica de Rusia, privándola de tecnologías y mercados vitales, y limitando de forma considerable su capacidad para mantener la guerra. Las sanciones se aplican a Rusia y Bielorrusia y son ampliación y extensión de las que ya se venían aplicando desde 2014, como consecuencia de injerencias rusas en Ucrania. Entre las sanciones se cuentan, entre otras:

- Los embargos de armas.
- Las restricciones a la admisión de personas incluidas en listas de sanciones (prohibición de viaje).
- La inmovilización de bienes pertenecientes a personas o entidades incluidas en listas de sanciones.
- Las sanciones económicas o restricciones aplicables en determinados sectores de actividad económica, como la prohibición de importar o exportar determinados bienes, la prohibición de invertir, la prohibición de prestar determinados servicios, etc.

Las sanciones individuales obligan a congelar el patrimonio en Europa de determinadas personas y entidades especialmente designadas. La congelación afecta no solo al patrimonio nominal del sancionado, sino que debe extenderse a los activos bajo su control. En este punto, es relevante la correcta identificación de la titularidad real. En aquellos casos en que el sancionado realiza acciones tendentes a la elusión de las sanciones, la prueba del control de sus bienes puede ser difícil. Las sanciones comerciales aumentan las posibilidades de contrabando, alterando el verdadero origen o destino de las mercancías y desviando los cobros y pagos a través de países terceros.

La prohibición de pagos con el sector público de Rusia y con las empresas rusas de determinados sectores puede conducir a la creación o consolidación de mecanismos de compensación de los flujos financieros derivados del comercio ruso, evitando la transferencia directa de fondos.

5. PRINCIPALES AMENAZAS DE BLANQUEO DE CAPITALES.

En la identificación de las ***amenazas*** dentro del ámbito de la lucha contra BC/FT debe seguirse la definición dada por GAFI: "*aquellas personas, grupos de personas o sus actividades que suponen un potencial peligro por su capacidad para causar daño al Estado, la sociedad, la economía u otros elementos fundamentales de la vida de un país".*

En el caso concreto del BC, las organizaciones delictivas y sus actividades constituyen amenazas que se aprovechan las vulnerabilidades del sistema para dar apariencia de legalidad a sus beneficios económicos ilícitos obtenidos de estas actividades delictivas.

La identificación de las principales amenazas existentes en las actividades de BC se lleva a cabo mediante los diferentes análisis y las aportaciones de aquellas instituciones públicas competentes en la persecución de este tipo de organizaciones y actividades.

En España, tal y como se recoge tanto en la Memoria Estadística Anual BC/FT publicados por la Comisión de Prevención, con información de inteligencia financiera del Sepblac y de las FCSE, como en el Sistema Estadístico de Criminalidad del Ministerio del Interior, las principales amenazas en materia de BC proceden de:

(i) El crimen organizado.
(ii) El tráfico de drogas.
(iii) Los delitos económicos y financieros, principalmente relacionados con fraudes y actividades de corrupción.

A estos delitos se añaden las amenazas relacionadas con las meras actividades de BC vinculadas a delitos cometidos en España y otros países.

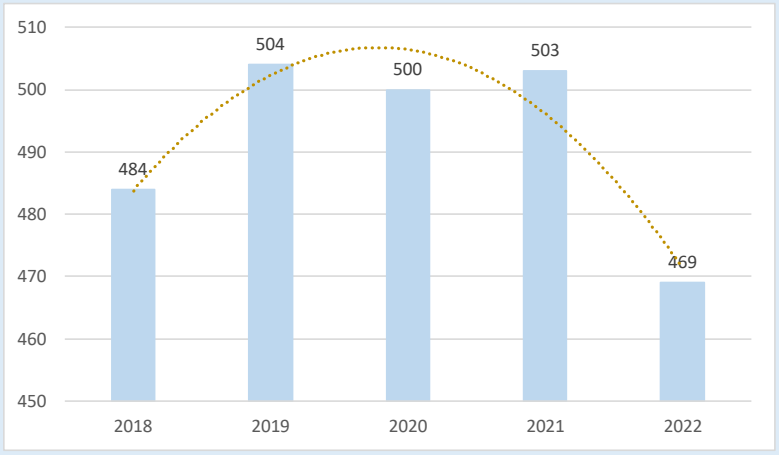
5.1. Crimen Organizado.

En la actualidad, hay diversos análisis que identifican al crimen organizado como una de las principales amenazas para la seguridad española. Entre ellos, se pueden mencionar la Estrategia de Seguridad Nacional 2021, la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (2019-2023) y el Informe Anual de Seguridad 2022.

Las conclusiones de estos estudios se refuerzan por los datos estadísticos publicados anualmente por el CITCO y por las cifras de delincuencia reflejadas en los informes del Ministerio del Interior, que determinan que el crimen organizado se trata de un fenómeno de naturaleza transnacional, flexible y opaca con una enorme capacidad de desestabilización, que puede afectar a estructuras y valores sociales, económicos o políticos.

Estas características hacen que el crimen organizado esté progresivamente interrelacionado con la ejecución de actividades ilícitas como el tráfico de drogas, los ataques de *ransomware*, la trata de seres humanos, la evasión de impuestos o el terrorismo, entre otras. El Informe de Seguridad Nacional 2022 confirma que cada vez es más frecuente la especialización y la generación de sinergias y conexiones entre organizaciones criminales para compartir o facilitar recursos.

CUADRO 2. Grupos de crimen organizado con actividad en España 2018-2022



Fuente: Elaboración propia, datos Ministerio del Interior-CITCO

La Estrategia de Seguridad Nacional 2021 planteó como líneas de acción para la lucha contra el crimen organizado y la delincuencia grave: (i) elaborar un plan estratégico de lucha contra el enriquecimiento ilícito de las organizaciones criminales y los delincuentes y (ii) desarrollar un plan estratégico específico nacional contra la trata y la explotación de seres humanos.

En el marco del desarrollo de estas líneas de acción, el Consejo de Seguridad Nacional aprobó en noviembre de 2021 el *"Plan Estratégico Nacional contra la Trata y la Explotación de Seres Humanos 2021-2023-PENTRA"*. Por otro lado, en febrero de 2024 se ha presentado "*Plan Estratégico de Lucha Contra el Enriquecimiento Ilícito de las Organizaciones Criminales y los Delincuentes– PELCEIL*". Ambos planes son coordinados por el CITCO con la participación de otras

autoridades[10] y vienen a dotar de mayor eficacia y operatividad a las diferentes medidas preventivas establecidas en cada ámbito y a impulsar nuevas acciones en ámbitos no abordados, en el caso del PENTRA, así como a optimizar las acciones de recuperación de activos ilícitos.

Se ha detectado la proliferación de actividades relacionadas con el crimen organizado, algunas emergentes a causa de las nuevas tecnologías y otras que han evolucionado por la utilización de éstas. Entre las operativas detectadas vinculadas al crimen organizado está el uso de sistemas *bancarios clandestinos /Underground Banking*. Esta actividad ha generado un nuevo ecosistema financiero complejo, creado y gestionado por las organizaciones criminales para facilitar su actividad criminal y beneficiarse de la misma. Las organizaciones criminales, especialmente las que actúan a nivel internacional y cuentan con gran capacidad económica, han incrementado la oferta de sistemas bancarios clandestinos una actividad criminal independiente, dando servicio a numerosas organizaciones criminales de diversa índole.

Este sistema financiero clandestino está controlado por profesionales que usan diferentes tipologías conocidas de blanqueo para la movilización de fondos. Entre los métodos utilizados en el ecosistema financiero clandestino, se incluyen el esquema de compensación tradicional como el *hawala*, en los que no solo se realizan operaciones de compensación efectivo con efectivo, sino que cada vez se detecta más operaciones de compensación efectivo-criptoactivos (CA) o CA-efectivo. Esta combinación agiliza el movimiento de fondos a nivel mundial y dificulta aún más la trazabilidad de los movimientos.

Por otro lado, este sistema clandestino se mezcla también con operaciones de blanqueo a través de transacciones comerciales internacionales (*trade-based money laundering*), en las que se mezclan flujos de dinero lícito e ilícito y operaciones reales con operaciones ficticias de importación y exportación a gran escala. En esta operativa comercial se utiliza tanto el sistema financiero oficial como el clandestino, y sirven para camuflar operativas de blanqueo y/o financiar actividades criminales a gran escala.

El fenómeno criminal de los sistemas bancarios clandestinos es una realidad extendida en la economía, la cual es muy difícil de cuantificar, dado que la ausencia de evidencias que permitan su identificación y persecución policial.

En el Informe de Seguridad Nacional 2022, destaca el tráfico de drogas como la manifestación más importante del crimen organizado. Sin embargo, en este documento se pone en relieve la evolución de esta actividad delictiva englobando dentro de la misma la existencia de grupos de carácter poli-criminal; la aparición y desarrollo del fenómeno "pandillero" (grupos violentos juveniles); y la actividad en España de nuevos grupos de carácter internacional con sede o con sus dirigentes ubicados en otros países (Países Bajos, Países del Golfo, Reino Unido etc.). Esta actividad internacional, que crea la generación de sinergias entre grupos criminales internacionales ha favorecido la generación de plataformas y estructuras criminales complejas con apoyos en diferentes países, lo que dificulta las investigaciones sobre las mismas y su desarticulación.

En el ámbito económico, los delitos relacionados con el cibercrimen son los que mayor crecimiento han experimentado, siendo los fraudes informáticos la actividad con más incidencia en este ámbito, favorecida por el uso de CA y monedas virtuales con técnicas que permiten la pérdida de trazabilidad de estos con el fin de ocultar su origen ilícito.

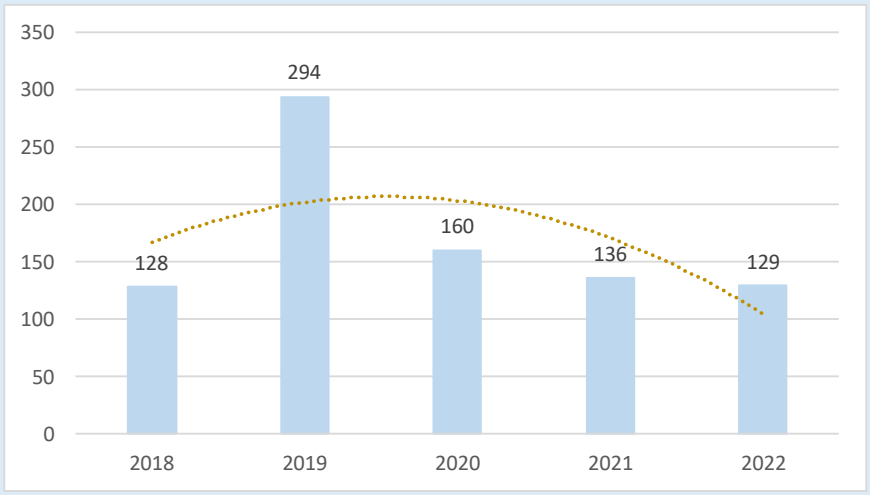
La respuesta del Ministerio del Interior con el fin de combatir estos ciberdelitos se articula de manera principal sobre la base del Plan Estratégico contra la Cibercriminalidad (PECC), cuyo foco es la prevención y cuenta como herramienta con el fomento de la colaboración entre las diferentes FCSE y los operadores jurídicos.

[10] FCSE, varios Ministerios (Igualdad, Inclusión, Seguridad Social y Migraciones, Trabajo y Economía Social, Justicia, Derechos Sociales y Agenda 2030, Educación y Exteriores, Economía, Comercio e Industria), Consejo General del Poder Judicial, Fiscalía General del Estado y Red Española Contra la Trata de Seres Humanos.

En este enfoque económico, no hay que olvidar que la articulación del crimen organizado bajo apariencia de negocios lícitos tiene como objetivo último la obtención de grandes beneficios económicos, generalmente dentro de estructuras complejas donde intervienen sociedades creadas para el fin delictivo u otras cuya actividad es lícita y se utilizan como medio para la canalización de fondos.[11].

En el ámbito social, el crimen organizado adquiere especial relevancia cuando implica acciones relacionadas con la trata de seres humanos como pueden ser mujeres que sufren explotación, menores víctimas de producción y distribución de material de abuso sexual infantil, o el tráfico y explotación de personas, en general. Este enfoque, no solo supone una amenaza para la seguridad nacional, sino que implica una grave vulneración de los derechos humanos que necesita acciones que favorezcan la prevención mediante la persecución eficaz de los actos de explotación derivados de los delitos de trata y la persecución y sanción penal de los individuos implicados, sin desatender la protección y atención de las victimas que han sido objeto de la trata.

CUADRO 3. Víctimas de trata sexual 2018-2022

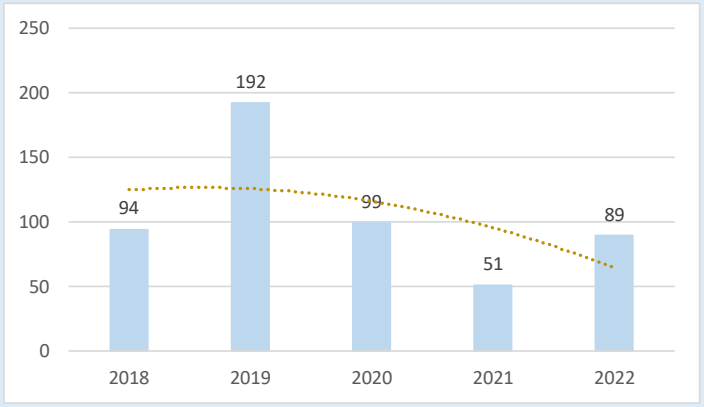


Fuente: Elaboración propia, datos Ministerio del Interior-CITCO

En el cuadro 3, vemos que las cifras de personas víctimas de trata sexual han disminuido en 2022 respecto 2021, según datos del Ministerio del Interior. Las personas identificadas como víctimas por trata laboral (cuadro 4) siguen con la misma tendencia del año 2020.

[11] https://www.guardiacivil.es/ga/prensa/noticias/8398.html
Primera operación con detenidos en España de la Fiscalía Europea contra una trama de fraude del IVA (elperiodico.com).

Cuadro 4. Víctimas por trata laboral 2018-2022



Fuente: Elaboración propia, datos Ministerio del Interior-CITCO

La guerra de Ucrania ha incrementado las amenazas relativas a la trata de seres humanos con fines de explotación sexual y laboral en Europa. Sin embargo, en España no se han identificado grandes cambios en lo que se refiere a las actividades de la delincuencia grave y organizada relacionadas con la guerra en Ucrania o derivada de ella.

Tras la puesta en marcha de las medidas restrictivas de la UE contra Rusia se ha incrementado, por un lado, la amenaza de la llegada de fondos ilícitos utilizando sistemas financieros clandestinos, testaferros y personas interpuestas para eludir las sanciones administrativas impuestas y, por otro, el tráfico de armas procedentes de la guerra por grupos organizados.

En definitiva, el crimen organizado es un fenómeno dinámico, en continua evolución, con gran capacidad de adaptación para la obtención de beneficios ilícitos que lleva implícita la ejecución de otras actividades delictivas como tráfico de drogas, tráficos ilícitos, terrorismo, fraudes, cibercrimen o violencia criminal y que presenta un abanico de actuación supranacional. Esta configuración hace que sea una amenaza global, donde el desarrollo de las nuevas tecnologías, la participación en el sistema financiero de nuevos agentes a través de los cuales se puede canalizar fondos y la configuración de la operativa de la sociedad, cada vez más digital, impulsada por la pandemia COVID-19, potencian los perjuicios que puede causar en el sistema, afectando a la sociedad, economía y seguridad nacional e internacional.

En la lucha contra los daños que llevan asociados las acciones del crimen organizado, la cooperación internacional y nacional de las diferentes FCSE es un factor decisivo. En España, durante el año 2022, se desarticularon total o parcialmente el 93% de los grupos detectados. Por otro lado, el 61% de los grupos presentaban actividad internacional. Entre los grupos vinculados con las **redes de tráfico de drogas,** los más relevantes son:

a) **Grupos relacionados con el tráfico de droga procedente de Latinoamérica** que operan en España en cooperación con redes locales que facilitan su introducción y distribución. En estos casos se produce una vinculación directa entre delito precedente y la actividad de blanqueo de capitales. Estos grupos que operan en España introducen la droga en Europa principalmente mediante rutas preestablecidas a través de nuestro país. Los fondos que generan se introducen en el sistema financiero a través de redes de personas y entidades, que incluyen empresas implicadas en el comercio de mercancías y servicios, lo cual permite justificar sus transferencias e ingresos mediante diversas vías (supuestas transacciones comerciales, ingresos en efectivo, correos humanos o remesas entre otros sistemas).
b) **Grupos relacionados con el tráfico de droga procedente del Magreb,** que al igual que en el caso anterior, operan en España en cooperación con redes locales que facilitan su introducción y distribución. España es, con diferencia, el país con más tráfico de cánnabis de la UE, como se analiza en el siguiente apartado. Por su

cercanía geográfica, estos grupos organizados utilizan España, sobre todo, como tránsito hacia otros destinos europeos, en coordinación con grupos criminales locales, lo que ha generado una situación grave de seguridad que afecta especialmente a la zona del Campo de Gibraltar. Este tráfico ilegal genera ingentes cantidades de dinero en efectivo, siendo frecuentes las operaciones de transporte de dinero en efectivo, correos humanos y las operaciones de ingreso en el sistema financiero amparadas en supuestas operaciones comerciales.

c) Grupos vinculados con **fraudes tributarios asociados a actividades comerciales**, principalmente a través de empresas de producción y distribución al por mayor de mercancías fabricadas en el extranjero y de su venta en la red minorista en todo el territorio nacional. Estos grupos principalmente de procedencia china y del este de Asia consiguen generar enormes cantidades dinero que vulnera la normativa tributaria y que envían al exterior (bien en efectivo, con un uso significativo de correos humanos, o mediante transferencias amparadas en sus actividades comerciales) o que invierten en España, principalmente mediante la compra de locales comerciales. Estas actividades de blanqueo procedentes de ilícitos fiscales también amparan en ocasiones otros delitos precedentes como delitos contra la libertad sexual, contra los derechos de los trabajadores, tráfico ilegal de drogas o juego ilícito, entre otros.

d) Grupos especializados en **delitos contra la propiedad**, robos en instalaciones empresariales, domicilios, tráfico ilícito de vehículos y otros delitos violentos contra entidades bancarias y establecimientos con mercancías de alto valor como joyas y arte. Se trata de grupos generalmente de origen extranjero, principalmente del este de Europa y oeste de Asia, en algunos casos itinerantes, que no siempre tienen una residencia estable en España. Por la propia naturaleza de los delitos cometidos y las medidas existentes en el propio sistema económico es difícil que los bienes obtenidos se integren en el sistema financiero español, por lo que es frecuente que los trasladen hasta otros territorios, en ocasiones fuera de la Unión Europea, en los que se ingresan en entidades financieras, se ofrecen a la venta, etc.

e) Grupos especializados en la **utilización fraudulenta de medios de pago,** especialmente las tarjetas de crédito y débito. Las debilidades del sistema y el número de fraudes han hecho que las entidades emisoras desarrollen complejos sistemas que garanticen la seguridad de los usuarios, expuestos a robos y al copiado ilegal de los datos. Los grupos que cometen estos delitos operan en todos los países de la UE, discriminando los territorios de residencia de los titulares, de captura de los datos, y de uso fraudulento. La extensión de la oferta de establecimientos en los que se puede operar telemáticamente para adquirir bienes y servicios, realizar apuestas o participar en juegos de azar, etc., ha supuesto la introducción de un elemento que favorece enormemente las operaciones de blanqueo de fondos procedentes de estos delitos.

f) Grupos especializados en **fraudes masivos de carácter telemático**. Hace varios años que las organizaciones especializadas en la lucha contra el crimen vienen alertando sobre una delincuencia muy especializada en la comisión de fraudes masivos, principalmente procedentes del oeste de África, mediante el envío de las originarias "*cartas nigerianas*", en las que se lanzan mensajes (postales, telefónicos, electrónicos, etc.) dirigidos a potenciales víctimas para obtener fondos. También se ha verificado la relación de estos grupos con otros delitos (entre ellos los que atentan contra la libertad sexual). Las operaciones financieras con los fondos remitidos por las víctimas son rápidamente objeto de transferencias mediante diversos sistemas, incluyendo el uso de entidades de pago y cuentas bancarias abiertas con identidades o actividades falsas.

g) Grupos que **realizan actividades delictivas en otras jurisdicciones, pero traen fondos ilícitos a España**. Es una delincuencia que, en España, en términos generales, no realiza acciones criminales concretas, pero realiza operaciones de blanqueo de capitales en compras de bienes de lujo y bienes inmuebles. Destaca la presencia de grupos procedentes de otros países europeos en los que cometen delitos relacionados con la corrupción, la extorsión y con delitos relacionados con tráficos ilícitos, que intentan establecer en España el lugar de inversión o de adquisición de las residencias de algunos de sus dirigentes e integrantes, en ocasiones mediante complejos esquemas de blanqueo de dinero. Estos grupos integran sus beneficios ilícitos a través

de complejas operaciones societarias y comerciales, en las que se utilizan sociedades mercantiles inscritas en distintas jurisdicciones, algunas de ellas en países de la UE, y cuyo reflejo bancario inicial se produce en países de todos los continentes, también en algunos casos países de la UE.

h) Grupos vinculados a **tramas de corrupción política o financiera**, tanto nacional como internacional. En términos generales, estos grupos realizan comportamientos con efectos en varios países, de tal forma que el país en el que se produce el hecho delictivo a través del cual se consuma la corrupción (malversación de fondos, cohecho, fraude, etc.) o el delito financiero correspondiente es diferente del de residencia de los autores, y diferente también de aquel en el que se reciben los fondos o se adquieren los bienes, mayoritariamente bienes inmuebles.

Los **grupos españoles** implicados en estos comportamientos realizan sus acciones delictivas en nuestro país, generalmente vinculadas a operaciones urbanísticas y de servicios públicos, y utilizan países extranjeros para mantener las cuentas y depósitos y para domiciliar las sociedades mercantiles bajo cuya titularidad mantienen esas cuentas.

Por su parte, los **grupos extranjeros** vinculados a estos delitos de corrupción eligen España como uno de los países donde destinar los fondos, mediante complejos esquemas de transferencia internacional por dos o más países, y la ulterior aplicación para la compra de bienes, generalmente bienes inmuebles de lujo en zonas turísticas, pero también en barrios de mayor nivel económico de las grandes ciudades.

Los métodos utilizados por estos grupos para canalizar fondos son muy diversos donde variando desde el uso de sistemas bancarios clandestinos donde se identifica la presencia de CA hasta la conducción de fondos a través del mercado del arte y las antigüedades dadas sus características de escasa o nula depreciación.

5.2. Tráfico de drogas[12].

El tráfico de drogas en España está vinculado al panorama europeo donde se observa que hay un incremento del consumo y disponibilidad de drogas en la sociedad.

Las circunstancias, el clima y la geografía de España hacen que sea considerado un país tradicional de tránsito y consumo de drogas.

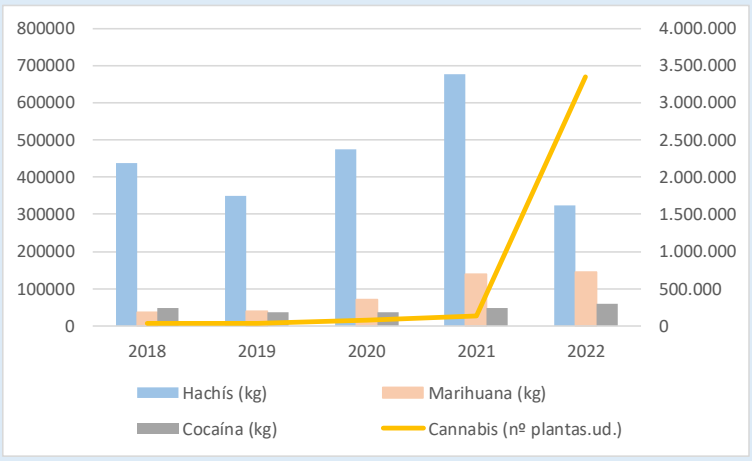
A pesar de que las sustancias que tienen una mayor presencia son el hachís y la cocaína, la Memoria de la Fiscalía General del Estado 2023 destaca como alarmantes la banalización del consumo de sustancias como el cánnabis y el papel de España en la actualidad, ya que se ha convertido en el primer productor de cánnabis en la UE.

Esta configuración como país productor genera un riesgo en el aumento del consumo y favorece la instalación en España de organizaciones criminales extranjeras. Esta realidad es la que en la actualidad está requiriendo mayores esfuerzos en las investigaciones policiales, ya que el tráfico de drogas puede llevar asociados otras actividades delictivas como son el crimen organizado, la trata de seres humanos, la evasión fiscal o el tráfico de armas. Las FCSE, a raíz de sus investigaciones, confirman el consumo de una serie de drogas caracterizadas por estar fuera de los convenios de fiscalización internacional, y que, pese a que por el momento no presentan cifras alarmantes, su consumo se está acelerando, especialmente por su publicidad online. Son las denominadas Nuevas Sustancias de Síntesis (NPS por sus siglas en inglés).

En cuanto a las incautaciones efectuadas, según los datos del Informe 2023 Sobre Alcohol, Drogas y Tabaco, en 2022 se decomisaron más de 389 toneladas. En el cuadro 5 se observa la evolución de la droga incautada.

[12] Memoria Fiscalía General del Estado 2023. Apartado Fiscalía Especial Antidroga.

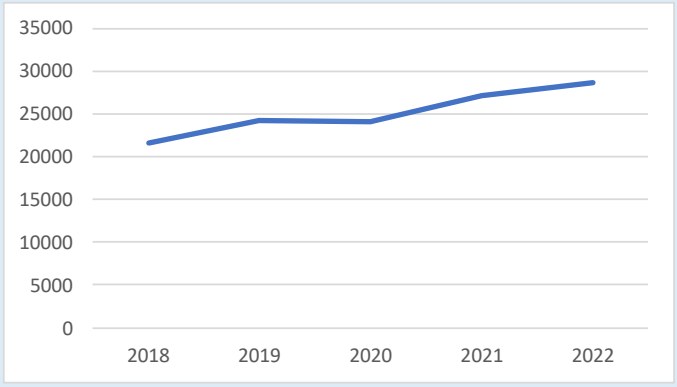
CUADRO 5. Evolución de la droga incautada en España 2018-2022



Fuente: Elaboración propia, datos Ministerio del Interior-CITCO

En 2022 se realizaron 28.678 detenciones por delitos de tráfico de drogas. En el cuadro 6 se puede ver la tendencia creciente que existe en el número de detenciones, alcanzándose el nivel más alto en el año 2022.

CUADRO 6 Detenciones por tráfico de drogas (2018-2022)



Fuente: Observatorio español de las drogas y Adicciones

El 55,7% de detenciones se produjeron por tráfico de cannábicos, seguidas por las realizadas por tráfico de cocaína (23,5%), las drogas de tipo anfetamínico (9,8%) y opiáceos (4,6%).

Según la Delegación del Plan Nacional contra las Drogas, los datos de consumo que proporciona periódicamente el Observatorio Español de la Droga y las Toxicomanías reflejan que el porcentaje de personas que han consumido cánnabis y cocaína se han incrementado desde el año 2020, mientras que el resto de las sustancias se mantienen en porcentajes similares.

El total de procedimientos tramitados en la Fiscalía Especial Antidroga por tráfico de drogas en 2022 fue de 21.740 lo que supone un incremento de más del 20% desde 2018, en los que, a pesar de la dificultad de identificación del delito precedente se considera que el BC es una cuestión trasversal en este tipo de actividad delictiva. Junto a Madrid (3.029 procedimientos que suponen un incremento del 13,74% en 2022) destacan las provincias de Sevilla y Las Palmas de Gran Canarias, que presentan un incremento del 17 % y 38%, respectivamente, desde 2021.

En cuanto a los condenados por tráfico de drogas por la Audiencia Nacional en 2022, los datos muestran que, de las 29 sentencias en materia de salud pública dictadas por la Sala de lo Penal de la Audiencia Nacional, han tenido como condenados 64 ciudadanos españoles, 59 extranjeros y 1 persona jurídica.

El Informe de Seguridad Nacional 2022 señala que el estrecho de Gibraltar y el mar de Alborán son zonas sensibles en relación con el narcotráfico. Con la finalidad de combatir esta amenaza, las FCSE se encuentran implicadas en diversos planes que requieren cooperación nacional entre ellas e internacional con el resto de las autoridades extranjeras[13].

El Informe sobre el Balance de Criminalidad del cuarto trimestre de 2022 muestra un aumento del 14,4% de los delitos de tráfico de drogas en 2022 respecto a 2019 y de 3,8% respecto a 2021, atribuyendo este aumento a la actuación de las FCSE, en el marco de planes específicos como el Plan Especial de Seguridad para el Campo de Gibraltar, siendo, en realidad, un indicador de actividad policial frente a este tipo de delitos.

El Plan Especial de Seguridad para el Campo de Gibraltar se encuentra prorrogado hasta el año 2025, siendo la cuarta prórroga realizada. Durante su tercera prórroga (con vigencia hasta el 31 de diciembre de 2023), se amplió su territorio de actuación a 3 provincias andaluzas, abarcando la totalidad de la costa sur española.

5.3. Delitos económicos y financieros: fraudes, delito fiscal, y casos vinculados a la corrupción.

El Informe de Seguridad Nacional 2022 identifica a los delitos económicos y financieros como la principal amenaza a la estabilidad económica y financiera de España. Este razonamiento está basado en los efectos nocivos que generan, tales como: caída en los índices de productividad; desviación de fondos que inicialmente están destinados al desarrollo de políticas públicas; alteración del orden socioeconómico; o la pérdida de legitimidad de los poderes públicos, que merma la confianza del ciudadano y reduce la credibilidad y reputación del país.

En 2022 se han incrementado las comunicaciones de operativas sospechosas relacionadas con el fraude en un 554% con respecto de 2019, seguido de aquellas vinculadas a delitos contra la Hacienda Pública. Los delitos del patrimonio asociados a fraudes y los delitos que engloban los fraudes fiscales de IVA representan el 43% de los delitos tipificados en las comunicaciones por indicio realizadas por los sujetos obligados en 2022.

La progresiva digitalización de la sociedad y, en particular, los avances en los sistemas de comunicaciones, el desarrollo de las redes sociales y la generalización del comercio online han abierto nuevas posibilidades para la realización de fraudes cometidos a través de medios tecnológicos (ciberfraude o ataques cibernéticos).

Gran parte de estos fraudes a través de medios tecnológicos son realizados por grupos internacionales de crimen organizado que reparten entre subgrupos altamente especializados la realización de cada una de las distintas fases del proceso del fraude, incluido el blanqueo de los beneficios obtenidos. Generalmente, esas fases se realizan en diferentes países, lo que añade dificultad a su investigación y persecución. La capacidad de estos grupos es tal que se ha llegado a calificar como *industrialización del fraude*.

El ciberfraude es una amenaza global que genera perjuicios individuales a personas y entidades directamente afectadas y socava la confianza del público en las nuevas tecnologías, la economía, el sistema financiero y las instituciones.

[13] Ejemplo de ellos se mencionan: Vigilancia Aduanera participa en la Operación PASCAL, a nivel nacional se colabora en la Campaña Naval ORION, la Policía Nacional y la Guardia Civil intervienen en el "Proyecto de cooperación portuaria", la Guardia Civil ha llevado a cabo entre los meses de julio y septiembre de 2022 la "Operación Puertos Seguros" o Salvamento Marítimo vigila intensamente la superficie marina mediante aviones y satélites con el fin de incrementar la seguridad marítima.

Esta globalidad está presente entre las actividades desarrolladas por los grupos de crimen organizado dedicados al fraude que, para blanquear los fondos obtenidos mediante su actividad delictiva, necesitan conseguir la perdida de trazabilidad de los fondos de las víctimas del fraude. Habitualmente, este tipo de blanqueo implica movimientos internacionales de fondos, conversión de divisas en dinero en efectivo y, más recientemente, la conversión en CA.

Entre los medios utilizados para realizar el BC con origen en el ciberfraude, se encuentra la utilización de cuentas bancarias para recoger directa o indirectamente los fondos de las víctimas para a continuación enviarlos, en la mayor parte de los casos, hacia otros países. La operativa que se observa en estas cuentas puede ser variada. Las entradas pueden proceder de las víctimas de los fraudes o de otras cuentas intermedias y se realizan, generalmente, mediante transferencias. Las salidas más frecuentes son transferencias internacionales y retiradas de dinero en efectivo (principalmente en el extranjero). En los últimos años, la compra de CA es el destino de gran parte de los fondos defraudados. Asimismo, los fondos pueden mezclarse con operaciones de comercio internacional, aplicándolos al pago de exportaciones (en efectivo o mediante transferencia) y realizando luego compensación con los importadores de los países destino de las mercancías exportadas.

Con el objetivo establecer límites al fraude tributario, entró en vigor la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego. Esta ley modificó el citado artículo 7 de la Ley 7/2012, de 29 de octubre, reduciendo el límite general de pagos en efectivo de 2.500 a 1.000 euros y, en el caso de las personas físicas particulares con domicilio fiscal fuera de España, de 15.000 a 10.000 euros.

CUADRO 7. Tipologías de fraude

Fraude a la Seguridad Social: existen diferentes modalidades de comisión de fraude a la Seguridad Social, pudiendo consistir en impagos de las contribuciones correspondientes a los trabajadores, o en la percepción de prestaciones o ayudas públicas por causas inexistentes. Este tipo de actividades fraudulentas inciden perjudicialmente sobre la competencia desleal; la economía sumergida; la corrupción; los derechos de los trabajadores; y el desarrollo de conductas asociadas a la trata de seres humanos para su explotación laboral, entre otras materias.

Tráfico de influencias, malversación de fondos, prevaricación y cohecho (propio e impropio): se trata de delitos vinculados a actividades de corrupción que suelen estar relacionadas con la decisión de autoridades públicas de otorgar a determinadas entidades privadas el desarrollo de actuaciones públicas mediante contratos, concesiones, licencias, etc., en muchos casos relacionados con servicios públicos o con obras públicas y licencias de carácter urbanístico. Estas decisiones pueden conllevar emisiones de facturas falsas; contraprestaciones económicas o materiales para la autoridad otorgante; o concesiones a entidades indirectamente controladas por la propia autoridad otorgante, lo que permite una legitimación automática de los beneficios obtenidos de la actividad delictiva.

Fraude tributario: junto a los delitos fiscales tradicionales por impago de impuestos a la Hacienda Pública (renta, patrimonio, sociedades), se mantienen las cifras de las modalidades delictivas relacionadas con el fraude en el IVA, bien evitando su pago o mediante la devolución fraudulenta de reembolsos del IVA por parte de las autoridades nacionales después de una cadena de transacciones (los denominados “carruseles”). En los últimos años la AEAT ha destinado una considerable cantidad de recursos a la persecución de estas conductas en vía judicial, recursos que se ven incrementados cada año.

Fraude aduanero: la actividad delictiva más relevante consiste en la importación de mercancías minusvalorando tanto las cuantías de producto con las que se comercia como los valores declarados en la Aduana, defraudando a la Hacienda de la UE en los derechos de importación (arancel). Estos fraudes tienen especial relevancia en productos importados de Asia. Los grupos criminales usan varios sistemas para evitar el pago de tributos y generar importantes beneficios vendiendo esos productos (auténticos o falsificados) a precios más bajos que sus equivalentes en el mercado, lo que genera situaciones de competencia desleal. La importancia y el número de operaciones desarrolladas por la AEAT en los últimos años han puesto de manifiesto la existencia de importantes operativas y sistemas de BC en estas actividades. Otros fraudes relevantes afectan al origen o clasificación arancelaria de las mercancías, así como el abuso de determinados regímenes tales como el de depósito distinto del aduanero y el régimen 42 (obtención de exención de IVA cuando las mercancías introducidas se expiden a otro estado de la UE).

Delitos societarios: se trata de comportamientos de naturaleza heterogénea llevados a cabo por administradores o ejecutivos de sociedades que, para lograr ciertos fines particulares, participan en el mercado en perjuicio de la propia sociedad, de sus socios o de terceros. En numerosas ocasiones vienen vinculados con delitos de falsedad documental societaria.

Falsedad en subvenciones públicas: consistente en la obtención indebida de recursos públicos a través del falseamiento de las condiciones requeridas para su concesión u ocultando las que la hubiesen impedido, o incumpliendo las condiciones o fines para los que la subvención fue concedida.

Fraude de inversiones: se trata de fraudes en los que se utiliza el engaño para convencer a la víctima para que invierta el dinero en productos de inversión, que no están regulados por la CNMV, o en CA (modalidad que se ha visto incrementada en los últimos años). Puede ser realizadas por individuos o sociedades (los denominados "chiringuitos financieros") sin estar autorizados para actuar en los mercados de valores ni prestar servicios de inversión previstos en la Ley del Mercado de Valores. Las víctimas son captadas vía telefónica o a través de un portal web y son defraudadas al hacer transferencias, a veces por cantidades millonarias, a las cuentas bancarias que se les indica. Existen tres modalidades principales: los chiringuitos financieros (*boiler room*), esquemas Ponzi y estafas piramidales.

5.4. Blanqueo de capitales por terceros y por delitos cometidos en el extranjero.

La transaccionalidad de las transacciones financieras en un sistema tan globalizado como el actual es un hecho evidente. Las investigaciones realizadas por las distintas autoridades nacionales demuestran la existencia de grupos de delincuencia organizada que están interconectados en múltiples países, facilitándose el BC en España (al igual que en otros países) de fondos procedentes de actividades delictivas cometidas en el extranjero, independientemente que la comisión del delito precedente tenga relación alguna con nuestro país.

Dentro de este marco, los cuerpos policiales han detectado operativas con conexiones nacionales e internacionales, vinculadas a la compraventa de bienes de lujo y obras de arte y al mercado inmobiliario español.

La compraventa de artículos de lujo es una actividad especialmente atractiva para el BC dado que, por sus características, no sólo acumulan mucho valor, sino que además no lo pierden con el paso del tiempo, lo cual permite a las organizaciones criminales recuperar la inversión inicial tras su venta, e incluso obtener mayores beneficios.

Por otro lado, el mercado inmobiliario español es un gran atractivo para el crimen organizado dadas las características económicas de éste y el carácter turístico de nuestro país. En relación con los beneficios que pueden resultar para el BC se destacan aspectos tales como:

- Es un sector tradicionalmente ligado a actividades de generación y ocultación de capitales de origen fiscalmente ilícito.
- La titularidad de bienes inmuebles admite muchas figuras jurídicas distintas, tanto de carácter nacional como internacional, e incluidas las formas de copropiedad temporal o espacial.
- La valoración de los bienes inmuebles tiene un marcado carácter subjetivo, ligado a aspectos no derivados directamente del propio bien.
- Es un sector muy sensible a comportamientos criminales relacionados con la corrupción.

En relación con las inversiones en bienes inmuebles hay que tener en cuenta los riesgos de blanqueo que entrañan los regímenes de ciudadanía por inversión (Golden Passport) y residencia por inversión (Golden Visa) que otorgan la ciudadanía o la residencia a nacionales de terceros países a cambio de consideraciones principalmente financieras. En España los Golden Passport no están contemplados, sin embargo, sí lo están los Golden Visa. La Ley 14/2013, de 27 de septiembre, de Apoyo a los Emprendedores y su Internacionalización, regula un visado de residencia para inversores y una autorización de residencia para inversores.

El visado de residencia para inversores va dirigido a extranjeros no residentes que se propongan entrar en territorio español con el fin de realizar una inversión significativa de capital. Este visado es necesario que sea solicitado por aquellos inversores interesados.

Según datos aportados por el Ministerio de Inclusión, Seguridad Social y Migraciones a *Transparencia International España*[14] sobre los visados de inversores concedidos desde el 1 de enero de 2017 hasta el 31 de marzo de 2022, se extrae que han sido concedidos un total de 6.200 visados a inversores de todas las nacionalidades, de los cuales un 96,18% fue concedido en virtud del supuesto de adquisición de bienes inmuebles.

Los riesgos asociados a este tipo de regímenes están ligados desde el punto de vista del BC a la corrupción, la elusión fiscal, el crimen organizado, la elusión de sanciones financieras internacionales o los movimientos transfronterizos de fondos.

A pesar de estos riesgos cabe mencionar que para realizar este tipo de inversiones inmobiliarias es necesaria la intervención, como mínimo, de notarios, registradores y entidades financieras. Estos sujetos obligados cumplen con las políticas y procedimientos establecidos en la Ley 10/2010, de 28 de abril, además de contar con potentes bases de datos con el fin de identificar la titularidad real de tales inversiones y asegurar el cumplimiento de las medidas de diligencia debida.

6. PRINCIPALES AMENAZAS DE FINANCIACIÓN DEL TERRORISMO[15].

El terrorismo sigue siendo una amenaza nacional e internacional puesto que la evolución del sistema financiero y las nuevas tecnologías generan nuevas oportunidades para la financiación y canalización de fondos de organizaciones terroristas.

[14] https://transparencia.org.es/estudios-y-publicaciones/la-adquisicion-de-la-residencia-en-espana-a-traves-de-golden-visas-principales-riesgos-y-desafios/

[15] Fuentes: “Informe de la Seguridad Nacional 2022”, “Memoria Anual FGE 2023. Fiscalía Audiencia Nacional” “Lucha antiterrorista contra ETA y el terrorismo internacional” - XII Legislatura. Ministerio del Interior.

La capacidad de adaptación de estos grupos terroristas a las barreras preventivas que se establecen por las FCSE plantea la necesidad de identificación y neutralización de las fuentes de financiación.

El terrorismo yihadista se ha fortalecido en África, especialmente en el Sahel, la cuenca del lago Chad y el Cuerno de África.

El terrorismo que persiste en España entraña actualmente características más complejas y diversificadas, siendo el terrorismo yihadista el que genera una mayor amenaza nacional a través de sus dos principales grupos, Dáesh y Al Qaeda, los cuales mantienen una presencia especialmente activa en África. El informe de Seguridad Nacional 2022 evalúa la posibilidad de la realización de acciones terroristas a través de la figura de los "lobos solitarios"[16].

Dentro de este término, se concentran las principales amenazas de la actividad yihadista en Españas que son, por un lado, la existencia de actores individuales y células independientes y, por otro, la figura de los *homegrown terrorist fighters* (en adelante, HTF) que son individuos radicalizados en países europeos, entre los que se incluye España, que hacen llamamientos terroristas a través de internet.

Por otro lado, en España, además de estas acciones individuales, predominan las redes logísticas de apoyo financiero -fundamentalmente Dáesh- y, principalmente, las células de captación, adoctrinamiento y reclutamiento de fieles, tanto en entornos físicos como virtuales.

En este ámbito las nuevas tecnologías adquieren importancia para la divulgación de ideas violentas y extremistas por terroristas con el fin de captar y reclutar a actores individuales a través de redes sociales, plataformas en línea o chats de juegos. Este último canal, es uno de los medios utilizados por los terroristas para comunicarse, radicalizar y reclutar sin dar a conocer el objetivo real del mensaje ya que la propaganda terrorista puede ocultarse en el contenido de los juegos. Dentro de este marco, se resalta la utilización de la inteligencia artificial para la obtención de recursos financieros con los que financiar el terrorismo. En relación con las nuevas tendencias para acometer actividades terroristas, se configura como amenaza para la seguridad nacional la posible utilización por grupos terroristas de vehículos aéreos pilotados de forma remota que pueden ser configurado como arma para la comisión de ataques terroristas.

Por otro lado, como se señalaba en el ANR de 2020, las organizaciones terroristas nacionales vinculadas al independentismo vasco (ETA) y al movimiento armado marxista-leninista (GRAPO) se encuentran desaparecidas o en proceso de desaparición. En este sentido, las actividades vinculadas a ETA, cada vez más residuales, se centran en la reivindicación de la amnistía sin condiciones, para todos los presos de ETA, así como el regreso de los expatriados.

En relación con las investigaciones por las FCSE, en 2022 se han llevado a cabo 100 investigaciones policiales. En el ámbito judicial, se han realizado 163 diligencias previas por terrorismo, que han resultado en 11 sentencias condenatorias y 25 personas condenadas por la Sala de lo Penal.

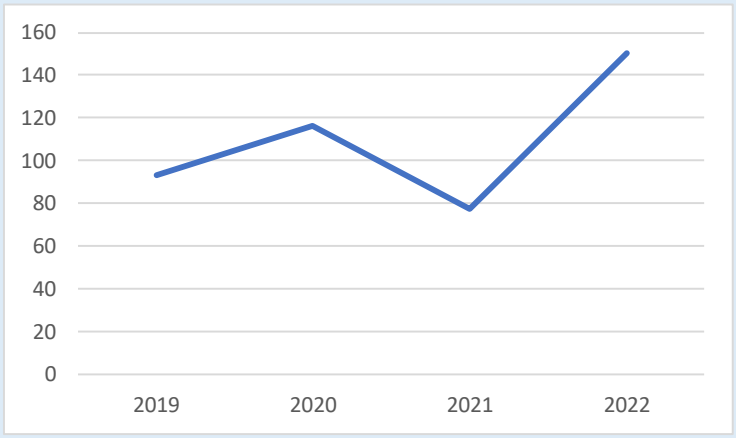
En cuanto a terrorismo nacional, a pesar de que la actividad vinculada a ETA es residual, en 2022 se han realizado varias operaciones policiales que han dejado 55 detenidos, principalmente por desorden público y cuyo foco de actuación ha sido la provincia de Álava.

Por otro lado, de acuerdo con la Memoria Anual de la Fiscalía de la Audiencia Nacional 2023, el terrorismo yihadista mantiene una tendencia alcista en cuanto a diligencias previas incoadas, siendo el dato de 132 para 2022 y suponiendo un 81% del total de las abiertas por terrorismo.

[16] Persona que realiza un acto terrorista sin in estar conectados directamente con un líder, ni recibir el apoyo de una organización o grupo.

En cuanto a las cifras totales de detenidos y procesados por actividades vinculadas con el terrorismo, el cuadro 8 se muestra como la tendencia es creciente, habiéndose experimentado un incremento del 94% en las detenciones respecto a 2019.

CUADRO 8. Detenciones por actividades vinculadas al terrorismo



Fuente: Memoria de la Fiscalía de la Audiencia Nacional 2023

La actividad contraterrorista al yihadismo en España se saldó con 17 investigaciones policiales en 2022 que culminaron en 36 detenidos y operaciones conjuntas con Marruecos, Austria y Suiza que resultaron en 4 detenciones más fruto del intercambio de información con terceros países.

6.1. Terrorismo yihadista.

El terrorismo yihadista se ha configurado como una amenaza permanente con un ámbito de actuación global. Los ataques terroristas en suelo europeo han sido constantes en la última década, impulsados por el surgimiento de Dáesh alimentados por múltiples factores internos y externos, tales como el episodio del conflicto palestino-israelí que se inició con el ataque de Hamás del 7 de octubre de 2023. Dáesh se mantiene como principal amenaza, convirtiéndose en el referente del terrorismo yihadista por su capacidad operativa, medios, proyección mediática y rápida expansión.

Sin embargo, estos grupos se caracterizan por su rápida mutabilidad y su adaptación a los cambios y estrategias seguidas contra ellos. Los atentados indiscriminados en lugares de concentración de personas, medios de transporte o infraestructuras críticas representan una tendencia actual del terrorismo yihadista, que opera tanto en células organizadas como de manera individual, con el fin de producir el mayor número de víctimas y un fuerte impacto propagandístico.

Las actividades llevadas a cabo por los integrantes de las estructuras terroristas yihadistas desarticuladas en España han sido principalmente de captación, reclutamiento, adoctrinamiento y envío de activistas a zonas de conflicto. Igualmente, se han producido detenciones por integración, apoyo logístico, actos de enaltecimiento del terrorismo y amenazas graves con fines terroristas, así como la persecución de la actividad terrorista individual. Internet y las redes sociales son investigadas, analizadas y perseguidas cuando se utilizan como espacio virtual terrorista o bien como su herramienta de comunicación.

Por tanto, los principales elementos y actividades relacionados con las amenazas yihadistas a las que se debe hacer frente son:

- Actualmente, el principal vector de amenaza viene asociado a los **terroristas o células autónomas** que puedan materializar, siguiendo criterios de oportunidad y con medios escasamente sofisticados, pero altamente letales, acciones contra los activos reiteradamente señalados en la propaganda yihadista o atacados en Occidente (grandes concentraciones de personas, lugares turísticos, personal militar y policial o lugares de culto de las distintas confesiones religiosas). No obstante, no pueden descartarse ataques organizados provenientes de células estructuradas vinculadas a Dáesh.

- Los **combatientes terroristas que retornan** de escenarios como Siria e Irak tras haber acumulado conocimiento y experiencia en el manejo de armamento, contactos y conocimiento de rutas y agentes facilitadores, además de actuar como dinamizadores tanto ideológicos como operativos. El proceso de envío de combatientes a zonas de conflicto se lleva a cabo mediante redes nacionales e internacionales, que ha supuesto que residentes en España se hayan desplazado a Siria e Irak, habiéndose detectado actividades de financiación para su desplazamiento y estancia en esas zonas.

- La radicalización, **captación y adoctrinamiento** con fines terroristas forman parte, asimismo, de las amenazas que han adquirido mayor protagonismo en los últimos años. Ello no sólo por las ideologías que los sustentan, sino también porque constituyen el estadio previo a que los individuos inmersos en dichos procesos se vinculen finalmente con grupos y organizaciones terroristas.

- El **desarrollo tecnológico** ha ampliado además el acceso a recursos disponibles para los grupos terroristas, incrementando su capacidad de **financiación, reclutamiento, adiestramiento, propaganda y enaltecimiento**. En un contexto de empleo generalizado de redes sociales crecen los riesgos de difusión de propaganda terrorista y de formas de radicalización y extremismo violento. Internet ha sido la más eficaz herramienta de propaganda y captación yihadista. La idea de la "yihad global" se ha materializado para miles de simpatizantes o seguidores mediante mensajes que distorsionan la realidad, con exaltación épica de los combatientes yihadistas. Los videos constituyen mensajes que expresan la necesidad de abrazar la violencia para combatir la injusticia y la incomprensión de Occidente.

- España, por su **situación geográfica** dentro del continente europeo, es más vulnerable frente a ciertos grupos terroristas. Su proximidad al Magreb, teniendo en cuenta la intensa actividad terrorista y contraterrorista en los países que lo componen, la convierten en foco de atención del terrorismo yihadista, que puede utilizar el elevado tránsito de personas para introducir elementos terroristas en España y el resto de Europa.

España está comprometida en la lucha contra el terrorismo con una respuesta basada en un modelo integral que incorpora su experiencia y coordina la acción con sus aliados, en las iniciativas internacionales y especialmente con la UE. Los distintos actores implicados en la acción antiterrorista están trabajando con la experiencia del pasado y la preparación constante del presente. Un terrorismo global, como es el yihadista, requiere de grandes dosis de cooperación internacional, pero al mismo tiempo se muestra con características autóctonas que hacen de él un terrorismo local; ello requiere de un trabajo estrechamente coordinado entre las FCSE (Policía Nacional y Guardia Civil), los Cuerpos de Policía de Mossos d'Esquadra y Ertzaintza, el CITCO, el CNI y el Sepblac.

España ha desarrollado, fruto del consenso democrático, una completa normativa que contiene herramientas de investigación eficaces, así como una nueva definición de actividades que se consideran terroristas y que comprenden esos espacios previos de transformación ideológica sin los cuales no existiría la acción violenta.

El trabajo durante estos años ha sido constante en todos estos frentes: análisis del fenómeno yihadista desde nuevos ángulos y metodologías, estudio de nuevos tipos penales y su adaptación a la realidad yihadista, análisis de inteligencia

criminal contextualizando el fenómeno del terrorismo del Dáesh, problemática de los menores y los retornados de zonas de conflicto, y estudio de la reconversión ideológica de los captados y adoctrinados.

6.2. Financiación del terrorismo yihadista.

España, por su experiencia en la lucha contra el terrorismo, es plenamente consciente de la necesidad de cortar las fuentes de financiación y de identificar y mitigar las vulnerabilidades del sistema para canalizar fondos, tanto de origen lícito como ilícito, para fines terroristas o para el apoyo a esos fines en cualquier forma.

En el caso del terrorismo yihadista, la financiación y las necesidades económicas de los grupos terroristas han evolucionado sustancialmente desde los atentados del 11 de septiembre de 2001 cuando existían movimientos de fondos de cierta relevancia a través del sistema financiero internacional. Actualmente, los últimos ataques en Europa, la mayoría de escasa planificación y dificultad, han necesitado de poco respaldo económico para su ejecución por dos motivos fundamentales: el primero de ellos por el escaso coste material de los atentados, reducidos muchos de ellos al empleo de armas blancas o vehículos; y, el segundo, por la ausencia de estructuras permanentes en el tiempo que requieran de unos recursos para su sostenimiento.

A raíz de las investigaciones iniciadas, se conoce que la financiación obtenida tiene como finalidades principales la adquisición de billetes de avión para los integrantes de células, la adquisición de componentes informáticos, alquiler de inmuebles o el propio mantenimiento en nuestro país. Igualmente ocurre sobre el destino dado a esos fondos. En años pasados, esos fondos tenían como finalidad el sustento del grupo terrorista en sí mismo o de alguno de sus miembros, mientras que en la actualidad está muy presente la sustentación indirecta de ese grupo terrorista, sobre todo con aquello que tiene que ver con los campos de detención, especialmente Al-Hol y Al-Roj.

Respecto a la financiación de los viajes de los combatientes terroristas desplazados para unirse a los grupos internacionales, principalmente Dáesh, se han detectado distintas modalidades y tipologías de obtención de fondos, tanto legales como ilegales, bien por los propios terroristas como por sus allegados o las organizaciones de apoyo.

Los métodos empleados para la canalización de fondos son variados como el uso de *crowfunding* y *métodos bancarios clandestinos*. Además, se ha puesto de manifiesto la utilización de *neobancos* que admiten ingresos en criptomonedas e internamente se transforman en dinero *fiat* con el fin de movilizar los fondos evitando las tradicionales entidades bancarias.

Por otro lado, se ha detectado el uso de **remesas internacionales** como medio para que las familias de desplazados desde Europa a Siria e Irak puedan enviar periódicamente fondos a los mismos, que se realizan en pequeñas cuantías y, a menudo, a través de métodos predeterminados y muy precisos, que implican el uso de terceros países y de intermediarios, lo que dificulta su detección.

6.3. Terrorismo de ETA.

ETA ha mantenido vigente el “cese de su actividad armada” hecho público en octubre de 2011 y, en consecuencia, no ha cometido ningún atentado. Se anunció su disolución como organización en primavera de 2018. También se ha constatado por las FCSE que los sistemas tradicionales de financiación de la banda terrorista, especialmente a través de la extorsión mediante el cobro del denominado “impuesto revolucionario” han cesado.

Algunos grupos disidentes fueron protagonistas de episodios de violencia de baja intensidad de tipo sabotajes, pintadas, cartelería, etc., tras la declaración del «cese de actividades» tratando de lograr un mayor respaldo entre la militancia abertzale entorno a campañas o actos en apoyo y solidaridad con los presos. Asimismo, algunos individuos vinculados a esos sectores han protagonizado actuaciones violentas y de carácter saboteador circunscritas al País

Vasco y Navarra y su evolución y desarrollo debe ser objeto de un adecuado control y seguimiento. No obstante, la capacidad de movilización mostrada y su peligrosidad no han constituido, por el momento, una amenaza significativa, aunque su evolución y desarrollo debe ser objeto de un adecuado control y seguimiento.

En lo que se refiere a sus **sistemas de financiación**, debe destacarse que tras el cese de la actividad terrorista también han finalizado las actividades de extorsión a personas físicas y jurídicas que tradicionalmente venían siendo un elemento relevante de ingresos del grupo terrorista.

6.4. Otros grupos terroristas.

En los últimos años la organización terrorista PCE(r)-GRAPO se mantiene en situación de debilidad, sin cometer actos terroristas, limitando sus acciones al campo del proselitismo y la captación dentro del entorno anarquista y de la izquierda radical. Pese a esta situación, nunca ha renunciado públicamente a la lucha armada ni a sus principios revolucionarios incompatibles con la legalidad vigente.

Por su parte, recientemente se ha detectado alguna actividad relacionada con el terrorismo vinculada a movimientos independentistas catalanes que es objeto de seguimiento por las autoridades correspondientes.

En relación con la actividad violenta protagonizada por personas o grupos de ideología anarquista, ésta permanece en un nivel bajo y contenido en España, aunque hay que mencionar la repercusión que tienen en nuestro país las campañas internacionales que se convocan desde las distintas páginas web anarquistas.

La acción policial ante el repunte de la actividad violenta durante los primeros años de esta década ha incidido claramente en la situación actual, en la que los actos violentos registrados se limitan a los ataques y sabotajes contra los tradicionales objetivos declarados por el colectivo, así como a provocar altercados y enfrentamientos con las unidades policiales durante la celebración de determinadas concentraciones y manifestaciones.

6.5. Estrategia Nacional Contra el Terrorismo.

La Estrategia Nacional Contra el Terrorismo (ENCOT) 2019, fue aprobada por el Consejo de Seguridad Nacional en sustitución de la anterior Estrategia Integral contra el Terrorismo Internacional y la Radicalización del año 2012, y se adapta a la Estrategia de Seguridad Nacional de 2017. Su actualización para el periodo 2023-2027, prevista para principios de 2024, comenzó en noviembre de 2022 mediante la constitución de un grupo de trabajo multidisciplinar.

La ENCOT es, a su vez, objeto de desarrollo a través de diferentes planes estratégicos sectoriales contra actividades vinculadas al terrorismo, como el **Plan Estratégico Nacional Contra la Financiación del Terrorismo** (PENCFIT) o el **Plan Estratégico contra la Radicalización Violenta** (PENCRAV), ambos aprobados el 6 de octubre de 2020 por el Consejo de Seguridad Nacional. En 2024 comenzará la actualización de ambos Planes Estratégicos, cuya próxima vigencia se circunscribe al periodo 2024-2028.

Desde la implantación del PENCFIT en octubre de 2020 y de la creación del Grupo III de Trabajo y Seguimiento del Plan (GRUSEFIT), han sido implementadas 26 acciones que se reflejaban en el PENCFIT.

Dichas acciones se han materializado en la adopción de acuerdos de colaboración de intercambio de información entre instituciones, así como en modificaciones y nuevas iniciativas legislativas, y programas de formación dirigidos tanto a FCSE, como a Magistrados, Jueces, Fiscales y letrados de la administración de justicia de la Audiencia Nacional

Adicionalmente, en el ámbito preventivo, la COPBLAC, a propuesta del Comité Permanente de Prevención del Blanqueo de Capitales, aprobó las ¨***Directrices Generales de la Estrategia de Prevención de la utilización del sistema financiero para la Financiación del Terrorismo¨,*** de 2018**.**

En cuanto al PENCRAV se designó al Ministerio del Interior a través del Comité Especializado contra el Terrorismo (en adelante, CECT) como responsable para su desarrollo e implementación en todo el territorio nacional, otorgando, además, la coordinación de estas labores a CITCO.

El nuevo PENCRAV, tiene como objetivo establecer un marco efectivo de prevención, conocimiento de los procesos y tratamiento de los extremismos violentos para lograr una sociedad más sensibilizada, consciente, segura y resiliente. Se configura como un documento ágil y actualizado, donde se identifican distintos ámbitos transversales de actuación denominados *esferas*, y se establecen sus correspondientes líneas de acción. Entre las principales que podemos mencionar: actuaciones de formación contra los radicalismos y actuaciones violentas dentro del ámbito policial; en el ámbito penitenciario, creación de herramientas para el suministro de información a autoridades judiciales y penitenciarias; e incremento de la cooperación nacional e internacional mediante la creación de grupos y asistencia a proyectos internacionales.

7. PRINCIPALES VULNERABILIDADES EN BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO.

Tal y como se exponía en el ANR de 2020, GAFI adopta la siguiente definición de vulnerabilidad

"Vulnerabilidad" *es aquella situación o circunstancia que puede ser aprovechada o utilizada por las organizaciones o personas que pretendan realizar actividades de blanqueo de capitales o financiación del* terrorismo.

En el ANR mencionado anteriormente se establecieron una serie de áreas de vulnerabilidad de carácter general que de forma horizontal podían y pueden tener incidencia en las actividades de BC/FT en los distintos sectores.

A. Vulnerabilidades derivadas de la población.
B. Vulnerabilidades derivadas de factores geográficos.
   - Operaciones con territorios de riesgo o con sus ciudadanos/entidades.
   - Operaciones con países de mayor presencia de organizaciones/ciudadanos relacionados con el terrorismo yihadista.
   - Operaciones en el área de Gibraltar.
C. Vulnerabilidades derivadas de la naturaleza de la entidad o actividad desarrollada.
D. Vulnerabilidades derivadas de los medios de pago, uso de efectivo y economía irregular.
E. Vulnerabilidades derivadas de las innovaciones tecnológicas en operaciones financieras.
   - Vulnerabilidades por uso del ciberespacio.
   - Vulnerabilidades por el uso de criptomonedas o CA.

7.1. Vulnerabilidades derivadas de la población.

Los rasgos que identifican las vulnerabilidades de los flujos migratorios siguen persistiendo principalmente por los movimientos de capitales internacionales que aumentan el riesgo de la introducción en el sistema financiero internacional de fondos de origen ilícito o con un fin ilícito.

La digitalización del envío de remesas de fondos a escala internacional es un hecho, y a su vez se ha visto favorecido por la pandemia COVID-19 y la aparición de nuevos agentes no financieros que ofrecen servicios de intermediación de pago.

España contaba con 48.085.361 de habitantes a finales de 2022, de los cuales 6.089.620 son extranjeros (un 12,7% de la población). La comunidad más numerosa proviene de Marruecos con 893.953 habitantes (con un crecimiento del 25,2% de la población respecto 2019), seguida de Rumanía (629.755), Colombia (453.911), Italia (301.791), Reino Unido (284.037), Venezuela (278.159) y China (219.929)[17].

Además, los flujos migratorios irregulares en 2022 han continuado registrándose, a pesar de que en este año el número de inmigrantes irregulares ha decrecido un 25,6% respecto el año anterior.

Datos de Banco de España muestran como las remesas enviadas desde España han experimentado un crecimiento del 10% con respecto a datos de 2021, viéndose focalizado este incremento en los envíos a Paraguay, Colombia, República Dominicana y Marruecos[18].

A pesar de esta digitalización, hay que tener en cuenta que el uso de dinero en efectivo por la comunidad inmigrante es muy alto y supone una vulnerabilidad para nuestro sistema ya que dificulta la trazabilidad de los fondos.

Otra vulnerabilidad derivada de la inmigración y las circunstancias económicas que rodean a este sector de la población es su susceptible utilización por organizaciones criminales con el objetivo de movilizar fondos cuyo origen está en su actividad delictiva. En este aspecto, cobra especial relevancia la figura del "mulero", que es la persona que a cambio de una comisión transfiere los fondos de estos grupos criminales.

7.2. Vulnerabilidades derivadas de factores geográficos.

7.2.1 Realización de operaciones con territorios de riesgo o con ciudadanos/ entidades de esos territorios.

En línea con lo expuesto en el ANR de 2020, se considera una vulnerabilidad la operativa que se realiza en España con territorios de alto riesgo o con ciudadanos o entidades de tales jurisdicciones.

El primer elemento de vulnerabilidades geográficas se deriva de las operaciones con jurisdicciones que presentan deficiencias estratégicas en sus sistemas de lucha contra el BC/FT. Por ello, el GAFI y la Comisión Europea elaboran y actualizan periódicamente las listas de países de riesgo que deben ser en todo caso tenidas en cuenta por las entidades españolas al aplicar sus medidas preventivas de BC/FT.

En este sentido, también deben ser tenidas en consideración aquellas listas de países no cooperantes en materia tributaria, elaboradas por España y por la UE, ya que, por su opacidad y su régimen tributario, estas jurisdicciones pueden presentar un riesgo más elevado de BC.

Para la identificación de territorios de riesgo existen diferentes criterios que se indican en la Guía Orientativa sobre el Riesgo geográfico en materia de BC/FT, emitida por la COPBLAC[19], que tiene como objetivo orientar a los sujetos obligados en esta materia.

[17] Datos INE.
[18] Véase cuadro 17.6a del Boletín Estadístico de Banco de España.
[19] http://www.tesoro.es/sites/default/files/guia_riesgo_geografico_en_materia_de_bc_ft.pdf.

En cualquier caso, corresponde a cada sujeto obligado, en función del sector en el que opere, del tipo y volumen de operaciones que realice, de su experiencia profesional y, sobre todo, de su evaluación de riesgos correspondiente, la determinación de la existencia de otros riesgos derivados de operar con determinados países o con sus nacionales.

Los **principales criterios de riesgo** a tener en consideración son que los países:

a) No tengan sistemas adecuados de prevención del BC/FT.
b) Estén sujetos a sanciones, embargos o medidas análogas aprobadas por la Unión Europea, Naciones Unidas u otras organizaciones internacionales.
c) Presenten niveles significativos de corrupción u otras actividades criminales.
d) Faciliten financiación o apoyo a actividades terroristas.
e) Presenten un sector financiero extraterritorial significativo (centros "off-shore").
f) Tengan la consideración de paraísos fiscales.

De este modo, la nacionalidad o residencia del cliente o de su titular real, los lugares de procedencia y de destino de los fondos y la presencia de posibles intermediarios, se convierten en factores de riesgo a tener en consideración, de forma que las entidades deberán extremar las precauciones al analizar los riesgos de operaciones en los casos en los que los clientes o sus fondos tengan vínculos con países considerados de especial riesgo en cada actividad y realicen operaciones con esas jurisdicciones.

La consideración de jurisdicción de alto riesgo principalmente se determina por las conocidas como listas gris y negra de GAFI *(Jurisdictions under Increased Monitoring/ High-Risk Jurisdictions subject to a Call for Action)* y los listados de países terceros de riesgo de la Comisión Europea *(High risk third countries- Delegated Regulation (EU) 2016/167).*

Según la información del Sepblac, las comunicaciones de operativa relacionada con jurisdicciones de riesgo es un 9% inferior en 2022 respecto a 2021.

7.2.2. Operaciones con países de mayor riesgo de financiación del terrorismo.

España por su situación geográfica se configura como uno de los países con mayor vulnerabilidad con relación a la financiación del terrorismo y en lo que se refiere a reclutamiento y captación de fieles por organizaciones terroristas relacionadas con el islamismo radical.

Además, debe prestarse atención al posible aprovechamiento de las relaciones comerciales de España con los países del Magreb y los flujos migratorios de ciudadanos de esta zona para estos fines. Adicionalmente, debe prestarse atención a la mayor vulnerabilidad de los sectores que operan de manera regular con países cuyo sistema político pudiera apoyar directa o indirectamente a grupos radicales en sus posicionamientos religiosos o ideológicos.

Para combatir estos riesgos es esencial la correcta identificación de los fondos, así como de los intervinientes en la operativa de recepción de remesas en España, mediante el establecimiento de entidades financieras con robustos sistemas preventivos.

7.2.3. Actividades en el área de Gibraltar.

Según el Informe de Seguridad Nacional 2022, un área especialmente vulnerable para ser utilizada por grupos criminales para el narcotráfico y contrabando, teniendo una alta exposición al riesgo de BC/FT y con gran vulnerabilidad frente a la ejecución de delitos e infracciones de este tipo tanto por vía terrestre, como marítima o aérea.

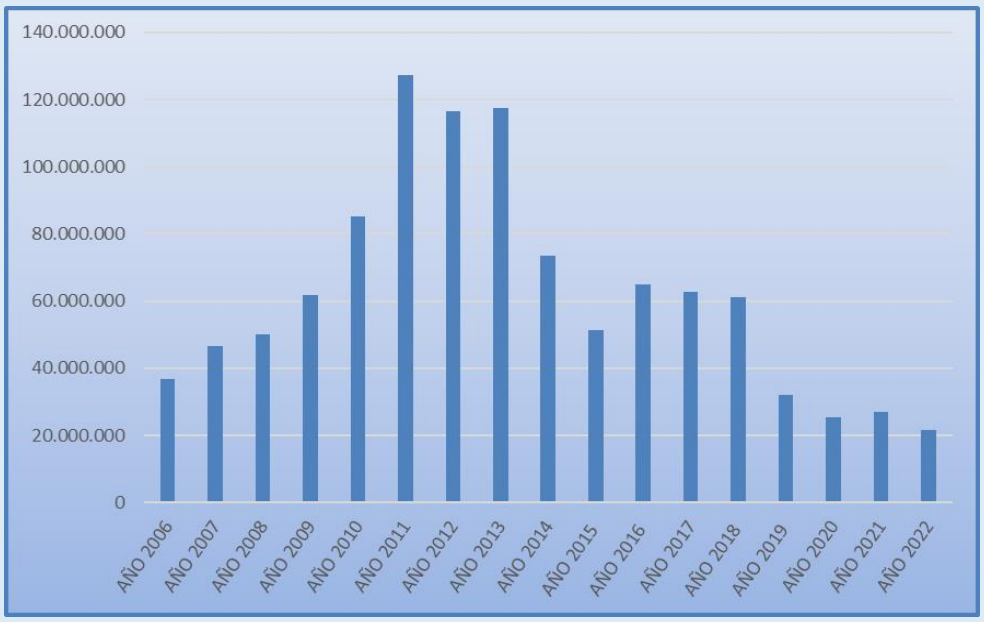
Como se ha mencionado en el apartado de amenazas, el III Plan Especial de Seguridad para el Campo de Gibraltar se amplió geográficamente incluyendo a tres provincias adicionales (Almería, Sevilla y Granada) bajo su paraguas de actuación con el fin de combatir a los grupos criminales que se dedican al tráfico de estupefacientes y el contrabando.

En este sentido, según datos del Ministerio del Interior, la actuación de las FCSE en el marco de dispositivos específicos como es el Plan Especial de Seguridad para el Campo de Gibraltar, el incremento de ha aflorado delitos por tráfico de drogas que en las estadísticas reflejan un incremento en un 14,4% desde 2019 se explica por la actuación de las FCSE en el marco de dispositivos específicos como es el Plan Especial de Seguridad para el Campo de Gibraltar. Tal y como ya se reflejó en el anterior ANR de 2020, deben también tenerse en consideración la vulnerabilidad que suponen las fronteras de Ceuta, Melilla y Gibraltar, para actividades de contrabando de productos (tabaco, telefonía móvil, material electrónico, etc.) que generan importantes movimientos de efectivo.

Los datos de declaraciones de movimientos en efectivo en frontera muestran cómo, de las tres fronteras seleccionadas, Gibraltar destaca como la aduana en la que más salidas de dinero en efectivo declarado se producen, con un 73% de declaraciones. En cuanto a las declaraciones de entrada de efectivo, Melilla está en un primer lugar con un 67% de declaraciones.

En relación con el contrabando, hay que tener en cuenta que a pesar del cierre de la aduana comercial en Ceuta y Melilla en 2019 y la apertura en enero de 2023, los datos muestran que esta actividad delictiva continúa siendo recurrente en nuestro país, pero con una menor incidencia, especialmente en lo que respecta a las entradas de tabaco desde Gibraltar, cuya incidencia ha venido descendiendo desde 2014.

CUADRO 9. Entradas de tabaco desde Gibraltar (2006-2022)



Fuente: A.E.A.T.

En relación con el tráfico de estupefacientes, se han detectado operaciones delictivas por grupos de criminalidad organizada donde se hace uso de efectivo, empleo de artículo de lujo o adquisición de inmuebles.

7.3. Vulnerabilidades derivadas de la naturaleza de la entidad o actividad desarrollada.

Al analizar las vulnerabilidades que pueden ser objeto de aprovechamiento por las estructuras delictivas para cometer actividades de BC/FT a través de la utilización de las entidades de distintos sectores, es necesario diferenciar entre los riesgos de carácter endógeno y los de carácter exógeno que pueden existir en cada tipo de entidad o actividad.

Dentro de los factores de riesgos intrínsecos o "endógenos" que se derivan de la propia entidad o actividad desarrollada están:

a) La posibilidad de crear o adquirir entidades o negocios con el fin de amparar actividades de BC procedentes de actividades ilícitas o con el fin de cometer actividades de FT. En España, casi todos los sujetos obligados pertenecen a sectores sometidos a licencia, a inscripción registral y al cumplimiento de requisitos de autorización, estando sometidos a un régimen de supervisión prudencial y de prevención del BC/FT.
b) La posibilidad de que exista un control directo o indirecto de la operativa de una entidad por las redes de BC/FT.
c) La posibilidad de que existan empleados/agentes de determinados tipos de entidades que estén vinculados con redes criminales, lo que permitiría usar sistemas planificados y elaborados de manejo de fondos ilegales sin conocimiento de la entidad y con mayor dificultad de ser detectados.

Los factores de riesgo extrínsecos o de carácter "exógeno" son aquellos que pueden permitir el abuso de una entidad por parte de las redes para fines de BC/FT, es decir, no se trata de que la entidad en sí misma sea un riesgo, sino que una entidad con un funcionamiento normal puede contar con una serie características que la hacen vulnerable y susceptible de utilización para operativas de BC/FT por diferentes razones, como podrían ser:

Una posible falta de compromiso con las políticas y medidas de prevención del BC/FT por parte de la entidad. Esta ausencia puede ser debida a una deliberada falta de aplicación de políticas preventivas por motivos de coste de implementación, por ignorancia negligente en el grado de desarrollo de estas medidas dentro de la entidad o por la importancia que se otorga a los ingresos generados por permitir una mayor laxitud en la implementación de los controles exigidos.

Un excesivo flujo de operaciones con determinados países o la existencia de un elevado número de clientes de ciertas nacionalidades pueden ser razones para utilizar a determinado tipo de entidad para operaciones de BC/FT. La ausencia de información o de procedimientos adecuados que permitan a las autoridades un preciso conocimiento sobre los titulares reales de los clientes que sean personas jurídicas. La falta de cultura en materia preventiva en lo referente a aquellas entidades que pasan a ser nuevos sujetos obligados

Adicionalmente, debe añadirse la posible falta de comunicación de los elementos de riesgo por parte de las autoridades competentes y de actualización de guías y normativa relevante. Estas son situaciones de riesgo a las que se enfrenta la política preventiva y sobre las que es necesaria una mayor vigilancia y rigor por parte de las autoridades nacionales a través de los mecanismos reguladores y fiscalizadores a su alcance.

7.4. Vulnerabilidades derivadas de los medios de pago, uso de efectivo y economía irregular[20].

La pandemia generada por el COVID-19 conllevó cambios hacia un modelo de vida más digital, aspecto que incidió igualmente en el empleo de los medios de pago. Al mismo tiempo, la digitalización de los medios de vida y la economía puede contribuir a revertir la tendencia a la despoblación en las zonas rurales.

Según el *Estudio sobre hábitos en el uso del efectivo 2022* del Banco de España, el dinero en efectivo es el medio de pago que se usa con mayor frecuencia, seguido por la tarjeta y los dispositivos móviles (teléfono y reloj), de tal manera que 3 de cada 5 españoles usa efectivo a diario, especialmente aquellos con estudios básicos y con una franja de edad de más de 45 años.

En este estudio, el efectivo vuelve a ocupar el primer lugar en cuanto a medio de pago minorista empleado en 2022 con un uso diario por el 64% de la población, mientras que en 2021 representaba el 35,9%[21], siendo en 2022 el uso de tarjeta bancaria como medio de pago el método utilizado por el 32% de la población.

En cuanto a la introducción de métodos de pago no tradicionales y observando su uso ocasional (no diario), los dispositivos móviles se configuran como tercer medio de pago por detrás del efectivo y la tarjeta bancaria. Por otro lado, el nuevo proveedor de servicios de pago (*Bizum*) es utilizado por un 44% de la población, disminuyendo al 1% en el uso diario como medio de pago.

Con relación a la obtención de efectivo, el 79% lo adquiere a través de cajeros automáticos por importes entre 20 y 50 euros principalmente. Sin embargo, un 6% de la población obtiene efectivo no bancarizado, es decir, de familia, amigos o trabajo, lo que revela la vulnerabilidad en el empleo de este medio de pago con fines de BC/FT.

Este riesgo está particularmente presente en zonas sin oficina bancaria estable, donde el 66,4% de la población que vive en zonas rurales tiene un cajero a más de 1 Km de distancia. En estos casos, la economía sumergida y la evasión fiscal se convierten en las principales vulnerabilidades en cuanto a la lucha contra el BC.

Sin embargo, las nuevas tecnologías han dado lugar a la introducción de pagos digitales, fomentados a raíz de las modificaciones en la PSD2 y la aparición de nuevos operadores que ofrecen nuevos instrumentos, modalidades y servicios de pago.

Teniendo en cuenta el uso de nuevos medios de pagos más digitales, se identifican una serie de riesgos:

- Incremento de operativas fraudulentas asociadas al fraude tipo phishing donde se obtienen datos de tarjetas de débito o crédito y acceso a monederos electrónicos.
- Uso de nuevos medios que favorecen la ocultación y falta de transparencia del origen de los fondos.
- Robo de identidad o prestación de la misma a cambio de una compensación (muleros) para la contratación de instrumentos de pagos que permiten la introducción de fondos de origen ilícito en el sistema.
- Globalidad en la aparición medios de pagos sin barreras fronterizas y falta de herramientas que permitan determinar realizar una efectiva trazabilidad de los flujos de fondos.

En el marco normativo español se ha adaptado a los nuevos requerimientos de información exigidos en la normativa europea en relación con declaración de los medios de pago, mediante la adopción de la intervención administrativa de Medios de Pago por la Orden ETD/1217/2022, de 29 de noviembre, mediante la cual se determina los modelos, criterios y forma de declaración aplicables para quienes, actuando por cuenta propia o de tercero, realicen los movimientos de pago previstos en el artículo 34 de la Ley 10/2010, de 28 de abril.

[20] Fuente: *Estudio sobre hábitos en el uso del efectivo 2022*, Banco de España.
[21] Encuesta Anual sobre el Efectivo de 2021, Banco de España.

7.5. Vulnerabilidades derivadas de innovaciones tecnológicas en operaciones financieras[22].

7.5.1. Vulnerabilidades por uso del ciberespacio.

La transformación digital de la sociedad, administraciones y sistema financiero, por un lado, ha agilizado y facilitado la vida de los ciudadanos y empresas en ciertos aspectos, pero, por otro, la dependencia de las tecnologías de la información ha generado un aumento de los riesgos en materia de BC/FT, así como de las vulnerabilidades ante posibles ciberataques.

Las vulnerabilidades han aumentado ante la posibilidad de sufrir ataques de este tipo ante la mejora la mejora técnica de los mismos y la implantación de unas medidas de seguridad eficaces que permiten ocultar su origen.

La digitalización de las Administraciones conlleva grandes oportunidades, pero a su vez se enfrentan a vulnerabilidades derivadas del uso tecnológico. Según el Informe de Seguridad Nacional 2022, el Ministerio de Defensa, por ejemplo, ha sufrido 2.035 *ciberincidentes*. Este hecho es reflejo del creciente esfuerzo de los cibercriminales en atacar las bases de datos de autoridades y organizaciones de servicio público, con el fin de obtener información de carácter personal para su uso con fines espurios, muchas veces, dentro del ámbito delictivo.

Dentro de la tipología de ciberataques a la que se encuentra expuesta España actualmente, destaca el fraude informático asociado a las estafas, siendo las modalidades ciberdelictivas más frecuentes en España las estafas de soporte técnico e inversiones, el *Business Email Compromise* (BEC), así como campañas masivas de phishing, y, cada vez más, de *smishing*.

Con relación a la financiación del terrorismo, el ciberespacio se ha convertido en una herramienta de fácil acceso para las organizaciones terroristas, permitiéndole una difusión instantánea de su mensaje y el acceso a nuevas formas de financiación que favorecen la ocultación de fondos y pérdida de trazabilidad usando las técnicas adecuadas para ello.

Los sujetos financieros españoles, conscientes de esta problemática, destinan un porcentaje importante de recursos humanos y monetarios a la ciberseguridad de su sistema tecnológico. Según estudios recientes la media del gasto en esta partida estaría en el 10% de presupuesto anual.

7.4.2 Vulnerabilidades por el uso de monedas y activos virtuales.

La propia naturaleza de los CA muestra la vulnerabilidad que puede experimentar el sistema financiero ante su uso, debido a la capacidad de: i) realizar operaciones transfronterizas con rapidez fuera del sistema financiero regulado, ii) enmascarar el origen y el destino de los fondos y iii) dificultar a los sujetos obligados la detección de operativas sospechosas.

Por otra parte, el diseño concreto del CA puede impedir aplicar técnicas tradicionales de trazabilidad. Se aprecia un mayor uso de estos CA privados como facilitador de delitos ciberdependientes, siendo especialmente reseñable en casos de *ransomware*.

Igualmente, las características inherentes asociadas a su tecnología subyacente (la cadena de bloques) facilita cierto anonimato en algunos tipos de operaciones o algunos tipos de CA, que pueden llegar a obstaculizar la detección de actividades delictivas por parte de las autoridades.

[22] Fuente: Informe de Seguridad Nacional 2022.

Sin embargo, la mera existencia de estas características en una actividad no implica automáticamente una operación ilícita. Por ejemplo, el uso de *cold wallets*, en *hardwares* o en papel, puede ser una herramienta legítima de protegerse contra los robos.

En esta misma línea, el uso de aplicaciones que permiten el acceso a la denominada *deep web* y que hace casi imposible una detección anticipada de la operativa, permiten que delincuentes y miembros del crimen organizado sean usuarios de estos métodos de ocultación de actividades delictivas y que gran parte de los pagos, en estos sitios de la red, se realicen con CA.

Por último, una de las vulnerabilidades sobre la seguridad informática que puede afectar a este sector son los ataques directos a PSCA. En España, la Guardia Civil, en la denominada Operación 3COIN, desarticuló en el verano de 2020 al grupo de ciberdelincuentes que lanzó un ataque directo a una empresa de custodia de criptomonedas por valor de 6 millones euros.[23]

En la actualidad, en España, están registrados 3 de los 10 PSCA con mayor actividad en nuestro país. Estos PSCA representan el 60,2% de la actividad de estos *exchangers*[24].

8. RIESGOS SECTORIALES.

El presente ANR tiene por objeto analizar aquellos sectores que hayan experimentado modificaciones normativas sustanciales, nuevas tendencias en su operativa, factores o características que determinen la necesidad de ser actualizados desde el punto de vista de los riesgos de incurrir en actividades de BC/FT desde la versión previa del ANR, aprobada en 2020. Para los sectores que ya se encontraban recogidos en el ANR de 2020, la actualización llevada a cabo en este análisis, no obstante, no conlleva una variación en la apreciación del nivel de riesgo otorgado previamente con la excepción de la ejecución de operaciones de pago por parte de las entidades de pago, riesgo que se ha visto incrementado de moderado a significativo. Adicionalmente, se ha completado el análisis de los CA y de los PSCA, cuyo análisis en 2020 fue mucho más genérico y centrado en el análisis genérico de servicios con monedas y activos virtuales. Atendiendo a las variables mencionadas en los subapartados siguiente se va a proceder al análisis de los siguientes sectores:

Riesgos sectores financieros:

a) Servicios de inversión en valores, gestoras de instituciones de inversión colectiva y gestoras de titulización.
b) Envío de dinero por entidades de pago.
c) Otros servicios de entidades de pago.
d) Operaciones con dinero electrónico.
e) Criptoactivos y proveedores de servicios de criptoactivos.

Riesgos sectores no financieros:

a) Actividades realizadas por los Notarios.
b) Actividades realizadas por los Registradores de la propiedad, mercantiles y de bienes muebles.

[23] https://www.guardiacivil.es/es/prensa/noticias/8134.html?versionImprimible=true
[24] Dentro de los 50 PSCA con mayor actividad que han sido analizados por Chainalysis.

8.1. Riesgos sector financiero.

a) Servicios de inversión, instituciones de inversión colectiva y sociedades gestoras.

Actividad, contexto y régimen normativo.

La actualización de este sector ha venido motivada por la actualización de la Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión en España en cuanto a la posibilidad de representación de títulos mediante tecnología de registros distribuidos (DLT), adicional a los sistemas de representación ya previstos mediante títulos o anotaciones en cuenta.

La Ley 6/2023, de 17 de marzo, se refiere, entre otras materias, a la emisión y oferta de instrumentos financieros, al régimen de autorización, condiciones de funcionamiento y régimen prudencial de las empresas de servicios de inversión, a la prestación de servicios y actividades de inversión en España por parte de empresas de terceros países, así como al régimen de supervisión, inspección y sanción a cargo de la Comisión Nacional del Mercado de Valores. Quedan comprendidos en el ámbito de la ley diversos instrumentos financieros, entre los que se incluyen los valores negociables, instrumentos del mercado monetario, acciones y participaciones en instituciones de inversión colectiva, en entidades de capital-riesgo y en entidades de inversión colectiva de tipo cerrado, y diversos instrumentos derivados como opciones, futuros y contratos financieros por diferencias.

Además, el sector también viene regulado por la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva (IIC o entidades de tipo abierto) y por la Ley 22/2014, de 12 de noviembre, que regula las entidades de capital-riesgo, otras entidades de inversión colectiva de tipo cerrado y las sociedades gestoras de entidades de inversión colectiva de tipo cerrado.

Estas entidades se encuentran sujetas a la autorización administrativa previa de la CNMV. El proceso de autorización requiere el cumplimiento de las obligaciones establecidas en la normativa y la emisión de un informe previo por parte del Sepblac relativo a la idoneidad de los órganos y procedimientos de prevención que la entidad en constitución tiene previsto aplicar de serle concedida la autorización solicitada. La CNMV es el órgano competente en materia de supervisión prudencial de los mercados de valores y de su actividad, mientras que la supervisión de prevención del BC/FT es desarrollada por el Sepblac y, en caso de Convenio, por la CNMV. Dicho Convenio fue firmado el 7 de julio de 2023.

Con relación al registro de valores en tecnología DTL cabe indicar que en la práctica todavía no se ha puesto en marcha ninguna iniciativa sobre esta posibilidad en el ámbito del mercado de valores. Esta iniciativa entraña nuevos riesgos principalmente en el modelo de negocio por la aparición de nuevos *players* y posibles cambios de roles de las entidades que intervienen, así como oportunidades al constituir una base de datos única que genere beneficios desde el punto vista de eficiencia, riesgos operativos y de costes.

- **Servicios de inversión.** En España, junto a las entidades de crédito, pueden prestar servicios de inversión las empresas de servicios de inversión (ESI):

- Las **sociedades y agencias de valores**. La diferencia entre unas y otras consiste en que las agencias de valores no pueden realizar actividades de inversión por cuenta propia, por lo que su actividad es la prestación de servicios de inversión a terceros, mientras que las sociedades de valores pueden también actuar por cuenta propia, además de

poder prestar el servicio de aseguramiento, y el servicio auxiliar de concesión de créditos para la operativa en valores.

Según los datos del Registro de la CNMV, a 31 de diciembre de 2022 existían en total 35 sociedades de valores y 60 agencias de valores nacionales. Adicionalmente, hay unas 900 ESI de la UE que pueden utilizar el pasaporte comunitario para operar en España bajo la modalidad de libre prestación de servicios y otras 51 entidades comunitarias con sucursal en España. El número de ESI europeas autorizadas a operar en España en libre prestación se ha reducido sensiblemente con el Brexit.

- Las **empresas de asesoramiento financiero** (EAF) ofrecen a sus clientes, como única actividad reservada, el servicio de asesoramiento en materia de inversión financiera. No pueden desarrollar funciones de depósito de valores o efectivo de clientes. Deben contar con la preceptiva autorización e inscribirse en el registro de la CNMV. A diciembre de 2022 había 143 EAF registradas, que en su conjunto contaban con 11 mil clientes -de los que aproximadamente 10 mil eran clientes minoristas-, un volumen asesorado de 19.000 millones de euros y 49 millones de euros de ingresos por asesoramiento. La mayoría de las EAF se dedican a clientes minoristas, mientras que 32 de ellas se dedican únicamente a clientes profesionales. Como puede observarse, su peso es, por el momento, limitado.

Adicionalmente, la regulación contempla otro tipo específico de ESI, las sociedades gestoras de cartera (SGC), que únicamente pueden prestar el servicio de inversión de gestión discrecional de carteras, si bien a 31 de diciembre de 2022 no figura ninguna en el registro, lo que se explica por el interés en obtener la autorización como sociedades o agencias de valores, que les permite un campo más amplio de actividades.

- **Inversión colectiva**. Las **Instituciones de Inversión Colectiva,** IIC, son entidades financieras que tienen por objeto invertir en activos comunes para un colectivo y repartir los rendimientos entre los inversores en función de los resultados conjuntos. Las IIC pueden constituirse como **fondos de inversión** y como **sociedades de inversión**. Ambos casos requieren una entidad financiera como depositaria de la cartera del vehículo, pero los fondos de inversión requieren, en todo caso, la existencia de una sociedad gestora (SGIIC), ya que carecen de personalidad jurídica, mientras que las sociedades pueden gestionar su patrimonio o recurrir a una sociedad gestora, si bien la gran mayoría son también gestionadas y administradas por SGIIC. Casi todas las SGIIC españolas (Fondos y Sociedades de Inversión) están asociadas a INVERCO, Asociación de Instituciones de Inversión Colectiva y Fondos de Pensiones.

-Los **fondos de inversión** pueden tener distintas categorías:

- **Fondos de inversión en activos financieros**. Pertenecen a una pluralidad de inversores que suscriben participaciones del fondo. Es el principal instrumento de inversión colectiva. Según datos de la CNMV, en diciembre de 2022 contaban con un patrimonio de 315.798 millones de euros.
- **Fondos de inversión inmobiliaria**. Invierten en activos inmobiliarios con el fin de obtener ingresos con su arrendamiento. Se rigen por lo dispuesto para fondos de carácter financiero. Deben tener un mínimo de 9 millones de euros desembolsados. A diciembre de 2022 únicamente había 2 fondos registrados, que se encontraban en proceso de liquidación.

- **IIC de inversión libre** ("*Hedge Funds"*). Productos complejos en los que el gestor adopta diferentes estrategias para maximizar la inversión de los partícipes del fondo. Están dirigidos con carácter general a inversores cualificados (grandes patrimonios, inversores institucionales, entidades profesionales). Su característica principal es que pueden invertir sin las limitaciones que tienen el resto de los fondos (todo tipo de activos, diversificación de sus inversiones y el endeudamiento). Por ello, ofrecen una posible mayor rentabilidad, pero también un mayor riesgo de pérdida de la inversión. Según datos de la CNMV, en España estaban registrados 54 fondos de inversión libre a diciembre de 2022.

- Las **sociedades de inversión de capital variable** (Sicav), así como sociedades de inversión inmobiliaria (SII) y sociedades de inversión libre (SIL). Las Sicav, que son el instrumento más extendido de los tres, son sociedades anónimas cuyo objeto social es invertir en activos financieros, y cuyos accionistas son los propios inversores. Requieren un mínimo de cien accionistas y 2,4 millones de euros. Tienen una fiscalidad del 1% si cumplen determinados requisitos. En diciembre de 2022 en España existían 21.091 SICAV con un patrimonio de 15.785 millones de euros. Su número ha venido disminuyendo en los últimos años. El número y patrimonio de las SII y SIL es muy inferior al de las SICAV.

- Las **sociedades gestoras de instituciones de inversión colectiva**, SGIIC, son sociedades anónimas que administran y gestionan los fondos y sociedades de inversión señalados, actuando en beneficio de los partícipes y accionistas. También pueden actuar como administradores y gestores de los vehículos de tipo cerrado. Las SGIIC están sometidas a diferentes requisitos, debiendo publicar cierta información individualizada de cada fondo de inversión (documentos con datos para el inversor; folleto; informe anual con cuenta de gestión y cuentas anuales e informes trimestrales/semestrales sobre patrimonio, número de participaciones o acciones en circulación, títulos en cartera…).

A finales de 2022 existían 123 sociedades gestoras de IIC en el registro de la CNMV, que administraban un patrimonio de unos 350.000 millones de euros de IIC, principalmente en fondos de inversión financiera. El sector cuenta con una elevada concentración ya que las 3 mayores SGIIC tienen una cuota conjunta aproximada del 40% del patrimonio total.

- **Entidades de inversión colectiva de tipo cerrado: Fondos y Sociedades de capital riesgo y otros vehículos de tipo cerrado**. Son aquellas entidades de inversión colectiva que, careciendo de un objetivo comercial o industrial, obtienen capital de una serie de inversores, mediante una actividad de comercialización, para invertirlo en todo tipo de activos financieros o no financieros, con arreglo a una política de inversión definida. En el caso del subtipo de fondos y sociedades de capital riesgo, su objeto es invertir temporalmente en empresas no cotizadas que no sean financieras ni inmobiliarias con el fin de que aumenten de valor y obtener un beneficio en retorno de la inversión efectuada. Estos vehículos de tipo cerrado se asemejan a los vehículos IIC en su carácter de inversión colectiva, pero se diferencian por la mayor flexibilidad en cuando a sus posibles inversiones, una menor liquidez y en que van dirigidos, básicamente, a inversores profesionales, aunque cada vez se comercializan más entre minoristas. Invierten principalmente en compañías del sector tecnológico y servicios, o energías renovables, fundamentalmente en empresas de reciente creación o reestructuradas, con alto potencial de crecimiento y un mayor riesgo. Son gestionadas por sociedades gestoras de entidades de tipo cerrado (SGEIC) o por SGIIC.

Las sociedades gestoras (SGEIC, anteriormente denominadas SGECR) se dedican a la administración y gestión de fondos de tipo cerrado y de activos de sociedades de tipo cerrado. Según el registro de la CNMV a finales de 2022 había 482 vehículos con forma societaria de fondos (de los que 319 eran fondos de capital riesgo -FCR-, 56 eran fondos de inversión de carácter cerrado (FICC), y el resto corresponde a otras modalidades con forma de fondos), y 373 vehículos con forma de sociedad (de los que 319 eran sociedades de capital riesgo -SCR- y el resto correspondía a otras modalidades con forma societaria). El año 2022 registró una cifra de inversión en capital privado y capital riesgo en 9.238 millones de euros en un total de 958 inversiones[25]. Los operadores internacionales concentraron el 80,2% de la inversión total, con una presencia muy relevante en las grandes operaciones.

Amenazas.

[25] Datos de SPAINCAP.

La operativa con este sector requiere un cierto nivel de conocimiento en materia de inversión por lo que en el ámbito de la financiación del terrorismo las amenazas son bajas y las probabilidades de uso por organizaciones terroristas para canalizar sus fondos son escasas y disminuyen a medida que se requiere un perfil inversor más alto.

Este mismo razonamiento puede utilizarse en el caso del BC. Sin embargo, la existencia de factores como las negociaciones en mercado extrabursátiles, el fraude que puede ser ejecutado mediante los denominados chiringuitos financieros o la desviación de fondos fruto de la corrupción, incrementan las amenazas de la utilización de los servicios de inversión con fines ilícitos. Las variables que pueden influir en el blanqueo son la constitución del servicio en su origen como delictivo, en caso del fraude de inversión, o la utilización de personas con elevado perfil inversor para la canalización de fondos que se han obtenido de forma ilícita.

Vulnerabilidades y riesgo sectorial.

Este sector viene caracterizado por la heterogeneidad de los actores y productos que lo integran, lo que puede derivar en distintos tipos y niveles de riesgos. Además, se debe tener en cuenta la interacción que se produce entre los subsectores y, sobre todo, la directa relación con otras partes del sector financiero, especialmente el sistema bancario, que tiene un peso muy relevante tanto por la prestación directa de servicios de inversión, como por pertenecer a grupos bancarios buena parte de las entidades citadas prestadoras de servicios de inversión, de inversión colectiva y otros.

Así, en el ámbito de la prestación de servicios de inversión, los bancos reportaban a finales de 2021 casi 12 millones de clientes, un volumen gestionado de 116.000 millones de euros, valores custodiados por importe de 3,5 billones de euros e ingresos por prestación de servicios de inversión por importe de 6.000 millones de euros, frente a unas cifras correspondientes a las ESI mucho más modestas: 300.000 clientes (40 veces menos), 9.000 millones de volumen gestionado (13 veces menos), 72.000 millones de euros de valores custodiados (50 veces menos), 900 millones de euros de ingresos (7 veces menos). Por su parte, en el ámbito de la gestión colectiva, el volumen gestionado que corresponde a grupos de bancarios supone más del 80% del total gestionado. En definitiva, los supervisores, investigadores y analistas de inteligencia financiera señalan riesgos de BC/FT asociados a estas actividades en relación, fundamentalmente, a los siguientes factores de **vulnerabilidad**:

- El uso de estructuras societarias que puedan dificultar la identificación del titular real de los valores.
- El uso de canales complejos que puedan dificultar la procedencia y trazabilidad de los fondos invertidos y que favorezcan el anonimato de los inversores.
- Las características y procedencia de los inversores y de sus intermediarios, especialmente cuando tienen vínculos con territorios de riesgo (*off-shore*, paraísos fiscales, territorios designados o no cooperantes en materia tributaria o en la lucha contra BC/FT), así como clientes que son personas con responsabilidad pública y casos en que los clientes actúan a través de titulares interpuestos.
- La existencia de prestadores de servicio sin licencia que a través del uso de las nuevas tecnologías y el incremento de la utilización de canales online para prestar tales servicios ven favorecida su actividad.
- El desconocimiento de los riesgos que afectan al uso de la tecnología de registros distribuidos (DLT) para el registro de los títulos valores.

Por otro lado, el uso de la tecnología *blockchain* requerirá la designación por el emisor de una o varias entidades que serán responsables de la inscripción y registro de los valores en el sistema que, entre otras funciones, llevarán la gestión de la identificación de los titulares de los derechos derivados de los valores negociables, así como de los distintos eventos corporativos, inscripciones o gravámenes que afecten a la emisión. Independientemente de que estas entidades designadas deberán contar con autorización para la prestación del servicio de custodia de valores, actividad reservada por ley a los prestadores de servicios de inversión registrados, básicamente bancos y empresas de servicios de inversión. Con ello, los riesgos en materia de blanqueo quedan limitados.

Como señala el SNRA de la UE, pese a que el riesgo de FT es bajo, existe un riesgo creciente de BC a través de mercados de capitales especialmente a través de facilitadores de este tipo de servicios o utilizando esquemas complejos y transfronterizos que facilitan la utilización de estos productos con fines de ocultación de la procedencia de los fondos y/o de sus titulares.

Sin embargo, dada su interacción con el sector bancario para la contratación de los servicios de inversión, los riesgos de ser utilizados estos productos con los tales fines disminuyen, teniendo en cuenta que el sector bancario español cuenta un sistema preventivo sólido y robusto. A pesar de ello, cuando intervienen entidades financieras o intermediarios cuya ubicación están en jurisdicciones de riesgos, off-shore o no hay certeza de cumplimiento de los estándares europeos en PBC/FT los riesgos aumentan y la vulnerabilidad del sector financiero español a los riesgos de PBC/FT se ve incrementada.

En todo caso, en su utilización con fines de BC se dan factores, como la viabilidad financiera del producto o la necesidad de conocer la calidad de la inversión, que suponen un freno al uso de estos instrumentos. Sin embargo, cuando las redes criminales pueden confiar en una planificación económica más compleja y utilizar facilitadores profesionales para este tipo de servicios, puede haber mayor atractivo para su utilización con fines de BC.

Cabe destacar el sector tiene gran concienciación frente a los riesgos de BC/FT. Más allá de la regulación y las obligaciones legales de diligencia debida, las entidades que prestan servicios de inversión y las sociedades gestoras implementan sistemas cada vez más completos y complejos de control interno en materia de prevención del BC/FT, adaptándose de forma continua a las necesidades del sistema financiero. También las entidades depositarias, imprescindibles en estos servicios, tiene deberes preventivos.

Conclusión.

Riesgos BC. El riesgo inherente de utilización de los servicios de inversión para actividades de BC es **alto** por la propia finalidad de obtener rentabilidad financiera de los fondos invertidos y por la existencia de diferentes vulnerabilidades derivadas de los tipos de productos de inversión y de los canales de inversión que pueden ayudar a ocultar el origen de los fondos y la identidad del titular real. Sin embargo, la regulación y supervisión de estos servicios, la concienciación de las entidades del sector en la aplicación de medidas prevención del BC/FT y las medidas de mitigación indicadas dirigidas a controlar las actuaciones de este tipo de entidades conducen a minorar el riesgo residual de BC, que debe calificarse como **moderado/significativo**, dependiendo del producto y del perfil de sus clientes.

Riesgos FT. A diferencia de los riesgos de BC, la propia naturaleza de este tipo de servicios vinculados a la rentabilidad financiera de productos implica mayor dificultad y menor atractivo y exposición para su uso con fines de FT, por lo que el riesgo residual de utilizar los servicios de inversiones en valores, los servicios financieros de las gestoras de instituciones de inversión colectiva y las sociedades gestoras de fondos de titulización para actividades de FT es considerado como **bajo.**

b) Envío de dinero por entidades de pago.

Actividad, contexto y régimen normativo.

La actualización de este sector ha venido motivada por las continuas amenazas que engloban la actividad de envío de dinero y por las evidencias derivadas las actuaciones supervisoras.

Los envíos de dinero hacia o desde el exterior por las entidades de pago, popularmente denominados envíos de remesas y conocidos internacionalmente por sus siglas en ingles MVTS[26], son considerados por GAFI y por el informe SNRA de la UE como de especial vulnerabilidad en materia de BC/FT.

El Reglamento 847/2015 relativo a las transferencias de fondos, se ha visto modificado por el Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados CA y por el que se modifica la Directiva (UE) 2015/849. En este reglamento se define las transferencias de fondos como *"toda transacción efectuada al menos parcialmente por medios electrónicos por cuenta de un ordenante a través de un proveedor de servicios de pago, con objeto de poner fondos a disposición de un beneficiario a través de un proveedor de servicios de pago, con independencia de que el ordenante y el beneficiario sean la misma persona y de que el proveedor de servicios de pago del ordenante y el del beneficiario sea el mismo, incluyendo: a) las transferencias de crédito, tal y como se definen en el artículo 4, punto 24, de la Directiva (UE) 2015/2366; b) los adeudos domiciliados, tal y como se definen en el artículo 4, punto 23, de la Directiva (UE) 2015/2366; c) los envíos de dinero, tal y como se definen en el artículo 4, punto 22, de la Directiva (UE) 2015/2366, sean nacionales o transfronterizos; d) las transferencias llevadas a cabo utilizando una tarjeta de pago, un instrumento de dinero electrónico, un teléfono móvil u otro dispositivo digital o informático, de prepago o pospago, de características similares".*

El Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que traspone la Directiva de Pagos Europea, define el *"servicio de envío de dinero"* como *"un servicio de pago que permite recibir fondos de un ordenante sin que se cree ninguna cuenta de pago a nombre del ordenante o del beneficiario, con el único fin de transferir una cantidad equivalente a un beneficiario o a otro proveedor de servicios de pago que actúe por cuenta del beneficiario o recibir fondos por cuenta del beneficiario y ponerlos a disposición de éste"*

En el SNRA de la UE se analiza esta actividad como *"Transferencias o envíos de dinero"* como un servicio de pago donde utiliza tanto dinero en efectivo como transferencias electrónicas.

Tradicionalmente este servicio ha sido conocido como el envío de remesas por inmigrantes a sus países de orígenes. A pesar de que la forma habitual de proceder en estos envíos de dinero es la utilización del efectivo, ya sea por existir una posible bancarización entre esta población, por la obtención de fondos procedentes de la economía sumergida o por ser una forma tradicional de remitir fondos, las transferencias o el uso de tarjetas a través de las plataformas de envío de dinero online desarrolladas por estas tradicionales *remesadoras* están cobrando cada día más una mayor importancia.

La mayoría de los clientes de este tipo de entidades son inmigrantes procedentes de países hispanoamericanos, norteafricanos y asiáticos, y también es frecuente que algunos negocios que actúan como agentes de las entidades

[26] Money and Value Transfer Services.

de pago sean gestionados por personas de estas nacionalidades, desarrollando simultáneamente en los mismos establecimientos otras actividades económicas no financieras, como los denominados *"locutorios".*

El servicio de envío de dinero sin la necesidad de creación de cuenta de pago está reservado a las entidades de pago. Estas entidades se regulan por el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

Las entidades de pago están sujetas a autorización del Banco de España, previo informe del Sepblac sobre la idoneidad de los órganos y procedimientos de prevención. Una vez obtenida la autorización, y tras su inscripción en el Registro Mercantil, se procederá a la inscripción en el Registro Especial de Entidades de Pago, en el que, además, deberán figurar sus agentes y sucursales. La supervisión prudencial del cumplimiento y mantenimiento de las condiciones de la autorización corresponde al Banco de España, y la supervisión de prevención del BC/FT al Sepblac, así como al Banco de España en caso de Convenio, firmado el 18 de marzo de 2021.

El volumen de actividad de estas entidades en España asciende a 18.026[27] millones de euros (11.570 millones de giros emitidos y 6.456 millones de giros recibidos), concentrándose el 89% de la actividad total del sector en 10 entidades.

El giro medio de los envíos se estima en 260 euros y los 10 principales países de destino de los giros emitidos son (en millones de euros): Colombia (1.112), Marruecos (991), Ecuador (668), República Dominicana (484), Pakistán (432), Honduras (404), Bolivia (396), Senegal (383), Paraguay (375) y Perú (354)[28].

El sector está formado, a 31 de diciembre de 2022, por 52 entidades de pago con establecimiento en España, de las cuales 25 cuentan con autorización para prestar servicios de envío de dinero y 21 prestan este servicio de forma exclusiva. El sector tiene un alto grado de concentración dado que las diez entidades principales acaparan cerca del 80% del volumen total. Casi la mitad de estas entidades (19) pertenecen a la Asociación Española de Entidades de Pago (AENPA).

Además de estas entidades, hay 10 entidades de pago exentas según el artículo 14 del Real Decreto-ley 19/2018, de 23 de noviembre, que realizan la actividad de envío de dinero. Estas entidades son sujetos obligados según lo establecido en el artículo 2.1 h). En el apartado 3 del artículo 2 se establece la posibilidad de exclusión, total o parcialmente, de estas entidades siempre que presenten un bajo riesgo de BC/FT.

Según datos del Banco de España, estas entidades han realizado 73.352 operaciones de envío de fondos que suponen casi 27 millones de euros. En comparativa con la actividad de envío de dinero, se observa que la operativa de estas entidades que recaen bajo la regulación del artículo 14 del Real Decreto-ley 19/2018, de 23 de noviembre, no es relevante.

Amenazas.

Las remesas enviadas a jurisdicciones de riesgo, especialmente aquellas señaladas por GAFI en relación con la financiación del terrorismo, presentan elevadas amenazas para los riesgos de BC/FT. Las posibilidades de fragmentación de envíos, el uso de efectivo o tarjetas prepago para remitir fondos o la escasa necesidad de elevados conocimientos financieros para realizar esta operativa convierten a este servicio financiero en una actividad de fácil acceso para la financiación del terrorismo.

Las organizaciones criminales utilizan esta vía para canalizar sus fondos y favorecer la pérdida de trazabilidad de los mismos mediante el envío, así como para realizar la actividad que es el origen del delito.

[27] Estimación, a 31 de diciembre de 2022, realizada por Sepblac según datos propios y datos del Banco de España. Los datos del Sepblac suponen el 50% de la actividad.
[28] Datos obtenidos de la actividad de estas entidades que declaran a Sepblac a diciembre de 2022.

Los fraudes son especialmente relevantes en el uso de este tipo de servicios, tanto en tipologías de fraude conocidos como *"cartas nigerianas"* como en la movilización de fondos fruto de estafas tipo *phishing* o fraude fiscal. Adicionalmente, el tráfico de drogas, el tráfico de seres humanos o el contrabando de mercancías son delitos que hacen un elevado uso de estos servicios de envío de dinero.

Las posibles operaciones de BC no sólo se refieren a las fragmentaciones de los envíos entre múltiples ordenantes a los países de destino para evitar su detección (actividades conocidas como *"pitufeo"*), sino también mediante la toma del control de estas agencias por las redes (al margen de la entidad) lo que permite efectuar envíos de dinero mediante la suplantación de identidades de los remitentes o mediante la falsificación de estas identidades realizadas a través de agentes vinculados a las propias redes de BC.

En los delitos de BC asociados a la operativa de envío de dinero cobra especialmente relevancia la figura del *"mulero"* que es la persona física que, a cambio de una compensación, es el actor principal en las transferencias de fondos. En este sentido, a pesar de que el efectivo sigue siendo el principal instrumento utilizado, se considera necesario la mención a las tarjetas prepago que no requieren la constitución de una cuenta de pago. La recarga de efectivo en estas tarjetas y su posterior uso para remitir fondos a través de plataformas de envío de dinero se configura como un método adicional para el movimiento de flujos monetarios que tiene como origen las actividades delictivas señaladas anteriormente.

Vulnerabilidades y riesgo sectorial.

El **riesgo inherente** del sector de entidades de pago es muy elevado[29] por diferentes motivos, relacionados tanto con factores endógenos como con factores exógenos.

El número total de extranjeros residentes en España a finales de 2022 ascendía a 6.089.620 personas, un 12,7% de la población. El uso de efectivo en este sector de la población es elevado, principalmente por la economía sumergida asociada al desarrollo de su actividad económica y las transferencias en forma de remesa a sus países de origen.

Las entidades de pago y sus sucursales y agencias presentan un riesgo superior a otros sujetos obligados por su capacidad para poder canalizar fondos, lo que les convierte en un sistema atractivo para transferir fondos ilícitos. Ello se debe, por un lado, a la atomización de sus operaciones, ya que un elevado número de clientes realiza muchas transacciones de importes pequeños y, por otro, a la existencia de un importante número de establecimientos de pequeño tamaño que gestionan transferencias de dinero en régimen de agencia (cada entidad de pago puede tener miles de agentes). Todo ello dificulta el adecuado control de estos establecimientos por parte de las autoridades y de las propias entidades de pago en las que se integran, lo que ha favorecido en años precedentes la utilización de agentes y establecimientos pequeños para actividades de BC/FT por parte de las redes criminales.

En este sentido, el agente es un punto clave en la prevención del blanqueo por la vulnerabilidad que representa esta figura frente a los riesgos de BC/FT, ya que la elevada rotación de agentes entre diferentes entidades de pago y la relación directa con el cliente les permite generar una sensación de fidelidad más orientada al servicio prestado al cliente que al cumplimiento normativo que tiene con la gestora.

Estos factores dificultan el control y supervisión de estos establecimientos por parte de las autoridades, convirtiéndose para las organizaciones criminales y terroristas en un sistema atractivo para transferir fondos ilícitos.

Riesgo residual. La implementación en los últimos años de medidas preventivas de BC/FT basadas en riesgo en la actividad de envíos de dinero ha supuesto un incremento del seguimiento y supervisión de estas operaciones y la

[29] En línea con los hallazgos del Informe de la EBA en relación con los riesgos PB/FT asociados a las Entidades de Pago y emitido en junio de 2023.

adopción de medidas específicas en materia de prevención por parte de las entidades de pago, las cuales han conducido a una mitigación significativa de los riesgos. Entre estas medidas destacan:

- Establecimiento de obligaciones más estrictas de diligencia debida de sus clientes. En concreto, la regulación española exige la identificación y comprobación de la identidad del cliente o de cualquier persona que lleve cabo una operación ocasional de envío de dinero, con independencia de su cuantía (a diferencia con lo exigido por la Directiva comunitaria – umbral de 1.000 euros-).
- Aprobación de unas obligaciones específicas de políticas de control interno de prevención del BC/FT para el sector.
- Exigencia de un sistema más riguroso de información sistemática a través de la Declaración Mensual Obligatoria que presentan estas entidades y que exige una información detallada de sus actividades conforme a diferentes criterios de clasificación.
- Creación de un registro de agentes de alto riesgo por parte del propio sector, a través de su asociación, AENPA.
- Intensificación de las actuaciones de supervisión y medidas sancionatorias.
- Acciones dirigidas a incrementar la sensibilización de las entidades en la prevención del BC/FT.
- Existencia de un Catálogo de Operaciones de Riesgo de BC/FT en el sector[30] de envíos de dinero.

Por su parte, las entidades de pago representan el segundo grupo de sujetos obligados en número de comunicaciones sospechosas, en concreto, las cifras anuales de comunicaciones por parte de las entidades del sector se sitúan en torno a las 1.000 comunicaciones de media desde el año 2017.

El resultado ha sido una mejora sustancial de la aplicación de las medidas preventivas, con un reforzamiento e incremento de controles y políticas de prevención, por lo que el riesgo de envío de dinero por entidades de pago ha pasado de ser alto a significativo.

En ningún caso debe vincularse el riesgo de las entidades de pago en relación con las actividades de sus clientes con el posible riesgo de las entidades de pago como clientes de otros sujetos obligados. En este caso, el incremento en la calidad y cantidad de las medidas, políticas y procedimientos internos adoptados en los últimos años por las entidades de pago, más las medidas implantadas por las entidades financieras, junto con la creciente colaboración entre ambos tipos de entidades, hacen que el riesgo residual global se haya reducido notablemente y presente una tendencia a seguir haciéndolo.

Conclusión.

Las actividades de envío de dinero por las entidades de pago tienen unos riesgos inherentes muy **altos** usarse con fines de BC/FT. Sin embargo, esos riesgos han sido objeto de mitigación por diferentes actuaciones y medidas que han ocasionado resultados muy positivos en la minoración global de riesgos.

Estas medidas específicamente dirigidas a las operaciones de envío de dinero actúan sobre diferentes ámbitos de actuación: reforzamiento del régimen de prevención por las entidades de pago; actividades inspectoras realizadas por las autoridades supervisoras (90 entre 2018 y 2022); obligaciones de información; acercamiento al sector por parte de las autoridades y elaboración conjunta de listas de operaciones de riesgo; coordinación entre entidades del sector y control de agentes de riesgo, entre otras actuaciones.

Todas estas medidas de mitigación aplicadas en los últimos años en el sector de entidades de pago han llevado a una mejora sustancial de la situación de riesgo del sector que ha pasado de ser alto a **significativo** para **BC** y para **FT**.

[30] http://www.tesoro.es/sites/default/files/cor_entidades_de_pago.pdf.

c) Otros servicios prestados por entidades de pago.

Actividad, contexto y régimen normativo.

La actualización de este sector ha venido motivada por el incremento de ejecuciones de operaciones de pago. A su vez, la accesibilidad al Sistema Nacional de Compensación Electrónica (en adelante, SNCE) y la declaración de las cuentas de pago por este sector al FTF han potenciado la revisión de la ficha de riesgo sectorial que se desarrolla a continuación.

La PSD2 traspuesta al ordenamiento jurídico español mediante el Real Decreto- Ley 19/2018, de 23 de noviembre, introdujo la prestación de servicios de pago adicionales al envío de dinero (analizado en el epígrafe anterior): ingresos y retiradas de cuentas de pago; transferencias, adeudos domiciliados y pagos efectuados con tarjetas (pagos a débito o a crédito); emisión de instrumentos de pago o adquisición de operaciones de pago; servicios de iniciación de pagos o servicios de información sobre cuentas. Las entidades de pago no pueden ofrecer depósitos o fondos reembolsables, ni emitir dinero electrónico, entre otras limitaciones a su actividad.

Como se ha indicado en el anterior capítulo, el sector de entidades de pago, a 31 de diciembre de 2022, está formado por 52 entidades de pago con establecimiento en España registradas en el Banco de España y, además, pueden operar 258 entidades de pago sin establecimiento, autorizadas en otros países europeos.

El número de entidades que ofrecen servicios distintos al envío de dinero son 27 según datos de Banco de España, aunque hay que incluir 4 entidades que están autorizadas a realizar envíos de dinero y otros servicios.

La PSD2 y su transposición a la regulación española sentaron las bases para promover la innovación y adopción de los servicios bancarios a las nuevas tecnologías. En diciembre de 2021, se modificó el reglamento del SNCE en España, permitiéndose que entidades de pago y de dinero electrónico sean entidades accesibles al sistema.

En España, a pesar de que los pagos se realizan mayoritariamente por entidades de crédito o con la intervención de éstas, las cuentas de pagos asociadas a entidades de pago o de dinero electrónico son cada vez más frecuentes, favoreciendo una mayor inclusión financiera de la población. La Directiva de Pagos, PSD2, y su transposición pasan a regular otros servicios que se prestan por entidades de pago y que no se sujetan a un marco específico. En concreto:

- Los servicios de **iniciación de operaciones** de pago. Estos servicios permiten iniciar una orden de pago, a petición del usuario, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago. Por tanto, un cliente autoriza al proveedor de estos servicios a acceder a sus cuentas de pago para pagar sus compras u otros servicios directamente al suministrador, sin necesidad de usar una tarjeta de pago o que la entidad financiera tenga que mediar en la operación.
- Los servicios de **agregación de cuentas.** Estos servicios consisten en la consolidación de la información sobre saldos y operaciones de varias cuentas de pago que un mismo cliente puede tener abiertas en diversas entidades financieras.

La naturaleza de estos servicios hace que las entidades de pago que realicen en exclusiva actividades de “iniciadores” de pago o de “agregadores” de información de cuentas sólo precisen tener el consentimiento del cliente y la información necesaria para poder prestar la actividad, sin necesidad de constituirse en administradores de las cuentas de pago, dado que no entran a gestionar fondos de sus clientes.

Amenazas.

Investigaciones policiales muestran como el uso de este tipo de servicios de pago donde interviene la creación de una cuenta de pago con el fin de realizar transacciones internacionales y ejecutar operaciones de pago con el objetivo de obtener los productos o servicios necesarios para llevar a cabo su operativa y financiación de actividades es un servicio utilizado por organizaciones terroristas.

La transaccionalidad de estos servicios de pago genera amenazas para el sistema preventivo español, especialmente cuando hay interacción con jurisdicciones donde la economía está poco bancarizada o son consideradas de alto riesgo de financiación del terrorismo.

En cuanto al BC, las amenazas son similares a las mencionadas para el servicio de envío de dinero, viéndose esta tipología de operativa favorecida por la digitalización de la economía y el acceso a estos servicios vía online, junto con la aparición de intermediarios que actúan como prestadores de servicios y dependiendo su infraestructura de pagos de una entidad de pago autorizada como tal.

Como se ha señalado en el apartado previo, las entidades de pago están sujetas a régimen de autorización, supervisión y registro por el Banco de España.

Vulnerabilidades y riesgo sectorial.

Las entidades de pago pueden realizar ejecuciones de pago inmediatas que implican la apertura de cuentas de pago. Esta actividad genera elementos de riesgos, principalmente en cuanto a la dificultad de identificación del titular real de esa cuenta, lo que supone unos **riesgos inherentes altos**.

La presencia de nuevos operadores que ofrecen servicios en la intermediación de pagos entre cliente y entidad puede suponer la apertura de cuentas de pago generalizadas a nombre del intermediario y donde se registran todas las transacciones de personas que operan a través de estos intermediarios. Esto dificulta el conocimiento del titular real de la operativa, generando riesgos desde el punto de vista de BC/FT para la entidad que es sujeto obligado.

En definitiva, las nuevas tecnologías han generado nuevos mercados en los que los operadores ofrecen nuevos instrumentos basados en transacciones electrónicas por el cliente, que pueden ser usadas u ordenadas desde cualquier terminal y en cualquier parte del mundo. En paralelo, se han desarrollado una amplísima gama de servicios que van más allá de la actividad de pago.

En cuanto a los iniciadores de pago/agregadores de información sobre cuentas, debe incidirse en el hecho de que precisan tener el consentimiento del cliente para prestar servicio y que actúan como meros intermediadores entre el destinatario del pago y el cliente, sin necesidad de constituirse en administradores de cuentas de pago. Por este motivo, las actividades de iniciación de pagos y de agregación de cuentas que realizan las entidades de pago presentan **riesgos inherentes** claramente **menores**, al no gestionar, en ningún caso, fondos de clientes.

Además, al no existir una relación contractual entre estos prestadores de servicios y el gestor de las cuentas, la normativa sobre servicios de pago impone para asegurar la integridad de los fondos y la confidencialidad de la información: 1) que en la comunicación entre ambas partes se utilicen estándares abiertos, comunes y seguros entre ambos, y 2) que en sus relaciones todos ellos adopten medidas de seguridad.

En todo caso, de conformidad con lo exigido por la normativa de la UE, estas entidades tienen la consideración de sujetos obligados en materia de prevención BC/FT, por lo que deben aplicar a las operaciones de pago y de iniciación de pagos los mismos controles preventivos, lo que viene a reducir aún más esos riesgos.

Finalmente, en cuanto a las entidades de pago que emiten tarjetas de crédito y débito, se exige una relación contractual con clientes particulares y entidades que efectúan consumos en sus tarjetas y autorizan a las entidades de pago a efectuar un adeudo domiciliario en la entidad de crédito en donde dichos clientes tienen una cuenta bancaria, siendo dicha entidad de crédito, a su vez, sujeto obligado. Por este motivo, las actividades que realizan

estas entidades de pago que emiten tarjetas de crédito y débito presentan riesgos inherentes menores, pero teniendo que establecer también mecanismos de control apropiados para evitar su utilización indebida.

Conclusión.

Por un lado, la posibilidad de ejecución de órdenes de pago y acceso al SNCE que permite la creación de en cuentas de pagos supone un riesgo de utilización para actividades de BC/FT. A pesar de que las entidades de crédito sean los principales emisores de cuentas de pago, el uso de dichas cuentas por entidades de pago y de dinero electrónico es cada vez mayor, lo que lleva a considerar que estos servicios presentan un riesgo residual **significativo** para ser utilizadas indebidamente (abusadas) con fines de **BC/FT**.

A pesar de este riesgo, desde enero de 2022 el Real Decreto-ley 7/2021, de 27 de abril, introdujo la obligatoriedad de declarar al FTF las cuentas de pago de entidades de pago y de dinero electrónico, reforzándose la supervisión a estas entidades a través de la declaración de cuentas.

Por otro lado, el riesgo residual de la operativa de iniciación de pagos es **moderado-bajo**, pues está ligado a la mera intermediación en el pago de productos o servicios sin gestionar los fondos del cliente. Es decir, una vez recibida la orden de iniciar el pago, se limitan a comprobar si hay fondos suficientes en la cuenta de pago del ordenante que éste le indique para proceder al pago, y en caso de haberlos, informar al vendedor de que se ha iniciado el pago.

En cuanto a la actividad de los agregadores de cuentas, su riesgo residual podría calificarse como **bajo** pues no intermedian en pago alguno y se limitan a consolidar información previamente analizada por los gestores de cuentas a los que, como sujetos obligados, les aplica el marco preventivo de BC/FT. No obstante, son entidades que concentran mucha información financiera agregada de los clientes y de sus fondos, y pueden desarrollar una labor importante en la detección de actividades relacionadas con BC/FT que no son detectadas por los otros sujetos obligados que gestionan las cuentas.

Finalmente, en cuanto a entidades de pago que emiten tarjetas de crédito y débito, su riesgo residual podría calificarse como **moderado** pues, en general, operan con fondos procedentes de otros sujetos obligados (mediante domiciliaciones bancarias). No obstante, como en el anterior caso, son entidades que concentran mucha información de los clientes y del destino o uso de sus fondos, y pueden desarrollar una labor importante en la detección de actividades relacionadas con el BC/FT que no son detectadas por los otros sujetos obligados que gestionan sus cuentas principales.

d) Operaciones con dinero electrónico.

Actividad, contexto y régimen normativo.

La actualización de este sector ha venido motivada por el incremento de ejecuciones de operaciones de pago realizadas por las entidades de dinero electrónico. A su vez, la accesibilidad al SNCE y la declaración de las cuentas de pago por este sector al FTF han potenciado la revisión de la ficha de riesgo sectorial que se desarrolla a continuación.

Las entidades de dinero electrónico, EDE, son aquellas autorizadas para emitir dinero electrónico que es admitido como medio de pago por empresas distintas a la entidad emisora. Se entiende por dinero electrónico el valor monetario representado por un crédito exigible a su emisor. Este valor, que se encuentra almacenado en un soporte electrónico, es emitido al recibir fondos de un importe cuyo valor no será inferior al valor monetario emitido y es aceptado como medio de pago por empresas distintas del emisor.

Su regulación se establece mediante Ley 21/2011, de 26 de julio, de dinero electrónico modificada por el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, y su reglamento de desarrollo aprobado por Real Decreto 778/2012, de 4 de mayo.

El proceso de creación de las entidades de dinero electrónico exige una serie de requisitos como: capital social nominativo mínimo de 350.000 euros, domicilio en territorio español, honorabilidad profesional y comercial, entre otros. Las entidades de dinero electrónico españolas deben contar con un informe previo del Sepblac valorando la idoneidad de los órganos y procedimiento previstos conforme a la documentación presentada de la estructura y procedimientos de prevención del BC/FT que van a aplicar cuando estén operativas.

El procedimiento para la apertura de sucursales y libre prestación de servicios en España por entidades de dinero electrónico de otros Estados miembros de la UE queda condicionado a que el Banco de España reciba una comunicación de la autoridad supervisora del país de origen de la entidad de dinero electrónico.

Según datos del Registro Especial de entidades de dinero electrónico gestionado por el Banco de España, a diciembre de 2022 existían 13 EDE registradas en España. Además, hay EDE comunitarias que podrían estar operando en España sin establecimiento.

Las EDE comparten la posibilidad de realizar operativas de pago con las entidades de pago (a excepción del envío de dinero). Por ello, desde diciembre de 2021 las entidades de dinero electrónico son entidades accesibles al SNCE y en virtud del RD 7/2021 deben declarar las cuentas de pago al FTF.

La innovación financiera ha contribuido al desarrollo de estas entidades mejorándose el grado de inclusión financiera de la sociedad, siendo algunas denominadas como los nuevos *neobancos*.

Amenazas.

Las EDE, en su operativa, guardan muchas similitudes con las entidades de pago. Por ello, las amenazas existentes para este sector son muy parecidas a las que les afectan a los sujetos obligados analizados en el epígrafe anterior. Por lo tanto, las amenazas de ser utilizadas para la financiación del terrorismo son altas especialmente cuando actúan de entidades financieras principales en países donde hay escasa bancarización o son considerados de alto riesgo.

Se ha constatado que algunos instrumentos de dinero electrónico como las tarjetas prepago han sido objeto de utilización en diferentes países para financiar actividades terroristas, principalmente vinculadas a grupos yihadistas, debido a la ausencia de exigencias de identificación del cliente por debajo de ciertos umbrales. También son

instrumentos susceptibles de uso por amenazas procedentes de terceros países en los que los sistemas de identificación de los adquirentes son menos rigurosos, lo que viene motivando un incremento en las restricciones de las regulaciones de los países europeos para operaciones con instrumentos anónimos.

La regulación española exige la identificación del cliente en todo caso respecto de las operaciones con dinero electrónico con independencia de su cuantía, aunque se admiten medidas simplificadas en los siguientes casos:

- Cuando el dinero electrónico no pueda recargarse y el importe almacenado no exceda de 250 euros.
- Cuando, en caso de que pueda recargarse, el importe total disponible en un año natural esté limitado a 2.500 euros, salvo cuando el titular del dinero electrónico solicite el reembolso de una cantidad igual o superior a 1.000 euros en el curso de ese mismo año natural.

En relación con el BC, la digitalización de la sociedad y la creación de potentes plataformas de pago por este tipo de sujetos obligados hacen que sean utilizadas por organizaciones criminales y por actores individuales para movilizar fondos de origen ilícito.

Investigaciones e informes estratégicos han mostrado la creación de cuentas de pago en EDE con el fin de movilizar fondos fruto de actividades delictivas realizadas por grandes grupos internacionales de crimen organizado cuya actividad está enfocada al fraude fiscal. De la misma forma, el uso de estos productos ha sido identificado por las agencias de inteligencia con el objetivo de canalizar fondos procedentes de estafas, trata de seres humanos o tráfico de drogas.

Vulnerabilidades y riesgo sectorial.

La posibilidad de fragmentación de las transacciones con dinero electrónico es una vulnerabilidad para los riesgos de FT, especialmente cuanto intervienen actores no incluidos en listas. La atomización de plataformas online de pago que facilitan la obtención de tarjetas prepago y los movimientos de dinero electrónico a nivel internacional constituyen una ventaja para la sociedad en cuanto a interoperabilidad y una vulnerabilidad en relación con el uso de estos servicios para la financiación del terrorismo y los flujos que provienen de actividades delictivas cometidas por grupos criminales.

Por tanto, el riesgo de penetración y actividad por parte de grupos de crimen organizado es alto. Dado que el sector de entidades de pago está sujeto a controles muy estrictos, preocupa el elevado riesgo de desplazamiento de transacciones electrónicas dentro del sector de dinero electrónico de movimientos de fondos vinculados a operaciones de BC/FT.

Los **riesgos inherentes** de su uso tanto para fines BC como FT son mayores a los de otros sistemas de pago. Ello es debido a que se trata de instrumentos que, en algunos países, aunque no en el caso de España, no suministran datos sobre los tenedores del dinero electrónico, ni sobre el origen de los fondos que se portan (a diferencia de las tarjetas de débito o crédito que, en el caso de España, contienen información del pagador y de su cuenta de pago vinculada), a que no exigen al portador de tarjetas prepago la titularidad de una cuenta corriente o similar, y a que permiten su rápida conversión por dinero en efectivo.

La proliferación de este tipo de servicios en países con menores requisitos preventivos para obtener la licencia de actividad por la autoridad nacional es un hecho. En este sentido, preocupa la posición actual de los agentes que prestan estos servicios ya que algunos han pasado a considerarse *neobancos* (sin tener licencia bancaria como tal).

En España se exige identificación en todo caso en el momento del ingreso de fondos, pero esa exigencia de identificación varía según el país emisor, que pueden establecer distintos umbrales, lo que influye en la exposición a los riesgos de su posible uso, tanto para BC como para fines de FT.

En definitiva, a pesar de que el dinero electrónico presenta más ventajas en cuanto a su trazabilidad, la velocidad de las transacciones junto a su transaccionalidad a nivel global y las comodidades del acceso a plataformas online hacen que las vulnerabilidades asociadas a este sector en relación con la exposición de riesgos de BC/FT sean altas.

Conclusión.

El sector de entidades de dinero electrónico tiene unos riesgos inherentes muy altos comunes para todo el sector. Estos riesgos son superiores para los casos de dinero electrónico cuya emisión se produce en otros países y cuyos controles sobre la identidad del titular y sobre los umbrales no gozan de los requerimientos exigidos a nivel nacional. Sin embargo, como se ha indicado, las modificaciones normativas específicas aprobadas para reforzar el régimen de prevención del BC/FT en estas entidades, el acercamiento al sector por parte de las autoridades reguladoras y supervisoras y el incremento de la aplicación de las políticas y procedimientos internos por parte de las entidades del sector, que incluyen una mejora en las comunicaciones por indicio, han llevado a una mejora sustancial de la situación de riesgo del sector que ha pasado de ser alto a **significativo** tanto para **BC** como para **FT**.

Entre las medidas mitigadoras que favorecen el control del sector de EDE es necesario mencionar que desde enero de 2022 el Real Decreto-ley 7/2021, de 27 de abril, introdujo la obligatoriedad de declarar al FTF de las cuentas de pago de entidades de pago y de dinero electrónico, reforzándose la supervisión a estas entidades a través de la declaración de cuentas.

e) Criptoactivos y Proveedores de Servicios de Criptoactivos.

Actividad, contexto y régimen normativo.

La actualización de este sector ha venido motivada por la elaboración del Análisis Sectorial de Riesgos de CA y PSCA que ha permitido la identificación, de forma exhaustiva, de las amenazas, vulnerabilidades y riesgos que afectan al sector.

A la fecha, el único marco aplicable al sector es el preventivo, en el que los únicos CA en que son objeto de regulación son las monedas virtuales, y los únicos servicios relacionados con estas cuyos proveedores tienen la consideración de sujetos obligados, son los de a) cambio de moneda virtual por moneda fiduciaria y b) la custodia de monederos electrónicos.

Sin perjuicio de que en la actualidad solo existan dos categorías de PSCA reconocidos como sujetos obligados en nuestra legislación, hay que tener en cuenta la reciente actualización del marco preventivo europeo, a través de los cambios ya incorporados en la Directiva 2015/849 por el Reglamento de transferencia de fondos y ciertos CA (UE) 2023/1113, de 31 de mayo (en adelante, RTFyCA) y que deberán ser aplicables en España antes del 31 de diciembre de 2024. Con estos cambios se incorporarán como sujetos obligados a los PSCA regulados en el Reglamento de mercados de CA (UE) 2023/1114 de 31 de mayo (en adelante, MiCA), salvo los que prestan servicios de asesoramiento, y se completará así nuestro alineamiento con los estándares GAFI.

En cuanto a datos, no se tiene certeza del número de PSCA que permanecen activos, de todas las redes y los CA con los que operan, así como del alcance de otros servicios que pudieran prestar además del de cambio y/o custodia. Sin embargo, se ha elaborado un estudio por Chainalysis a petición de la COPBLAC, donde se señala que dentro de los 50

que presentan mayor volumen de actividad en España, los 10 primeros concentran el 85,5% de esta actividad con CA y los tres primeros que representan el 60,2% de la actividad están inscriptos en el registro de Banco de España, lo cual mitiga el riesgo.

Este registro fue creado en octubre de 2021 y es un requisito perceptivo para todos los operadores que quieran prestar este tipo de servicios en España.

A 29 de junio de 2023, figuraban inscritos en el Registro de Proveedores de Servicios de cambio de moneda virtual por fiduciaria y/o custodia de monederos electrónicos del Banco de España, 76 proveedores, de los cuales, 41 ofrecen servicios de cambio, 4 de custodia, y 31 ofrecen ambos. La gran mayoría tienen sede en España, excepto 21 que operan en libre prestación de servicios.

De acuerdo con el Índice de adopción cripto global que fue actualizado con el Informe de Situación del sector en España de junio 2023, España se sitúa en el puesto 34 de nivel de adopción de entre un total de 146 países. Además, se sitúa en el puesto 99 en volumen de transacciones P2P, lo que denota que la mayor actividad se concentra en mercados centralizados (puesto 27), donde canalizó algo menos de dos terceras partes de los CA, y descentralizados (puesto 24), donde se sitúa cuatro puntos porcentuales por encima de la adopción global.

Sin embargo, al contextualizar la operativa de CA con la actividad en moneda fiduciaria en España, se observa que la operativa de recepción de volumen de CA en comparativa con el importe de la operativa SEPA (relativa a transferencias), supondría un 5,8% de esta actividad.

Algunos de los cambios detectados por las autoridades españolas, tras las diversas caídas en el valor de las CA unido a factores como la velocidad de la transacción o las bajas comisiones, muestran un mayor empleo de *stablecoins* (theter, USDT) que mantienen un valor casi constante en el tiempo referenciado al dólar o al euro. Según datos proporcionados por Chainalysis, en relación con flujos de entrada y salida de España de CA, las *stablecoins* son también las dominantes entre el bitcoin, el ethereum y otros activos virtuales[31].

Amenazas.

Las principales amenazas en materia de BC/FT o financiación de la proliferación (en adelante, FP) no difieren en general de las del mundo *fiat*, pero la canalización de fondos ligados a terrorismo, proliferación, extorsión, estafa, fraude, evasión fiscal, tráfico de drogas, de armas o de seres humanos pueden resultar difícilmente trazables cuando en la cadena de transmisión intervienen el uso de CA, y más aún de PSCA ubicados en territorios no cooperantes o con una legislación más laxa.

Según datos de Chainalysis el volumen de actividad de CA considerada de riesgo en el 0,4% (0,6% a nivel global y 0,7% para Europa Occidental), y estima en el 0,1% la considerada como ilícita (0,4% a nivel global e idéntica a la europea).

Las principales amenazas en España para las actividades de financiación del terrorismo vendrían derivadas de la evolución del terrorismo yihadista, donde la operativa investigada por las autoridades que forman parte de las FCSE, se ha detectado el empleo de *privacy coins*. Además, se identifican el uso de *bots* por parte de los grupos terroristas con el fin de crear numerosas direcciones e individualizando una dirección por cada donación y dificultando así la trazabilidad.

La minería de CA puede facilitar la movilización de fondos de organizaciones terroristas debido al carácter descentralizado de los CA, el pseudo-anonimato y privacidad que ofrecen muchas criptomonedas.

En definitiva, las amenazas vinculadas al terrorismo y armas de destrucción masiva afectan al uso de CA con el objetivo de canalizar la financiación y para la compra de armas de destrucción.

[31] https://www.guardiacivil.es/es/prensa/noticias/8124.html

En relación con el BC, las principales amenazas provienen de las actividades delictivas de grupos criminales y vinculadas al tráfico de drogas y a los delitos económicos y financieros, principalmente relacionados con fraudes y actividades de corrupción. Además, es necesario recalcar que dentro de la operativa vinculada a fraudes, los ataques de *ransomware* en los que se hace uso de CA son uno de los principales delitos identificados por los FCSE en sus investigaciones.

Vulnerabilidades y riesgo sectorial.

Para las vulnerabilidades véase lo expuesto en el apartado 5.3.2.

Conclusión.

El riesgo inherente de utilización de los **activos o monedas virtuales** con fines BC/FT es **alto**. La falta de regulación suficiente aplicable, la facilidad de acceso a este tipo de activos, la opacidad de su funcionamiento y el anonimato de las partes que intervienen, así como el carácter transfronterizo del fenómeno, son elementos de riesgo que deben tenerse en consideración.

No obstante, en España debido a que el volumen total en circulación es escaso (66,45 mil millones de dólares entre marzo 2022 y 2023) a su limitada utilización como medio de pago (supone un 5,8% de la transferencias, transferencias inmediatas y traspasos SEPA) y a que las cifras de emisión de token digitales son muy pequeñas y son objeto de control por la CNMV, el riesgo real de su uso con fines BC/FT debe considerarse minorado en relación con el elevado riesgo inherente.

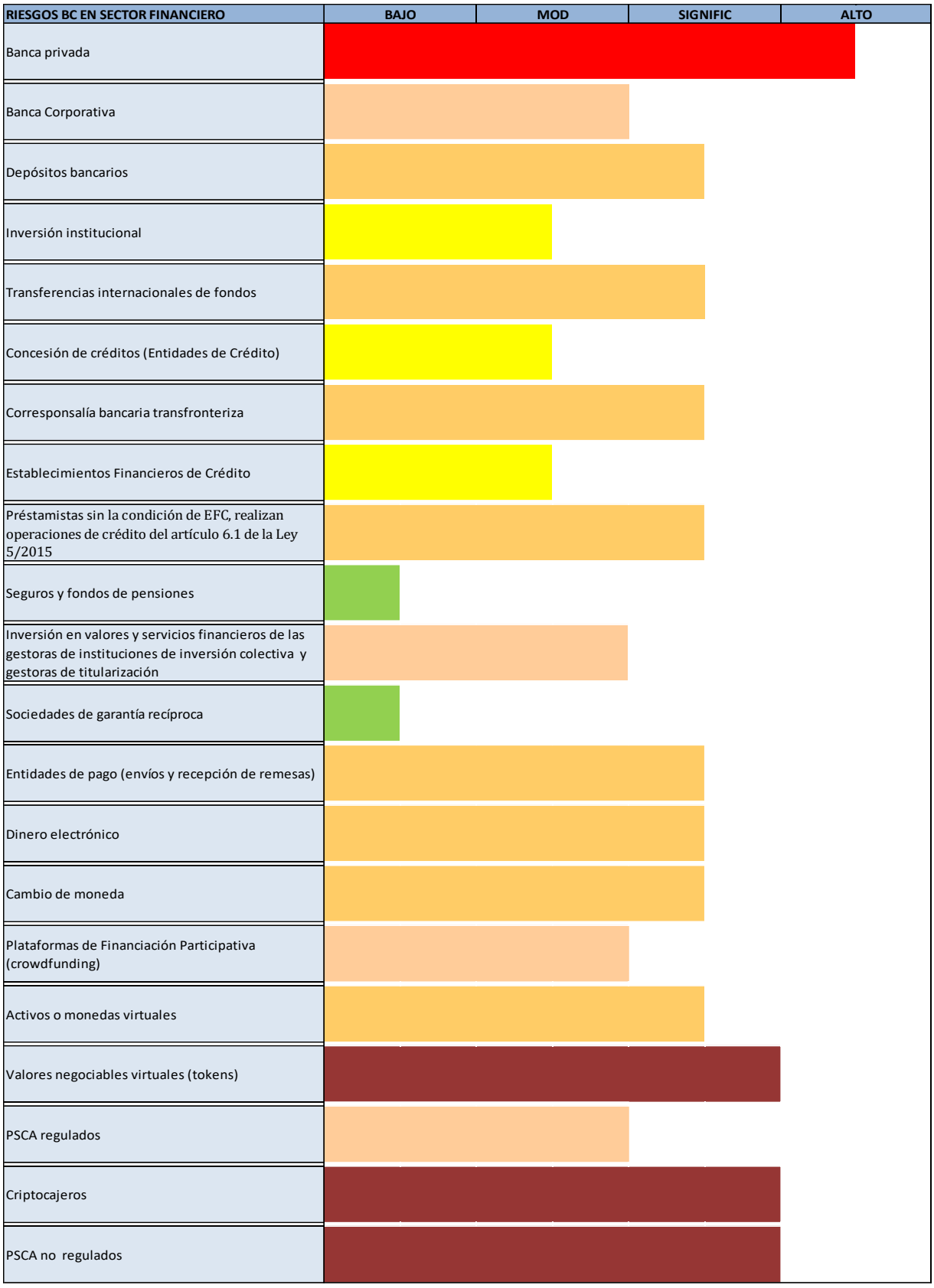
Teniendo todo ello en consideración, las **monedas virtuales** constituyen un riesgo residual **significativo/moderado** para su uso tanto en actividades de BC como de FT, calificación que se obtiene de su escaso uso y de las investigaciones, realizadas hasta el momento, en las que se ha analizado la utilización de monedas y activos virtuales con estas finalidades. No obstante, debe reiterarse que la dificultad que implica la detección y seguimiento de estas operaciones únicamente ha permitido la identificación de casos puntuales y, que, de momento, han ofrecido cifras de escasa relevancia.

Esos riesgos son inferiores para la utilización de los **valores negociables virtuales (tokens)**: aunque tienen un nivel **significativo** para actividades de BC, el riesgo residual debe considerarse **moderado** para actividades de FT y financiación de la proliferación, ya que la propia naturaleza de este tipo de servicios de inversión está vinculada a una posible rentabilidad financiera de productos que implica mayor dificultad de gestión y una menor exposición al riesgo para su uso con estos fines de FT y financiación de la proliferación.

Los **PSCA regulados** en España tienen un riesgo inherente **significativo** en materia de BC/FT, calificación que se obtiene teniendo en cuenta el tipo de servicios que prestan, relaciones no presenciales, operatividad y por existencia de PSCA regulados no registrados y su riesgo residual es **moderado**, mientras que el riesgo residual para los ***criptocajeros*** se mantiene en **significativo**.

Los **PSCA no regulados** en España tienen un riesgo inherente alto en materia de BC/ FT, por la operativa que realizan teniendo en cuenta que no se limitan a servicios de custodia y de cambio de criptomoneda por moneda fiduciaria, sino que abarcan actividades con CA en las que puede incrementarse los riesgos derivados de su transaccionalidad, *transterritorialidad* y la falta de conocimiento en la aplicación de las medidas nacionales en materia de PB/FT. Su riesgo residual es **significativo**, principalmente por la cuota de actividad realizada por 3 PCSA que sí están inscritos en el registro del Banco de España.

CUADRO DE RIESGO BC SECTOR FINANCIERO[32]



[32] El cuadro contiene toda la información de todos los sectores analizados en el ANR de 2020 y no solo los modificados en esta adenda.

CUADRO DE RIESGO FT SECTOR FINANCIERO[33]



[33] El cuadro contiene toda la información de todos los sectores analizados en el ANR de 2020 y no solo los modificados en esta adenda.

f) Uso de dinero en efectivo, movimientos de efectivo y negocios con uso intensivo de efectivo.

Actividad, contexto y régimen normativo.

La actualización de este sector ha venido motivada la modificación normativa en cuanto a declaración de movimientos de pago que alinea la regulación española a las disposiciones establecidas en el Reglamento de Ejecución (UE) 2021/776 de la Comisión de 11 de mayo de 2021. Además, se ha tenido en cuenta el elevado empleo de efectivo por la sociedad española, siendo considerado actualmente, según el *Estudio sobre hábitos en el uso del efectivo 2022* del Banco de España, como el primer método de pago empleado en España.

Como se ha descrito en el capítulo de vulnerabilidades, las transacciones en efectivo son muy comunes en España, siendo el efectivo el primer método de pago utilizado, y aunque existe una creciente generalización de otros formatos de transacciones, todavía se realiza una importante cantidad de operaciones en efectivo en las que intervienen particulares y, en menor medida, empresas.

Estas transacciones y los movimientos físicos de dinero en efectivo se han limitado en España de forma progresiva. Los movimientos de medios de pago han sido objeto de gran atención desde la perspectiva de la prevención del BC/FT, y la evidencia de la utilización de elevadas cantidades de efectivo en esquemas delictivos ha venido motivando mayores limitaciones y controles a su uso desde 2003, año en que se aprueba el régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior y sobre determinadas medidas de prevención de BC.

La necesidad de control de los movimientos de medios de pago ha sido reafirmada a nivel europeo por diferente normativa relativa a los controles de la entrada o salida de efectivo de la Unión, incrementando progresivamente las obligaciones existentes y la coordinación entre los Estados miembros. El Reglamento (UE) 2018/1672 hizo extensivas estas obligaciones al oro, tarjetas prepago y al efectivo enviado por correo o transportado como mercancía o mediante servicios de mensajería. Si el efectivo se envía por otros medios (efectivo no acompañado), las autoridades competentes estarán facultadas para pedir al expedidor o al destinatario que realicen una declaración de revelación de información y para llevar a cabo controles de cualquier envío, paquete o medio de transporte que pueda contener efectivo.

En aras de homogeneizar las declaraciones de movimientos en Europa, el Reglamento de Ejecución (UE) 2021/776 de la Comisión de 11 de mayo de 2021 estableció los modelos de determinados formularios, así como las normas técnicas para el intercambio efectivo de información en virtud del Reglamento (UE) 2018/1672 del Parlamento Europeo y del Consejo, relativo a los controles de la entrada o salida de efectivo de la Unión. Este reglamento fue complementado a nivel nacional con la Orden ETD/1217/2022, de 29 de noviembre, por la que se regulan las declaraciones de movimientos de medios de pago en el ámbito de la prevención del BC/FT.

En el ámbito nacional las personas que realicen movimientos de medios de pago tienen obligación de declaración cuando alcancen o superen los 10.000 euros al salir y entrar en España, o los 100.000 euros al desplazarse dentro del territorio nacional. En el caso de movimientos por territorio nacional o bien movimientos de entrada o salida en el territorio nacional de medios de pago acompañados, procedentes o con destino a un Estado Miembro, tales declaraciones debe formalizarse a través del modelo S1 (en caso de no ser acompañados la declaración se realiza mediante S2). En el caso de movimientos de entrada o salida en el territorio nacional de medios de pago acompañados, procedentes o con destino a un país tercero, deberá presentarse el modelo E1 (en caso de no ser acompañados la declaración se realiza mediante E2).

Las declaraciones por movimiento de medios de pago superiores a 100.000 euros dentro de España se incrementaron considerablemente en 2020 respecto años anteriores. Sin embargo, los datos de 2021 y 2022 se sitúan en cifras similares

a las existentes en prepandemia, lo que confirma que la utilización de dinero en efectivo como medio de pago legítimo es decreciente debido a las progresivas medidas de prevención y control adoptadas a nivel nacional en relación con los pagos realizados de este modo.

Por su parte, los movimientos de medios de pago en frontera experimentaron un decrecimiento en los años de pandemia, reduciéndose en un 64% en 2020 y un 57% en 2021. En 2022, esta cifra, se ha incrementado considerablemente, encontrándose el número de declaraciones en cifras similares a las de 2019, mientras que las cantidades declaradas de entrada muestran un ascenso del 143% y las de salida de un 125% respecto el año mencionado.

Por otro lado, el artículo 27.1 del Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, establece la obligación delas entidades de crédito de comunicar al Sepblac, con carácter mensual, el número y cuantía de las operaciones que lleven aparejado movimientos de efectivo por cantidades superiores a 30.000 euros sin abono o cargo en cuenta del cliente y, adicionalmente, señala que los sujetos obligados deben comunicar mensualmente las operaciones de envío de dinero.

Por otro lado, la legislación tributaria ha endurecido las posibilidades de pago en efectivo ante la estrecha vinculación del uso de efectivo con delitos de índole económica y posible utilización con fines de BC/FT. Así, el límite de pagos en efectivo se ha reducido de 2.500 a 1.000 cuando se trate de transacciones comerciales y de 15.000 a 10.000 euros cuando una de las partes sea un no residente y no actúe en calidad de empresario y profesional, lo que tiene innegables efectos en la prevención del uso de dinero en efectivo con fines de BC/FT.

Amenazas.

La relación existente entre el efectivo y algunas **amenazas** procedentes de la delincuencia organizada y la financiación del terrorismo es una evidencia, dadas las características del efectivo que favorecen el abuso de los movimientos de efectivo con fines delictivos. De esta manera, se tiene conocimiento de redes dedicadas a contrabando, tráfico de drogas, delitos contra la libertad sexual, tráfico de seres humanos, contrabando de mercancías ilegales, fraudes y estafas, etc., que ejecutan sus delitos en gran medida mediante disposiciones en efectivo, ya que es este el único medio de garantizar la imposibilidad de trazabilidad de los fondos por parte de las autoridades encargadas de la investigación y represión de estas conductas.

Vulnerabilidades y riesgos.

Los riesgos inherentes del movimiento del dinero en efectivo y su posible utilización con fines de BC/FT son muy elevados. Como ya se ha señalado al analizar sus vulnerabilidades como medio de pago, el uso habitual del efectivo en nuestro país supone un riesgo relevante de ser utilizado con fines ilegítimos. El anonimato y la falta de trazabilidad de los fondos impiden la comprobación del origen (lícito o ilícito), permiten su transmisión a terceros con fines ilícitos, su blanqueo a través de la integración de dichos fondos en el sistema financiero, la adquisición de otros bienes ilícitos o el desarrollo de actividades criminales.

Riesgos inherentes de BC. Los riesgos inherentes del uso de efectivo en BC son muy elevados (es muy frecuente el uso de billetes de 50 euros). Las restricciones, el mayor conocimiento por parte de las entidades del sistema financiero y de otros sujetos obligados del uso de efectivo con fines BC y las crecientes dificultades de ingreso de efectivo en el sistema financiero nacional vienen motivando la disminución de su uso como forma de pago. Estas medidas también contribuyen a una mayor ocultación y a la salida de grandes cantidades de efectivo hacia terceros países a través de diferentes mecanismos, generalmente usando **billetes de alta denominación**, debido a que suponen una ventaja para su almacenaje y transporte, por ocupar menos espacio y ser más fáciles de ocultar.

Este **movimiento transfronterizo** de fondos dificulta mucho a las autoridades el rastreo del producto de un delito y la identificación de evidencias de su origen ilícito y, además, permite que el proceso de blanqueo de esos fondos se realice con mayor facilidad en otro país en el que no hay evidencias o sospechas de que el efectivo sea producto de un acto ilícito.

Incluso si el efectivo se detecta en el país de destino, las implicaciones legales y prácticas pueden frustrar los esfuerzos para procesar a los delincuentes y decomisar el efectivo.

En otras ocasiones, los fondos de delitos cometidos en el exterior o cometidos en España y que fueron objeto de transporte al exterior, son objeto de entrada en nuestro país con el fin de utilizarse con apariencia de legalidad (por ejemplo, simulando ingresos por actividades comerciales).

El informe SNRA de la UE también señala el atractivo que supone el movimiento de efectivo para organizaciones delictivas con el objetivo de blanquear dinero de origen ilícito. Por lo general, estas personas llevan consigo importes más bajos que son más difíciles de detectar y pueden no estar sujetas a la obligación de declarar que afecta a las personas físicas que transportan 10.000 euros o más.

Estos riesgos de uso de efectivo con fines de BC también han sido detectados en aquellos **negocios en los que existe un mayor uso de efectivo**, ya que este tipo de entidades o profesiones pueden ser utilizadas por las redes criminales para mezclar el efectivo de origen ilícito con el de origen lícito que ingresa este tipo de negocios. Pese a las limitaciones existentes al uso de efectivo en las transacciones comerciales (1.000 euros) que se describen en este apartado y al conocimiento de las autoridades y del sector financiero de este tipo de prácticas, el riesgo de ingresar efectivo de origen ilícito en el sistema financiero a través de estos negocios sigue siendo elevado.

Riesgos inherentes de FT. Como ya se ha señalado, las especiales características del efectivo (anonimato, fácil transporte, ausencia de trazabilidad, etc.) lo convierten en un elemento fundamental en las actividades de financiación del terrorismo.

Los fondos en efectivo son utilizados para la financiación de los terroristas individuales y de grupos terroristas, sus células, sus gastos habituales de mantenimiento (alojamiento, transporte, manutención…), sus actividades (adoctrinamiento, formación propaganda, uso de redes sociales...), sus grupos de apoyo y, por supuesto, la adquisición de armamento y materiales para actividades terroristas.

Al igual que en el caso de BC, el movimiento de fondos en efectivo es de enorme relevancia, si bien su detección es todavía más compleja debido, por un lado, a que, como se ha puesto de manifiesto, las **cuantías para FT son muy inferiores a las de BC** e incluso inferiores a los límites internacionales para declarar esos movimientos (generalmente 10.000 euros) y, por otro, debido a la procedencia, en ocasiones, legítima de los fondos destinados a FT.

Igualmente, como también pone de manifiesto el SNRA de la UE, ha quedado demostrado que los grupos terroristas han hecho uso de diversas técnicas para trasladar efectivo a través de las fronteras exteriores, especialmente en el caso de las organizaciones más grandes. Esta amenaza es especialmente importante con respecto al movimiento desde la UE a terceros países. Además, se han identificado casos en los que combatientes terroristas extranjeros se han convertido en mensajeros de efectivo para financiar sus viajes y estadías en zonas de conflicto.

En lo que se refiere a aquellos **negocios en los que existe un mayor uso de efectivo**, se han detectado casos de utilización de este tipo de entidades para fines de FT, y aunque este tipo de sistemas de financiación requiere de un mayor conocimiento técnico para camuflar fondos de diferentes procedencias y de la realización de gastos de inversión iniciales, se considera que el nivel de riesgo todavía es significativo.

Riesgos residuales de BC y de FT.

El conocimiento del elevado riesgo del uso de efectivo ha llevado al establecimiento de determinadas limitaciones normativas para el control de su utilización, que son aplicadas tanto por las autoridades como por el sector privado. Entre otras medidas cabe señalar las siguientes:

- Las personas físicas tienen la obligación legal de presentar una declaración administrativa cuando realicen movimientos físicos de dinero en efectivo (u otros medios de pago), ya sea dentro del territorio nacional (100.000 euros) como cruzando las fronteras españolas (10.000 euros).

- En el periodo 2019-2022 se han recibido una media anual de 12.764 declaraciones de movimiento de efectivo en frontera (por un promedio anual de 754 millones de euros), y de 2.970 declaraciones de movimiento dentro del territorio nacional (por un promedio anual de 573 millones de euros).
- Se establece una limitación a los pagos en efectivo a partir de 1.000 euros cuando uno de los intervinientes actúa en calidad de empresario o profesional, además de los pagos o ingresos realizados en entidades de crédito y de 10.000 euros cuando una de las partes sea un no residente.
- Existe la obligación de declarar los ingresos y retiradas en entidades de crédito por importe igual o superior a 100.000 euros en efectivo (o su contravalor en moneda extranjera). En el periodo 2019-2022 se han realizado una media anual de 8.531 ingresos/retiradas de efectivo por importe igual o superior a 100.000 euros.
- Los fondos sujetos a declaración administrativa en frontera por superar los 10.000 euros y que no sean declarados, serán objeto de intervención automática. Esta labor se realiza por los funcionarios aduaneros o policiales al comprobar el cumplimiento de la obligación de declaración. En el periodo 2019-2022 se ha intervenido una media anual superior a 14 millones de euros por esta falta de declaración.
- El incumplimiento de las obligaciones legales de declaración da lugar a la incoación del correspondiente procedimiento sancionador, aplicándose las multas correspondientes. En el periodo 2019-2022 el número anual medio de sanciones impuestas por estos incumplimientos se sitúa en 367 sanciones al año.
- Los sujetos obligados deben comunicar mensualmente el número y cuantía de operaciones que lleven aparejados movimientos de efectivo superiores a 30.000 euros sin abono o cargo en la cuenta del cliente. Esta obligación afecta a los sujetos obligados que realicen operaciones de envío de dinero en efectivo por importe superior a 1.500 euros. En el periodo 2019-2022 el número anual medio se sitúa en 588.500 operaciones.

CUADRO 10. Datos sobre movimientos de efectivo

Movimientos de medios de pago por territorio nacional iguales o superiores a 100.000 €

	2018	2019	2020	2021	2022
Movimientos de medios de pago por territorio nacional (con declaración) *					
Nº operaciones	2.530	2.744	4.187	2.380	2.570
Importe total (€)	482.567.654	546.130.748	758.524.056	459.119.478	528.663.055
Actas de intervención dentro de España (sin declaración)					
Nº de intervenciones	33	27	50	41	33
Cuantías intervenidas (€)	5.175.824	7.325.673	12.909.148	10.936.880	10.499.225
Cuantías confiscadas (€) (por sanción)	3.753.554	2.854.354	1.992.823	4.455.293	3.917.089

Fuente: SEPBLAC y SGICMC

Movimientos de efectivo en frontera superiores o iguales a 10.000 €

Declaraciones por movimiento de medios de pago en efectivo en frontera por importe superior o igual a 10.000 €	**2018**	**2019**	**2020**	**2021**	**2022**
Nº operaciones de entrada	7.629	8.060	2.892	3.442	7.202
Importe total (€)	337.308.112	359.732.062	146.051.168	217.257.843	873.001.186
Nº operaciones de salida	9.274	9.945	5.228	5.636	8.649
Importe total (€)	304.678.831	310.924.046	151.995.938	257.772.104	699.665.723

Fuente: SEPBLAC

Actas de intervención en frontera por importe superior o igual a 10.000 euros (sin declaración)

	2018	2019	2020	2021	2022
Nº actas por infracción	**459**	**484**	**301**	**342**	**341**
Nº entradas	152	143	155	195	191
Nº salidas	307	341	146	147	150
Cuantías intervenidas (€)	19.256.280	23.077.088	11.897.015	7.161.058	15.255.694
Cuantías confiscadas (€) (por sanción)	9.890.480	7.536.095	5.556.782	4.703.538	3.329.212

Fuente: SEPBLAC

Conclusión.

Como se ha indicado, los movimientos de efectivo tienen unos riesgos inherentes muy **altos** para BC/ FT. No obstante, existe un alto grado de conocimiento en este ámbito que ha motivado desde hace años una profunda regulación, control y sanción en materia de prevención del BC/FT: los análisis sectoriales de riegos y los datos estadísticos recabados han permitido establecer las tipologías, puntos geográficos principales de entrada y salida del territorio nacional, perfiles (diferenciados por entradas y salidas, por puntos geográficos…), destinos preferentes, rutas seguidas, monedas más utilizadas, etc., lo que ha permitido una progresiva especialización de las autoridades aduaneras y policiales y la adopción de medidas focalizadas en los mayores riesgos detectados, así como actuaciones de control con el objeto de garantizar la adecuada tributación derivada de la titularidad y transmisión de las monedas virtuales y del origen de los fondos utilizados en la adquisición de las mismas.

La adaptación de la normativa española a la regulación europea, unida a las exigencias de declaración adicionales que se hace en nuestro país y al alto grado de cooperación nacional y control por parte de los servicios aduaneros han incidido

en una continua mitigación del nivel del riesgo de ser utilizado para operaciones de BC/FT que tienen tanto el movimiento de fondos en efectivo como los negocios con mayor uso de efectivo, habiéndose adoptado al respecto medidas de distinta naturaleza.

Movimientos de efectivo. A pesar de las numerosas medidas adoptadas y los medios empleados, el número de viajeros que se mueven por las fronteras de España es muy elevado y el volumen potencial de fondos transportados también, lo que unido a los riesgos inherentes del efectivo (anonimato, falta de trazabilidad, fácil transporte, etc.) justifican que el **riesgo residual** para **BC** y para **FT** de los movimientos de efectivo sigue siendo considerado **alto**.

Negocios con uso habitual de efectivo. Por los elementos de riesgo inherentes del efectivo ya señalados, el riesgo de ingreso de efectivo de origen ilícito en el sistema financiero a través de negocios con uso habitual de efectivo con fines de **BC** es **significativo/alto**. Sin embargo, en el caso de fines de **FT**, por las circunstancias anteriormente señaladas, este riesgo es menor que en el caso del movimiento de efectivo, pero lo suficientemente relevante para ser considerado como **significativo**.

CUADRO RIESGOS DE BC DE MOVIMIENTOS DE EFECTIVO

RIESGOS BC EN USO DE DINERO EN EFECTIVO	BAJO	MOD	SIGNIFIC	ALTO
El uso de dinero en efectivo				
Negocios con uso habitual de efectivo				

CUADRO RIESGOS DE FT DE MOVIMIENTOS DE EFECTIVO

RIESGOS FT EN USO DE DINERO EN EFECTIVO Y DE MONEDAS VIRTUALES	BAJO	MOD	SIGNIFIC	ALTO
El uso de dinero en efectivo				
Negocios con uso habitual de efectivo				

8.2. Riesgo sectores no financieros.

a) Actividades realizadas por los notarios.

Actividad, contexto y régimen normativo.

La actualización de este sector ha venido motivada la creación del Registro Central de Titularidades Reales a través del Real Decreto 609/2023, de 11 de julio, donde además se aprueba su reglamento de funcionamiento. Por otro, lado se han realizado actuaciones supervisoras que han puesto de manifiesto las amenazas y riesgos que afectan a este sector.

El notario es un funcionario público del Estado, que accede al cargo mediante oposición y cuya función es proporcionar a los ciudadanos la seguridad jurídica que establece la Constitución en el ámbito del tráfico jurídico extrajudicial. Es un profesional del Derecho que ejerce en régimen de competencia, aunque los aranceles son comunes a todos ellos. A 31 de diciembre de 2022, en España existen unos 2.691 notarios en activo, organizados en 17 colegios notariales y repartidos por todo el territorio español. Los colegios notariales les apoyan en su función y controlan su actuación. Los decanos de estos colegios integran el Consejo General del Notariado, que representa al colectivo a nivel nacional. Los notarios dependen jerárquicamente de la Dirección General de Seguridad Jurídica y Fe Pública del Ministerio de Presidencia, Justicia y relaciones con las Cortes.

La Ley 10/2010, de 28 de abril, establece que los notarios son sujetos obligados, si bien no estarán sujetos los actos notariales y registrales que carezcan de contenido económico o patrimonial o no sean relevantes a efectos de prevención del BC/FT.

En el ejercicio de sus obligaciones preventivas en materia de BC/FT, en desarrollo del artículo 27 de la Ley 10/2010, de 28 de abril, su reglamento establece en su artículo 44 la necesaria incorporación de los notarios al órgano centralizado de prevención (OCP). La creación del OCP tiene por objeto intensificar y potenciar la colaboración de los profesionales colegiados con las autoridades judiciales, policiales y administrativas, permitiendo un mayor nivel de especialización en estas tareas dentro del colectivo de sujetos obligados. Su creación persigue un objetivo doble:

- Facilitar el cumplimiento por parte cada uno de los notarios de la normativa preventiva, al contar con un órgano especializado encargado de las funciones de tipo administrativo o procedimental y que, asimismo, canaliza las comunicaciones de operativa sospechosa, mejora su calidad y las agiliza.
- Homogeneizar las medidas aplicadas por el colectivo, evitando potenciales interpretaciones divergentes sobre el alcance y significado de las obligaciones.

El Órgano Centralizado de Prevención del Blanqueo de Capitales del Consejo General del Notariado fue creado en diciembre de 2005 como consecuencia directa de la publicación de la Orden EHA/2963/2005, de 20 de septiembre. La incorporación de los notarios es, como se ha indicado anteriormente, obligatoria.

El Consejo General del Notariado dispone del Índice Único Informatizado Notarial, en el que se registran los actos notariales. El OCP del Consejo General del Notariado tiene acceso a ese registro.

Los notarios cuentan con una amplia base de datos sobre titularidades reales, a la cual se le dio acceso en 2021 a la AEAT mediante la firma de un convenio para reforzar la lucha contra el fraude fiscal.

Adicionalmente, el Real Decreto 609/2023, de 11 de julio, ha creado el Registro Central de Titularidades Reales y aprueba su reglamento de funcionamiento. Este Registro integra, entre otras fuentes, la información obrante en las bases de datos notariales.

De conformidad con lo dispuesto en la Ley 11/2023, de 8 de mayo, de digitalización de las actuaciones notariales y registrales, desde el 9 de noviembre de 2023, los notarios pueden prestar a distancia algunos servicios notariales, fundamentalmente de carácter mercantil. Entre estos actos están los actos societarios, pólizas mercantiles, diversos tipos de poderes notariales, cartas de pago, cancelación de garantías, testimonios de legitimación, los testamentos en situación de epidemia y, en algunos casos, conciliaciones y actos y negocios jurídicos, entre otros. Los tramites se realizan a través de la sede electrónica notarial, mediante videoconferencia y firma electrónica avanzada. La estimación del sector es que se podrían a llegar a autorizar y firmar por vía notarial más de 3.200.000 documentos notariales al año.

Amenazas.

El riesgo de BC en las operaciones notariales se está vinculado al hecho de que prácticamente todas las operaciones inmobiliarias y mercantiles deben ser intervenidas o autorizadas ante notario y, como en el caso de otros fedatarios públicos, de la apariencia de legalidad que otorgan las escrituras públicas a los bienes y activos incluidos en las mismas en favor de quien pretende obtener el disfrute de un bien conseguido con fondos ilícitos.

Teniendo en cuenta que el objetivo de todos los tipos de amenazas es conseguir la legitimidad formal de las operaciones conferida por las instituciones públicas, el papel de las escrituras notariales es clave dentro de este proceso de encubrimiento de la ilegitimidad.

Además, la constitución de sociedades controladas por organizaciones terroristas o con el fin de movilizar fondos cuyo objetivo último sea la financiación de estos grupos es una de las principales amenazas en el ámbito de la financiación del terrorismo.

Esto mismo se puede trasladar al BC y al abuso de organizaciones criminales del ejercicio de la función notarial con el fin de dar cumplimiento a los delitos para los que fueron constituidas.

La constitución de entramados empresariales donde la titularidad real no se puede identificar adecuadamente por la presencia de fideicomisos y testaferros en operaciones societarias o de compraventa de inmuebles son la principal amenaza para lograr combatir las actividades del crimen organizado.

Vulnerabilidades y riesgo sectorial.

Los factores que hacen vulnerable al sector notarial ante los riesgos de BC/FT vienen derivados de su propia actividad, especialmente en los siguientes actos:

- La creación de sociedades, y en particular las de responsabilidad limitada y la transmisión de sus participaciones.
- Las compraventas de propiedades inmobiliarias.

En ocasiones, en varios actos notariales ligados entre sí, pueden intervenir diferentes notarios. Este factor dificulta la visión completa de la operativa, por lo que las vulnerabilidades del sector aumentan en estos casos.

Los notarios tienen la obligación de abstención, según el artículo 19 de la Ley 10/2010, de 28 de abril, en los términos establecidos en el apartado 2 de dicho artículo *"A efectos de esta Ley se entenderá por justa causa que motive la negativa a la autorización del notario o su deber de abstención la presencia en la operación bien de varios indicadores de riesgo de los señalados por el órgano centralizado de prevención o bien de indicio manifiesto de simulación o fraude de ley. Para ello, y sin perjuicio de lo dispuesto en el artículo 24, el notario recabará del cliente los datos precisos para valorar la concurrencia de tales indicadores o circunstancias en la operación".*

El factor de riesgo endógeno de penetración dentro del sector notarial es bajo debido a la especialidad del acceso a la profesión y a las condiciones que regulan su ejercicio. Sin embargo, el factor de riesgo exógeno de abuso de los servicios notariales con estos fines es muy alto. Estos riesgos se derivan de la necesidad y capacidad de los criminales de simular ante el notario la legitimidad de las operaciones que pretenden realizar y del origen de los fondos con los que se realizan esas operaciones, con el objetivo último de conseguir la escritura notarial que otorgue una apariencia de legitimidad a esa titularidad de bienes o activos.

Este riesgo de BC/FT en las operaciones notariales puede identificarse a través de una serie de indicadores de riesgo, definidos por el OCP, que son simplemente circunstancias fácticas cuya experiencia demuestra estar asociada en la práctica, principalmente, a los sistemas de BC, como lo revelan las sentencias judiciales, el propio análisis de riesgo del OCP o las operaciones de clasificación realizadas por organismos internacionales.

De los casi 400 diferentes tipos de operaciones realizadas por los notarios, la constitución de sociedades y sus transmisiones junto con las compraventas inmobiliarias representan la mayor parte del riesgo, como hemos mencionado anteriormente. Este riesgo es bastante significativo tanto si nos referimos a las operaciones remitidas en comunicaciones por indicio por los notarios como a las operaciones analizadas y remitidas al Sepblac por el OCP del Notariado, puesto que estos actos notariales suponen 15 % de la actividad realizada por los notarios y el 51% de la operativa comunicada corresponde a esta operativa.

Junto a las dos operaciones anteriores, las tres operaciones de mayor riesgo de BC que añadidas a las dos anteriores representarían más del 70% de todas las operaciones de riesgo informadas, serían:

- Las de aumento de capital de las compañías.
- Las de préstamos / reconocimientos de la deuda.
- Los actos de protocolización.

En general, existe un grado considerable de correspondencia entre los tipos de operaciones de riesgo percibidos por los notarios y los que finalmente informa el OCP al Sepblac. Sin embargo, hay casos en que la importancia de ciertas operaciones aumenta después de los análisis efectuados por el OCP de las circunstancias percibidas por el notario. El caso más llamativo ocurre con los actos de protocolización, respecto a los cuales el OCP aprecia un nivel significativamente más alto de riesgo de blanqueo que el percibido típicamente por los notarios.

Con respecto a los indicadores de riesgo, generalmente se mantienen los mismos niveles que en las operaciones. Sin embargo, la proporción de algunos de los indicadores aumenta tras un examen específico por el OCP, como en el caso de los dos indicadores que involucran la presencia de un territorio de alto riesgo (parte que actúa y origen de los fondos). La misma situación ocurre con la presencia de individuos con respecto a los cuales hay informes de participación en actividades delictivas, como resultado de la investigación adicional que ocurre durante la fase de análisis realizada a posteriori por en el OCP.

Un análisis general de los riesgos de los tipos de operaciones e indicadores revela lo siguiente:

- La venta y compra de bienes inmuebles con mayor nivel de riesgo se produce en aquellos casos que involucran personas o fondos de territorios de alto riesgo, ya sea que se lleven a cabo entre partes entre las que exista algún tipo de vinculación, o donde se observen discrepancias significativas en el precio declarado; así como las compraventas en áreas del territorio español donde se conoce que hay una utilización intensiva de efectivo.
- Las ventas y compras de acciones con mayor nivel de riesgo son aquellas en las que el precio se considera anormalmente bajo o en aquellas que tienen lugar dentro de un grupo o secuencia de operaciones sin ninguna explicación lógica económica o comercial particular. El mayor nivel de riesgo asociado a la incorporación de empresas suele darse cuando se trata de múltiples empresas preconstituidas o, en particular, cuando el fundador las utiliza para otros fines.

- En el caso de las ampliaciones de capital, el riesgo más elevado se produce cuando se utilizan fondos o activos procedentes de territorios de alto riesgo o cuando dichos fondos o activos aportados no guardan correspondencia con las características de la empresa que aumenta su capital o son difíciles de valorar o acreditar su existencia, en particular en el caso de las aportaciones de créditos contra terceros o la propia empresa y en la aportación de acciones o participaciones de sociedades de países terceros.
- En el caso de las operaciones de financiación (préstamos y reconocimientos de deuda), el mayor nivel de riesgo se basa en la presencia de prestamistas individuales distintos de las entidades de crédito, y en casos de repetida participación del mismo prestamista (privado) o prestatario en varias operaciones en un corto período de tiempo.
- Debe subrayarse que las transmisiones de participaciones de sociedades limitadas (S.L.) realizadas en documento privado y en el extranjero quedan fuera del control de los notarios, aunque en este caso se producen actos de notarización en las delegaciones consulares correspondientes y sus riesgos están siendo objeto de mitigación mediante el convenio para su monitorización por el OCP firmado en 2020.
- También quedan fuera del control de los notarios las transmisiones de acciones de sociedades anónimas que no eleven a público su acuerdo privado.

Conclusión.

Su condición de fedatarios públicos, cuya participación es imprescindible en numerosos tipos de operaciones, motiva que los intentos de su utilización por terceros para legalizar operaciones de BC sean inevitables. Su intervención en la vida económica es muy importante, por cuanto la gran mayoría de las transacciones inmobiliarias y de las operaciones societarias requieren su intervención. El riesgo de BC/FT es superior en cierto tipo de operaciones: transmisiones de participaciones en compañías de responsabilidad limitada; ventas de propiedades inmobiliarias; operaciones de aumentos de capital de las compañías y préstamos/reconocimientos de deuda.

Los notarios han desarrollado en España un sistema de detección del BC/FT avanzado como consecuencia de la implantación del Órgano Centralizado de Prevención en el Consejo General del Notariado, que aplica herramientas muy desarrolladas, 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.

Estas herramientas tan desarrolladas y el amplio grado de conocimiento y concienciación entre los profesionales que le ha llevado a ser uno de los sectores que más operaciones por indicio comunican al Sepblac, permite minorar considerablemente el riesgo residual. Por estos motivos, y debido a la propia naturaleza de las operaciones objeto de notarización, se valora el riesgo residual de ser utilizados para operaciones de **FT** como **bajo/moderado**.

Sin embargo, este riesgo es superior en cierto tipo de operaciones: transmisiones de participaciones en compañías de responsabilidad limitada; las ventas de propiedades inmobiliarias; operaciones de aumentos de capital de las compañías y préstamos/reconocimientos de deuda. Estas operaciones son numéricamente bastante relevantes dentro de la profesión notarial lo que motiva que el riesgo residual en **BC** sea catalogado como **moderado**.

b) Actividades realizadas por registradores de la propiedad, mercantiles y de bienes muebles.

Actividad, contexto y régimen normativo.

La actualización de este sector ha venido motivada la creación del Registro Central de Titularidades Reales a través del Real Decreto 609/2023, de 11 de julio, donde además se aprueba su reglamento de funcionamiento.

Los registradores de la propiedad, mercantiles y de bienes muebles son funcionarios públicos del Estado que acceden al cargo mediante oposición y cuya función es la llevanza de los registros de la propiedad, mercantiles y de bienes muebles existentes en España. Los registradores calificarán, bajo su responsabilidad, la legalidad de los documentos de toda clase en cuya virtud se solicite la inscripción. Para que se produzca la inscripción de los documentos en los registros correspondientes es necesario que el registrador la califique favorablemente.

Según la legislación sólo tendrán acceso registral los documentos instrumentados en escritura pública o resolución judicial o administrativa, por lo que todo trámite registral implica la intervención previa de un notario, un juez o una autoridad administrativa, salvo las excepciones legalmente establecidas. Esta es la regla general en los Registros de la Propiedad y en los Registros Mercantiles, aunque también existen supuestos de documentación privada que accede al registro, si bien de forma minoritaria en los registros de la propiedad (instancia de herederos únicos, o distribución de hipotecas) o más habitualmente en los registros mercantiles (nombramiento y cese de administradores, o nombramientos de auditores). Por su parte, en los Registros de Bienes Muebles la regla general es el acceso mediante documentación privada (modelos de contratos de arrendamiento financiero aprobados).

En España hay 1.078 registradores (2022), que perciben sus honorarios según el arancel que aprueba el Ministerio de Presidencia, Justicia y relaciones con las Cortes, y que costea los gastos necesarios para el funcionamiento y conservación de los Registros. Los registradores no operan en régimen de competencia, sino por razón de circunscripción territorial, de forma que para los ciudadanos no existe libertad de elección de registro. Esta singularidad supone una garantía adicional ya que en el ejercicio de sus funciones los registradores no están sometidos al mercado, lo que opera positivamente en la prevención del BC/FT.

En el ejercicio de sus obligaciones preventivas en materia de BC/FT, como también se menciona en el análisis de los notarios, la Ley 10/2010, de 28 de abril, contempla la posibilidad de creación de órganos centralizados de prevención de las profesiones colegiadas. La creación un órgano centralizado de prevención tiene por objeto intensificar y potenciar la colaboración de los profesionales colegiados con las autoridades judiciales, policiales y administrativas, permitiendo un mayor nivel de especialización en estas tareas dentro del colectivo de sujetos obligados. Su creación persigue un objetivo doble:

- Facilitar el cumplimiento por parte de los sujetos individuales de la normativa preventiva, al contar con un órgano especializado encargado de las funciones de tipo administrativo o procedimental y que, asimismo, canaliza las comunicaciones de operativa sospechosa, mejora su calidad y las agiliza.
- Homogeneizar las medidas aplicadas por el colectivo, evitando potenciales interpretaciones divergentes sobre el alcance y significado de las obligaciones.

El órgano centralizado de prevención de los registradores, creado en 2015, se denomina Centro Registral Antiblanqueo (CRAB) y su inscripción tiene carácter obligatorio.

En 2018 por Orden Ministerial se crearon los modelos para presentación en el Registro Mercantil de las cuentas anuales de las sociedades mercantiles, estableciendo la obligatoria declaración y actualización de la titularidad real de las mismas,

la cual es objeto de inscripción en el registro de Titularidades Reales (RETIR). Este sistema incide de manera muy favorable en los sistemas nacionales de control de la titularidad real y en su grado de conocimiento por parte de las autoridades y de los sujetos obligados, en línea con las exigencias nacionales e internacionales de lucha contra el BC/FT.

El Real Decreto 609/2023, de 11 de julio, por el que se crea el Registro Central de Titularidades Reales y que aprueba su reglamento de funcionamiento establece obligaciones a los registradores de comprobación de la identidad del titular real. Por lo tanto, los registradores el ejercicio de su función registral habrán acudido a dicho registro con el fin de darle cumplimiento a esta obligación.

La obligaciones de cumplimiento de diligencia debida se ven reforzadas además por la reciente modificación de la Disposición Adicional Tercera de la Ley 10/2010, de 28 de abril, en virtud del Real Decreto-ley 5/2023, de 28 de junio, que establece que los sujetos obligados no pueden basarse únicamente en la información contenida en el RCTIR, debiendo realizar comprobaciones adicionales, salvo que se trate de relaciones de negocio o clientes sometidos a medidas simplificadas de diligencia debida, y siempre que la información obtenida sea razonablemente satisfactoria y no ofrezca motivos de sospecha.

Amenazas.

El riesgo de BC en las operaciones registrales se deriva de que prácticamente la operativa de registro que realizan estos sujetos obligados y las amenazas de la legalidad formal de los documentos otorgados por los profesionales de este sector.

El registro de operativas mercantiles donde intervienen sociedades constituidas en jurisdicciones de riesgo u off-shore que además están tituladas por fideicomisos suponen una amenaza para el sistema puesto que hay riesgos de estar de controladas por organizaciones terroristas o creadas con el fin de movilizar fondos que se orienten a financiar a dichas organizaciones.

Esto mismo se puede trasladar al BC y al abuso de organizaciones criminales del ejercicio de la función registral con el fin dar cumplimiento a los delitos para los que fueron constituidas.

La constitución de entramados empresariales donde la titularidad real no puede identificar adecuadamente por la presencia de fideicomisos son la principal amenaza para lograr combatir las actividades del crimen organizado.

Vulnerabilidades y riesgo sectorial.

La fe pública atribuida a los registradores queda bajo la salvaguarda de los tribunales, aplicándosele el principio de legitimación, por el que se presume dueño al titular del derecho inscrito frente a terceros, una situación muy codiciada por quien pretende obtener el disfrute de un bien conseguido con fondos ilícitos. El objetivo último de las actividades de BC es conseguir que los bienes y activos procedentes de actividades ilícitas encuentren la legitimidad formal conferida por las instituciones públicas, por lo que el papel de las inscripciones en los registros públicos es clave dentro de este proceso de encubrimiento del origen y búsqueda de apariencia de legitimidad.

El factor de **riesgo endógeno** de penetración dentro del sector es inexistente debido a la especialidad del régimen del acceso a la profesión y a las condiciones que regulan su ejercicio. Sin embargo, esta función de fe pública, publicidad y garantía frente a terceros incide en que el factor de **riesgo exógeno** de abuso de los servicios registrales con estos fines por parte de las organizaciones criminales sea alto.

Por tanto, los **riesgos inherentes** se derivan de las actuaciones de los criminales con objeto de aparentar legitimidad de las operaciones inmobiliarias y comerciales que se pretenden realizar y del origen de los fondos con los que se realizan esas operaciones, con el objetivo último de conseguir la inscripción registral que otorgue su validez formal ante terceros. Las principales operaciones objeto de riesgo en las operaciones registrales son similares a las señaladas en el análisis de

las actividades notariales (compraventas inmobiliarias, transmisiones de participaciones societarias, operaciones de préstamo…).

Por estos motivos, en España, como en el resto de Europa, los registradores son legalmente sujetos obligados en materia de prevención del BC/FT, pese a no ser unos de las profesiones designadas por el GAFI. Sus funciones preventivas, coordinadas a través del Centro Registral Antiblanqueo, CRAB, ocupan un lugar muy relevante dentro del esquema preventivo nacional, disminuyendo significativamente los riesgos inherentes que acompañan a las actividades registrales.

Existen, por tanto, numerosos factores de mitigación: el acceso a la profesión mediante oposición que garantiza una alta formación jurídica; el hecho de que no operen en régimen de competencia; la existencia del CRAB especializado en materia de prevención de blanqueo que coordina las políticas preventivas, la identificación de riesgos y las comunicaciones de operaciones sospechosas; y el juicio de legalidad que realizan los registradores al calificar los documentos judiciales, administrativos, notariales y privados que pretenden ser inscritos.

Conclusión.

Las funciones profesionales que tienen atribuidas, la obligación legal de registrar determinadas operaciones y la garantía jurídica que otorga el registro para operaciones tanto de carácter mercantil como inmobiliario, motivan que la participación de los registradores sea imprescindible para obtener la presunción de legalidad que el propio registro refleja, lo que inevitablemente incide en el riesgo desde un punto de vista de BC/FT.

Sin embargo, las especiales condiciones de acceso a la profesión y la estricta regulación y condiciones de su ejercicio permiten descartar riesgos intrínsecos de intentos de involucrar al sector en tramas de BC/FT. Además, son sujetos obligados que han desarrollado un órgano centralizado de prevención, el CRAB, que les permite disponer, a nivel de todo el colectivo profesional, de un sistema de prevención muy avanzado.

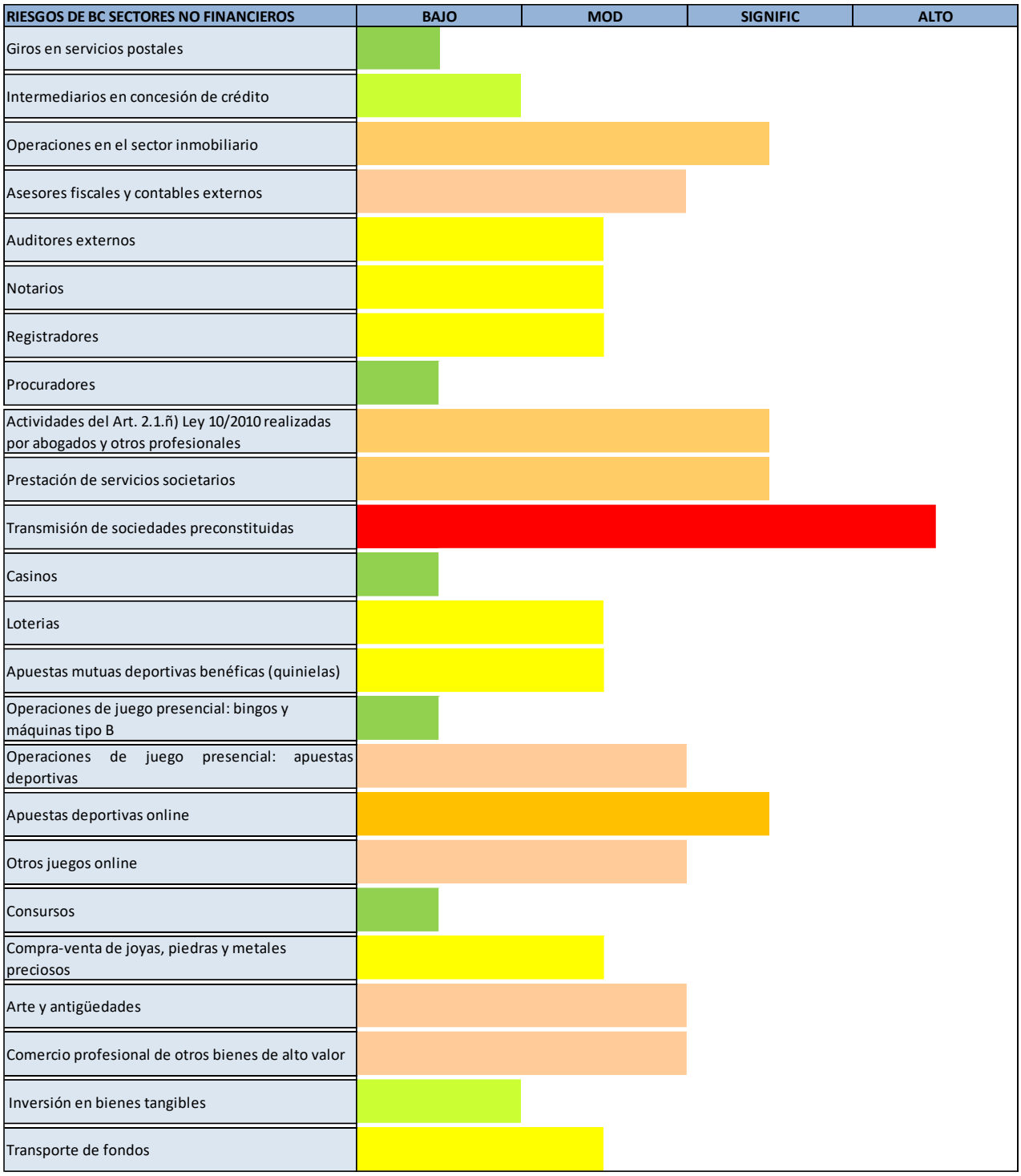
La obligación de presentación ante el Registro Mercantil de la información de titularidad real junto al depósito de cuentas anuales, y la existencia del Registro de Titularidades Reales (RETIR) cuya llevanza corresponde a los registradores mercantiles, permite disponer de los datos sobre titularidades de las sociedades de forma automatizada y con contenido estructurado, la cual es, a su vez, utilizada por autoridades públicas y por sujetos obligados. Además, el Real Decreto 609/2023, de 11 de julio, por el que se crea el Registro Central de Titularidades Reales y que aprueba su reglamento de funcionamiento establece obligaciones a los registradores de comprobación de la identidad del titular real. Esta normativa refuerza el cumplimiento de las medidas de diligencia debida de este sector.

Finalmente, la obligación de registro de todas las personas físicas o jurídicas que de forma empresarial o profesional presten servicios calificados como de servicios a sociedades (o servicios societarios prestados por terceros), deben realizar la inscripción en el Registro Mercantil competente por razón de su domicilio, practicándose conforme al Reglamento del Registro Mercantil.

Riesgos FT. La intervención de los registradores en determinadas operaciones y ciertos tipos de negocios susceptibles de ser utilizados para actividades de FT inciden en el riesgo de FT. No obstante, los tipos de operaciones que deben elevarse a registro no se corresponden actualmente con la operativa de riesgo de FT existente en nuestro país, por lo que, con carácter general, se considera que el nivel de riesgo residual tiene un nivel **bajo/moderado**.

Riesgos BC. El riesgo es superior para operaciones de BC debido a determinados tipos de operaciones de riesgo: las ventas de propiedades inmobiliarias, los préstamos/ reconocimientos de deuda y las operaciones societarias de diversa naturaleza, tales como los aumentos de capital y la transmisión de participaciones (acto que no se inscribe en los Registros mercantiles desde 1.995, teniendo su único reflejo en los libros privados de registro de acciones y participaciones que llevan las empresas y con acceso restringido a los socios). Todas ellas son operaciones habituales en el ejercicio de la profesión que motivan que el riesgo residual de su utilización sea catalogado como **moderado**.

CUADRO RIESGOS DE BC EN SECTORES NO FINANCIEROS[34]



[34] El cuadro contiene toda la información de todos los sectores analizados en el ANR de 2020 y no solo los modificados en esta adenda.

CUADRO RIESGOS DE BC EN SECTORES NO FINANCIEROS[35]

RIESGOS DE FT SECTORES NO FINANCIEROS BC	BAJO	MOD	SIGNIFIC	ALTO
Giros en servicios postales				
Intermediarios en concesión de crédito				
Operaciones en el sector inmobiliario				
Asesores fiscales y contables externos				
Auditores externos				
Notarios				
Registradores				
Procuradores				
Actividades del Art. 2.1.ñ) Ley 10/2010 realizadas por abogados y otros profesionales				
Prestación de servicios societarios				
Transmisión de sociedades preconstituidas				
Casinos				
Loterias				
Apuestas mutuas deportivas benéficas (quinielas)				
Operaciones de juego presencial: bingos y máquinas tipo B				
Operaciones de juego presencial: apuestas deportivas				
Apuestas deportivas online				
Otros juegos online				
Consursos				
Compra-venta de joyas, piedras y metales preciosos				
Arte y antigüedades				
Comercio profesional de otros bienes de alto valor				
Inversión en bienes tangibles				
Transporte de fondos				

[35] El cuadro contiene toda la información de todos los sectores analizados en el ANR de 2020 y no solo los modificados en esta adenda.

9. RIESGOS DE NO IMPLEMENTACIÓN O EVASIÓN DE LAS SANCIONES FINANCIERAS INTERNACIONALES.

Las Recomendaciones del GAFI exigen a los países implementar regímenes de sanciones financieras para cumplir con las Resoluciones del Consejo de Seguridad de Naciones Unidas (en adelante, CSNU) relativas a la prevención y represión del terrorismo y el financiamiento del terrorismo, y a la prevención, represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento (R.6, R.7, RI.10 y RI.11). Asimismo, los países deben identificar, evaluar y entender los riesgos de financiamiento del terrorismo y financiamiento de la proliferación, entendidos estos últimos como cualquier posible incumplimiento, la falta de implementación o la evasión de las sanciones financieras en materia de no proliferación.

En línea con los estándares del GAFI, en el presente capítulo se analizan los riesgos de vulneración de las sanciones financieras internacionales impuestas en virtud de Resoluciones del CSNU. Asimismo, se analizarán las sanciones en el marco de la Unión Europea (UE).

9.1. Concepto de sanciones financieras internacionales.

Las *sanciones internacionales* son medidas coercitivas que no implican el uso de la fuerza armada y que puede adoptar el CSNU en virtud del Capítulo VII de la Carta de Naciones Unidas, con la intención de influir sobre las acciones o las políticas de los Estados o de otros sujetos de la comunidad internacional a fin de mantener o restablecer la paz y la seguridad internacionales. Las sanciones internacionales pueden revestir una tipología muy variada, desde la interrupción total o parcial de las relaciones económicas y de las comunicaciones, hasta la ruptura de relaciones diplomáticas.

Por otra parte, la UE puede adoptar *medidas restrictivas* (sanciones), bien sobre una base autónoma o en ejecución de las Resoluciones del CSNU. Estas medidas deben ser coherentes con la realización de los objetivos de la Política Exterior y de Seguridad Común (PESC), tal y como se establece en el artículo 21 del Tratado de la Unión Europea (TUE). A nivel de la UE cabe hablar, por tanto, de tres tipologías de regímenes de sanciones, en función del organismo del que emanan y de su alcance:

- Los *regímenes de sanciones de las NN.UU.*, cuya transposición al ordenamiento comunitario se realiza mediante la adopción de reglamentos europeos, vinculantes y directamente aplicables en todos los Estados Miembros.
- Los *regímenes mixtos* de sanciones, en los cuales la UE decide reforzar las sanciones de las NN.UU. aplicando medidas adicionales a las impuestas por el CSNU.
- Los *regímenes autónomos* de la UE, en aquellos casos en que la propia UE decida adoptar medidas restrictivas por propia iniciativa.

Así las cosas, a los efectos del presente análisis constituyen ***sanciones financieras internacionales*** aquellas medidas coercitivas de naturaleza financiera que adoptan el CSNU y la UE a fin de prevenir y reprimir el terrorismo y el financiamiento del terrorismo, y de prevenir, reprimir e interrumpir la proliferación de armas de destrucción masiva y su financiamiento. Las sanciones financieras internacionales conllevan la obligación para todas las personas físicas o jurídicas (con independencia de que sean sujetos obligados de la Ley 10/2010, de 28 de abril) de inmovilizar (congelar) todos los fondos, otros activos financieros y recursos económicos cuya propiedad, tenencia o control corresponda, directa o indirectamente, a personas físicas o jurídicas, entidades, organismos o grupos incluidos en las listas consolidadas sanciones del CSNU y de la UE. Asimismo, conllevan la prohibición de poner a disposición directa o indirecta de los sujetos sancionados, o de utilizar en su beneficio, cualquier tipo de fondos, otros activos financieros o recursos económicos.

Se entenderá por '*fondos, otros activos financieros y recursos económicos*' los bienes de cualquier tipo, tangibles o intangibles, muebles o inmuebles, y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos bienes, incluidos créditos bancarios, cheques de viaje, cheques bancarios, giros, acciones, títulos, obligaciones, letras de cambio y cartas de crédito, entre otros.

Se entenderá por '*congelación de fondos, otros activos financieros y recursos económicos*' el hecho de impedir cualquier movimiento, transferencia, alteración, utilización o transacción que pudiera dar lugar a un cambio del volumen, importe, localización, propiedad, posesión, naturaleza o destino de esos fondos, otros activos financieros y recursos económicos.

El incumplimiento de la obligación de inmovilización o de la prohibición de puesta a disposición de fondos, otros activos financieros y recursos económicos de personas o entidades designadas supone la comisión de una infracción administrativa por parte de aquellas personas físicas o jurídicas que están obligadas a hacerlo.

9.2. Sanciones financieras internacionales relacionadas con el terrorismo y la financiación del terrorismo.

El CSNU ha adoptado sucesivas Resoluciones por las que se imponen medidas coercitivas que incluyen la obligación para todas las personas físicas y jurídicas, de naturaleza financiera o no financiera, de los Estados de la comunidad internacional, de congelar los fondos y demás activos financieros o recursos económicos de las personas y entidades que sean incluidas en las listas aprobadas en esas Resoluciones:

- Por sus vínculos o pertenencia a grupos terroristas internacionales (Resoluciones CSNU 1267 (1999), 1988 (2011), 1989 (2011), 2253 (2015), 2610 (2021) y sucesivas).
- A solicitud de un país tercero formulada con base en sus propias listas domésticas de personas/entidades vinculadas con el terrorismo (Resolución CSNU 1373 (2001)).

Dichas Resoluciones del CSNU han sido incorporadas al ordenamiento comunitario a través de los siguientes actos de la Unión (y sus sucesivas modificaciones y actualizaciones).

En España, la aplicación de las sanciones financieras internacionales se encuentra regulada por la propia Ley 10/2010, de 28 de abril, (artículo 42), por su Reglamento (artículos 47 y 48), y por el Real Decreto 413/2015, de 29 de mayo, por el que se aprueba el Reglamento de la Comisión de Vigilancia de Actividades de Financiación del Terrorismo.

Además, conforme a la regulación vigente, el Consejo de Ministros podrá acordar la aplicación de contramedidas financieras respecto de países terceros que supongan riesgos más elevados de blanqueo de capitales, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva (artículo 42.2 de la Ley 10/2010, de 28 de abril).

9.3. Sanciones financieras internacionales relacionadas con la proliferación de Armas de Destrucción Masiva (ADM).

La proliferación de armas de destrucción masiva (ADM), ya sean nucleares, químicas, radiológicas o biológicas, además de sus medios de dispersión, suponen una grave amenaza para la paz y seguridad internacionales y afectan directamente a la Seguridad Nacional. Los programas de producción de ADM pueden realizarlos los Estados, pero también actores no estatales.

Las capacidades de los Estados para realizar actividades o programas de proliferación son diferentes de las de los actores no estatales, incluidas sus capacidades de financiación y del grado de accesibilidad a infraestructuras y a entidades nacionales para la materialización de esos programas.

En el caso de los actores estatales debe destacarse además que, por lo general, comportan el riesgo de un comportamiento similar por parte de aquellos países con los que se mantenga algún tipo de enfrentamiento o conflicto, que procederán a aumentar sus actividades de producción y comercialización de ADM. Este riesgo de escalada armamentística se define como "proliferación".

Existen varios tratados internacionales vigentes relacionados con la No Proliferación a los que España se ha adherido.

Uno de los principales desafíos es el control de material de doble uso, para evitar que productos y tecnología que tienen usos tanto civiles como militares puedan ser empleados con fines ilícitos. El Tratado sobre la no proliferación de las armas nucleares y el sistema de salvaguardias del Organismo Internacional de la Energía Atómica han contribuido a frenar y, en algunos casos, a invertir la propagación de la capacidad militar nuclear, pero no han podido impedirla por completo.

En 2004 el CSNU aprobó la Resolución 1540 que prohíbe a los Estados miembros suministrar cualquier tipo de apoyo a los agentes no estatales que traten de adquirir, fabricar, poseer, transportar, transferir o emplear ADM y sus vectores. Pero también el CSNU amplió esa prohibición identificando países concretos.

La posibilidad de que sustancias químicas tóxicas puedan ser empleadas contra personas es de especial preocupación. No sólo por incurrir en la violación del Derecho Internacional Humanitario por el uso de armas químicas contra civiles en conflicto, además, existe el riesgo que grupos terroristas puedan utilizar las armas químicas fuera de zonas de conflicto para realizar actos terroristas.

Las sanciones financieras internacionales aprobadas por el CSNU dirigidas a la prevención, supresión y disrupción de ADM están expresamente relacionadas con las actividades de la República Popular Democrática de Corea e Irán, si bien en el caso de Irán ha de señalarse que el 18 de octubre de 2023 se levantaron todas las sanciones impuestas por el CSNU en virtud de la resolución 2231 (2015).

En el marco de la UE, en 2003 se aprobó la Estrategia de la UE contra la proliferación de armas de destrucción masiva y, desde entonces, se vienen adoptando una serie de Decisiones (PESC) de actualización y seguimiento (años 2006, 2008, 2013 y 2017). La última es la Decisión (PESC) 2023/654 del Consejo, de 20 de marzo de 2023, de apoyo a la aplicación de la Resolución 1540 (2004) del Consejo de Seguridad de las Naciones Unidas sobre la no proliferación de las armas de destrucción masiva y sus sistemas vectores. Dicha Estrategia está concebida para prevenir, disuadir, detener y, si es posible, eliminar los programas de armas de destrucción masiva (ADM) en todo el mundo y tiene como puntos clave:

- *Multilateralismo*: Reforzar los mecanismos internacionales de no proliferación y trabajar para mejorar los sistemas de verificación de las violaciones de las normas dispuestas en los tratados multilaterales.
- *Prevención*: Fomentar un entorno estable a escala regional e internacional, a través del refuerzo de programas que promuevan el desarme y de la incorporación del objetivo de no proliferación a todas las actividades políticas, diplomáticas y económicas de la UE.
- *Cooperación internacional*: Trabajar en estrecha colaboración con socios clave como los Estados Unidos, la OTAN y asistir a terceros países.

España viene señalando la proliferación de ADM como un riesgo para la seguridad del país y así se recoge en la Estrategia de Seguridad Nacional, que ha sido objeto de actualización en 2022. Además, la agresión de Rusia a Ucrania ha elevado el riesgo de financiación de la proliferación por parte de Rusia, tal y como ha recogido la declaración pública de GAFI.

Además de la aplicación de las sanciones financieras internacionales ya referidas anteriormente para los casos de inclusión en listas internacionales de terrorismo, que se enumeran en la Ley 10/2010, de 28 de abril, y en su Reglamento, y que afectan a las listas relacionadas con proliferación de ADM, se cuenta con una regulación específica del comercio exterior de material de defensa y de doble uso, concretamente, el Real Decreto 679/2014, de 1 de agosto, aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.

El sistema punitivo y sancionador se articula a través de dos normas:

A. El Código Penal, (Ley Orgánica 10/1995, de 23 de noviembre), que en sus artículos 566 a 568 del Capítulo V "De la tenencia, tráfico y depósito de armas, municiones o explosivos" tipifica el tráfico de armas dentro de los delitos contra el orden público, sancionando aquellas conductas que supongan un atentado grave contra la paz y la tranquilidad públicas.
B. La Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando, que:
    - Sanciona como delito (o infracción administrativa) la exportación importación, introducción, expedición o realización de cualquier otra operación sujeta al control sin autorización, o habiéndola obtenido fraudulentamente, de material de defensa o de doble uso.
    - Tipifica como delito la realización de dichas conductas cuando su objeto sean drogas tóxicas, estupefacientes, sustancias psicotrópicas, armas, explosivos, agentes biológicos o toxinas, sustancias químicas tóxicas y sus precursores, o cualesquiera otros bienes cuya tenencia constituya delito, o cuando el contrabando se realice a través de una organización, con independencia del valor de los bienes, mercancías o géneros.

9.4. Vulnerabilidades y riesgo sectorial.

Existe un alto nivel de conocimiento por las entidades, especialmente las financieras, de sus obligaciones en este campo. No obstante, debido al contexto de internacionalización y creciente interrelación financiera entre los países siempre hay riesgo de incurrir en operaciones relacionadas con algún régimen de sanciones del CSNU o que estén vinculadas a la proliferación de AMD.

A. Sanciones financieras internacionales relacionadas con el terrorismo y la financiación del terrorismo.

En España no han existido casos de detección de personas o entidades incluidas en listas de la UE o de Naciones Unidas (Resolución CSNU 1267 y posteriores) ni de personas o entidades incluidas en listas de otros países (Resolución CSNU 1373) que fuesen clientes o interviniesen en operaciones con personas físicas o jurídicas españolas. Sin embargo, teniendo en cuenta los factores de vulnerabilidad derivados del volumen de operaciones internacionales, su posible complejidad y el alto número de clientes intervinientes, se considera que existe un **riesgo inherente** de carácter moderado de operar con este tipo de clientes, principalmente vinculados a las entidades del sector financiero con mayor presencia y desarrollo de actividades en el ámbito internacional.

Adicionalmente, desde GAFI se ha puesto de manifiesto la existencia de demoras en la aplicación de la Resoluciones del CSNU motivadas por los retrasos en la publicación de los Reglamentos por la UE, ya que son esos Reglamentos los que confieren obligatoriedad jurídica a las Resoluciones del CSNU, lo que también señalan podría incidir en un mayor riesgo de incumplimiento y de evasión de las sanciones financieras. Con el fin de mitigar esta vulnerabilidad derivada de los plazos, existen proyectos para modificar próximamente la regulación específica en esta materia al objeto de adecuarse a las Resoluciones del CSNU.

No obstante, los sujetos obligados, especialmente los del sector financiero, tienen un alto grado de conocimiento de sus obligaciones de proceder a las oportunas congelaciones de fondos y recursos económicos de las personas y entidades listadas por el CSNU y realizar las notificaciones oportunas en su caso. Este conocimiento es especialmente relevante en el sector de entidades de crédito, que serían los sujetos de mayo riesgo en materia de sanciones financieras internacionales, debido a su mayor presencia internacional y diversidad de clientes, habiendo establecidos sistemas internos para efectuar las comprobaciones y un seguimiento continuo de las listas internacionales emitidas por el CSNU.

Por otra parte, las autoridades supervisoras realizan un seguimiento para comprobar si las entidades financieras y los sujetos obligados no financieros cumplen sus obligaciones legales. Además, el Sepblac ha publicado una *Guía de Buenas Prácticas para la Aplicación de listas de personas y entidades sujetas a sanciones y contramedidas financieras internacionales*[36], con el fin de orientar a todos aquellos obligados al cumplimiento de tales deberes.

B. Sanciones financieras internacionales relacionadas con la proliferación de ADM.

Existen en nuestro país una serie de factores de riesgo que deben ser tenidos en cuenta:

- La relevante producción española de equipamientos industriales y de tecnología.
- Las exportaciones de material de defensa y doble uso. En el año 2022 el valor de las exportaciones realizadas de material de defensa totalizó 4.091,3 millones de euros, con un incremento del 24,3% con respecto al año anterior. El 47,8% de las mismas se realizó a países de la UE/OTAN, Por su parte, las exportaciones de doble uso en 2022 tuvieron un valor de 289 millones de euros (principalmente a Singapur Noruega) frente a 232 millones de euros en el año anterior[37].
- El alto volumen de actividad comercial, principalmente a través del tráfico marítimo y los puertos nacionales.
- La creciente deslocalización de industrias vinculadas con tecnologías sensibles en países en desarrollo que pueden ser empleados para realizar operaciones indirectas a través de nuestro país.

Por otro lado, cabe resaltar que en el caso de España:

- Nuestro país no se constituye como un centro de servicios financieros internacionales de referencia.
- La República Popular Democrática de Corea ha clausurado su embajada en España.
- La Junta Interministerial de Comercio Exterior de Material de Defensa y Doble Uso, JIMDDU, compuesta por representantes de las instituciones públicas competentes en el control del comercio internacional de este tipo de materiales, mantiene reuniones de carácter mensual con el fin de comprobar y autorizar las importaciones y exportaciones de material de defensa y doble uso. Además, el Sepblac se ha incorporado a los trabajos preparatorios de la JIMDDU, fortaleciéndose así el sistema.

Estos factores pueden implicar la existencia de **riesgos inherentes** de realización de actividades dirigidas a camuflar operaciones de proliferación ADM con materiales producidos en España, sin necesidad de que haya una relación directa entre la entidad que realiza una transacción u operación comercial y el país o la persona/entidad que se encuentra listada. Es importante tener en cuenta que los puntos intermediarios no siempre están situados en

[36] https://www.sepblac.es/wp-content/uploads/2018/03/aplicacion_de_listas_de_personas_y_entidades_sujetas_a_sanciones_y_contramedidas_financieras_internacionales.pdf.

[37] "Estadísticas españolas de exportación de material de defensa, de otro material y de productos y tecnologías de doble uso, año 2022". Ministerio de Industria, Comercio y Turismo.

jurisdicciones de alto riesgo ya que, en ocasiones, se utilizan países que tradicionalmente han sido de menos riesgo para dar mayor legitimidad a la operación y, de esta manera, quedar sometidos a un escrutinio menos exhaustivo. Este tipo de operaciones pueden ser dirigidas a países intermediarios mediante triangulación de las exportaciones desde nuestro país por los denominados "proliferadores", que suponen la amenaza en esta materia, y son los encargados de realizar la adquisición del material y la transacción comercial de su envío al destino final.

Todo ello determina que el riesgo inherente de que se produzcan en España actividades relacionadas con la proliferación de ADM debe considerarse moderado.

Sin embargo, este riesgo inherente se ve disminuido por la aprobación de un régimen específico a nivel nacional dirigido a su mitigación que incluye regulación, procedimientos de autorización por parte de organismos interdepartamentales que realizan reuniones periódicas y tienen competencias tasadas con el fin de coordinar tanto las autorizaciones como los sistemas de control de estas operaciones, lo que lleva a calificar este riesgo residual como bajo/moderado.

9.5. Conclusiones.

A. Sanciones financieras internacionales relacionadas con el terrorismo y la financiación del terrorismo.

Pese a que el riesgo inherente de que las entidades financieras sean utilizadas con fines de vulnerar las sanciones financieras internacionales establecidas por el CSNU y por la UE en materia de terrorismo es considerado como de grado medio, las medidas normativas existentes, las obligaciones preventivas establecidas para el sector, los controles administrativos, el conocimiento que tiene el sector de sus deberes y la inexistencia de casos en España, motivan que **el riesgo residual** sea considerado, en general, como bajo. No obstante, en función del tipo y tamaño de entidad, su volumen de transacciones, tipos de operaciones desarrolladas, número de clientes procedentes o que tengan negocios con determinados países de riesgo inciden en una mayor cualificación del riesgo. Por lo tanto, aquellas entidades financieras con una mayor presencia en esos países o que desarrollen actividad con los nacionales o entidades de esos países de riesgo deben ser consideradas como de riesgo moderado, por lo que se considera que el riesgo residual en el sector es **bajo/moderado**, dependiendo del tipo de entidad financiera.

Por su parte, en el caso del **sector no financiero**, las entidades de mayor tamaño utilizan buenas herramientas de detección de persona y entidades listadas, y aunque las entidades de menor tamaño no disponen de sistemas de detección tan avanzados, son conocedoras de la obligación de verificar la inclusión en las listas y actuar en consecuencia. En cualquier caso, debido a la naturaleza de la actividad que desarrollan el nivel de riesgo es muy escaso, sin que hayan detectado casos en nuestro país, por lo que el riesgo residual debe considerarse **bajo.**

B. Sanciones financieras internacionales relacionadas con la proliferación de ADM.

El volumen de operaciones comerciales relacionadas con material de defensa y de doble uso pueden implicar la existencia de vulnerabilidades para la evasión del régimen de sanciones. Sin embargo, pese a que el riesgo inherente de que las entidades financieras sean utilizadas con fines de vulnerar las sanciones financieras internacionales establecidas por el CSNU en materia de proliferación de ADM es considerado como moderado, la ausencia de relaciones financieras y comerciales con estos países unido a las medidas normativas existentes, las obligaciones para el sector, los controles administrativos y la coordinación nacional motivan que el riesgo residual de evadir las sanciones por proliferación de AMD, sea considerado, en general, como **bajo**. No obstante, al igual que en el caso de las

sanciones financieras por inclusión en listas internacionales de terrorismo, el tipo de entidad, su volumen de transacciones, los tipos de operaciones desarrolladas, el número de clientes que tengan negocios o los vínculos con esos países incidirán en una mayor cualificación del riesgo. Por lo tanto, aquellas **entidades financieras** con una mayor presencia en esos países o con actividad con los nacionales o entidades de esos países de riesgo, deben ser consideradas como de riesgo moderado, por lo que se considera que el riesgo residual en el sector es **bajo/moderado**, dependiendo del tipo de entidad.

Por su parte, en el caso de las **entidades del sector no financiero** debido a la presencia inexistente de actividad con estos países el riesgo debe considerarse **bajo.**

10. MEDIDAS ADOPTADAS.

10.1. Medidas adoptadas de carácter general.

Estrategia de Seguridad Nacional.

La ***"Estrategia de Seguridad Nacional"*** aprobada en 2017, que actualizaba la anterior Estrategia del año 2013, identificaba quince ámbitos de actuación, entre los que en el ANR de 2020 se mencionaron cinco, de los cuales se exponen las principales realizaciones conseguidas:

- La seguridad económica y financiera. Ampliación del número de países y jurisdicciones con los que se realiza el intercambio automático de información financiera, refuerzo de la resiliencia de los bancos y aumento de estabilidad financiera de la Eurozona como consecuencia de las normas emitidas para la reducción de riesgos y la protección de los depósitos dentro de la Unión Bancaria, la mejora de la coordinación de la supervisión macroprudencial a nivel nacional[38] y el Plan de Recuperación, Transformación y Resiliencia que traza una hoja de ruta para la recuperación del crecimiento económico, la modernización de la economía y la creación de empleo, para la reconstrucción económica sólida, inclusiva y resiliente tras la crisis de la COVID-19.
- La lucha contra el crimen organizado. Refuerzo de la formación especializada en distintos aspectos de la lucha contra el terrorismo y el crimen organizado, incluyendo la investigación, la inteligencia estratégica y la actuación, dirigida a las FCSE, Fuerzas Armadas, AEAT y el Sepblac; incremento en el intercambio de información sobre el tráfico de drogas y el crimen organizado; potenciación de la coordinación internacional en la lucha contra el crimen organizado; impulso de la generación de la inteligencia operacional y estratégica que se elabora a nivel nacional y especialmente en el marco de los planes de respuesta especial como el desarrollado en el Campo de Gibraltar; en el primer trimestre del 2020, se aprobaron los Planes anuales de inspección de precursores de drogas y de explosivos, claves para evitar el desvío de estas sustancias hacia la fabricación ilícita de drogas y explosivos y para comprobar el cumplimiento de la normativa nacional y comunitaria.
- La lucha contra el terrorismo. En el ámbito preventivo, España mantiene su presencia en varias misiones, así como en el incremento de cooperación haciendo uso de la inteligencia financiera; en el de la protección se ha incrementado la coordinación entre las diferentes unidades de inteligencia y se han elaborado planes de contingencia; en el ámbito de la persecución, siguen existiendo numerosas operaciones policiales que culminan en sentencias y detenciones.
- La ciberseguridad: desarrollo de nuevas herramientas con el objetivo de reforzar las capacidades; aprobación de Guía Nacional de Notificación y Gestión de Ciberincidentes; desde el CNI se puso en marcha un plan de sensibilización, vigilancia y protección de las redes informáticas de los organismos nacionales dedicados a la investigación científica del sector sanitario y de biotecnología; diversas operaciones y misiones realizadas por los FCSE; celebración del Foro Nacional de Ciberseguridad que tiene como objetivo aumentar la cooperación público privada; aprobación Plan de Lucha contra la Cibercriminalidad.
- La no proliferación de armas de destrucción masiva. España ha mantenido su participación en los principales regímenes de control de exportaciones; actuaciones de coordinación con autoridades aduaneras de la UE con el fin de prevenir movimientos ilícitos de productos y tecnología de doble uso; colaboración con la Asociación Internacional contra la Impunidad para el Uso de Armas Químicas, que se crea con el objetivo de aumentar el intercambio de información sobre los ataques con armas químicas e identifica públicamente a personas y entidades sancionadas por su participación en el uso de estas armas.

[38] Real Decreto 102/2019, de 1 de marzo, por el que se crea la Autoridad Macroprudencial Consejo de Estabilidad Financiera, se establece su régimen jurídico y se desarrollan determinados aspectos relativos a las herramientas macroprudenciales.

Hay que tener en cuenta que debido al impacto de la pandemia de la COVID-19 y el incremento en el empleo de estrategias híbridas se consideró necesario una revisión estratégica que permitiese enfrentar los riesgos y las amenazas en un renovado contexto de globalización, condicionado por una mayor incertidumbre y un cambio acelerado.

La actual Estrategia de Seguridad Nacional 2021 tiene un marco de actuación de 3 años. En su capítulo 3 se enumeran 16 riesgos y amenazas que vulneran la Seguridad Nacional, entre los cuales destacan:

- Terrorismo y radicalización violenta.
- Amenazas a las infraestructuras críticas.
- Vulnerabilidad del ciberespacio.
- Inestabilidad económica y financiera.
- Crimen organizado y delincuencia grave.
- Proliferación de armas de destrucción masiva.

Estrategia Nacional Contra el Crimen Organizado y la Delincuencia Grave.

Una de las prioridades de la Estrategia es la lucha contra la trata de seres humanos, con una línea de acción específica dedicada a establecer un Plan Estratégico específico nacional contra la trata y la explotación de seres humanos (PENTRA).

De acuerdo con lo previsto en la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023, se ha continuado impulsando la generación de la inteligencia operacional y estratégica que se elabora a nivel nacional y especialmente en el marco de los planes de respuesta especial como el desarrollado en el Campo de Gibraltar o las órdenes de servicio y planes de actuación sobre actividades como el fraude contra la hacienda pública y la seguridad social o la trata de seres humanos.

Por primera vez, EUROPOL ha difundido, de manera diferenciada, el Informe Europeo de Evaluación de la Amenaza al Crimen Organizado (SOCTA), haciendo una evaluación exhaustiva de las amenazas que suponen los delitos financieros y económicos en el ámbito de la UE, con el fin de, por un lado, reflejar la omnipresencia y el carácter destructivo de los delitos financieros y económicos que afectan a los países de nuestro entorno y, por otro, ayudar a todas las partes interesadas a desentrañar la gran variedad de delitos financieros y económicos. En concreto, en el citado informe analiza todos los delitos financieros y económicos que afectan a la UE, como el BC, la corrupción, el fraude, los delitos contra la propiedad intelectual y falsificación de mercancías y divisas.

Estrategia Nacional Contra el Terrorismo.

El Comité Especializado Contra el Terrorismo (CECT) creó el Grupo I de Trabajo de Seguimiento y Evaluación de la Estrategia Nacional Contra el Terrorismo (ENCOT), el cual, en su Informe de Evaluación de la ENCOT (IEE) de 2020, señaló 30 medidas prioritarias para luchar contra el terrorismo.

En el periodo comprendido entre 2020-2023 se han llevado a cabo diversas acciones, muchas de las cuales están recogidas dentro del marco del Plan Estratégico Nacional contra la Financiación del Terrorismo (PENCFIT) y del Plan Estratégico Nacional de Prevención y Lucha Contra la Radicalización Violenta (PENCRAV). Estos planes fueron aprobados por el Consejo de Seguridad Nacional en su reunión del 6 de octubre de 2020.

En el punto 4.6 se ha desarrollado algunos de las realizaciones del PENCFIT y del PENCRAV.

10.2. Otras medidas de mitigación de carácter específico.

Ampliación de los sujetos obligados: prestadores de servicios de activos virtuales y otros.

El Real Decreto-ley 7/2021, de 27 de abril, estableció que aquellas personas que desarrollasen actividades de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos, deberán estar inscritas en un registro constituido en el Banco de España. Esta modificación normativa, que afectó a la Ley 10/2010, de 28 de abril, permitió incluir a los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos como sujetos obligados.

Esta adaptación normativa facilitó acercar a nuestra legislación preventiva al cumplimiento de los estándares internacionales de GAFI y adoptar lo establecido en la Directiva UE 2018/843 sobre la incorporación de los prestadores de servicios de cambio de moneda virtual por moneda de curso legal o entre monedas diferentes monedas virtuales y aquellos que ofrecen servicio de custodia de monederos electrónicos en la Ley 10/2010, de 28 de abril.

Además, se introdujo una disposición adicional segunda que obliga a los PSCA a su inscripción en un registro especial en el Banco de España. Para conseguir la inscripción, dichas entidades deben acreditar la existencia de procedimientos y órganos adecuados de prevención del BC/FT. La existencia de tales procedimientos la revisa el Servicio Ejecutivo de la Comisión, que debe emitir un informe al respecto para su incorporación en el expediente administrativo de registro que se sigue en el Banco de España.

El Real Decreto 7/2021, de 27 de abril, incluye como sujetos obligados:

- Entidades aseguradoras autorizadas que operen con inversiones y no sólo en el ramo de vida.
- Entidades de dinero electrónico y las de pago se les añaden las personas físicas y jurídicas referidas en los artículos 14 y 15 del Real Decreto Ley 19/2018, de 23 de noviembre.
- Las personas que desarrollen profesionalmente alguna actividad prevista en el artículo 6.1 de la Ley 5/2015, de 27 de abril, o que desarrollen actividades de concesión de préstamos previstas en la Ley 5/2019, de 15 de marzo.
- Quienes se dediquen profesionalmente a actividades de arrendamiento de bienes inmuebles que implique una transacción por una renta total anual, igual o superior a 120.000 euros o mensual igual o superior a 10.000 euros.
- Los auditores de cuentas, contables externos, asesores fiscales y cualquier otra persona que se comprometa a prestar de manera directa o a través de otras personas relacionadas, ayuda material, asistencia o asesoramiento en cuestiones fiscales como actividad empresarial o profesional principal.
- Se agregan los intermediarios en el comercio de objetos de arte o antigüedades, así como las personas que almacenen o comercien con objetos de arte o antigüedades o actúen como intermediarios en el comercio de objetos de arte o antigüedades cuando lo lleven a cabo en puertos francos.

Reforzamiento de los sistemas de control transfronterizo de los movimientos de efectivo y medios de pago.

El Reglamento de Ejecución (UE) 2021/776 de la Comisión de 11 de mayo de 2021 estableció los modelos de determinados formularios, así como las normas técnicas para el intercambio efectivo de información en virtud del Reglamento (UE) 2018/1672 del Parlamento Europeo y del Consejo, relativo a los controles de la entrada o salida de efectivo de la Unión. Este reglamento fue complementado con la Orden ETD/1217/2022, de 29 de noviembre, por la que se regulan las declaraciones de movimientos de medios de pago en el ámbito de la prevención del BC/FT.

En el caso de España, existe la obligación de declarar los movimientos de medios de pago de carácter intracomunitario por encima de 10.000 euros y los movimientos dentro del territorio nacional a partir de un umbral de 100.000 euros.

En este sentido, se modificaron los **modelos de declaración** de movimiento de medios de pago para ampliar y precisar la información relacionada con estos movimientos.

La modificación normativa de 2022 afectó al régimen de declaración de movimientos de medios de pago establecido en el artículo 34 de la Ley 10/2010, de 28 de abril. Las novedades más importantes fueron las siguientes:

- La obligación de declaración a la entrada y salida del territorio español impuesta a las personas físicas que viajen con medios de pago por importe igual o superior a los 10.000 euros se extendió a los movimientos de medios de pago realizados sin acompañamiento de persona física, tales como envíos postales, envíos por mensajería, equipaje no acompañado o carga en contenedores.
- Se añadió que, a los efectos de la ley, se consideran medios de pago las materias primas utilizadas como depósitos de valor de gran liquidez, como el oro.

Creación de Registro Central de Titularidad Real e interconexión con registros UE y mayor transparencia e información sobre los prestadores de servicios a sociedades y fideicomisos tipo trust.

El Registro Central de Titularidades Reales (RCTIR) se puso en marcha el 19 de septiembre de 2023. Es un registro central único en todo el territorio nacional, gestionado por el Ministerio de Presidencia, Justicia y relaciones con las Cortes, y que tiene su sede en la Dirección General de Seguridad Jurídica y Fe Pública, que es el órgano encargado de su gestión y responsable del mismo.

El RCTIR tiene por objeto recoger y dar publicidad a la información sobre titularidad real vigente relativa a todas las personas jurídicas españolas y los fideicomisos tipo trust y entidades o estructuras sin personalidad jurídica análogas que operan en España. El RCTIR cuenta con datos de carácter histórico existentes sobre las personas jurídicas españolas y los fideicomisos tipo trust y entidades o estructuras sin personalidad jurídica análogas que operan en España, que serán accesibles por las autoridades. La finalidad es lograr una mayor transparencia en la utilización de sociedades y otras entidades jurídicas, fideicomisos del tipo «trust» e instrumentos jurídicos análogos, que permita defender la integridad del sistema financiero.

El RCTIR obtendrá su información en relación con personas jurídicas españolas a partir de fuentes oficiales, como el Colegio de Registradores de la Propiedad, Mercantiles y Bienes Muebles de España (a través de los Registros Mercantiles) o el Consejo General del Notariado, e incluirá además el registro de fideicomisos tipo trust y otros instrumentos jurídicos análogos a los trust que operan en España mediante la declaración directa por el fiduciario, permitiendo la consulta de la titularidad real de todos ellos.

Novedades en la consulta y activos declarables en el Fichero de Titularidades Financieras.

La Ley orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales transpone la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, regula el acceso FTF.

Su finalidad es mejorar el enjuiciamiento de los delitos financieros, luchar contra el BC/FT, así como prevenir los delitos fiscales. La modificación normativa busca favorecer el intercambio de información en la lucha contra el BC/FT y permite el acceso al FTF a autoridades que estén cursando investigaciones tengan como objeto la prevención, detección, investigación y enjuiciamiento de infracciones penales graves.

Además, se destaca la supresión de la previa autorización judicial o del Ministerio Fiscal para que las FCSE accedan al FTF. La información que se comparte contiene los datos identificativos de los titulares de las cuentas, pero no incluye información acerca de saldos ni movimientos. Es decir, se permite acceder a la identificación del producto financiero,

de la entidad de crédito y de los titulares y autorizados de la cuenta o producto. Sin embargo, en el caso de requerir un acceso más allá de estos datos, sí será necesaria previa autorización judicial o del Ministerio Fiscal.

Además, otras modificaciones vinieron a ampliar la información contenida en el FTF. Concretamente, la disposición final primera de la Ley Orgánica 9/2022, de 28 de julio, modificó el artículo 43 de la Ley 10/2010, de 28 de abril, de prevención del BC/FT, introduciendo, entre otros, los siguientes cambios:

- La obligación de declarar al FTF, que hasta entonces se limitaba a las entidades de crédito, se extendió a las entidades de pago y a las entidades de dinero electrónico.
- También se extendió el listado de los tipos de productos cuya declaración al Fichero de Titularidades Financiera es obligatoria, añadiendo a ese listado cualquier tipo de cuenta de pago y los contratos de alquiler de cajas de seguridad.
- En cuanto al contenido de las declaraciones, pasó a ser preceptiva la declaración de los titulares reales de los productos.

Incremento de la cooperación nacional.

La Ley 18/2022, de 28 de septiembre, mediante su Disposición Adicional Segunda, modificó la Ley 10/2010, de 28 de abril, de prevención del BC/FT.

Entre las novedades introducidas por esa modificación, hay dos que impulsan la mitigación del riesgo:

- El añadido de un artículo 32 ter, que posibilita que los sujetos obligados pertenecientes a una misma categoría de las establecidas en el artículo 2 de la ley podrán crear sistemas comunes de información, almacenamiento y, en su caso, acceso a la información y documentación recopilada para el cumplimiento de las obligaciones de diligencia.
- El añadido del artículo 33, referido a los ficheros centralizados de prevención del fraude, para el intercambio de información entre sujetos obligados.

Adicionalmente, se han renovado los Convenios de supervisión con los supervisores prudenciales (Banco de España, CNMV y Dirección General de Seguros y Fondos de Pensiones), reforzando la cooperación existente en materia de supervisión de BC/FT.

Cambio en el sistema de valoración de las comunicaciones por indicio.

Entre las funciones del Servicio Ejecutivo de la Comisión se encuentra la valoración de calidad de las comunicaciones recibidas de los sujetos obligados. Recientemente, se introdujeron cambios en el sistema de valoración, introduciéndose nuevos elementos en la valoración para la mejora de dichas valoraciones, como el factor relevancia, referido a la cuantificación de varios factores: la gravedad de las posibles actividades delictivas subyacentes a las operaciones comunicadas, el importe total de las operaciones comunicadas, la profundidad del análisis integral o la novedad de las tipologías informadas.

Medidas supervisoras.

Junto con las investigaciones realizadas por los FCSE, las supervisiones realizadas a los sujetos obligados son unas de las principales medidas adaptadas por las autoridades para la mitigación de riesgos. En los últimos años, el Sepblac, en su faceta de autoridad supervisora, ha realizado determinadas inspecciones dirigidas a sujetos obligados de

sectores concretos que, por sus características, presentan riesgo de BC/FT. Entre ellas se encuentran inspecciones sectoriales, temáticas, peticiones de información estructurada a sujetos obligados y consideración de los factores de riesgos identificados en el ANR de 2020 para evaluar los riesgos de los sujetos obligados.

Medidas en materia de sanciones financieras.

Desde la aprobación del Análisis Nacional de Riesgos del año 2020, se han llevado a cabo una serie de medidas con la finalidad de mejorar la implementación de sanciones financieras internacionales.

A nivel operativo, se ha creado el Grupo de Trabajo de Seguimiento de Ejecución de Sanciones y el Grupo Ad Hoc Activos Inmovilizados y Retenidos. Ambos grupos están formados por representantes de departamentos con competencias en la implementación de sanciones internacionales. El primer grupo tiene un carácter más estratégico, formado por representantes de los departamentos directivos competentes, enfocado en la coordinación de la actividad de todos ellos en cada uno de sus campos. Por otro lado, el Grupo Ad Hoc de Activos Inmovilizados y Retenidos tiene un carácter mucho más operativo, dedicado al intercambio de información, detección y congelación de activos.

En materia de difusión y concienciación, en la Subdirección General de Inspección y Control de Movimientos de Capitales se ha creado el correo institucional sancionesfinancieras@economia.gob.es como canal de consulta hacia el sector público como privado, con carácter general. Esto ha permitido aumentar el alcance de la difusión de todas las actualizaciones y novedades en materia de sanciones internacionales, así como la aclaración de dudas y consultas de carácter técnico sobre su implementación. Desde modo, se ha pasado de 4 consultas recibidas en materia de sanciones financieras internacionales en el año 2021 a las 220 del año 2022.

Además, se ha procedido a la actualización de toda la documentación disponible en la página web de la Dirección General del Tesoro y Política Financiera en esta materia, que incluye nuevas guías y orientaciones en materia de implementación de sanciones financieras internacionales, un nuevo documento para la solicitud de descongelación de fondos, enlaces a preguntas frecuentes respondidas por la Comisión Europea y un nuevo canal de *whistleblowing*.

11. CONCLUSIONES.

Desde la aprobación del pasado ANR, el sistema preventivo español se ha enfrentado a novedades y cambios, tanto exógenos como endógenos que **hacían necesaria la actualización de los riesgos identificados en 2020.**

Entre estos hitos podemos destacar la adaptación de la V Directiva relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo a la regulación española de prevención de BC/FT que ha fortalecido el sistema preventivo español con medidas tales como la incorporación de nuevos sujetos obligados, el reforzamiento del sistema de identificación de los titulares reales de las personas jurídicas o la modificación de los activos sometidos a declaración y la ampliación del número de entidades declarantes.

Del mismo modo, la pandemia COVID-19 conllevó nuevos retos para el sistema preventivo español, especialmente vinculados a las actividades delictivas que aprovecharon las debilidades que surgieron por la acelerada necesidad de digitalización de la economía y sociedad española.

Asimismo, la actividad transfronteriza en Europa ha visto incrementado su riesgo con la guerra entre Rusia y Ucrania en lo relativo a los movimientos de efectivo de la población migrante, el desvío de las armas utilizadas en el conflicto a fines delictivos, el comercio de material de defensa y doble uso o la utilización de canales clandestinos para los flujos monetarios con el fin de evadir sanciones.

Las **amenazas** de BC identificadas en España fruto de la cooperación nacional entre autoridades están en línea con las expuestas en la anterior versión del ANR: crimen organizado, tráfico de drogas y delitos económicos y financieros asociados a fraude y corrupción. A pesar de que los grupos de crimen organizado con actividad en España han disminuido, la interconexión entre diferentes organizaciones internacionales ha crecido, de la misma manera que lo ha hecho la combinación de diferentes delitos subyacentes asociado a fraudes, tráfico de drogas o trata de seres humanos.

Los fraudes en los que se hace uso de operativa digital son los que representan la mayor amenaza en la actualidad, donde la figura del denominado “mulero” y la creación de cuentas mulas para la movilización de flujos monetarios, dificultan el objetivo de lograr la trazabilidad de los fondos y la identificación del infractor real.

En cuanto al tráfico de drogas, a pesar de que las sustancias que tienen una mayor presencia son el hachís y la cocaína, es preocupante la configuración de España como primer productor de cánnabis en la UE, así como la alerta sobre la circulación y consumo entre la población española de una serie de drogas que se encuentran fuera de los convenios de fiscalización internacional, denominadas *Nuevas Sustancias de Síntesis*.

Por otro lado, el terrorismo yihadista se sigue configurando como la tipología de mayor amenaza global. La financiación a través de pequeñas células o individuos radicales que hacen uso de la fragmentación de los fondos y criptoactivos que dificultan la transparencia y trazabilidad es un hecho.

Las **vulnerabilidades** detectadas en España que fomentan los riesgos asociados a estas amenazas se configuran como factores asociados a la población y al número de inmigrantes; a factores geográficos derivados de la determinación de áreas nacionales con una mayor exposición a riesgos de BC; al elevado uso de efectivo; o al incremento de la presencia de innovaciones tecnológicas en la economía española.

En relación con los **sectores evaluados** en esta actualización caben destacar que, aunque no han experimentado un cambio en sus riesgos residuales, con excepción de la ejecución de operaciones de pago (otros servicios de entidades de pago), determinadas circunstancias como modificaciones normativas, actuaciones supervisoras o cambios en características específicas han impulsado un análisis de los riesgos que les afectan.

Finalmente, se ha realizado una evaluación de las medidas mitigadoras propuestas en el anterior ANR que se han visto adoptadas a la fecha. Con carácter general, factores asociados a la lucha contra el crimen organizado, la

ciberseguridad, la no proliferación o lucha contra el terrorismo se han visto alcanzado. En este último punto, resultan especialmente relevantes, las acciones realizadas en el marco del ENCOT y sus planes estratégicos (PENCFIT y PENCRAV). Con carácter específico, adquiere importancia las medidas implantadas a raíz la trasposición a la normativa nacional de la V Directiva (creación del Registro Titularidades Reales, incorporación sujetos obligados...), así como una mayor vigilancia en las declaraciones de los movimientos transfronterizos de fondos y las actuaciones supervisoras realizadas.

A pesar de lo conseguido, hay que tener en cuenta que, en la actualidad, el sistema preventivo español se enfrenta continuamente a nuevos retos que surgen a raíz de nuevas operativas detectadas, nuevos agentes que interactúan o necesidades identificadas. Por ello, el seguimiento continuado en la ejecución de las acciones planteadas dentro de las estrategias nacionales que configuran las medidas mitigadoras de carácter general es un elemento crucial. En un ámbito más específico, se han establecido medidas que aborden carencias observadas en el plano legislativo, supervisor, de investigación o de persecución judicial.

12. ESTADÍSTICAS.

Véase la publicación de la Memoria de Información Estadística 2018-2022 y su Anexo.

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

Abreviaturas utilizadas

AEAT. Agencia Estatal de Administración Tributaria.

AEB. Asociación Española de Banca.

AEF. Asociación Española de Fundaciones.

AECID. Agencia Española de Cooperación Internacional para el Desarrollo.

AEJPR. Asociación Española de Joyeros, Plateros y Relojeros,

AENPA. Asociación Española de Entidades de Pago.

ANR. Análisis Nacional de Riesgos.

ASNEF. Asociación Nacional de Establecimientos Financieros de Crédito.

BC. Blanqueo de capitales.

BC/FT. Blanqueo de Capitales y Financiación del Terrorismo.

BCE. Banco Central Europeo.

CA. Criptoactivos.

CECA. Confederación Española de Cajas de Ahorros.

CECT. Comité Especializado contra la lucha del Terrorismo.

CGI. Comisaría General de Información. Policía Nacional.

CGPJ. Comisaría General de la Policía Judicial. Policía Nacional.

CGPJ. Consejo General del Poder Judicial.

CITCO. Centro de Inteligencia contra el Terrorismo y el Crimen Organizado.

CNI. Centro Nacional de Inteligencia.

CNMV. Comisión nacional del Mercado de Valores.

CRAB. Centro Registral Antiblanqueo.

DGSFP. Dirección General de Seguros y Fondos de Pensiones.

EAF. Empresas de Asesoramiento Financiero.

EBA. Autoridad Bancaria Europea.

EDE. Entidades de Dinero Electrónico.

EFC. Establecimientos Financieros de Crédito.

ENCOyDG. Estrategia Nacional contra el Crimen Organizado y Delincuencia Grave.

ENCOT. Estrategia Nacional Contra el Terrorismo.

FGE. Fiscalía General del Estado.

FT. Financiación del terrorismo.

FTF. Fichero de Titularidades Financieras.

GAFI. Grupo de Acción Financiera Internacional.

GOIF. Grupo Operativo de Inteligencia Financiera.

GRUSEFIT. Grupo III de Trabajo y Seguimiento del Plan Estratégico Nacional de Lucha Contra la Financiación del Terrorismo

ICAC. Instituto de Contabilidad y Auditoría de Cuentas.

ICO. Initial Coin Offering. Oferta inicial de monedas (criptoactivos).

IIC. Instituciones de Inversión Colectiva.

JI. Jefatura de Información de la Guardia Civil.

OCP. Órgano Centralizado de Prevención.

ONGD. Organizaciones No Gubernamentales de Desarrollo.

OSFL. Organizaciones Sin Fines de Lucro.

PFP. Plataformas de Financiación Participativa.

PELCEIL- Plan Estratégico de lucha contra el Enriquecimiento Ilícito de las organizaciones criminales y los delincuentes.

PENCFIT. Plan Estratégico Nacional de Lucha Contra la Financiación del Terrorismo.

PENCRAV. Plan Estratégico Nacional de Prevención y Lucha contra la Radicalización Violenta.

PEP- PRP. Personas de Responsabilidad Pública.

PSCA. Proveedores de Servicios de Criptoactivos

RECTIR. Registro de Titularidad Real.

SAREB. Sociedad de Gestión de Activos Procedentes de la Reestructuración Bancaria.

SEPBLAC. Servicio Ejecutivo de Prevención del Blanqueo de Capitales.

SGR. Sociedades de Garantía Recíproca.

SGIIC. Sociedades Gestoras de Instituciones de Inversión Colectiva.

SICAV. Sociedades de Inversión Colectiva en Activos Variables.

SNCE. Sistema Nacional de Compensación Electrónica.

SNRA. (UE) Supra-National Risk Assessment. Análisis Supranacional de Riesgos de la UE.

SOCIMI. Sociedades Cotizadas de Inversión en el Mercado Inmobiliario.

SVA. Servicio de Vigilancia Aduanera.

UCO. Unidad Central Operativa de la Guardia Civil.

UDEF. Unidad Central de Delincuencia Económica y Fiscal. Policía Nacional.

UIF. Unidad de Inteligencia Financiera.

UNACC. Unión Nacional de Cooperativas de Crédito.

UNODC. Oficina de Naciones Unidas contra las Drogas y el Crimen.

UNSCR. Resoluciones del Consejo de Seguridad de Naciones Unidas.

UTPJ. Unidad Técnica de la Policía Judicial de la Guardia Civil.

Lista de principales disposiciones normativas

- Ley 19/2003, de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior.
- Ley 4/2010, de 10 de marzo, para la ejecución en la UE de resoluciones judiciales de decomiso.
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la UE.
- Ley 13/2011, de 27 de mayo, de regulación del juego.
- Real Decreto-ley 11/2018, de 31 de agosto, de transposición de directivas en materia de protección de los compromisos por pensiones con los trabajadores, prevención del BC y requisitos de entrada y residencia de nacionales de países terceros.
- Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del BC, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores.
- Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas.
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
- Real Decreto-ley 5/2023, de 28 de junio, por el que se adoptan y prorrogan determinadas medidas de respuesta a las consecuencias económicas y sociales de la Guerra de Ucrania, de apoyo a la reconstrucción de la isla de La Palma y a otras situaciones de vulnerabilidad; de transposición de Directivas de la Unión Europea en materia de modificaciones estructurales de sociedades mercantiles y conciliación de la vida familiar y la vida profesional de los progenitores y los cuidadores; y de ejecución y cumplimiento del Derecho de la Unión Europea.
- Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Real Decreto 413/2015, de 29 de mayo, por el que se aprueba el Reglamento de la Comisión de Vigilancia de Actividades de Financiación del Terrorismo.
- Real Decreto 948/2015, de 23 de octubre, regula la Oficina de Recuperación y Gestión de Activos.
- Real Decreto 609/2023, de 11 de julio, por el que se crea el Registro Central de Titularidades Reales y se aprueba su Reglamento.
- Orden ECO/2652/2002, de 24 de octubre, y Orden EHA/1464/2010, de 28 de mayo, por la que se desarrollan las obligaciones de comunicación de operaciones en relación con determinados países al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.
- Orden EHA/2963/2005, de 20 de septiembre, reguladora del Órgano Centralizado de Prevención en materia de blanqueo de capitales en el Consejo General del Notariado.
- Orden EHA/1439/2006, de 3 de mayo, reguladora de la declaración de movimientos de medios de pago en el ámbito de la prevención del blanqueo de capitales.
- Orden EHA/2619/2006, de 28 de julio, por la que se desarrollan determinadas obligaciones de prevención del blanqueo de capitales de los sujetos obligados que realicen actividad de cambio de moneda o gestión de transferencias con el exterior.
- Orden EHA/2444/2007, de 31 de julio, en relación con el informe de experto externo sobre los procedimientos y órganos de control interno y comunicación establecidos para prevenir el blanqueo de capitales.
- Orden EHA/114/2008, de 29 de enero, reguladora del cumplimiento de determinadas obligaciones de los notarios en el ámbito de la prevención del blanqueo de capitales.

- Orden ECC/2503/2014, de 29 de diciembre, por la que se crea el fichero de datos de carácter personal denominado «Fichero de Titularidades Financieras» (FTF).
- Orden ECC/2402/2015, de 11 de noviembre, por la que se crea el Órgano Centralizado de Prevención del blanqueo de capitales y de la financiación del terrorismo del Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles.
- Orden ETD/1217/2022, de 29 de noviembre, por la que se regulan las declaraciones de movimientos de medios de pago en el ámbito de la prevención del blanqueo de capitales y de la financiación del terrorismo.