



EVALUACIÓN NACIONAL DE RIESGOS **FINANCIAMIENTO DE LA PROLIFERACIÓN** 2016-2021



MILAFT

Mesa Intersectorial sobre Prevención
y Combate al Lavado de Activos y
al Financiamiento del Terrorismo





EVALUACIÓN NACIONAL DE RIESGOS FINANCIAMIENTO DE LA PROLIFERACIÓN 2016-2021

MILAFT

Mesa Intersectorial sobre Prevención
y Combate al Lavado de Activos y
al Financiamiento del Terrorismo



CONTENIDOS

04	INTRODUCCIÓN
08	CAPÍTULO I: MARCO CONCEPTUAL Y METODOLOGÍA EVALUACIÓN NACIONAL DE RIESGOS DE FINANCIAMIENTO DE LA PROLIFERACIÓN
08	Marco conceptual de la proliferación de armas de destrucción masiva y su financiamiento
12	Metodología de trabajo
16	CAPÍTULO II: ESTÁNDARES INTERNACIONALES, CONTEXTO DE LA PROLIFERACIÓN Y SU FINANCIAMIENTO EN CHILE
16	Estándares internacionales sobre FP
17	Marco regulatorio nacional e implementación de las resoluciones del CSNU
19	Funcionamiento del Sistema Nacional ALA/CFT con respecto al financiamiento de la proliferación
25	CAPÍTULO III: DIAGNÓSTICO DEL FENÓMENO DE FINANCIAMIENTO DE LA PROLIFERACIÓN EN CHILE
25	Estrategia Nacional para Prevenir y Combatir el LA/FT y Plan de Acción 2018-2020
26	Resultados de la Evaluación Mutua de Chile por parte del Gafilat
28	Análisis de los Reportes del Grupo de Expertos que apoya al Comité de Sanciones 1718 y menciona a Chile en materia de financiamiento de la proliferación
31	CAPÍTULO IV: AMENAZAS DEL FINANCIAMIENTO DE LA PROLIFERACIÓN
41	CAPÍTULO V: IDENTIFICACIÓN DE VULNERABILIDADES RELACIONADAS CON EL FINANCIAMIENTO DE LA PROLIFERACIÓN
41	1. Vulnerabilidades asociadas con la comprensión del riesgo de FP
42	2. Vulnerabilidades asociadas con la implementación de las SFD de FP
43	3. Vulnerabilidades asociadas con la infraestructura TI, ciberseguridad y actividades de comercio exterior
46	4. Vulnerabilidades asociadas con los nuevos productos y servicios de pago
49	CAPÍTULO VI: IDENTIFICACIÓN DE MITIGANTES RELACIONADOS CON EL FINANCIAMIENTO DE LA PROLIFERACIÓN
49	1. Monitoreo de las SFD por parte del sector financiero
49	2. Supervisión del cumplimiento de las medidas relativas a las SFD por parte de las entidades reportantes
50	3. Inexistencia de relaciones diplomáticas entre la RPDC y Chile
52	CAPÍTULO VII: EVALUACIÓN DE LOS RIESGOS DEL FINANCIAMIENTO DE LA PROLIFERACIÓN PARA CHILE
54	ANEXOS
54	ANEXO 1: Otras Convenciones, Tratados o Acuerdos en los que Chile participa relacionados con las ADM.
55	ANEXO 2: Tabla con decretos del Minrel que han dispuesto el cumplimiento de las Resoluciones del CSNU en materia de FP.
57	BIBLIOGRAFÍA
59	NOTAS AL PIE



INTRODUCCIÓN

INTRODUCCIÓN

La resolución 1540 sobre la no proliferación de armas de destrucción masiva del Consejo de Seguridad de las Naciones Unidas (CSNU), del 28 de abril de 2004, establece las obligaciones para todos los Estados Miembros de desarrollar y hacer cumplir las medidas legales y reglamentarias apropiadas contra la proliferación de armas químicas, biológicas, radiológicas y nucleares, y sus sistemas vectores, en particular, para prevenir la difusión de armas de destrucción masiva a actores no estatales.

Esta resolución establece que todos los Estados deben abstenerse de suministrar cualquier tipo de apoyo a los agentes no estatales que traten de desarrollar, adquirir, fabricar, poseer, transportar, transferir o emplear armas nucleares, químicas o biológicas y sus sistemas vectores, en particular con fines terroristas. La resolución obliga a todos los Estados a adoptar y aplicar leyes eficaces con ese fin, así como también otras medidas eficaces para prevenir la proliferación de estas armas y sus sistemas vectores a agentes no estatales, en particular con fines terroristas.

Las armas de destrucción masiva y sus sistemas vectores constituyen una preocupación constante para la comunidad internacional, debido a las consecuencias catastróficas que su uso ha tenido. En este sentido, el Grupo de Acción Financiera Internacional (GAFI) recomienda a los países dar pasos apropiados para identificar, evaluar y entender los riesgos de lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva (LA/FT/FP), de manera continua, así como para gestionar y mitigar los riesgos identificados (Recomendación N°1).

En 2012, el GAFI incorporó la Recomendación N°7, que llama a los países a implementar regímenes de sanciones financieras dirigidas para cumplir con las Resoluciones del CSNU relativas a la prevención y represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento (FP).

Dichas Resoluciones exigen a los países que congelen sin demora los fondos u otros activos de, y que aseguren que ningún fondo u otro activo se ponga a disposición, directa o indirectamente, de o para el beneficio de, alguna persona o entidad designada por o bajo la autoridad del CSNU dentro del Capítulo VII de la Carta de las Naciones Unidas, para evitar que los fondos/activos queden a disposición de quienes cometan o intenten financiar la proliferación.

Desde el año 2020, el GAFI ha ampliado su enfoque a la necesidad de que los países comprendan de forma integral estas amenazas, con el propósito de desarrollar políticas públicas, e implementen las medidas pertinentes para su combate tanto en el sector privado como público.

Desde el año 2013, el país cuenta con una Estrategia Nacional Prevenir y Combatir el LA/FT, cuyos planes de acción (2014-2017 y 2018-2020) han sido desarrollados e implementados por una veintena de organismos públicos coordinados por la UAF, con el apoyo de la Mesa Intersectorial sobre Prevención y Combate al LA/FT (MILAFT).

La MILAFT es una Comisión de carácter permanente, que tiene como misión asesorar al Presidente(a) de la República en la coordinación de las acciones, planes y programas de los distintos actores institucionales en materia de prevención, detección y persecución del LA/FT.

Creada a través del Decreto N° 1.724, de 2016, del Ministerio de Hacienda, la Mesa debe, además, hacer seguimiento al avance de los objetivos planteados en la Estrategia Nacional.

Sus 15 miembros permanentes son:

- Ministerio del Interior y Seguridad Pública
- Ministerio de Relaciones Exteriores
- Ministerio de Hacienda
- Ministerio Secretaría General de la Presidencia
- Carabineros de Chile (a través del Departamento O.S.7 de Drogas, Departamento O.S.9 de Investigación de Organizaciones Criminales y la Dirección de Inteligencia (Dipolcar))
- Comisión para el Mercado Financiero
- Dirección General del Territorio Marítimo y Marina Mercante de la Armada de Chile
- Policía de Investigaciones (a través de las brigadas investigadoras del lavado de activos (Brilac) y del crimen organizado (Brico))
- Servicio de Impuestos Internos
- Servicio Nacional de Aduanas
- Servicio Nacional para la Prevención y la Rehabilitación del Consumo de Drogas y Alcohol
- Superintendencia de Casinos de Juego
- Superintendencia de Pensiones
- Superintendencia de Seguridad Social
- Unidad de Análisis Financiero (actúa como Secretaría Técnica).

Destacar que, en 2023, la MILAFT invitó a participar en sus mesas técnicas de trabajo a:

- Agencia Nacional de Inteligencia
- Banco Central de Chile
- Consejo de Defensa del Estado
- Contraloría General de la República
- Dirección del Crédito Prendario
- Gendarmería de Chile
- Instituto de Salud Pública
- Ministerio Público
- Servicio Agrícola y Ganadero
- Servicio de Registro Civil e Identificación
- Ministerio de Economía, Fomento y Turismo
- Ministerio de Justicia y Derechos Humanos
- Poder Judicial (Corte Suprema)
- Tesorería General de la República

En línea con los estándares internacionales, en marzo de 2017, Chile, a través de la Unidad de Análisis Financiero (UAF), en su calidad de coordinador del Sistema Nacional Antilavado de

Activos y contra el Financiamiento del Terrorismo (ALA/CFT), presentó a la comunidad la Evaluación Nacional de Riesgos de Lavado de Activos y Financiamiento del Terrorismo (ENR-LA/FT).

El documento tuvo por objetivo analizar las amenazas y vulnerabilidades económicas y legales que tiene el país frente al LA/FT, y su consiguiente impacto, de manera que las autoridades puedan diseñar medidas y políticas esenciales para combatirlos, y ejercer una priorización y asignación de recursos eficiente.

Sin embargo, dada las actualizaciones del estándar internacional en materia de proliferación de armas de destrucción masiva y su financiamiento, la amenaza que conlleva y la visión estratégica que se necesita para enfrentar el fenómeno, durante el año 2023, las instituciones miembros de la Estrategia Nacional para Prevenir y Combatir el LA/FT, coordinadas por la UAF, con el apoyo de la MILAFT, trabajaron en una actualización de la ENR, separándola en tres volúmenes: ENR de lavado de activos (ENR-LA), ENR de financiamiento del terrorismo (ENR-FT) y ENR de financiamiento de la proliferación (ENR-FP).

Lo anterior, amplía el perímetro de acción del Sistema Nacional ALA/CFT al incluir los riesgos del país al FP y la necesidad de implementar medidas para prevenirlos y mitigarlos.

Así, la presente ENR-FP actúa como una aproximación al fenómeno de la proliferación y su financiamiento en relación con Chile. Este documento propone generar y ampliar el conocimiento del FP en el Sistema Nacional ALA/CFT, toda vez que aborda los conceptos clave asociados e identifica posibles amenazas, vulnerabilidades y mitigantes, posicionándose como la primera ENR-FP.

Para evaluar los riesgos de Chile al FP se analizaron las amenazas, vulnerabilidades y mitigantes del periodo 2016-2021, tomando como base la metodología implementada en el año 2017, pero ajustada a las más recientes

recomendaciones del GAFI. Es así como se han considerado las directrices incluidas en la **“Guía para la evaluación de riesgo de financiamiento de la proliferación”**, de junio de 2021, en la cual el GAFI plantea los siguientes objetivos y alcances (GAFI, 2021, pág. 7).

- a.** Proporcionar orientación para ayudar a los sectores público y privado a aplicar los nuevos requisitos para identificar, evaluar y comprender su riesgo de FP.
- b.** Proporcionar orientación para ayudar a los sectores público y privado a aplicar el requisito de mitigar los riesgos de FP que identifiquen.
- c.** Proporcionar orientación adicional a los supervisores/organismos autorreguladores (SRB) sobre la supervisión o el seguimiento de la evaluación y mitigación del riesgo de FP.

A objeto de dar a conocer la evaluación de los riesgos de FP que tiene el país, el presente documento se divide en siete apartados: El primero detalla la metodología utilizada para la elaboración de la ENR y entrega los conceptos involucrados en esta materia; el segundo, contextualiza el fenómeno de la proliferación y su financiamiento en Chile, considerando el funcionamiento del Sistema Nacional ALA/CFT y el marco normativo legal existente, además de los estándares internacionales en esta materia; y el tercer apartado realiza un diagnóstico del FP en el país. Mientras, en el cuarto, quinto y sexto apartados se abordan las amenazas, vulnerabilidades y mitigantes identificadas en el país. Y, por último, en el séptimo se desprende el riesgo y conclusiones relacionadas con el fenómeno del FP en Chile.

En línea con las ENR-LA y ENR-FT este instrumento está sujeto a una revisión y actualización continua. Esto, en la medida que se identifiquen y evalúen nuevas amenazas y vulnerabilidades, de acuerdo con la evolución del contexto nacional e internacional, así como también, situaciones o acciones que actúen como mitigantes.



CAPÍTULO I:
MARCO CONCEPTUAL Y METODOLOGÍA
EVALUACIÓN NACIONAL DE RIESGOS
DEL FINANCIAMIENTO DE LA
PROLIFERACIÓN

CAPÍTULO I: MARCO CONCEPTUAL Y METODOLOGÍA EVALUACIÓN NACIONAL DE RIESGOS DEL FINANCIAMIENTO DE LA PROLIFERACIÓN

MARCO CONCEPTUAL DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA Y SU FINANCIAMIENTO

En este apartado se identifican los principales conceptos asociados al fenómeno de la proliferación y su financiamiento.

ARMAS DE DESTRUCCIÓN MASIVA, SISTEMAS VECTORES Y MATERIALES CONEXOS

La Comisión sobre Armamentos Convencionales de las Naciones Unidas entregó, en agosto de 1948, la primera definición formal aplicable para el concepto de **Armas de Destrucción Masiva (ADM)**: “Armas atómicas explosivas, armas de material radioactivo, armas químicas y biológicas letales, y cualquier arma desarrollada en el futuro que tenga características comparables, en términos destructivos, a las armas atómicas u otras mencionadas con anterioridad”¹.

En términos generales, según expresa la Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA, por su sigla en inglés), las ADM tienen el potencial de matar, en un instante, “a millones de personas, poner en peligro el medioambiente y alterar de forma fundamental el mundo y la vida de futuras generaciones dado sus efectos catastróficos” (UNODA, 2022).

El CSNU define los **sistemas vectores** como los “misiles, cohetes y otros sistemas no tripulados capaces de transportar armas nucleares, químicas o biológicas, diseñados especialmente para ese fin”. Mientras que por **materiales conexos** se consideran aquellos “materiales, equipo y tecnología abarcados por los tratados y los mecanismos multilaterales pertinentes o incluidos en listas nacionales de control, que se podrían utilizar para el diseño, el desarrollo, la producción o el empleo de armas nucleares, químicas y biológicas y sus sistemas vectores”.

El GAFI (2008) complementó la definición de materiales conexos señalando que corresponden a bienes diversos como componentes de un arma o insumos para su elaboración. A modo de ejemplo, una maquinaria utilizada con un objetivo lícito, pero que puede emplearse en la construcción de componentes para un sistema vector de ADM.

PROLIFERACIÓN DE ADM

Se entiende por proliferación de ADM, en adelante proliferación, la transferencia y exportación de armas nucleares, químicas o biológicas, sus sistemas vectores y materiales conexos. Podría incluir, entre otras, tecnología, bienes, software, servicios o experticia (GAFI, 2008).

FINANCIAMIENTO DE LA PROLIFERACIÓN DE ADM

Es importante señalar que para el financiamiento de la proliferación (FP) aún no existe una definición acordada a nivel internacional. Por ello, para los fines de este documento se considerarán las referencias entregadas por el GAFI, los años 2008 y 2010, respecto del trabajo conjunto realizado por diversos expertos en la materia para su elaboración.

En relación con el financiamiento de la proliferación de ADM, en adelante financiamiento de la proliferación (FP), se entenderá como (GAFI, 2010):

¿QUE ES EL FINANCIAMIENTO DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA?

“el acto de proveer fondos o servicios financieros que son usados, en su totalidad o en parte, para la manufactura, compra, posesión, desarrollo, exportación, transbordo, intermediación, transporte, transferencia, almacenamiento o uso de armas nucleares, químicas o biológicas, así como también de sus sistemas vectores y materiales conexos (incluyendo tecnologías y bienes de uso dual utilizados para propósitos ilegítimos). Todo esto incumpliendo las normativas de cada país, o cuando sea el caso, de las obligaciones internacionales”



En el año 2010, a modo de complemento, el GAFI señaló que el FP podría contribuir a la inestabilidad global y a la pérdida de vidas humanas debido a la utilización de ADM, dado que facilita el movimiento y el desarrollo de elementos sensibles a la proliferación. También indicó que los proliferadores tienden a usar dinero en efectivo, o abusan de los sectores formales e informales del sistema financiero internacional para comerciar bienes útiles destinados a la proliferación. De esta manera, las instituciones financieras, de forma involuntaria, pueden actuar como facilitadoras de estos actos.

ROL DEL CSNU EN LA PREVENCIÓN DE LA PROLIFERACIÓN DE ADM Y SU FINANCIAMIENTO

La Carta de la ONU² entrega al CSNU³ la facultad de determinar la existencia de toda amenaza a la paz, quebrantamiento de la misma o acto de agresión y podrá realizar las recomendaciones o tomar las decisiones sobre qué medidas tomar para mantener o restablecer la paz y seguridad internacional⁴.

En el contexto del FP, el CSNU tiene la facultad para imponer sanciones a fin de mantener la paz y seguridad internacionales. Para el desarrollo de este documento se tendrá como objeto aquellas

sanciones relacionadas con medidas económicas y/o comerciales, embargo de armas y restricciones financieras, las cuales no requieren el uso de la fuerza armada⁵.

Desde el año 1966, el CSNU ha establecido 30 regímenes de sanciones que no han implicado el uso de la fuerza armada. De estos, 15 se encuentran activos y tienen como foco la resolución de conflictos de manera política, la no proliferación de armas nucleares y la lucha contra el terrorismo (CSNU, 2022).

Haciendo uso de las facultades descritas anteriormente, el CSNU, en materia de prevención de la proliferación y su financiamiento, ha abordado estos fenómenos desde dos perspectivas. La primera comprende un enfoque de aplicación global materializada a través de la Resolución 1540 (2004), mientras que la segunda posee un enfoque específico, esto es, a través de la aplicación de sanciones financieras dirigidas contra determinados Estados, y que hoy se traduce en las Resoluciones 1718 y 2231.

Es importante considerar que toda resolución dictada por el CSNU es obligatoria para los Estados parte de Naciones Unidas, aun cuando dichos Estados no hayan ratificado los tratados sobre los cuales se fundan las resoluciones⁶.

RESOLUCIONES DEL CSNU Y LA PREVENCIÓN DE LA PROLIFERACIÓN DE ADM Y SU FINANCIAMIENTO

Con el fin de prevenir, reprimir e interrumpir la proliferación y su financiamiento, **las Resoluciones del CSNU** referidas a este ámbito son las siguientes:

• Enfoque comprehensivo:

► **La Resolución 1540 (2004):** El 28 de abril de 2004, el CSNU aprobó, por unanimidad, la Resolución 1540 en la cual se afirma que la proliferación de las armas nucleares, químicas y biológicas, así como sus sistemas vectores, constituyen una amenaza a la paz y a la seguridad internacionales. Al respecto, entrega disposiciones amplias en relación con:

- Controles de exportación.
- La prohibición del financiamiento de actividades relacionadas con la proliferación llevadas a cabo por agentes no estatales.
- En términos de provisión de fondos y servicios financieros, relacionados con la exportación y transbordo de bienes que puedan contribuir a la proliferación, solicita a los países establecer, desarrollar, revisar y mantener controles adecuados en este sentido.

La Resolución 1540 es el primer instrumento internacional que menciona expresamente el fenómeno del FP y la necesidad de que los Estados implementen los controles necesarios para impedirla. Esta Resolución es el precedente fundamental para el trabajo que el GAFI desarrolló posteriormente en el

marco de la incorporación de este fenómeno a sus estándares en 2008 y, posteriormente, en 2012 a través de la Recomendación N°7.

• Enfoque restrictivo:

Estas corresponden a resoluciones específicas dictadas contra Estados, grupos, entidades o personas determinadas. En el uso de sus facultades, en estos casos, el CSNU concluyó que determinadas acciones provocadas por los mismos amenazan la paz y seguridad internacional.

Por lo anterior, de 15 regímenes de sanciones vigentes, 1 contempla medidas que impiden la proliferación de ADM y su financiamiento. En este caso, el objetivo es restringir a la República Popular Democrática de Corea (RPDC o Corea del Norte) de acciones que le permitan generar relaciones comerciales con sus pares, grupos, entidades y personas, por medio de limitaciones a sus importaciones, exportaciones, o prohibiciones comerciales, entre otras, a fin de prevenir la proliferación de ADM y su financiamiento. Dentro de este régimen se pueden encontrar sanciones específicamente enfocadas a impedir la recaudación de recursos para dichos fines, conocidas como sanciones financieras dirigidas (SFD).

Irán es otro caso que se encuentra en un régimen especial. A diferencia del anterior, el régimen de sanciones impuesto por el CSNU se encuentra terminado bajo el compromiso del cumplimiento del Plan de Acción Integral Conjunto (PAIC), suscrito en julio de 2015 (Resolución 2231 (2015)), entre ese país y Estados Unidos, Reino Unido, Rusia, Francia y China (los cinco miembros permanentes del CSNU), en un intento de impedir que Irán se dote de armas nucleares.

► **Resolución 1718 (2006) y sus sucesoras:**

Son sanciones dirigidas en contra de la RPDC, producto de las trasgresiones reiteradas a las Resoluciones del Consejo de Seguridad de Naciones Unidas.

► **Resolución 2231 (2015):**

Tiene como objetivo a Irán, y formaliza la aplicación del Plan de Acción Integral Conjunto (PAIC) que deja en pausa el régimen de sanciones que tenía vigencia desde 2006. El PAIC cambió la mirada que el CSNU tenía sobre la cuestión nuclear iraní, pues a través de esta Resolución Irán se comprometió a tomar diversos compromisos que permiten monitorear el uso pacífico de su programa nuclear, permitiéndole reiniciar relaciones de cooperación, económicas y comerciales. Sin perjuicio de lo anterior, la Resolución agregó nuevas restricciones y mantuvo SFD hacia algunos individuos y entidades del país. En caso de incumplimiento del PAIC por parte de Irán, las Resoluciones anteriores a esta retomarán su vigencia⁷. El PAIC tienen

un plazo de implementación de 10 años, siempre y cuando Irán cumpla los términos. Expirado el plazo dejará de tener efecto el Plan al igual que las Resoluciones que aplican el régimen de sanciones⁸.

SANCIONES FINANCIERAS DIRIGIDAS (SFD)

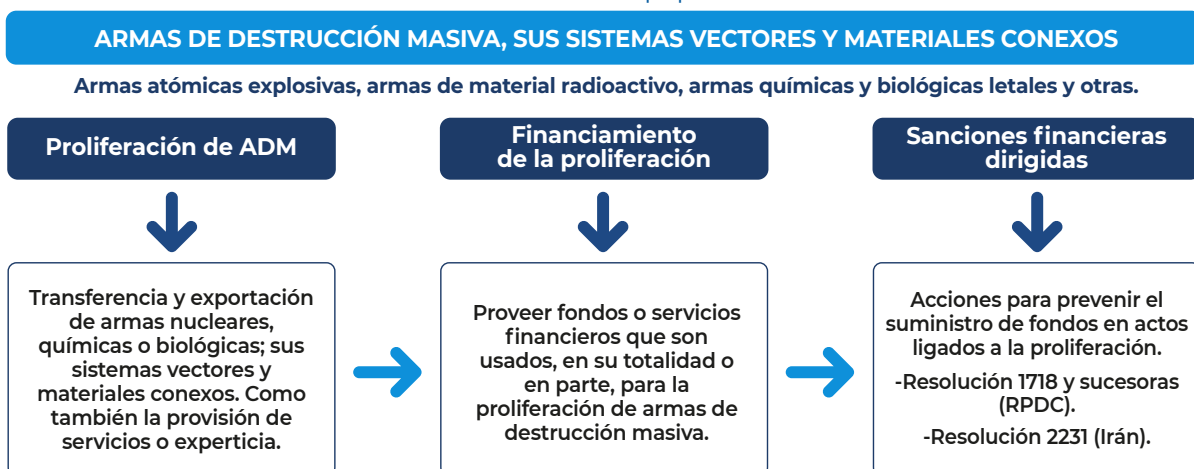
Se aplican las denominadas Sanciones Financieras Dirigidas (SFD) con el objetivo de prevenir la destinación de fondos para acciones ligadas a la proliferación. Al respecto, el GAFI indica que estas corresponden “tanto al congelamiento de activos como a las prohibiciones para prevenir que los fondos u otros activos sean suministrados, directa o indirectamente, para el beneficio de las personas y entidades designadas” (GAFI, actualización octubre 2021).

Las Resoluciones del CSNU que contemplan SFD relacionadas con el FP son la Resolución 1718 (2006) y sus sucesoras, y la Resolución 2231 (2015) ambas descritas anteriormente.

ILUSTRACIÓN 1

Resumen de conceptos relacionados con la proliferación y su financiamiento

Fuente: Elaboración propia UAF.



METODOLOGÍA DE TRABAJO

Esta primera Evaluación Nacional de Riesgos de FP elaborada por Chile a fin de caracterizar el fenómeno, basa su metodología en la recopilación de información cualitativa disponible a nivel nacional e internacional, para analizar el contexto del periodo 2016-2021. Esto, debido a que el país no cuenta con suficientes antecedentes cuantitativos necesarios para abordar la ocurrencia de este fenómeno.

En este contexto, la metodología utilizada está en línea con propuestas formuladas por organismos internacionales: GAFI, en función de sus pautas y recomendaciones mundiales para que los países ejecuten un adecuado y eficaz combate del LA/FT/FP, y The Royal United Services Institute (RUSI), grupo de expertos dedicado a la investigación en defensa y seguridad internacional.

En este sentido, se establece un proceso de levantamiento de información que contempla fuentes nacionales y extranjeras, tendientes a complementar los análisis y conclusiones sobre el fenómeno de FP.

A continuación se detallan las actividades llevadas a cabo para este propósito, así como los documentos considerados en la identificación y examen de las amenazas, vulnerabilidades y mitigantes, que serán posteriormente abordados en este documento.

1. Levantamiento de información: Se llevó a cabo un proceso de revisión, análisis y verificación de la bibliografía relacionada a la temática del FP en el país, que contempló, entre otras materias:

a. Informes del Panel o Grupo de Expertos que apoya al Comité de Sanciones 1718 del CSNU sobre la República Popular Democrática de Corea⁹: Se analizó información contenida en 10 reportes elaborados por el Grupo de Expertos en el periodo comprendido entre los años 2015 y 2021.

b. Documentos publicados por entidades internacionales:

Se consideraron las Recomendaciones y reportes del GAFI relacionados con esta materia, guías e informes elaborados por instituciones no gubernamentales especializadas en la temática (por ejemplo, el RUSI), reportes de tipologías de proliferación y FP internacionales, y casos de infracción a los controles de exportación, entre otra información disponible públicamente. Asimismo, se realizó una revisión de evaluaciones de riesgos de FP desarrolladas por países referentes en el tema.

c. Informe de Evaluación Mutua de Chile (IEM):

Publicado en septiembre del 2021 por parte del Grupo de Acción Financiera de Latinoamérica (Gafilat). Este insumo analiza el nivel de cumplimiento de Chile de las 40 Recomendaciones del GAFI y el grado de efectividad del Sistema Nacional ALA/CFT.

d. Estándares internacionales:

Se revisaron las convenciones, tratados internacionales y Resoluciones del CSNU relevantes que fijan el espacio o rango de acción de las naciones a nivel global, y establecen los estándares en relación con la proliferación y su financiamiento.

e. A nivel nacional:

Se utilizó información de diversa índole (a modo de ejemplo, comercial y financiera), proveniente, principalmente, del Servicio Nacional de Aduanas, Ministerio de Relaciones Exteriores, policías (PDI, Carabineros y Dirección General del Territorio Marítimo y de Marina Mercante de la Armada (Directemar), y de la Unidad de Análisis Financiero, entre otras, que, a nivel agregado, facilitan la determinación de amenazas, vulnerabilidades y mitigantes. También se revisó información relacionada con el marco normativo o regulatorio vigente en el país en la materia, datos de comercio exterior y otra disponible públicamente.

f. Mesas de trabajo con expertos temáticos.

Se consideraron los resultados de las mesas de trabajo con personas que, dada su experiencia, conocimientos e idoneidad, constituyen un punto de referencia respecto de la comprensión del fenómeno del FP, y han sido identificados para obtener su opinión.

En el marco de la Mesa Técnica (MT) de Riesgos de LA/FT/FP de la MILAFT, durante el 2023 se revisaron los antecedentes levantados en materia de proliferación y su financiamiento.

En esta MT participaron representantes de instituciones que abordan estas materias, tanto directa como indirectamente, entre las que se cuentan la Agencia Nacional de Inteligencia (ANI), las policías (Carabineros de Chile y la Policía de Investigaciones) y otras instituciones de participación permanente como el Ministerio Público y el Ministerio del Interior y Seguridad Pública, entre otras.

2. Identificación de los riesgos del FP: Luego del análisis de la información recolectada, se determinaron las eventuales amenazas, vulnerabilidades y mitigantes de las acciones/actividades que podrían impactar al país, de lo cual se procedió a:

a. Determinar las amenazas actuales: Con el objetivo de identificar amenazas que podría enfrentar el país respecto del FP, se realizó una recopilación y análisis de la información registrada en los reportes publicados por el Grupo de Expertos y el documento del RUSI “Guide to Conducting a National Proliferation Financing Risk Assessment”, que clasifica y define las amenazas de FP en tres categorías:

i. Productos y servicios financieros relacionados con el comercio de bienes sensibles a la proliferación: Corresponden a aquellos que pueden usarse de manera directa o modificada

en el desarrollo de ADM, de sus sistemas vectores y de materiales relacionados. También incluyen productos/servicios financieros vinculados con operaciones de comercio exterior y su transporte.

ii. Actividades de obtención de fondos (lícitas e ilícitas): Generan ingresos para, eventualmente, financiar la adquisición o desarrollo de ADM o de sus sistemas vectores.

iii. Infraestructura financiera y corporativa que apoye el movimiento financiero y de bienes: Cualquier tipo de infraestructura financiera o corporativa que sustente a las actividades mencionadas en las dos categorías anteriores. Incluye la provisión de activos o servicios financieros a personas/entidades sujetas a sanciones financieras directas de FP.

b. Determinar las vulnerabilidades: En general, las vulnerabilidades son materias, contextos (económicos, sociales, políticos, tecnológicos, entre otros) u otras situaciones que pueden ser aprovechadas por las amenazas o explotadas para facilitar y apoyar a las mismas. Para este caso, las vulnerabilidades deben entenderse como características propias del país¹⁰, susceptibles de ser aprovechadas no solo por personas o entidades designadas para el FP, sino también en maniobras que infringen o evaden las SFD o por terceros relacionados que actúan como intermediadores o controladores, en desacato a las disposiciones contenidas en las Resoluciones del CSNU sobre la materia.

Para identificar las vulnerabilidades se revisó tanto el marco normativo vigente relacionado con las materias identificadas en las actividades consideradas como

amenazas de FP, como también la información registrada en el IEM de Chile¹¹ el cual reveló, entre otros, las fortalezas y debilidades del Sistema Nacional ALA/CFT respecto del fenómeno de FP.

c. Determinar los mitigantes: Se consideraron como mitigantes aquellos factores económicos o demográficos que actúan como una defensa estructural y/o natural ante la presencia de amenazas. Estos factores permiten disminuir la probabilidad de ocurrencia de eventos dañinos o indeseados en el contexto del FP¹².

Para determinar e identificar los principales mitigantes, la información utilizada proviene, principalmente, de lo registrado en el IEM de Chile por parte del Gafilat, en el cual se evaluó, entre otras materias, la normativa relacionada con las SFD de FP en el país. Asimismo, se incorporó información que se consideró relevante, relacionada con materias de seguridad de la información y ciberseguridad, comercio exterior, entre otras.

ILUSTRACIÓN 2 Resumen de la Metodología de la Evaluación Nacional de Riesgos del FP de Chile

Fuente: Elaboración propia UAF.





CAPÍTULO II: ESTÁNDARES INTERNACIONALES, CONTEXTO DE LA PROLIFERACIÓN Y SU FINANCIAMIENTO EN CHILE

CAPÍTULO II: ESTÁNDARES INTERNACIONALES, CONTEXTO DE LA PROLIFERACIÓN Y SU FINANCIAMIENTO EN CHILE

Este capítulo aborda el funcionamiento del Sistema Nacional ALA/CFT con respecto al fenómeno del FP, el marco regulatorio nacional vigente y la implementación de las Resoluciones del CSNU.

ESTÁNDARES INTERNACIONALES SOBRE FP

La prevención y combate de la proliferación y su financiamiento forman parte de un esfuerzo internacional, impulsado por una serie de organismos intergubernamentales especializados en la materia.

La Resolución 1540 (2004) del CSNU junto con integrar en un documento los tratados y convenciones internacionales sobre la materia, obliga a los países miembros de Naciones Unidas, firmantes o no de dichos tratados, a tomar acciones concretas en contra de la proliferación y su financiamiento.

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL (GAFI)

El Grupo de Acción Financiera Internacional (GAFI o FATF, por su sigla en inglés) es un organismo intergubernamental creado en París, Francia, en 1989, por el Grupo de los Siete, para establecer estándares y promover la aplicación efectiva de medidas legales, regulatorias y operativas para combatir el lavado de activos (LA), el financiamiento del terrorismo (FT) y otras amenazas relacionadas con la integridad del sistema financiero internacional.

Para ello emite una serie de Recomendaciones, reconocidas como el estándar internacional de lucha contra el lavado de activos, el financiamiento del terrorismo y el de la proliferación de armas de destrucción masiva (LA/FT/FP).

Un hito es la incorporación de la generación de estándares internacionales en FP en el mandato del GAFI en 2008¹³. Desde el año 2012, el GAFI incorporó la Recomendación N°7 que establece la implementación de SFD para cumplir con las Resoluciones del CSNU relativas a la prevención, represión e interrupción de la proliferación y su financiamiento.

Adicionalmente, en 2020, el GAFI incorporó la obligación de evaluar los riesgos asociados con la Recomendación N°7. El GAFI reconoce la estrecha conexión que existe entre el FP, el terrorismo y su financiamiento, fenómeno que comenzó a abordarse integralmente en el país.

Chile ha generado normativa con el fin de prevenir y reprimir el FP, en línea con el cumplimiento de las normas internacionales. Esto, orientado a la implementación de los tratados, convenciones, y resoluciones del CSNU relacionados con la proliferación y su financiamiento. Asimismo, ha trabajado en medidas para cumplir con las Recomendaciones del GAFI¹⁴.

Comité contra la no proliferación en virtud de la resolución 1540 (2004)

El 28 de abril de 2004, el CSNU aprobó por unanimidad la Resolución 1540 (2004), en virtud del Capítulo VII de la Carta de las Naciones Unidas. En dicha Resolución se afirma que la proliferación de las armas nucleares, químicas y biológicas, así como sus sistemas vectores, constituye una amenaza a la paz y la seguridad internacionales. Desde 2006, el CSNU ha prorrogado el mandato del Comité a objeto de fortalecer las relaciones de cooperación con la comunidad internacional, a fin de facilitar que todos los Estados apliquen la Resolución 1540.

MARCO REGULATORIO NACIONAL E IMPLEMENTACIÓN DE LAS RESOLUCIONES DEL CSNU

NORMATIVA E INICIATIVAS PARA LA IMPLEMENTACIÓN DE LAS RESOLUCIONES DEL CSNU EN CHILE

Ministerio de Relaciones Exteriores

A través de decretos supremos del Ministerio de Relaciones Exteriores de Chile (Minrel), se han incorporado al ordenamiento jurídico nacional las Resoluciones dictadas por el CSNU en materia de proliferación y su financiamiento. La implementación de estas se sintetiza de la siguiente forma:

Con el fin de prevenir y reprimir el FP, las Resoluciones del CSNU vinculantes para Chile en la materia son:

- **Resolución 1540 (2004).**
- **Resolución 1718 (2006) relativa a Corea del Norte y sus sucesoras.**
- **Resolución 2231 (2015) relativa a la cuestión nuclear de Irán.**

1. Implementación de la Resolución 1540 (2004) del CSNU en Chile: Este proceso es liderado por el Minrel, que desde el año 2004 ha implementado distintos hitos para su ejecución:

- Creación del Comité Interministerial para la Implementación y Cumplimiento de las Resoluciones del CSNU, año 2012. Esta instancia actúa como coordinadora en la implementación y cumplimiento de dichas Resoluciones, así como también de las emanadas por órganos subsidiarios al CSNU, por medio de la asesoría a los Ministerios. Durante el 2017 se creó el Sub-Comité 1540,

cuya finalidad consiste en implementar las disposiciones de la Resolución 1540. Se encuentra integrado por distintas instituciones públicas, entre las que destacan el Servicio Nacional de Aduanas, la UAF y la Agencia Nacional de Inteligencia (ANI)¹⁵ (Minrel, 2017, pág. 3).

- En septiembre de 2016 se promulgó el Decreto 145 del Minrel, el cual dispone el cumplimiento de la Resolución 1540, y establece que las autoridades y órganos del Estado velen para que, en el ámbito de sus funciones, se ejecuten las disposiciones allí contenidas.
- En agosto de 2017, la Misión Permanente de Chile ante las Naciones Unidas presentó al Comité del CSNU el Plan de Acción Nacional 2017-2021 para la Implementación de la Resolución 1540 del CSNU (PANIR 1540)¹⁶, desarrollado conjuntamente entre el Minrel y la ANI. El PANIR 1540 incluyó cinco áreas de trabajo: **(1)** legislación, **(2)** creación de capacidades y entrenamiento, **(3)** cooperación internacional, **(4)** fortalecimiento institucional y **(5)** concientización del ámbito público y privado, sociedad civil y academia. Tres de estas cinco áreas incluyen medidas específicas o explícitas relacionadas con el financiamiento de la proliferación (Minrel, 2017, págs. 6-13).

2. Implementación de las Resoluciones que aplican SFD en el marco del FP en Chile: La Misión Permanente de Chile ante la ONU presentó, en noviembre de 2011, un informe sobre las medidas adoptadas en virtud de la Resolución 1718 del CSNU, en concordancia con el párrafo 11 de dicho dictamen (CSNU, 2011). En ese documento se informó que:

- El país tomó la decisión de poner término a toda relación de cooperación, tanto de carácter técnico como comercial, con la RPDC¹⁷ (CSNU, 2011, pág. 2).

- El Decreto Supremo N°366 del Minrel, publicado en 2007, contiene la decisión del Gobierno de Chile de cumplir con la Resolución 1718 del CSNU, a través de la adopción de medidas contra la RPDC. Además, indica que las autoridades y órganos del Estado deben velar por el cumplimiento de las disposiciones de la Resolución 1718 del CSNU, dentro del marco de sus funciones¹⁸. (CSNU, 2011, pág. 2)
- En Chile, la Ley N°17.798 sobre control de armas somete a control los materiales indicados en el párrafo 8, apartado a) acápites i) y ii), de la Resolución 1718, siendo la Dirección General de Movilización Nacional (DGMN) la encargada de realizar la supervigilancia y control de armas, explosivos, entre otros bienes en el país. (CSNU, 2011, pág. 2)
- Con respecto a la Resolución 2231 del CSNU sobre la República Islámica de Irán, relativa a la cuestión nuclear de Irán, en agosto de 2019 se promulgó el Decreto N°128 del Minrel, que constató la decisión del Gobierno de Chile de dar cumplimiento a la Resolución 2231 del CSNU. Además, señala que las autoridades y órganos del Estado deben velar por el cumplimiento de las disposiciones de la Resolución 2231 del CSNU, dentro del marco de sus funciones.

2.1 Sanciones Financieras Dirigidas impuestas por el CSNU, bajo las Resoluciones 1718 (RPDC) y 2231 (Irán): En relación con las SFD impuestas por el CSNU, bajo las Resoluciones 1718 (RPDC) y 2231 (Irán), Chile cuenta con un marco normativo y un mecanismo que ejecuta la aplicación de dichas SFD en los términos requeridos por las Resoluciones¹⁹.

El Minrel, a través del Decreto 214 (2020), estableció las medidas que implementan las Resoluciones del CSNU para la prevención y represión del financiamiento de actividades que afecten la paz y seguridad internacionales, en

particular del financiamiento del terrorismo (incluye la Resolución 1373) y financiamiento de la proliferación. Con este decreto se difundió información relativa a las listas, aplicación de medidas y SFD, junto con el intercambio de información y cooperación internacional.

Asimismo, se definió el rol de los organismos de la administración del Estado:

- **Ministerio de Relaciones Exteriores:** Será el punto de contacto y enlace con el CSNU y sus Comités, así como con otras organizaciones o entidades relacionadas con esta normativa. También es el actor encargado de recibir la información sobre las actualizaciones enviadas por el CSNU respecto de las personas/entidades designadas por los Comités del CSNU de FT y FP, las cuales son remitidas luego a la UAF²⁰.
- **Unidad de Análisis Financiero:** Luego de recibir la información desde el Minrel, y dentro de sus atribuciones legales, podrá solicitar o adoptar las medidas para prevenir y reprimir el FP, además de requerir y recopilar información pertinente con el objetivo de identificar, bajo determinados criterios, a las personas/entidades susceptibles de ser incluidos o eliminados de las listas designadas por los respectivos Comités del CSNU de FT y FP. Posteriormente, la UAF tendrá que remitir la información sobre personas/entidades identificadas al Minrel, de manera confidencial, recomendando su inclusión/eliminación de esos listados.

En el Anexo 2 de este documento se incluyen los Decretos del Minrel que han dispuesto el cumplimiento de las resoluciones del CSNU relacionadas con la proliferación y el FP.

Marco normativo nacional relativo a la proliferación y su financiamiento

Los principales instrumentos legales que rigen en temas de proliferación en Chile tienen relación con el control de seguridad sobre actividades que puedan contribuir al comercio ilícito de mercancías estratégicas asociadas con la amenaza química, biológica, radiológica o nuclear. Estas normativas corresponden a:

- Ley N°17.798, sobre control de armas y explosivos.
- Ley N°18.302, de seguridad nuclear.
- Ley N°21.250, que implementa la Convención de armas químicas y biológicas²¹.

Estas normas abordan temas relacionados con la fabricación, adquisición, posesión, desarrollo, transporte, transferencia, utilización, participación como cómplice en las actividades mencionadas y ayuda con medios de entrega (medios de lanzamiento: misiles, cohetes y otros sistemas no tripulados capaces de transportar armas nucleares, químicas o biológicas que estén especialmente diseñados para ese uso).

En este ámbito, una de las instituciones encargadas de fiscalizar e implementar controles al comercio estratégico es el Servicio Nacional de Aduanas, el cual, al detectar alguna irregularidad, debe realizar la denuncia a los organismos correspondientes para la investigación de delitos relacionados con la proliferación de ADM, o en su defecto puede remitir un Reporte de Operación Sospechosa a la Unidad de Análisis Financiero²².

Al respecto, está en proceso legislativo un proyecto de ley que crea la Comisión de Comercio Estratégico y regula la exportación de material de uso dual y de defensa, y otras materias que indica²³.

En relación con el control de armas, en Chile, el Decreto 400 (2022) fija el texto refundido, coordinado y sistematizado de la Ley N°17.798 que aborda la materia. Este cuerpo legal incluye

a las armas de destrucción masiva dentro de sus componentes, estableciendo la prohibición de su posesión o tenencia²⁴. La infracción a esta prohibición se encuentra sancionada con pena de presidio mayor en su grado mínimo a medio. Asimismo, también existe sanción cuando se financia a grupos paramilitares que pudieran emplear este tipo de armamento²⁵.

Es necesario considerar que el FP no se encuentra tipificado como delito en la legislación chilena.

FUNCIONAMIENTO DEL SISTEMA NACIONAL ALA/CFT CON RESPECTO AL FINANCIAMIENTO DE LA PROLIFERACIÓN

La Ley N°19.913 constituye una estructura normativa del Sistema Nacional ALA/CFT, compuesto por tres pilares fundamentales: Prevención, detección y persecución-sanción.

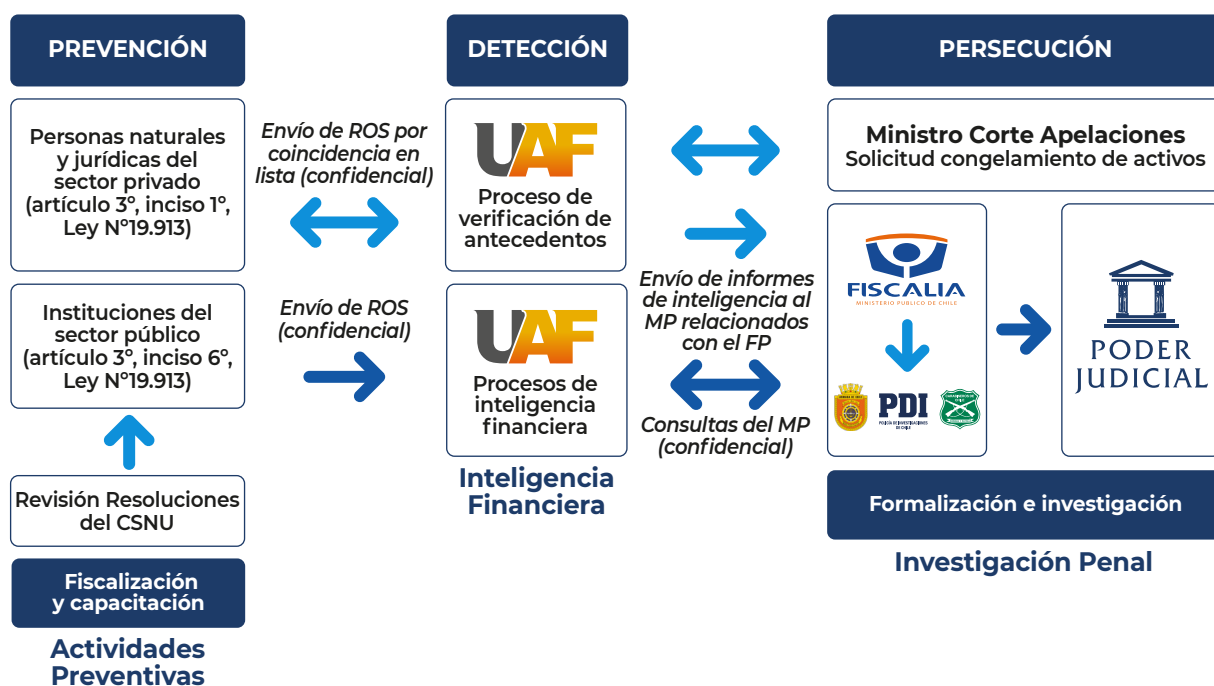
El Sistema lo integran instituciones públicas reguladoras, supervisoras y persecutoras²⁶ del LA/FT, además de todos los sujetos obligados (S.O.) a informar operaciones sospechosas a la UAF (expresamente señalados en el artículo 3° de la Ley N°19.913), a través de un Reporte de Operaciones Sospechosas (ROS).

A continuación se expone una síntesis del funcionamiento de Sistema Nacional ALA/CFT, respecto del fenómeno del financiamiento de la proliferación en el país.

ILUSTRACIÓN 3

Resumen del Funcionamiento del Sistema Nacional ALA/CFT respecto al fenómeno del FP

Fuente: Elaboración propia UAF.



PREVENCIÓN

En este ámbito actúan los organismos reguladores del país y las personas naturales y jurídicas, de los sectores público y privado, expresamente señaladas en el artículo 3° de la Ley N°19.913 (sujetos obligados).

Dichas entidades deben implementar políticas y procedimientos de prevención y detección del LA/FT, conforme las características organizacionales propias y sus matrices de riesgos, todo lo cual debe plasmarse en un Manual de Prevención (circulares N°49, 54 y 60 de la UAF).

Con el objetivo de prevenir el FP, el país cuenta con un marco normativo y un mecanismo que implementa la aplicación de las SFD, en los términos requeridos por las resoluciones del CSNU. La normativa vigente en esta materia se establece

a partir de la Ley N°19.913 y de las circulares emitidas por la UAF, que deben ser cumplidas por todas las entidades reportantes reguladas.

En cuanto a la detección de personas naturales o jurídicas listadas en las Resoluciones del CSNU, se establece que "los sujetos obligados, en la circunstancia de **detectar a alguna persona, empresa o entidad que esté mencionada en cualquiera de los listados de las Resoluciones del CSNU que sancionan el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva (...), deberán enviar a la UAF, de forma inmediata, un ROS informando de dicho hallazgo, a efectos de que la UAF pueda proceder a tomar la medida de congelamiento de activos establecida en el artículo 38° de la Ley N°19.913**"²⁷ (circulares N°49, 54 y 60).

Respecto del cumplimiento de las obligaciones de revisión de listados de las Resoluciones del CSNU por parte de los sujetos obligados, la normativa establece el deber de efectuar estas consultas mediante la implementación de procedimientos específicos, los que deben ser incluidos en un Manual de Prevención e implementados de manera efectiva. Para ello, la UAF, a través de su página web, provee la información necesaria para el cumplimiento de dichas medidas por parte de los sujetos obligados²⁸.

Asimismo, se establece como obligación contar con procedimientos, en los respectivos Manuales de Prevención, que aseguren la revisión y chequeo permanente y oportuno de los listados de los Comités de Sanciones del CSNU, y existan medios de verificación que permitan acreditar el cumplimiento de dichas obligaciones.

Cabe destacar que las instituciones del sector público responsables de la implementación de la Resolución 1540 (Minrel, Aduanas, DGMN, entre otras) son sujetos obligados de la UAF y, por ende, deben remitir a este Servicio las operaciones sospechosas que detecten en el ejercicio de sus funciones, a través de un ROS.

Actividades de difusión y capacitación

La UAF cuenta con un Plan de Capacitación dirigido tanto al sector privado como al público, que desarrolla contenidos para la prevención y detección del LA/FT/FP, y orienta el uso de señales de alerta sobre la materia y la implementación de procedimientos que permitan el envío oportuno y confidencial de los ROS.

Las actividades de capacitación ponen especial énfasis en la obligación de las entidades reportantes de revisar y chequear permanentemente a sus clientes en los listados emitidos por las Resoluciones del CSNU sobre FT y FP.

De manera complementaria, desde el segundo semestre de 2019, las materias relacionadas con FP son parte de los contenidos permanentes de las actividades de capacitación realizadas por la UAF, tanto en su formato presencial como a distancia (cursos e-Learning, sin costo).

Las actividades de capacitación ponen especial énfasis en la obligación de las entidades reportantes de revisar y chequear permanentemente a sus clientes en los listados emitidos por las Resoluciones del CSNU sobre FT y FP.

A ello se suma que para orientar a las entidades reportantes, y al público en general, respecto de las situaciones que se deben considerar como sospechosas de LA/FT/FP, la UAF elaboró y emitió una versión actualizada de su Guía de Señales de Alerta, que describe los comportamientos o características de ciertas personas o transacciones, que podrían conducir a detectar oportunamente una “operación sospechosa” de FP²⁹.

DETECCIÓN

1. Reporte de Operación Sospechosa por coincidencia en listados del CSNU

Los sujetos obligados deben revisar, permanentemente, los listados de las Resoluciones del CSNU sobre FT y FP, y reportar de manera inmediata a la UAF, sin análisis previo, a través de un ROS, en caso de encontrar alguna coincidencia en lista, a efectos de que la UAF pueda proceder a tomar la medida de congelamiento de activos establecida en el artículo 38° de la Ley N°19.913³⁰.

Dentro de las 24 horas siguientes a la recepción de antecedentes (a través de un ROS) que acrediten que las personas naturales o jurídicas individualizadas en las listas confeccionadas por el CSNU pretenden realizar un acto, transacción u operación financiera, la UAF deberá solicitar a

un ministro de la Corte de Apelaciones de Santiago la adopción de medidas necesarias para evitar el uso, aprovechamiento, beneficio o destino de cualquier clase de bienes, valores o dinero materia de acto, transacción u operación, sin previo aviso al afectado y por un plazo determinado. La vigencia de las medidas decretadas por el ministro de la Corte no podrá exceder de treinta días, prorrogables por resolución fundada.

2. Reporte de Operación Sospechosa vinculado a posibles actividades de FP

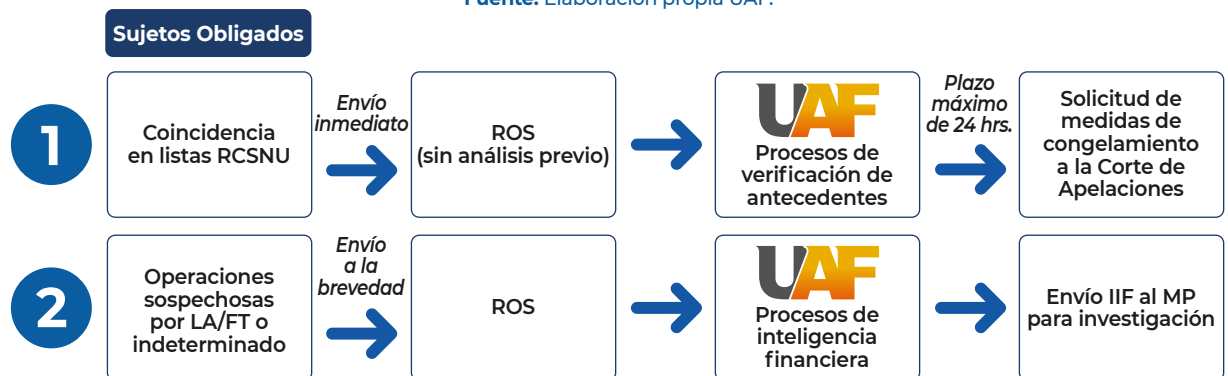
Cuando alguna de las personas naturales o jurídicas expresamente señaladas en el artículo 3° de la Ley N°19.913 advierte, en el ejercicio de su actividad o funciones, algún acto, operación o transacción que, de acuerdo a la normativa cumpla con los criterios de “sospecha” de FP, tiene la obligación legal de remitir inmediatamente esos antecedentes a la UAF a través de un ROS.

Para ello, los sujetos obligados deben analizar las operaciones y determinar, de acuerdo a sus políticas y procedimientos de sus propios sistemas preventivos del LA/FT, si se está o no en presencia de una operación sospechosa que deba ser reportada a la UAF.

Una vez recibido el ROS, la UAF activa sus procesos de inteligencia financiera, con el único objetivo de detectar señales indiciarias de LA, FT o indeterminado. De haberlas, la UAF elabora y envía confidencial y oportunamente un Informe de Inteligencia Financiera al Ministerio Público, única institución responsable de investigar y perseguir penalmente a los responsables de un delito.

ILUSTRACIÓN 4 Formas de reportar un ROS a la UAF y su proceso de análisis

Fuente: Elaboración propia UAF.



PERSECUCIÓN Y SANCIÓN

La investigación y persecución penal que pudieran ocurrir por posibles delitos relacionados con el FP, debe ser dirigida en forma exclusiva por el Ministerio Público. Pueden colaborar las unidades especializadas de las policías, cuyos efectivos participan bajo dirección del fiscal de la causa.

IMPORTANTE

Es importante señalar que el FP no se encuentra tipificado como delito en la mayoría de las jurisdicciones a nivel internacional, incluyendo Chile. En cambio, en el país sí están tipificados otros delitos que podrían relacionarse de manera indirecta con el FP, los cuales podrían cometerse con el objetivo de obtener fondos (tráfico de drogas, delitos cibernéticos, entre otros) y utilizarlos para financiar la proliferación.



CAPÍTULO III: DIAGNÓSTICO DEL FENÓMENO DE FINANCIAMIENTO DE LA PROLIFERACIÓN EN CHILE

CAPÍTULO III: DIAGNÓSTICO DEL FENÓMENO DE FINANCIAMIENTO DE LA PROLIFERACIÓN EN CHILE

En Chile no se han identificado investigaciones, casos judicializados y/o formalizados por delitos que pudiesen estar relacionados con actividades de proliferación y su financiamiento. En línea con ello, la UAF tampoco ha recibido reportes de operaciones sospechosas asociados al FP.

Durante el periodo de análisis, en el país tampoco se han detectado coincidencias con el nombre de personas enlistadas por el CSNU, ni han existido casos de congelamiento de activos relacionados con las Resoluciones del CSNU respecto de sanciones financieras dirigidas a causa del FP.

A continuación se identifica el fenómeno del FP en Chile, integrando, principalmente, la información respecto de:

- La Estrategia Nacional para Prevenir y Combatir el LA/FT, que incorpora los planteamientos del sector privado y público;
- El Informe de Evaluación Mutua de Chile por parte del Gafilat y sus acciones recomendadas con base en este fenómeno;
- Las menciones del país en los reportes del Grupo de Expertos relativos al FP.

ESTRATEGIA NACIONAL PARA PREVENIR Y COMBATIR EL LA/FT Y PLAN DE ACCIÓN 2018-2020

Con el objetivo de proteger al país de los graves daños que provocan los delitos de LA/FT, el Gobierno de Chile lanzó, en diciembre de 2013, una Estrategia Nacional para prevenir y combatir ambos ilícitos, con un Plan de Acción que se desarrolló entre los años 2014 y 2017.

Durante el 2018, la segunda versión de la Estrategia Nacional ALA/CFT se construyó como

una instancia de integración, organización y coordinación interinstitucional en las áreas de prevención, detección y persecución penal del LA/FT, a fin de fortalecer la integridad de los sectores financiero y no financiero del país.

Con el objetivo de proteger a la economía nacional ante las amenazas de estos actos ilícitos, se trabajó en la implementación de medidas antiLA/FT/FP, para fortalecer la integridad de los sectores financieros y no financiero del país.

El Plan de Acción 2018-2020 fue el resultado del trabajo de 17 instituciones públicas, apoyado por la MILAFT, el cual estuvo orientado a seis líneas estratégicas identificadas por las propias entidades miembros de la EN³¹: **(1)** Actualización de la normativa ALA/CFT, **(2)** Supervisión basada en riesgos, **(3)** Investigación patrimonial y aumento del decomiso, **(4)** Fortalecimiento de las capacidades y habilidades para la prevención y combate del LA/FT (Capacitación), **(5)** Cooperación y coordinación interinstitucional y **(6)** Financiamiento del terrorismo y el de la proliferación de armas de destrucción masiva.

Este Plan contempló la problemática del FT y el FP como uno de los ejes estratégicos para fortalecer el sistema de regulación, detección y sanción, en particular la línea estratégica N°6 de "Financiamiento del terrorismo y el de la proliferación".

A través de ese eje se abordaron dos aspectos fundamentales:

1. Evaluar y formular propuestas de reformas legales necesarias para la incorporación de la normativa internacional en materia de FT y FP, y el pleno cumplimiento de los estándares internacionales: Para dar cumplimiento a este propósito, en julio de 2019 se publicó en el Diario Oficial la Ley N°21.163, que incorporó las Resoluciones del CSNU referentes al FT y a la proliferación en el artículo 38° de la Ley N°19.913.

2. Realizar los ajustes operativos y de coordinación entre las instituciones encargadas de la prevención, detección y persecución del FT y FP: En el periodo se efectuaron reuniones para coordinar aspectos operativos en materia de prevención, detección y persecución del FT y del FP.

En 2023, los miembros de la Estrategia Nacional, con el apoyo de la MILAFT iniciaron el trabajo de elaboración de un nuevo Plan de Acción, con miras a los años 2023-2027, a través de 5 mesas técnicas permanentes sobre: Actualización legislativa, Riesgos de LA/FT/FP, Supervisión y regulación, Persecución penal e Inteligencia financiera.

RESULTADOS DE LA EVALUACIÓN MUTUA DE CHILE POR PARTE DEL GAFILAT

El Grupo de Acción Financiera de Latinoamérica (Gafilat, ex Gafisud) es una organización intergubernamental de base regional, que promueve la implementación y mejora continua de políticas para combatir el LA/FT/FP.

Se creó formalmente el 8 de diciembre de 2000 en Cartagena de Indias, Colombia, bajo el modelo del GAFI; por tanto, adhiere sus 40 Recomendaciones y, además, apoya a sus miembros a implementarlas, a través de medidas de capacitación y evaluaciones mutuas.

Las evaluaciones de Chile corresponden a los años 2006, 2010 y 2019-2021. Esta última se realizó en el marco de la IV Ronda de Evaluaciones Mutuas. El periodo evaluado comprendió las acciones adoptadas por nuestro país entre 2015 y 2019, ambos años inclusive, para prevenir y combatir el LA/FT, según la nueva Metodología del GAFI (aprobada en 2012), que comprende criterios de revisión de cumplimiento técnico de las 40R del GAFI (marco normativo del país) y de efectividad real del Sistema Nacional ALA/CFT, basada en un enfoque de riesgo (medido a través de 11 Resultados Inmediatos). Durante el

proceso de evaluación, y en su calidad de representante de Chile ante el Gafilat, la UAF actuó como coordinador y punto de enlace.

En julio de 2021, el Pleno de Representantes del Gafilat aprobó el Informe Final de la Evaluación Mutua de Chile, el cual fue publicado en septiembre de ese año. De las 40R, el país logró 12 Cumplidas, 18 Mayoritariamente Cumplidas, 9 Parcialmente Cumplidas y ninguna No Cumplida. Respecto de la efectividad del Sistema Nacional ALA/CFT, el país fue calificado en 3 Resultados Inmediatos con “Sustancial”, 7 “Moderado” y 1 “Bajo”. Con estos niveles de cumplimiento, el Pleno decidió someter al país a un proceso de seguimiento intensificado, lo que significa que Chile, cada seis meses, deberá dar cuenta de los avances para superar las deficiencias detectadas (GAFILAT, 2021).

En lo que respecta al FP, los hallazgos y acciones recomendadas por el Gafilat son las siguientes:

<p>Cumplimiento Técnico Recomendación 7: Sanciones financieras dirigidas relacionadas a la proliferación</p>	<p>Recomendación N°7 (Sanciones financieras dirigidas relacionadas con la proliferación) Parcialmente Cumplida³².</p> <p>El país cuenta con un marco para aplicar medidas de SFD por FP. Sin embargo, el régimen cuenta con las siguientes deficiencias:</p> <ul style="list-style-type: none"> (i) Existen dudas en cuanto a si el sistema permite la implementación sin demora³³ de las SFD. (ii) La implementación de las medidas de congelamiento puede ser ordenada solo respecto de los S.O. de la Ley N°19.913 y no con alcance general. (iii) Existen dudas acerca de si podría revocarse la medida de congelamiento del artículo 38° de la Ley N°19.913 más allá de los casos de homonimia o remoción de la lista. (iv) El marco normativo no requiere que la obligación de aplicar SFD recaiga sobre todas las personas naturales y jurídicas del país. (v) Se advierten limitaciones en cuanto al alcance de los bienes objeto del congelamiento en el marco de la Ley N°19.913. No se evidencia que se hayan implementado procedimientos de conocimiento público para presentar solicitudes de remoción de las listas de las RCSNU de FP, de acuerdo con lo requerido por el criterio, por lo que no se prevén procedimientos que permitan a las personas y entidades listadas presentar una petición de remoción del listado al Punto Focal, de acuerdo con la Resolución 1730 del CSNU.
<p>Efectividad Resultado Inmediato II: “A las personas y entidades involucradas en la proliferación de armas de destrucción masiva se les impide recaudar, trasladar y utilizar fondos, a tono con las Resoluciones del Consejo de Seguridad de las Naciones Unidas relevantes”</p>	<p>Resultado Inmediato II (Sanciones financieras de FP) Nivel Moderado³⁴.</p> <p>Hallazgos principales:</p> <ul style="list-style-type: none"> • Chile cuenta con normativa que le permite imponer SFD relacionadas con la FP. No obstante, en ciertos supuestos, la implementación sin demora de las medidas podría verse afectada por las etapas previstas en el procedimiento respectivo y por las deficiencias identificadas, si bien debe notarse que los sectores de mayor materialidad del sector financiero cuentan, en general, con posibilidad de actuar con prontitud. • El país, a través de la UAF, disemina de manera oportuna las listas del CSNU y sus actualizaciones, que pueden ser consultadas en su sitio web por todos los S.O. de la Ley N°19.913. • Los S.O. financieros de la Ley N°19.913 parecen tener un nivel acertado sobre las obligaciones relacionadas con la implementación de las SFD en materia FP. Sin embargo, el sector de las APNFD tiene oportunidades de mejora. <p>Acciones recomendadas:</p> <ul style="list-style-type: none"> • Reformar el marco normativo para garantizar la implementación sin demora de SFD por FP de manera inmediata por parte de todos los S.O. de la Ley N°19.913. En particular: modificar la normativa para que las SFD puedan ser implementadas sin demora, ampliar el alcance de las medidas de congelamiento para que se apliquen de forma general y no solo por el S.O. reportante de la UAF, establecer la prohibición general de suministro de fondos u otros activos a personas o entidades designadas o para su beneficio, ampliar el plazo de vigencia y abordar las demás deficiencias técnicas identificadas en relación con la Recomendación N°7. • Emitir guías adicionales y crear mecanismos de concientización y capacitación para los S.O. de la Ley N°19.913, especialmente para las APNFD, para propiciar la consulta de las listas del CSNU de manera permanente. Se debe profundizar en el trabajo con los S.O. no financieros, a fin de que comprendan la importancia de su rol en la prevención del FP, así como el que ya se realiza con los delitos de LA y el FT. • Asegurarse de que todos los S.O. de la Ley N°19.913 estén sujetos a monitoreo permanente y sanciones por infracciones en sus obligaciones respecto de la implementación de las Resoluciones del SNU sobre FP. • Establecer un sistema que notifique o alerte a los S.O. de la Ley N°19.913 cuando exista un cambio en las listas del CSNU.

ANÁLISIS DE LOS REPORTES DEL GRUPO DE EXPERTOS QUE APOYA AL COMITÉ DE SANCIONES 1718 Y MENCIONA A CHILE EN MATERIA DE FINANCIAMIENTO DE LA PROLIFERACIÓN³⁵

Para esta ENR-FP se recopiló y analizó información registrada en 10 reportes publicados por el Grupo de Expertos del Comité 1718 del CSNU entre los años 2015 y 2021³⁶.

El contenido estuvo relacionado con actividades comerciales y financieras realizadas por la RPDC de manera ilícita, junto con las diversas maniobras de evasión que intentó emplear para violar las sanciones impuestas por el CSNU. Asimismo, se consideró el comercio exterior con Irán.

A continuación se expone el siguiente cuadro que sintetiza las menciones de Chile por el Grupo de Expertos del Comité 1718 del CSNU, junto con la información complementaria que se dispone:

TABLA 1
Menciones del Grupo de Expertos y antecedentes de Chile en materia de FP

Fuente: Elaboración propia UAF.

Acciones / Antecedentes	Grupo de expertos	Antecedentes Chile
Operaciones comerciales	Chile figura como uno de los países que ha realizado operaciones comerciales (de importación y/o exportación) tanto con la RPDC, como con Irán en el periodo considerado. Dichas operaciones comerciales habrían tenido relación con bienes de lujo (vino) e importación de materias primas (carbón/hierro) ³⁷ (CSNU, 2018).	RPDC: Según cifras oficiales del Servicio Nacional de Aduanas, el país no ha tenido intercambio comercial con la RPDC en el periodo considerado. Las cifras informadas por el Grupo de Expertos respecto de las citadas operaciones corresponden a un error de registro por parte de la institución nacional competente en esta materia, considerando como país contraparte a la RPDC, cuando en realidad correspondía a Corea del Sur. Irán: Se han realizado operaciones comerciales entre Chile e Irán ³⁸ , principalmente exportaciones de productos forestales y sus derivados, y otros productos no mineros. Mientras que las importaciones, fundamentalmente, son aquellas derivadas del petróleo (SNA, 2020a) (SNA, 2020b).
Ciberataques u otras acciones similares	El reporte del Grupo de Expertos abordó tres ciberataques ocurridos en el país contra entidades financieras, posiblemente ejecutados por grupos de hackers ligados a la RPDC. (CSNU, 2019a) (CSNU, 2019b) (CSNU, 2021)	Chile efectivamente ha sido objeto de ciberataques contra instituciones financieras, incluido un banco que en el año 2018 sufrió un secuestro de datos y dinero (más de USD 10 millones). A través de las investigaciones, el banco confirmó el origen internacional del ataque, incidente que fue reportado a las autoridades y jurisdicciones correspondientes.

Por tanto, dadas las situaciones descritas en los informes, en primera instancia Chile ha sido identificado como una eventual fuente de ingresos para la RPDC, ya sea mediante actividades comerciales restringidas o prohibidas, o como objetivo de ciberataques que buscarían obtener fondos provenientes de instituciones financieras, los que habrían sido ejecutadas, presuntamente, por actores ligados a la RPDC.

Por otro lado, es importante precisar los siguientes puntos respecto del desempeño de Chile en materia de FP. En este sentido, en los informes del Grupo de Expertos que apoya al Comité de Sanciones 1718, Chile:

- No es identificado como país de tránsito de movimientos financieros realizados por personas/entidades designadas o relacionados.
- No se le identifica ni menciona en los reportes analizados como país de tránsito de mercancías restringidas o prohibidas con origen/destino en la RPDC, ni con actividades relacionadas con corresponsalía bancaria, operatoria financiera de diplomáticos o personas/entidades ligadas a ese Estado.
- No se le asocia con la utilización de personas jurídicas, situadas en el país, para desarrollar maniobras de ocultamiento de beneficiarios finales, ni el uso de productos de compañías de seguros.
- No está mencionado como un país vulnerado en su infraestructura financiera o corporativa por parte de personas/entidades designadas o relacionadas con actividades de FP.
- No ha sido involucrado en operaciones o uso de productos o servicios financieros en operaciones comerciales que incluyan mercancía sensible o de uso dual, ni otra relación de negocios (por ejemplo, restaurantes) vinculada con trabajadores de la RPDC.

CAPÍTULO IV: AMENAZAS DEL FINANCIAMIENTO DE LA PROLIFERACIÓN



CAPÍTULO IV: AMENAZAS DEL FINANCIAMIENTO DE LA PROLIFERACIÓN

Con el objetivo de identificar las amenazas de FP en Chile, se han considerado documentos elaborados por el GAFI, RUSI y el Grupo de Expertos que apoya al Comité de Sanciones 1718 que supervisa las sanciones impuestas por el CSNU a la RPDC.

En el periodo de análisis, la RPDC es indicado como el mayor foco de amenazas en torno a la proliferación y su financiamiento. Esto debido a su continuo desarrollo de ADM, pese a las distintas sanciones sectoriales y financieras que ha sido objeto. En este escenario, Chile podría quedar, eventualmente, expuesto.

En relación con Irán, dado que se encuentra en un régimen especial, el régimen de sanciones impuesto por el CSNU a Irán se encuentra en pausa bajo el compromiso del cumplimiento del PAIC. En términos comerciales, Chile no realizó operaciones de comercio con Irán relacionadas con cualquier tipo de bien asociado a equipos, materiales o tecnología de tipo nuclear, de misiles, naves, vehículos de combate, sistemas de artillería, o la prestación por sus nacionales o desde su territorio, de capacitación técnica, servicios financieros, asesorías relacionadas con el suministro, venta, transferencia, fabricación, mantenimiento o utilización de las armas y materiales conexos mencionados, entre otras. Tampoco mantiene medidas de sanciones financieras dirigidas asociadas con personas/entidades designadas de este país⁴⁰.

Por tanto, las amenazas de FP descritas en este apartado tienen su origen en las actividades y operaciones realizadas por la RPDC identificadas en los reportes del Grupo de Expertos. Las amenazas se identificaron de la manera descrita, debido a que Chile no cuenta con antecedentes de casos o situaciones relacionadas con el FP, ya sean operaciones sospechosas, investigaciones, sentencias, entre otros. Por tanto, el análisis de esta información se vincula con los potenciales riesgos que podría enfrentar el país.

Las amenazas identificadas se clasificaron en tres categorías⁴¹:

1. Productos y servicios financieros relacionados con el comercio de bienes sensibles a la proliferación:

Corresponden a aquellos que pueden usarse de manera directas o modificados en el desarrollo de ADM, de sus sistemas vectores y de materiales relacionados. También incluyen a productos/servicios financieros vinculados con operaciones de comercio exterior y su transporte.

2. Actividades de obtención de fondos (lícitas e ilícitas):

Generan ingresos para eventualmente financiar la adquisición o desarrollo de ADM o de sus sistemas vectores.

3. Infraestructura financiera y corporativa que apoye el movimiento financiero y de bienes:

Cualquier tipo de infraestructura financiera o corporativa que sustente a las actividades mencionadas en las dos categorías anteriores. Incluye la provisión de activos o servicios financieros a personas/entidades sujetas a sanciones financieras directas de FP.

En este sentido, se realizó un análisis de los reportes publicados por el Grupo de Expertos, identificando el conjunto de operaciones que podrían ser clasificadas en alguna de las tres categorías anteriormente señaladas y que, a su vez, constituirían amenazas eventuales para Chile, de acuerdo con su naturaleza. Estas acciones permitieron a la RPDC generar y obtener ingresos para, eventualmente, financiar sus programas de desarrollo de ADM, sistemas vectores o de material relacionado, y para acceder al sistema financiero internacional a través de diversas maniobras de evasión de las sanciones aplicadas.

Es así como no se identificaron amenazas relacionadas con la primera categoría expuesta, esto es, asociadas con productos y servicios financieros relacionados con el comercio de

bienes sensibles a la proliferación. En cambio, se identificaron cuatro amenazas relacionadas con actividades de obtención de fondos (lícitas e ilícitas), y tres asociadas con el uso de

infraestructura financiera y corporativa que apoye el movimiento financiero y de bienes, según el siguiente detalle:

TABLA 2
Amenazas identificadas, según categoría

Fuente: Elaboración propia UAF.

Tipo amenaza relacionada con ⁴² :	Amenaza
Actividades de obtención de fondos (lícitas e ilícitas).	1. Ciberataques, utilización de plataformas de tecnología de la información y operación con activos virtuales (entre otras actividades similares).
	2. Exportación/venta de carbón, hierro, acero, arena, entre otros.
	3. Artículos de lujo (particularmente, fabricación de ropa deportiva en la RPDC y otro tipo de vestimenta para la exportación). Bebidas alcohólicas (entre otras) ⁴³ .
	4. Envío de trabajadores al extranjero o presencia de ciudadanos RPDC (o países de riesgo).
Uso de infraestructura financiera y corporativa que apoye el movimiento financiero y de bienes.	5. Utilización de personas jurídicas (incluidas ficticias), por ejemplo, para ocultar información sobre los beneficiarios finales.
	6. Actividad bancaria: Representantes de bancos de la RPDC en el extranjero y operatoria financiera de diplomáticos y otros funcionarios de la RPDC.
	7. Uso de productos de compañías de seguros.

A continuación, se presenta una descripción general de las siete amenazas identificadas, que incluyen los métodos utilizados por la RPDC para obtener ingresos de manera ilícita y acceder al sistema financiero internacional.

1. Ciberataques, utilización de plataformas de tecnología de la información y operación con activos virtuales (entre otras actividades similares).

En el periodo, según lo registrado en los reportes del Grupo de Expertos, la RPDC ha generado recursos ilícitos para financiar sus programas de ADM, a través de ciberataques dirigidos contra instituciones financieras, de minería e intermediarios de activos virtuales.

Los agentes de la RPDC roban este tipo de activos con el propósito de blanquear los recursos que provienen de la evasión de sanciones financieras. Asimismo, existirían nexos entre la RPDC y distintos grupos dedicados a delitos cibernéticos que desarrollan e implementan, entre otras materias, un conjunto de herramientas maliciosas para realizar ataques informáticos a diversas instituciones.

Al año 2019, estaban siendo investigados a lo menos 35 ataques en 17 países (incluidos 2 casos en Chile), en el contexto de evasión de las sanciones financieras determinadas en las resoluciones del CSNU. Estos tuvieron como objetivos instituciones financieras y plataformas de activos virtuales.

En el año 2020 se registraron ciberataques contra industrias del sector de defensa a nivel global, perpetrados por actores ligados a la RPDC. En estos intentaron acceder a tecnología militar y extraer información con el propósito de generar ganancias ilícitas. También se identificaron ataques hacia empresas farmacéuticas que desarrollaban vacunas contra la Covid-19.

Para la obtención de criptoactivos de forma ilícita, los métodos utilizados por actores ligados a la RPDC fueron:

- La utilización del sistema de la Sociedad para las Comunicaciones Financieras Interbancarias Internacionales (SWIFT, por su sigla en inglés) para realizar transferencias, accediendo a la infraestructura bancaria.
- Acceso a infraestructura administradora de la red de cajeros automáticos.
- Minería y robo de activos virtuales.
- Operaciones de ingeniería social⁴⁴.
- Uso de programas informáticos maliciosos⁴⁵.
- Esquemas de ofertas de empleo (falsas), a través de diversos mecanismos, incluido el phishing por correo electrónico⁴⁶.
- Esquemas de phishing y phishing focalizado o “spearphishing”, en particular enfocados hacia intermediarios de criptoactivos.

Para transformar los activos virtuales obtenidos de manera ilícita en moneda fiduciaria, la RPDC utilizó redes de proveedores de servicios de activos virtuales sometidos a escasa regulación, y otros servicios de intermediación extraoficiales⁴⁷. Con este motivo, la RPDC continuó focalizándose en proveedores de activos virtuales OTC (fuera de rueda), principalmente localizados en China. También apuntaron hacia empresas que prestan servicios P2P⁴⁸ o aquellas que no requieren información de debida diligencia del cliente (DDC).

En Chile, el reporte del Grupo de Expertos abordó dos casos ocurridos el año 2018, y uno en proceso de investigación del año 2020:

- El primero involucra el robo de USD 10 millones desde una entidad bancaria nacional a través de transacciones SWIFT no autorizadas, cuyo destino fueron principalmente cuentas en Hong-Kong. Para lograr su objetivo, los delincuentes distrajeron la atención de los funcionarios bancarios mediante la inutilización de alrededor de 9.000 computadores, a través de un programa malicioso. Según información de Estados Unidos, los autores estarían vinculados con una organización que es parte de la Oficina General de Reconocimiento de la RPDC.
- El segundo se ejecutó bajo la aplicación de ingeniería social y su objetivo fue la red interbancaria “Redbanc”. A través de una red social, los hackers contactaron a un empleado de la compañía simulando una oferta laboral. Realizaron una entrevista en español vía teleconferencia y una vez obtenida su confianza, lograron que descargara un programa malicioso (malware). De acuerdo con la empresa, este ataque no tuvo impacto y los servicios pudieron seguir operando con normalidad.
- El tercer ataque (septiembre de 2020) fue a otra entidad bancaria nacional. A partir de fuentes de información públicas, el Grupo de Expertos indicó que está investigando presuntos ataques en los que habría participación de actores relacionados con la RPDC.

En este sentido, se ha indicado que hackers ligados a la RPDC estarían involucrados en este ciberataque, dada su sofisticación, magnitud y escala. Esto según información de conocimiento público, a través de medios de comunicación⁴⁹ especializados en economía/ finanzas y empresas de ciberseguridad.

Los ciberataques ocurridos se podrían categorizar de bajo impacto, tanto por los montos involucrados como por la infraestructura financiera/tecnológica afectada y la disrupción operacional ocasionada.

Sin embargo, no es posible descartar la ocurrencia de ciberataques que puedan tener mayores consecuencias en comparación con los ocurridos. No solo respecto de la dimensión de los montos, sino que afecten la continuidad operacional de los servicios financieros asociados.

Este punto constituye uno de los riesgos relevantes que enfrentaría Chile respecto del FP, a nivel de la seguridad informática, institucional y sectorial.

2. Exportación/venta de carbón, hierro, acero, arena, entre otros.

Respecto de la RPDC, las principales mercancías exportadas de manera ilegal fueron el carbón, así como los minerales, hierro, arena y productos textiles. Para el periodo analizado, la RPDC exportó carbón junto con otros ítems prohibidos, mayoritariamente, hacia zonas o aguas territoriales de jurisdicción china.

La RPDC modificó su forma de transporte marítimo de carbón, ya que se efectuó a través de transbordos entre buques. Para eludir las sanciones establecidas en las diversas resoluciones del CSNU, traspasó la carga desde embarcaciones con bandera de la RPDC, o controlados por este país, hacia naves chinas⁵⁰.

Mediante diversos métodos, incluso combinados, ha buscado ocultar el real origen del carbón u otros bienes comercializados, y esconder sus buques del rastreo marítimo en las bases de datos. Estos patrones de operación se han mantenido durante el periodo analizado, caracterizándose de la siguiente forma:

- Uso de redes de intermediarios a través de empresas de pantalla o ficticias en otros países.
- Rutas de navegación engañosas.
- Manipulación o cese de las señales de transmisión de localización de buques.
- Manipulación o adulteración de las banderas de los buques, de los números de identidad o los tipos de buques.
- Uso de documentos falsos.

Según el Grupo de Expertos, en el año 2017, Chile figuró con importaciones por alrededor de USD 35.000 en carbón/hierro con origen en la RPDC. Cabe aclarar que estas cifras informadas por el Grupo de Expertos respecto de las citadas operaciones, corresponden a un error de registro por parte de la institución nacional competente en la materia, considerando como país contraparte a la RPDC, cuando en realidad correspondía a Corea del Sur, por lo que es posible señalar que no existió comercio exterior de estas mercancías con la RPDC en el periodo señalado.

3. Artículos de lujo (particularmente, fabricación de ropa deportiva en la RPDC y otro tipo de vestimenta para la exportación), bebidas alcohólicas (entre otras).

En el periodo revisado se identificó la exportación/importación de bienes destinados, eventualmente, al financiamiento directo o indirecto de programas de ADM, incluso por parte de personas/entidades designadas. En particular, en lo concerniente a la transacción de mercancías para generación de ingresos se reconocieron:

- Al menos desde el año 2014, la RPDC se dedica a la fabricación y exportación de ropa deportiva de lujo⁵¹ u otro tipo de vestimentas. Con este objetivo, utiliza mano de obra de bajo costo y genera ingresos por parte de empresas creadas en conjunto con firmas extranjeras.

- Envíos de bebidas alcohólicas⁵² a la RPDC. Los reportes indicaron ventas de estos productos por parte de algunos países europeos y Chile⁵³.

Respecto de este último ítem, en el periodo comprendido entre junio de 2016 y agosto de 2017, el Grupo de Expertos consignó ventas de bebidas alcohólicas por parte de Chile, en particular vino, por un monto aproximado de USD 290 mil. Sin embargo, según cifras oficiales de comercio exterior publicadas por el Servicio Nacional de Aduanas, no se registró comercio con la RPDC en el periodo analizado entre 2016 y 2021⁵⁴.

Considerando lo expuesto anteriormente, Chile no registró actividad de comercio exterior con la RPDC, al menos desde el año 2012, según cifras estadísticas del mencionado Servicio.

Por tanto, es nula la exposición de Chile ante la RPDC como contraparte en cuanto a actividades comerciales restringidas o prohibidas mediante las resoluciones del CSNU. De esta manera, el país cumple con las diversas sanciones sectoriales y comerciales dispuestas en las Resoluciones del CSNU contra la RPDC.

4. Envío de trabajadores al extranjero o presencia de ciudadanos de la RPDC (o países de riesgo).

El envío de trabajadores al extranjero para generar ingresos es otra de las formas de recaudación de fondos de la RPDC, identificadas en los reportes del Grupo de Expertos⁵⁵. Los trabajadores de la RPDC se desempeñarían en diferentes rubros, como en las áreas de tecnologías de la información (TI)⁵⁶, construcción, arte, salud, deporte, hotelería, textil, electrónica y agricultura. También se identificaron restaurantes de la RPDC en distintos países del sudeste asiático que, en algunos casos, operaban de forma posterior al plazo de repatriación.

A modo de ejemplo, en Ecuador se registraron profesionales de la acupuntura y traductores, cuyo contrato en el país vencía en mayo de 2020.

Ecuador informó que se aplicaron las medidas para terminar los contratos de estos trabajadores y repatriarlos a la RPDC. En otros casos se han detectado profesionales de la salud en países de Asia y África.

Uno de los métodos utilizados es el ingreso a los países en calidad de turistas o con visas de estudiante, situación que se ha identificado en Rusia y, eventualmente, en China⁵⁷. Se indicó también que la legislación nacional de varios países permite la generación de ingresos a estos trabajadores, bajo determinadas circunstancias.

En el caso de Chile, por medio de su Misión Permanente ante la ONU, se informó que, en el periodo comprendido entre los años 2005 y 2014, el país entregó 63 visas sujetas a contrato a nacionales de la RPDC. De estas, ninguna se encuentra vigente a junio de 2020 y desde el año 2015 en adelante no se han otorgado visas de esta naturaleza a nacionales de la RPDC.

Respecto de la cooperación científica/técnica con personas o grupos, patrocinados por la RPDC, este tipo de actividades están suspendidas bajo las disposiciones de la Resolución 2321 del CSNU del año 2016. En este sentido, la Misión Permanente de Chile señaló, en abril de 2017⁵⁸, que no mantiene este tipo de programas o cooperación con las personas o grupos mencionados patrocinados por la RPDC, o que la representen oficialmente.

Considerando lo expuesto anteriormente, Chile no registra en su territorio ciudadanos de la RPDC en calidad de turistas, estudiantes o trabajadores. En este sentido, considerando las diversas sanciones dispuestas en las Resoluciones del CSNU respecto de la RPDC y sus personas/entidades, Chile presenta una menor probabilidad de ocurrencia de ingreso de ciudadanos de la RPDC por vías legales o formales sin el debido registro y motivos plausibles de ingreso.

Junto con lo anterior, se tiene una menor probabilidad de ingreso ilegal, particularmente por su lejanía geográfica, escasos motivos de

ingreso relacionados con arraigo familiar, estudios, o asociados a actividades comerciales, dada la inexistencia de estas.

Además, Chile no mantiene misiones o instalaciones diplomáticas de la RPDC en el país que justifiquen el ingreso/salida de dichos ciudadanos al territorio nacional.

5. Utilización de la banca corresponsal y de personas jurídicas para ocultar información sobre los beneficiarios finales.

La información recibida por el Grupo de Expertos señala que la RPDC ha accedido al sistema financiero internacional para realizar pagos a proveedores y ocultar la información sobre los beneficiarios finales en sus operaciones. Entre los métodos utilizados se cuentan las empresas ficticias, joint-ventures, uso del nombre de asociados extranjeros, servicios de criptoactivos, utilización de banca corresponsal, representantes bancarios en el extranjero, cuentas off-shore, entre otros.

Se ha constatado que, de forma involuntaria, empresas de servicios corporativos tales como instituciones financieras a través de servicios de la banca corresponsal, han prestado apoyo o asesoría a personas y/o entidades ligadas a la RPDC, para el desarrollo de actividades prohibidas. En este sentido, se constató que empresas y misiones diplomáticas de la RPDC abrieron cuentas bancarias y prestaban los mismos servicios que entregaría una institución financiera.

Estos métodos y técnicas de ocultamiento tienen como objetivo a Estados con débiles estándares de supervisión financiera, normas y/o regulaciones. Según indicó uno de los reportes del Grupo de Expertos, “los ingresos ilícitos generados por las actividades de evasión de sanciones y lavadas a través de estas redes apoya, tanto directa como indirectamente, a los programas de ADM y misiles balísticos de la RPDC”.

En cuanto a las relaciones de banca corresponsal en Chile, estas instituciones cuentan con un marco jurídico que les permite enfrentar las relaciones de corresponsalía, entre otras materias, con la banca transnacional, obtener información para una mayor comprensión de los negocios, verificar la reputación, la calidad de su supervisión, y evaluar políticas y procedimientos para la detección de operaciones sospechosas de LA/FT.

6. Actividad bancaria: Representantes de bancos de la RPDC en el extranjero y operatoria financiera de diplomáticos y otros funcionarios de la RPDC.

Estas actividades permiten la evasión de sanciones por parte de la RPDC, al realizar operaciones comerciales contrarias a las disposiciones de las Resoluciones del CSNU.

Los representantes de bancos de la RPDC controlan cuentas bancarias y realizan operaciones con altos montos de dinero en efectivo. Las principales técnicas de evasión empleadas por los representantes de la RPDC, que operan a nivel internacional para abrir cuentas bancarias, incluyeron el uso de terceros extranjeros, de empresas ficticias y, en algunos casos, usaron las propias embajadas para sus operaciones bancarias.

Asimismo, la investigación del Grupo de Expertos reveló deficiencias en la DDC de algunas instituciones financieras extranjeras. También se observó la triangulación de pagos a través de representantes de bancos en el extranjero de la RPDC en operaciones financieras relacionadas con el comercio de carbón y petróleo.

También se ha intentado el acceso a fondos en cuentas congeladas, a través de funcionarios(as) en embajadas y documentación sospechosa/falsa. Para evitar sanciones tales como la congelación de activos o el límite de cuentas bancarias, utilizan a familiares, empresas ficticias y operan en otras jurisdicciones para abrir cuentas. Al abrir estas cuentas, también utilizan

diferentes direcciones, nombres de empresas ficticias o de distintos miembros de la familia, diferentes versiones de un nombre, etcétera.

Asimismo, se ha constatado la existencia de diplomáticos de la RPDC que adquieren artículos prohibidos a nombre de empresas relacionadas con entidades designadas. Para esto, utilizan a terceros países con motivo de evadir sanciones y remitir los bienes a la RPDC, o utilizan la identificación ciudadana de otro país para cumplir con ese objetivo.

A través de la nota verbal de abril de 2017, la Misión Permanente de Chile ante ONU informó que no existían instituciones bancarias, ni sucursales o representaciones de bancos de la RPDC en Chile, en cumplimiento con lo dispuesto en el párrafo 31 de la resolución 2321 (2016) del CSNU⁵⁹.

En este ámbito en específico, la exposición del sistema bancario chileno es baja debido a la inexistencia de instituciones bancarias, sucursales o representaciones de bancos de la RPDC. Por tanto, en el país, el riesgo de actividades de FP a través de esta vía directa de operaciones de instituciones financieras ligadas a la RPDC es inexistente.

En términos de requerimientos para ingresar al mercado financiero doméstico, el funcionamiento de la mayoría de las instituciones financieras en el país es autorizado por sus supervisores prudenciales. A modo de ejemplo, la Comisión para el Mercado Financiero (CMF)⁶⁰, junto con la Superintendencia de Casinos de Juego, tienen procedimientos para otorgar licencias de operaciones de las entidades bajo su regulación prudencial. Adicionalmente, todas las entidades financieras deben registrarse ante la UAF, la cual tiene la facultad para aceptar o denegar el registro (casi en su totalidad, porque la persona natural o jurídica no ejerce el giro expresamente señalado en el artículo 3° de la Ley N°19.913).

En particular, en el caso del sector bancario, el otorgamiento de licencia tiene tres etapas:

autorización provisional, autorización de existencia y autorización de funcionamiento. Las entidades deben presentar diversos documentos que acrediten la información de solvencia, capital mínimo exigido, estatutos de la sociedad, estructura, procedimientos y controles, entre otras materias.

7. Uso de productos de compañías de seguros

Según la información del Grupo de Expertos, han existido casos en que las compañías aseguradoras han otorgado cobertura a buques que transportan mercancía prohibida y/o productos de ahorro o seguros de vida a personas naturales. En algunos casos, se constató la usurpación de identidad de buques relacionados con la RPDC; en consecuencia, compañías de seguros brindaron cobertura en desconocimiento de tales hechos.

En otra ocasión, se señaló que un diplomático de la RPDC abrió cuentas bancarias en instituciones europeas, utilizando diversas técnicas de evasión y luego contrató seguros de vida con ahorro, monto que pudo retirar de forma posterior.

En este sentido, según lo registrado en los reportes del Grupo de Expertos, el país no ha sido nombrado en situaciones relacionadas con esta materia.

SÍNTESIS DE LAS AMENAZAS DE FP ASOCIADAS CON CHILE

Con base en la información del Grupo de Expertos, se han identificado las siguientes amenazas que enfrenta Chile y su nivel de incidencia:

TABLA 3
Resumen de las Amenazas identificadas para el país de acuerdo a los reportes del Grupo de Expertos

Fuente: Elaboración propia UAF empleando información obtenida de los reportes del Grupo de Expertos.

(*) La situación de estas transacciones se explicó anteriormente en el apartado correspondiente.

Tipo amenaza relacionada con ⁶¹ :	Amenaza	Participación de Chile	Nivel de incidencia estimado
Actividades de obtención de fondos (lícitas e ilícitas).	1. Ciberataques, utilización de plataformas de tecnología de la información, y operación con activos virtuales (entre otras actividades similares).	Sí: 2018: Dos ciberataques a entidades financieras (métodos ramsonware e ingeniería social). 2020: Un ciberataque a una entidad financiera (método ramsonware).	Alto
	2. Artículos de lujo (particularmente, fabricación de ropa deportiva en la RPDC y otro tipo de vestimenta para la exportación). Bebidas alcohólicas (entre otras) ⁶² .	Sí: 2017: Venta de bebidas alcohólicas (vino) a personas/entidades de la RPDC (USD 290.000) (*).	Medio
	3. Exportación/venta de carbón, hierro, acero, arena, entre otros.	Sí: 2017: Importación de carbón desde la RPDC (USD 35.000) (*).	Bajo
	4. Envío de trabajadores al extranjero o presencia de ciudadanos RPDC (o países de riesgo).	No	Bajo
Uso de infraestructura financiera y corporativa que apoye el movimiento financiero y de bienes.	5. Utilización de personas jurídicas (incluidas ficticias), por ejemplo, para ocultar información sobre los beneficiarios finales.	No	Bajo
	6. Actividad bancaria: Representantes de bancos de la RPDC en el extranjero y operatoria financiera de diplomáticos y otros funcionarios(as) de la RPDC.	No	Bajo
	7. Uso de productos de compañías de seguros.	No	Bajo

Con lo anterior, el nivel de incidencia estimado se asignó de acuerdo con los siguientes criterios:

- **Alto:** Está asociado a actividades o hechos (ciberataques) en los que efectivamente ha estado involucrado el país, o las operaciones han sido nombradas en los informes del Grupo de Expertos. Si bien las actividades registradas han tenido un impacto menor, tanto a nivel de las entidades involucradas como para el sistema financiero en su conjunto, no es posible descartar que en un futuro puedan ocurrir situaciones de mayor impacto, tanto a nivel individual en relación con ciertas entidades, como a nivel sistémico respecto del sistema financiero doméstico.
- **Medio:** Si bien el país ha sido mencionado en actividades relacionadas con operaciones comerciales (de importación o exportación) con la RPDC, se ha visto expuesto en menor medida a estas operaciones, tanto a nivel de actividades como en los montos asociados. Asimismo, tal como se mencionó anteriormente, según datos del Servicio Nacional de Aduanas, no existió intercambio comercial con la RPDC en el periodo mencionado, lo cual contrasta con la información registrada por el Grupo de Expertos en sus reportes.
- **Bajo:** Respecto de las actividades u operaciones mencionadas, el país no mostró una exposición en estas materias, según lo registrado en los reportes del Grupo de Expertos. Sin embargo, no es posible descartar una futura ocurrencia de alguno de estos hechos, dada la naturaleza de dichas actividades, en particular aquellas en las cuales la lejanía geográfica no es relevante, por ejemplo, relacionadas con la utilización de personas jurídicas ficticias para ocultar el beneficiario final de ciertas operaciones financieras.



CAPÍTULO V:
IDENTIFICACIÓN DE VULNERABILIDADES
RELACIONADAS CON EL FINANCIAMIENTO
DE LA PROLIFERACIÓN

CAPÍTULO V: IDENTIFICACIÓN DE VULNERABILIDADES RELACIONADAS CON EL FINANCIAMIENTO DE LA PROLIFERACIÓN

Según el GAFI, las personas/entidades designadas exploran nuevas y diversas formas de evadir las SFD de FP, donde el factor geográfico no es una limitante para RPDC e Irán. En los reportes del Grupo de Expertos se dio cuenta de movimientos en países de África y Europa, y se identificaron operaciones financieras en países con débiles controles antiLA/FT/FP, para encubrir el flujo de fondos⁶³.

Las vulnerabilidades podrían ser, eventualmente, explotadas con el propósito de infringir o evadir las sanciones impuestas por las Resoluciones del CSNU, por parte de personas/entidades designadas u otras relacionadas.

En este apartado se identifican las principales vulnerabilidades del país con base en los resultados expuesto en el Informe de Evaluación Mutua de Chile (IEM), y reportes que abordan el comercio exterior del país, ciberseguridad e infraestructura en tecnología de la información (TI), nuevos productos y servicios de pago. Las vulnerabilidades se asocian principalmente con:

1. Comprensión del riesgo de FP.
2. Implementación de las SFD de FP.
3. Infraestructura TI, ciberseguridad y actividades de comercio.
4. Nuevos productos y servicios de pago.

1. VULNERABILIDADES ASOCIADAS CON LA COMPRESIÓN DEL RIESGO DE FP

El IEM de Chile detectó la existencia de brechas respecto del conocimiento de los riesgos de FP, la frecuencia y/o automatización en la revisión de las sanciones del CSNU por parte de entidades reportantes de algunos sectores económicos, y la no inclusión de entidades reportantes de ciertos sectores relevantes para el Sistema Nacional ALA/CFT/CFP.

En cuanto a las obligaciones relacionadas con las SFD de FP, el IEM indicó que si bien las entidades financieras tienen un nivel aceptable en su cumplimiento, las entidades reportantes de ciertos sectores APNFD muestran un nivel de comprensión menor en estas materias, por lo que existen mayores desafíos y oportunidades de mejora en este sentido.

En esa línea, de acuerdo con lo registrado en el IEM de Chile, si bien ciertos sectores pertenecientes a las APNFD mostraron una revisión periódica de las listas de designaciones del CSNU, esta no se realizaría con la frecuencia que se estima necesario lo que, eventualmente, podría traer como consecuencia dificultades en que las acciones de congelamiento de activos se realicen sin demora, en caso de existir coincidencias en listas.

Asimismo, algunas APNFD tales como los notarios y las empresas de gestión inmobiliaria, no cuentan con sistemas o procesos automatizados que emitan alertas cuando se produzcan cambios en las listas de designaciones. Ello facilitaría una pronta detección de coincidencias de nombres en listas y una verificación continua que traería como consecuencia una mayor rapidez en los procesos de reporte de dichas actividades.

El IEM de Chile también identificó como una deficiencia la no inclusión en calidad de entidades reportantes a las empresas exportadoras de materiales de uso dual y cualquier otro actor involucrado en este rubro, los que ejercen corretaje internacional de material sensible. Junto con estos, el IEM precisó que tampoco la ley considera como entidades reportantes de la UAF a los abogados, contadores, proveedores de servicios societarios y los comerciantes de piedras y metales preciosos⁶⁴.

Por tanto, las distintas deficiencias mencionadas constituyen una vulnerabilidad para que eventuales actividades u operaciones de FP no sean prevenidas, detectadas e investigadas en el país.

2. VULNERABILIDADES ASOCIADAS CON LA IMPLEMENTACIÓN DE LAS SFD DE FP

En cuanto a la implementación sin demora de las medidas de SFD de FP, el artículo 38° de la Ley N°19.913 permite el congelamiento de activos de las personas/entidades designadas derivadas de las Resoluciones del CSNU relacionadas con el FP. De manera general, el mecanismo involucra que la UAF solicite a la Corte de Apelaciones las medidas de congelamiento de activos en un lapso de 24 horas, desde la recepción de la información proveniente de los sujetos obligados.

A su vez, la Corte debe resolver en un plazo no mayor a 24 horas la solicitud, mientras que la vigencia de las medidas adoptadas es de máximo 30 días, prorrogables por resolución fundada. Ya decretadas estas medidas de congelamiento de activos, la UAF comunica a la entidad reportante las acciones adoptadas para que las aplique en un plazo no mayor a las 24 horas.

Respecto de la implementación de las SFD de FP, el IEM indicó que el régimen antiFP del país podría exceder la noción “sin demora”⁶⁵ del estándar, debido al tiempo que existiría entre la verificación de las listas del CSNU por parte de la entidad reportante, el envío del ROS asociado y la posterior aplicación de medidas de congelamiento de activos ordenadas por los tribunales de justicia.

Alcance de las medidas de SFD de FP: El IEM indicó que en Chile no se advierten disposiciones en la legislación respecto de que el congelamiento de activos pueda ser aplicad, tal como señala el estándar a:

- Todos los activos que pertenezcan o sean controlados por las personas/entidades designadas.
- Los activos pertenecientes/controlados de manera total o en conjunto, de manera

directa o indirecta, por personas/entidades designadas.

- Los activos que provengan de otros activos pertenecientes/controlados, de manera directa o indirecta, por personas/entidades designadas.
- Activos de personas/entidades que actúan en nombre o bajo las directrices de personas/entidades designadas.

Respecto del alcance de las SFD, el IEM indicó que la obligación de aplicar estas medidas recae solo para las entidades reportantes incluidas en la legislación vigente, y no es aplicable a todas las personas naturales y jurídicas que operen en el país.

Asimismo, las medidas de congelamiento de activos son ordenadas solo respecto de la entidad que reportó la operación y no con un alcance general (por ejemplo, todo el sistema financiero).

En relación con lo anterior, la legislación chilena contempla la posibilidad de apelación, con el objetivo de revocar las medidas de congelamiento. En este sentido, el IEM manifestó dudas acerca de la revocación del congelamiento de activos en situaciones distintas a la homonimia o eliminación de las listas de designaciones de FP.

Según lo observado por el IEM, el país tampoco cuenta con disposiciones normativas que prohíban a todas las personas en el territorio nacional la provisión de activos a personas/entidades designadas.

Las situaciones mencionadas constituyen una vulnerabilidad al Sistema Nacional ALA/CFT/CFP, debido a las deficiencias normativas del país. En consecuencia, eventuales actividades de FP podrían no ser detectadas a tiempo, o aplicarse medidas de congelamiento solo sobre algunos activos de la persona/entidad designada. Lo anterior, podría suscitar esquemas de FP que permitan eludir la aplicación de SFD por parte de las entidades del país.

3. VULNERABILIDADES ASOCIADAS CON LA INFRAESTRUCTURA TI, CIBERSEGURIDAD Y ACTIVIDADES DE COMERCIO EXTERIOR

CIBERSEGURIDAD E INFRAESTRUCTURA TECNOLÓGICA DEL SISTEMA FINANCIERO EN CHILE

Los Reportes de Riesgos Globales⁶⁶ anuales publicados por el Foro Económico Mundial (FEM), en los últimos cinco años, han incluido sucesivamente a los ciberataques de gran escala⁶⁷ entre los 10 riesgos globales en términos de probabilidad de ocurrencia, y en tres de los cinco años en el top 10 en términos de impacto. Adicionalmente, entre 2019 y 2021 estos reportes han incluido a las disrupciones en la infraestructura de TI⁶⁸, en el grupo de los 10 riesgos globales en términos de impacto.

Según indican estos reportes, al año 2020 más de la mitad de la población a nivel global tenía acceso a internet, y aproximadamente 2 de cada 3 personas poseía un dispositivo móvil. Si bien lo anterior genera beneficios tanto económicos como sociales a la población, también existen situaciones que representan un riesgo significativo, tales como la falta de un marco de gobernanza tecnológica global, la inseguridad cibernética y el acceso desigual a internet, entre otras materias. Asimismo, menciona como riesgos a la incertidumbre geopolítica y geoeconómica, las cuales amenazarían los potenciales de desarrollo de las nuevas tecnologías.

De acuerdo con estos reportes del FEM, los ciberataques a infraestructura crítica han sido frecuentes en los sectores energéticos, atención de salud y transporte, los cuales han afectado incluso a ciudades completas. En Estados Unidos se estimó una escasa probabilidad de detección y enjuiciamiento, de alrededor del 0,05%. Además, se calculó que existirían más de 21.000 millones

de dispositivos tecnológicos a nivel mundial, mientras que los ataques asociados a estos dispositivos aumentaron alrededor del 300% en el primer semestre del 2019. Los daños por ciberataques podrían alcanzar los USD 6.000 millones, según la empresa de ciberseguridad Cybersecurity Ventures.

De acuerdo con el Estudio de Madurez de Ciberseguridad en Chile⁶⁹ realizado por International Data Corporation (IDC)⁷⁰, que analizó el estado de la ciberseguridad en las grandes empresas y corporaciones chilenas, a través de la medición de los avances en esta materia⁷¹, el 61% de estas empresas avanzó hacia mayores niveles de madurez, en particular en las dimensiones de procesos y tecnologías de seguridad de TI, mientras que sobre el 40% aún tiene como desafío el fortalecimiento de las habilidades de su capital humano, las capacidades asociadas a la administración del riesgo y la visión estratégica, así como también fortalecer la cultura relacionada con la responsabilidad compartida asociada a la ciberseguridad. Asimismo, el estudio indicó que las corporaciones nacionales avanzaron en mayor medida en su madurez en seguridad de TI, respecto de las grandes empresas.

Cabe señalar que los tres ciberataques registrados en Chile en el periodo considerado, involucraron ataques a través de la utilización de ransomwares, e ingeniería social, que comprometieron los sistemas y procesos informáticos de las entidades financieras afectadas.

Respecto de lo señalado previamente, en relación con el sector bancario nacional, en diciembre de 2020 entró en vigencia la actualización de normas de seguridad de la información y ciberseguridad, cuya adhesión es considerada en la evaluación de la gestión y solvencia realizada por la CMF a los bancos, en relación con los riesgos operacionales. En este sentido, se incorporó el capítulo 20-10 a la Recopilación Actualizada de Normas (RAN, Capítulo 20-10), que incluyó los lineamientos mínimos para los bancos para una adecuada gestión de los riesgos relativos a la seguridad de la información y ciberseguridad⁷².

Esta normativa considera, entre otras materias, elementos generales de gestión, gestión de riesgos de seguridad de la información y ciberseguridad, protección de activos críticos de ciberseguridad⁷³ y detección de amenazas y vulnerabilidades, además de respuesta y recuperación de las actividades ante incidentes⁷⁴.

En el marco de lo anterior, el supervisor evalúa la pertinencia del sistema de gestión de la entidad bancaria, de acuerdo con ciertos elementos tales como: la existencia de una estructura organizacional con personal especializado en lo relativo a la seguridad de la información y ciberseguridad; aprobación de políticas para la gestión de estos riesgos; un nivel aprobado de disponibilidad mínimo en la entrega de los servicios a través de plataformas tecnológicas; determinación de los activos críticos de ciberseguridad; identificación de amenazas que puedan dañar los activos de información, sus vulnerabilidades y consecuencias relacionadas con la pérdida de confidencialidad, integridad y disponibilidad, entre otros aspectos.

COMERCIO EXTERIOR Y CONTROL DE EXPORTACIONES

En materia de comercio exterior, en el periodo 2016-2020, en particular sobre los medios de transporte en que se genera este intercambio comercial, se tiene que Chile, en términos de carga (en toneladas), el 96,6% de las exportaciones y el 90,6% de las importaciones se realizaron vía marítima, seguida de la terrestre. En términos de montos, el 88,7% de los asociados a exportaciones (montos FOB) y el 76,6% de los relacionados con importaciones (montos CIF) se asociaron a transporte vía marítima seguido del aéreo, en ambos casos.

GRÁFICO 1
Part. % exportaciones e importaciones (toneladas), por tipo de transporte. 2016-2020

Fuente: Elaboración propia UAF, con datos del Servicio Nacional de Aduanas.

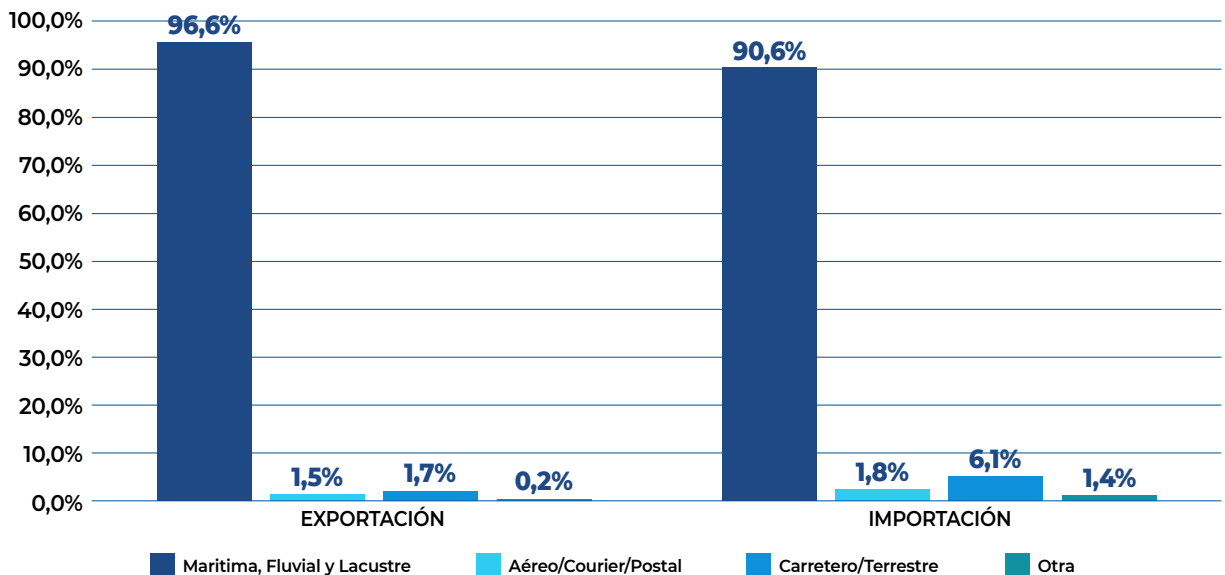
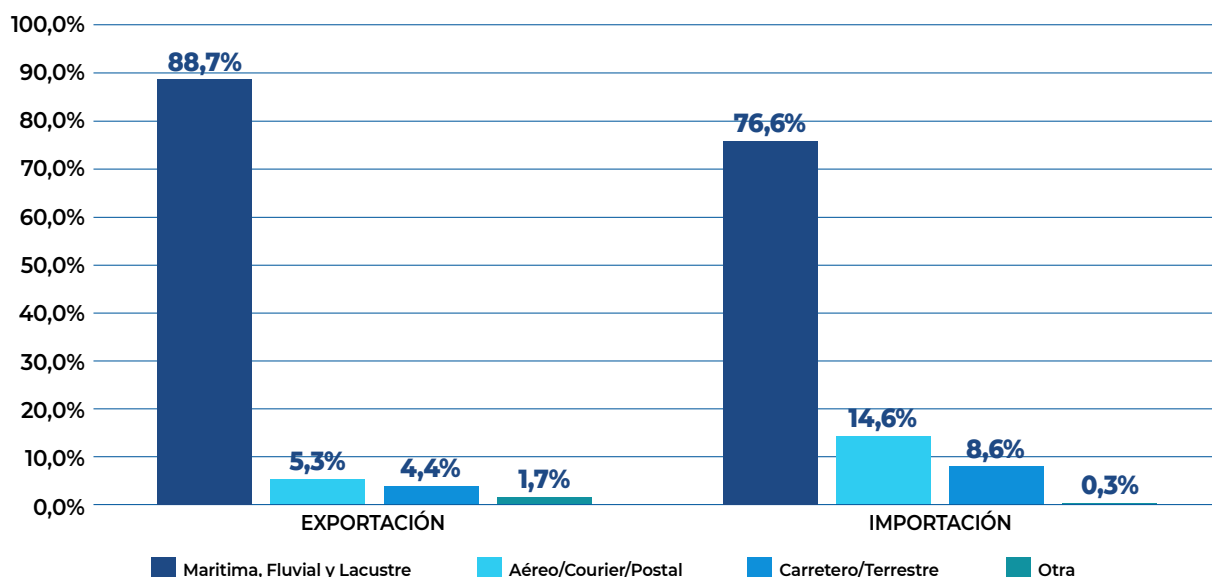


GRÁFICO 2
Part. % exportaciones e importaciones (montos), por tipo de transporte. 2016-2020

Fuente: Elaboración propia UAF, con datos del Servicio Nacional de Aduanas.



Medidas de interdicción y transporte. En el país, en las operaciones de interdicción marítima participa la Directemar, organismo de la Armada de Chile que tiene por objetivo velar por el cumplimiento de las leyes y acuerdos internacionales vigentes, y fiscalizar las actividades de índole marítimo en la jurisdicción nacional, entre otras materias. Para este tipo de operaciones, también existe una coordinación interinstitucional entre con el Servicio Nacional de Aduanas y las policías.

Chile, en 2015, por medio del Servicio Nacional de Aduanas adoptó modificaciones en un conjunto de disposiciones relacionadas con el contrabando de mercancías, las cuales apoyan el cumplimiento de las medidas de interdicción y transporte requeridas en la Resolución 2270 del CSNU, del 2016.

En relación con el comercio de mercancías prohibidas, este delito está contemplado en la normativa chilena. La Ordenanza de Aduanas, en su artículo 168°, indica que incurre en el delito de

contrabando aquel *“que introduzca al territorio nacional, o extraiga de él, mercancías cuya importación o exportación, respectivamente, se encuentren prohibidas”*. También incurre en este delito *“el que extraiga mercancías del país por lugares no habilitados o sin presentarlas a la Aduana”*.

Esta Ordenanza también establece sanciones con pena de presidio y multa cuando exista una declaración maliciosamente falsa, ya sea de origen, peso, cantidad o contenido de las mercancías de exportación. También aplica lo anterior a aquellos que falsifiquen certificaciones o análisis (ya sea material o ideológicamente) usados para establecer el origen, peso, cantidad o contenido de las mercancías de exportación. Asimismo, establece que serán sancionados los consignantes de mercancías que salen del país, *“que presenten documentos falsos, adulterados o parcializados, para servir de base a la confección de las declaraciones, determinándose a través de ellos la clasificación o valor de las mercancías”*. (Ordenanza de Aduanas, 2005)

Es importante destacar que los materiales de uso dual regulados en Chile son los categorizados como peligrosos, que representan un riesgo inminente para la población tales como armas, explosivos, entre otros. La mayoría de los otros bienes sensibles son inocuos, y corresponden, por ejemplo, a partes, componentes o piezas de equipos, los cuales no están regulados como bienes de uso dual en Chile.

Al respecto, el país no cuenta con una normativa relacionada con controles al Comercio Estratégico, lo que constituye una vulnerabilidad en este aspecto⁷⁵.

El conjunto de situaciones descritas anteriormente, esto es, deficiencias asociadas a la ciberseguridad de instituciones (públicas y privadas) en Chile, con particular atención en aquellas del sector financiero (por su eventual impacto), además de la ausencia de una normativa que regule el comercio estratégico, constituyen vulnerabilidades que podrían ser aprovechadas por las amenazas identificadas.

En el primer caso, estas vulnerabilidades podrían hacer atractivo a ciertos sectores como blancos de ciberataques, tanto para sustraer fondos de manera ilícita, como para el secuestro de datos y exigencia de pago por su liberación. En el segundo caso, la ausencia de una normativa relacionada con el material o bienes de uso dual podría generar incentivos para utilizar al país como vía intermediaria (o de paso) para comercializar y enviar al extranjero ciertas partes o componentes de uso dual sin mayor trazabilidad.

4. VULNERABILIDADES ASOCIADAS CON LOS NUEVOS PRODUCTOS Y SERVICIOS DE PAGO

Una de las vulnerabilidades tiene relación con los nuevos productos y servicios de pago que han surgido a nivel global, en línea con las nuevas tecnologías, cuyas características los hacen atractivos para el LA/FT/FP.

El reporte del GAFI denominado “Emerging Terrorist Financing Risk”, publicado en octubre de 2015, indica que los nuevos métodos de pago, electrónicos y en línea, presentan una vulnerabilidad emergente, la cual podría incrementarse a medida que aumente o se masifique su uso. Algunas de las características que comparten estos productos y servicios consisten en:

- Su acceso es posible a nivel global, sin mediar barreras fronterizas, lo que trae como consecuencia mayor rapidez en la transferencia de fondos de un país a otro.
- Dificultad en la identificación del beneficiario final de estas transacciones, independiente de que puedan ser rastreadas.

En este sentido, dentro de los productos y servicios analizados en este reporte destacaron:

- **Activos virtuales:** Diseñados para transmitir valor en línea. Sus principales características radican en que ofrecen anonimato para transferir fondos internacionalmente (tanto a nivel de usuarios como de transacciones) y permiten mover fondos rápidamente de un país a otro, por lo que los productos y servicios de pago a través de activos virtuales han llamado la atención de grupos criminales, y presentan riesgos de LA/FT/FP.

- **Tarjetas de prepago:** Corresponden a tarjetas que son precargadas con un monto fijo de dinero o valor electrónico. Según indica este informe, las tarjetas de prepago de mayor preocupación corresponden a las tarjetas de ciclo abierto, que permiten girar dinero de cajeros automáticos.
- **Servicios de pago a través de internet:** Proveen al cliente con mecanismos online para acceder a cuentas prefinanciadas, las cuales pueden ser usadas para transferir fondos a otras cuentas del mismo proveedor. Los destinatarios de los fondos podrían no tener una obligación de registrarse con el proveedor para recibir los fondos.

intermediarios (en el caso de los activos virtuales) para mover los fondos por distintas jurisdicciones, o con el afán de obstaculizar la trazabilidad de los mismos, lo que dificultaría prevenir, detectar y/o detener este flujo de activos ilícitos.

Respecto de las deficiencias detectadas en estas materias, el IEM de Chile indicó que no se advierte la identificación y evaluación de riesgos relacionados con el desarrollo de **“nuevos productos y prácticas comerciales, y al uso de nuevas tecnologías o tecnologías en desarrollo para productos nuevos o productos existentes”**.

Además, señaló que si bien se identificaron disposiciones para algunas actividades financieras, no se cuenta con un marco jurídico aplicable al sector financiero en su totalidad, con el objetivo de que realicen evaluaciones de riesgos de forma previa al lanzamiento o uso de tales productos, prácticas y/o tecnologías⁷⁶.

Por tanto, los atributos de estos nuevos productos y servicios de pago, que involucran tanto a los activos virtuales como a las tarjetas de prepago y los servicios de pago online, derivan en vulnerabilidades para el Sistema Nacional ALA/CFT/CFP. Esto, debido a que personas/entidades designadas o vinculadas a la proliferación podrían realizar actividades de FP, y utilizar estos productos y servicios, aprovechando **1)** sus características de anonimato para ocultar el origen/destino de los fondos y el beneficiario final, **2)** la rapidez en el movimiento de fondos para complejizar la trazabilidad de los mismos y **3)** la inexistencia de barreras fronterizas e



CAPÍTULO VI: IDENTIFICACIÓN DE MITIGANTES RELACIONADOS CON EL FINANCIAMIENTO DE LA PROLIFERACIÓN

CAPÍTULO VI: IDENTIFICACIÓN DE MITIGANTES RELACIONADOS CON EL FINANCIAMIENTO DE LA PROLIFERACIÓN

Según el GAFI, los elementos considerados de importancia para la mitigación del riesgo de FP, para constituir un sistema robusto para la implementación de SFD, son:

- Una evaluación nacional de riesgos (a nivel país e institucional).
- Marco normativo efectivo.
- Difusión de las sanciones a todas las entidades pertinentes.
- Intercambio de información, cooperación y coordinación nacional efectivos.
- Control y aplicación del cumplimiento.
- Capacitación regular y en profundidad (realizada por los sectores público y privado) en las temáticas de los riesgos y obligaciones respecto de las SFD de FP.

A continuación, se describen los principales mitigantes identificados, mayormente relacionados con el marco normativo vigente, en relación con el FP en Chile.

1. MONITOREO DE LAS SFD POR PARTE DEL SECTOR FINANCIERO

Las entidades reportantes tienen el deber de revisar permanentemente los listados del CSNU. También están obligadas a informar a la UAF sobre todos los actos, transacciones u operaciones realizadas (o que intenten realizar) las personas/entidades designadas en las Resoluciones del CSNU relacionadas con el FP, al detectar o existir coincidencias en las listas con este tipo de personas/entidades. La UAF, al analizar los datos recibidos, podrá requerir la implementación del congelamiento de activos de estas personas/entidades designadas al ministro de la Corte de Apelaciones,

procedimiento descrito en detalle en el artículo 38° de la Ley N°19.913.

Respecto de lo anterior, el IEM de Chile indicó que las entidades reportantes, especialmente las pertenecientes al sector financiero, son conscientes de su deber de verificar de forma permanente el listado de personas/entidades designadas establecido por el CSNU. De hecho, las instituciones financieras realizan monitoreo automático a estos listados. Asimismo, señaló que, en general, las entidades reportantes realizan estas revisiones mediante sus sistemas y que cuentan con proveedores externos y/o herramientas sistematizadas que permiten verificar las operaciones. Asimismo, destacó que, en gran parte de los Manuales de Prevención del LA/FT, las entidades reportantes tienen incluidas obligaciones de revisión de estos listados del CSNU, respecto del FPT y FP.

2. SUPERVISIÓN DEL CUMPLIMIENTO DE LAS MEDIDAS RELATIVAS A LAS SFD POR PARTE DE LAS ENTIDADES REPORTANTES

La UAF tiene la facultad de supervisar el cumplimiento por parte de las entidades reportantes de las medidas relacionadas con las SFD de FP y, en caso de incumplimiento, sancionarlas de acuerdo con la Ley.

En relación con la aplicación de las Resoluciones del CSNU, las autoridades que garantizan su cumplimiento corresponden al Ministerio de Relaciones Exteriores, que recibe las notificaciones del CSNU a través de su Misión Permanente ante la ONU, la cual se encarga de su difusión a las entidades nacionales competentes.

Según el IEM de Chile, la UAF es el supervisor principal encargado de la verificación del cumplimiento de estas medidas por parte de las entidades reportantes. La UAF también verifica la

obligación por parte de las entidades reportantes de revisión de los listados del CSNU y los Manuales de Prevención del LA/FT⁷⁷.

Entre los años 2015 y 2019, la UAF detectó 339 incumplimientos en la revisión y chequeo de los listados de las Resoluciones del CSNU por parte de las entidades reportantes, lo que derivó en 268 procesos sancionatorios terminados con sanción, lo que equivale a que el 79,1% del total de incumplimientos fue sancionado por la UAF en el periodo.

Adicionalmente, en el marco de los procesos de inteligencia financiera y monitoreo de la UAF, se emplean diversos sistemas y productos tecnológicos. En particular, cuenta con un Sistema de Monitoreo Estratégico que corresponde a un sistema de detección, búsqueda continua, recursiva de patrones y tipologías de riesgos de LA/FT/FP, generando alertas automáticas al proceso de análisis operativo, siendo capaz de analizar, de forma masiva, registros y transacciones a través de diversos algoritmos. El uso de tecnología de “machine learning” es parte central en estos procesos.

En resumen, los sistemas de monitoreo de la UAF permiten un sólido proceso de priorización-asignación y, de corresponder, a un completo proceso de análisis con alto valor agregado. Además, incorporan las listas del CSNU y también integra la información que la UAF revisa mediante una herramienta interna de análisis.

3. INEXISTENCIA DE RELACIONES DIPLOMÁTICAS ENTRE LA RPDC Y CHILE

Al año 2023, la RPDC no registra Embajada en Chile y el país tampoco tiene una Embajada en la RPDC⁷⁸.

A nivel latinoamericano, cinco países registran embajadas de la RPDC en sus territorios: Brasil, Cuba, México, Perú y Venezuela, mientras que tres de ellos tienen embajadas en territorio norcoreano (Brasil, Cuba y Venezuela)⁷⁹.

Lo anterior deriva en una baja incidencia de diplomáticos de la RPDC con presencia permanente en el país, lo cual elimina cualquier actividad asociada que pueda ser considerada como una amenaza de FP; no obstante, no elimina la posibilidad de tránsito desde países vecinos que posean embajadas.



CAPÍTULO VI:

EVALUACIÓN DE LOS RIESGOS DEL FINANCIAMIENTO DE LA PROLIFERACIÓN PARA CHILE

CAPÍTULO VII: EVALUACIÓN DE LOS RIESGOS DEL FINANCIAMIENTO DE LA PROLIFERACIÓN PARA CHILE

De acuerdo con lo expuesto anteriormente, respecto de las amenazas, vulnerabilidades y mitigantes identificadas, en Chile no se han detectado actividades relacionadas con el FP de manera directa. En este sentido, el país no cuenta con antecedentes de casos o situaciones relacionadas con el FP, ya sean operaciones sospechosas, investigaciones, sentencias, entre otros.

Sin embargo, instituciones financieras del país han sido objeto de ciberataques, presuntamente perpetrados por actores ligados a la RPDC, con el potencial objetivo de financiar actividades de proliferación de ADM. En el periodo analizado se registraron tres casos (dos casos ocurridos el año 2018 y uno el año 2020), los cuales se podrían categorizar de bajo impacto, tanto por el nivel de montos involucrados como por la infraestructura financiera/tecnológica afectada y la disrupción operacional ocasionada.

En este sentido no es posible descartar la ocurrencia de ciberataques que puedan tener un mayor impacto o mayores consecuencias, tanto a nivel de montos involucrados como en la afectación de la continuidad operacional de los servicios financieros asociados, por lo que esta amenaza en particular, dado el aprovechamiento de ciertas vulnerabilidades, tales como el nivel de comprensión del riesgo de FP por parte de las entidades reportantes, la infraestructura de TI, los nuevos productos/servicios de pago (incluyendo activos virtuales), entre otras, colocan a los ciberataques, principalmente, como uno de los factores de riesgo relevantes para Chile.

Al contrario, no se identificaron otras actividades que podrían aprovechar las vulnerabilidades mencionadas, tales como operaciones de comercio exterior de materias primas como carbón, hierro u otros minerales, presencia de ciudadanos de la RPDC con contrato de trabajo en Chile, utilización de personas jurídicas y/o actividad bancaria relacionada para mover fondos a través del país, o uso de productos de compañías de seguro.

Dado lo anterior, el **riesgo estimado de FP en Chile es bajo**, principalmente determinado por las actividades de ciberataques registradas en el país, y que podrían aprovechar en el futuro, principalmente, aquellas vulnerabilidades relacionadas con la comprensión del riesgo de FP, infraestructura TI, ciberseguridad y nuevos productos/servicios de pagos (incluidas las operaciones con activos virtuales), cuyo impacto si bien en el pasado no ha sido relevante a nivel operacional ni en la afectación de la infraestructura financiera/tecnológica involucrada, no es posible descartar un impacto mayor en posibles eventos futuros.



ANEXOS

ANEXOS

ANEXO 1: OTRAS CONVENCIONES, TRATADOS O ACUERDOS EN LOS QUE CHILE PARTICIPA RELACIONADOS CON LAS ADM.

- **Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear:** Fue adoptado por Naciones Unidas el año 2005, entrando en vigor en julio de 2007, después de que 22 países se hicieran parte. Fue ratificado por Chile el 27 de septiembre de 2010, y publicado en el Diario Oficial en abril de 2011 bajo el Decreto 252 del Ministerio de Relaciones que promulgó dicho Convenio. Este instrumento sanciona a quien "ilícita e intencionalmente" posea material radioactivo, o fabrique o posea dispositivos relacionados con el objetivo de causar la muerte o daños, incluidos a bienes y medio ambiente. También sanciona la amenaza (verosímil) utilizando este tipo de material o dispositivo, y la solicitud ilícita bajo amenaza de los mismos, la participación como cómplice, organizador/instigador o que contribuya en los actos mencionados anteriormente.
- **Convención sobre la Protección Física de los Materiales Nucleares:** En 1980 esta Convención quedó abierta para la firma de los estados, entrando en vigor en 1987 cuando 21 estados la habían ratificado. Chile depositó el instrumento de Adhesión el 27 de abril 1994. Mediante la publicación en el Diario Oficial del Decreto 1.121 del Ministerio de Relaciones Exteriores entró en vigencia en nuestro país el 17 de octubre de 1994. En julio de 2005, los Estados Parte de la Convención aprobaron una enmienda a la misma, la cual entró en vigor en mayo de 2016. *Mientras que las obligaciones de protección física previstas en la Convención abarcaban los materiales nucleares durante su transporte internacional, la Enmienda (2005) estableció una obligación jurídicamente vinculante de los Estados Partes de proteger las instalaciones y los materiales nucleares para su uso, almacenamiento y transporte interno con fines pacíficos. Asimismo, prevé una mayor cooperación entre los Estados en lo que se refiere a la adopción rápida de medidas para localizar y recuperar materiales nucleares robados u objeto de contrabando, mitigar cualesquiera consecuencias radiológicas derivadas de sabotajes y prevenir y combatir delitos conexos. La Convención y su enmienda son los únicos instrumentos internacionales jurídicamente vinculantes a escala internacional en la esfera de la protección física de los materiales nucleares⁸⁰.* La aceptación de dicha enmienda por parte de nuestro país fue depositada el 12 de marzo de 2009 y pasó a formar parte de nuestra legislación en febrero de 2017, a través de la publicación en el Diario Oficial del Decreto 132 del Ministerio de Relaciones Exteriores.
- **Tratado de Prohibición Completa de los Ensayos Nucleares:** Después de 25 años desde la fecha de su adopción en 1996, este tratado aún no ha entrado en vigor, a pesar de contar con la firma de 185 Estados. Esto se debe a que para entrar en vigencia debe contar con a lo menos la ratificación de los 44 Estados listados en el Anexo 2 de este tratado, presente al momento de su aprobación, 8 de los cuales aún no lo ratifican (Estados Unidos, China, Irán, Israel, Egipto, India, Pakistán y Corea del Norte). En particular, este Tratado prohíbe llevar a cabo, incitar, participar o permitir ensayos nucleares en el territorio de los Estados parte, entre otras materias. Chile es parte de los 36 Estados listados en el Anexo 2 del tratado que han firmado y ratificado este instrumento. Ello, porque Chile firmó el Tratado el 24 de septiembre de 1996, y lo ratificó el 12 de julio del año 2000.

- **Protocolo sobre la prohibición del empleo en la guerra de gases asfixiantes, tóxicos o similares y de medios bacteriológicos (Protocolo de Ginebra):** Es un Protocolo para la prohibición del uso de armas químicas y biológicas en situación de guerra, que entró en vigor el 8 de febrero de 1928 como respuesta a los catastróficos resultados de la Primera Guerra Mundial, cuando por primera vez se atestiguó el uso moderno de armas químicas. Fue firmado por Chile el 17 de junio de 1925 y ratificado el 2 de julio de 1935.
- **Código de La Haya contra la Proliferación de Misiles Balísticos Vectores de Armas de Destrucción Masiva (HCoC, por sus siglas en inglés):** Orientado a fortalecer los objetivos y mecanismos de desarme y no proliferación, en particular de los sistemas de misiles balísticos capaces de transportar ADM. Este código,

junto con el Régimen de Control de Tecnología de Misiles (MCTR), son los únicos instrumentos multilaterales enfocados a evitar la diseminación de misiles balísticos capaces de transportar ADM. El Código entró en vigencia en 2002 y se gestó fuera del alero de Naciones Unidas. Sin perjuicio de ello, existen varias resoluciones de la ONU que lo respaldan. Actualmente, 143 Estados lo han suscrito, Chile incluido (el 25 de noviembre de 2002).

ANEXO 2: TABLA CON DECRETOS DEL MINREL QUE HAN DISPUESTO EL CUMPLIMIENTO DE LAS RESOLUCIONES DEL CSNU EN MATERIA DE FP

TABLA 4
Decretos que dan cumplimiento a las Resoluciones del CSNU en materia de FP

Fuente: Elaboración propia UAF.

Decreto	Detalle	Promulgación	Publicación
Decreto 366	Da cumplimiento a la Resolución 1718, de 2006, del CSNU, que adopta medidas contra la RPDC.	09-11-2006	20-06-2007
Decreto 127	Da cumplimiento a las Resoluciones 1874 de 2009 y 1928 de 2010 del CSNU, que adoptan medidas contra la RPDC.	27-09-2011	21-02-2012
Decreto 30	Da cumplimiento a la Resolución 2094, de 2013, del CSNU, que impone medidas a la RPDC.	04-04-2013	17-10-2013
Decreto 9	Da cumplimiento a las Resoluciones 2087 (2013), 2270 (2016) y 2321 (2016), aprobadas por el CSNU, relativas a la RPDC.	10-01-2017	15-07-2017
Decreto 116	Dispone el cumplimiento de la Resolución 2356 (2017) y sus anexos i y ii, aprobada por el CSNU, relativa a la RPDC.	22-06-2017	09-11-2017
Decreto 186	Dispone el cumplimiento de las Resoluciones 2371 (2017) y sus anexos i y ii, y 2375 (2017) y sus anexos i y ii, aprobadas por el CSNU, relativas a la RPDC.	02-10-2017	29-03-2018
Decreto 100	Dispone el cumplimiento de la Resolución 2397 (2017) y sus anexos i y ii, aprobada por el CSNU, relativa a la RPDC.	02-04-2018	08-07-2019
Decreto 128	Dispone el cumplimiento de la resolución 2231 (2015), aprobada por el CSNU, relativa a la cuestión nuclear de Irán.	08-08-2019	09-01-2020
Decreto 214	Establece medidas que implementan las Resoluciones del CSNU para la prevención y represión del financiamiento, directo e indirecto, de actividades que afecten la paz y seguridad internacionales.	17-12-2019	11-09-2020



BIBLIOGRAFÍA

BIBLIOGRAFÍA

- CSNU. (30 de noviembre de 2011). *Consejo de Seguridad de la ONU. Nota verbal de fecha 18 de noviembre de 2011 dirigida al Presidente del Comité por la Misión Permanente de Chile ante las Naciones Unidas. Comité del Consejo de Seguridad establecido en virtud de la resolución 1718*. Obtenido de <https://undocs.org/es/S/AC.49/2011/15>
- CSNU. (2016). *Consejo de Seguridad de la ONU. Nota verbal de fecha 8 de julio de 2016 dirigida al Presidente del Comité por la Misión Permanente de Chile ante las Naciones Unidas*. Organización de las Naciones Unidas. Nueva York. Obtenido de https://www.un.org/ga/search/view_doc.asp?symbol=S/AC.49/2016/40
- CSNU. (5 de marzo de 2018). *Consejo de Seguridad de la ONU, Informe final del Grupo de Expertos establecido en virtud de la resolución 2345 (2017), S/2018/171*. Organización de las Naciones Unidas. Nueva York. Obtenido de <https://undocs.org/es/S/2018/171>
- CSNU. (30 de agosto de 2019a). *Consejo de Seguridad de la ONU. Informe de mitad de período del Grupo de Expertos establecido en virtud de la resolución 2464 (2019), S/2019/691*. Organización de las Naciones Unidas. Nueva York. Obtenido de <https://undocs.org/es/S/2019/691>
- CSNU. (5 de marzo de 2019b). *Consejo de Seguridad de la ONU. Informe final del Grupo de Expertos establecido en virtud de la resolución 2407 (2018), S/2019/171*. Organización de las Naciones Unidas. Nueva York. Obtenido de <https://undocs.org/es/S/2019/171>
- CSNU. (4 de marzo de 2021). *Consejo de Seguridad de la ONU. Informe final del Grupo de Expertos establecido en virtud de la resolución 2515 (2020)*. Obtenido de <https://undocs.org/es/S/2021/211>
- CSNU. (2022). *Consejo de Seguridad de la ONU. Sanciones*. Obtenido de <https://www.un.org/securitycouncil/es/sanctions/information>
- GAFI. (18 de junio de 2008). *Financial Action Task Force. Proliferation Financing Report*. Obtenido de <https://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>
- GAFI. (febrero de 2010). *Financial Action Task Force. Combating Proliferation Financing*. Obtenido de <https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf>
- GAFI. (agosto de 2021). *Financial Action Task Force. Anti-money laundering and counter-terrorist financing measures, Japan. Mutual Evaluation Report*. Obtenido de <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-japan-2021.html>
- GAFI. (junio de 2021). *Grupo de Acción Financiera Internacional. Guía para la evaluación y mitigación de riesgo de financiamiento de la proliferación*. Obtenido de <https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/traduccion/4104-guia-del-gafi-para-la-evaluacion-y-mitigacion-de-riesgo-de-financiamiento-de-la-proliferacion>
- GAFI. (actualización octubre 2021). *Grupo de Acción Financiera Internacional. Estándares Internacionales sobre la Lucha contra el Lavado de Activos y El Financiamiento del Terrorismo, y el Financiamiento de la Proliferación de Armas de Destrucción Masiva*. Obtenido de https://www.uaf.cl/descargas/legislacion/internacionales/GAFI_Recomendaciones_102021.pdf
- GAFILAT. (septiembre de 2021). *Grupo de Acción Financiera de Latinoamérica. Informe Evaluación Mutua de la República de Chile*. Obtenido de <https://www.gafilat.org/index.php/es/noticias/145-informe-de-evaluacion-mutua-de-la-republica-de-chile>
- Ley 19.913. (18 de diciembre de 2003). *Ministerio de Hacienda. Crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos. Artículos 19 y 20*. Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=219119>
- Minrel. (18 de agosto de 2017). *Ministerio de Relaciones Exteriores. Plan de Acción Nacional 2017-2021 para la Implementación de la Resolución 1540 del Consejo de Seguridad de las Naciones Unidas*. Obtenido de https://www.un.org/es/sc/1540/national-implementation/pdf/chile_action_plan_es.pdf
- Ordenanza de Aduanas. (2005). *Aprueba el texto refundido, coordinado y sistematizado del decreto con fuerza de ley de hacienda n°213, de 1953, sobre ordenanza de aduanas*. Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=238919&idParte=>
- RUSI. (mayo de 2019). *Royal United Services Institute. Guide to Conducting a National Proliferation Financing Risk Assessment*. Obtenido de <https://rusi.org/explore-our-research/publications/special-resources/guide-conducting-national-proliferation-financing-risk-assessment>
- SNA. (2020a). *Servicio Nacional de Aduanas. Exportaciones por país y productos. Chile*. Obtenido de <https://www.aduana.cl/exportaciones-por-pais-y-producto/aduana/2020-05-19/105505.html>
- SNA. (2020b). *Servicio Nacional de Aduanas. Importaciones por país y productos. Chile*. Obtenido de <https://www.aduana.cl/importaciones-por-pais-y-producto/aduana/2020-05-15/100754.html>
- UNODA. (2022). *Oficina de Asuntos de Desarme de las Naciones Unidas*. Obtenido de <https://www.un.org/disarmament/>



NOTAS AL PIE

NOTAS AL PIE

1. Esta definición fue adoptada por la Asamblea General de Naciones Unidas a través de la Resolución 32/84 sobre la Prohibición del desarrollo y de la fabricación de nuevos tipos de armas de destrucción en masa y de nuevos sistemas de tales armas. Parte B, punto 3. Sesión N°100 del 12 de diciembre de 1970.
2. En el origen de la Organización de Naciones Unidas en 1945, y específicamente en la Carta Fundamental que la crea, se establecen seis órganos principales, entre los cuales está el CSNU. Artículo 7° de la Carta de la ONU establece como principales órganos de Naciones Unidas: Asamblea General, Consejo de Seguridad, Consejo Económico y Social, Consejo de Administración Fiduciaria, Corte Internacional de Justicia y la Secretaría.
3. ***“A fin de asegurar una acción rápida y eficaz por parte de las Naciones Unidas, sus Miembros confieren al CSNU la responsabilidad primordial de mantener la paz y la seguridad internacional, y reconocen que el Consejo actúa a nombre de ellos al desempeñar las funciones que le impone aquella responsabilidad”*** Artículo 24 n°1 de la Carta de Naciones Unidas.
4. Ver artículo 39° de la Carta de Naciones Unidas.
5. Estas sanciones se establecen en el artículo 41° del Capítulo VII de la Carta de las Naciones Unidas, sosteniendo que: ***“El Consejo de Seguridad podrá decidir qué medidas que no impliquen el uso de la fuerza armada han de emplearse para hacer efectivas sus decisiones, y podrá instar a los Miembros de las Naciones Unidas a que apliquen dichas medidas, que podrán comprender la interrupción total o parcial de las relaciones económicas y de las comunicaciones ferroviarias, marítimas, aéreas, postales, telegráficas, radioeléctricas, y otros medios de comunicación, así como la ruptura de relaciones diplomáticas”***.
6. Artículo 25° de la Carta de la ONU: Los Miembros de las Naciones Unidas convienen en aceptar y cumplir las decisiones del CSNU de acuerdo con esta Carta.
7. Resoluciones 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), 1929 (2010) y 2224 (2015).
8. Párrafo 8 y 9 de la Resolución 2231 (2015) CSNU.
9. Desde ahora en adelante denominado en este documento como “Grupo de Expertos”.
10. Tales como su estructura económica, social, regulatoria, la seguridad de la infraestructura tecnológica de sus instituciones, entre otras materias.
11. Respecto del FP, el país obtuvo un cumplimiento parcial de la Recomendación N°7, que evaluó el cumplimiento técnico asociado a las SFD relacionadas con la proliferación, y un nivel de efectividad Moderado en el Resultado Inmediato N°11, con respecto a las sanciones financieras de FP.
12. En este caso, corresponden a acciones de infracción, no implementación y/o evasión de las SFD de FP, así también la realización de actividades restringidas y/o prohibidas por parte de la RPDC, que les permita obtener recursos para, eventualmente, financiar programas de ADM y/o acceder al sistema financiero internacional y mover sus fondos de manera menos restrictiva.
13. Los estándares que promueve el GAFI están contenidos en las 40 Recomendaciones, emitidas en febrero de 2012 y cuya última actualización data de febrero de 2023.
14. En el Anexo 1 de este documento se incluyen otros instrumentos internacionales en los que participa Chile.
15. El Subcomité de la Resolución 1540 es presidido por la Dirección de Seguridad Internacional y Humana (DISIN), del Ministerio de Relaciones Exteriores, a través de su Unidad de no Proliferación y Control de Armas (DISIN-NPCA). Dentro de las principales actividades de esta Unidad se encuentran: Presidir la Mesa de Coordinación sobre Tráfico Ilícito de Armas; representar autoridades en diversas comisiones o comités relacionados con la exportación de material bélico; implementación de Resoluciones del CSNU; y participar en la Comisión de Seguridad de Emergencias Radiológicas. También participa en la actualización de los reglamentos de la Ley N°17.798 (control de armas) y de la Ley N°21.250 (implementación de Convenciones de Armas Químicas y Biológicas); e identifica la interdicción de mercancías estratégicas y ADM que está dirigida a las agencias responsables en seguridad fronteriza, para lo cual planifica estas tareas en con el Servicio Nacional de Aduanas y la Comisión Chile de Energía Nuclear (CChEN).
16. Presentado en conformidad con el numeral 8 de la Resolución 1977 (2011) y numeral 5 de la Resolución 2325 (2016), ambas sucesoras de la Resolución 1540, los cuales alientan a los Estados a preparar planes de acción nacionales de forma voluntaria, que indiquen sus prioridades y planes para aplicar las disposiciones de la Resolución 1540 y, posteriormente, presentar dicho plan al Comité 1540. Este Plan contó también con el apoyo de expertos del Comité 1540 de las Naciones Unidas y del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA).
17. En línea con el inciso segundo del artículo 5° de la Constitución Política de la República se dispone, entre otras materias, que es deber de los órganos del Estado respetar “los tratados internacionales ratificados por Chile y que se encuentren vigentes”.
18. Destacar que, si las Resoluciones del CSNU contienen medidas coercitivas aplicables en la jurisdicción del Estado Miembro, estas deben ser incorporadas al ordenamiento jurídico interno, de forma previa. En este sentido, y en relación con las 9 Resoluciones sucesoras de la Resolución 1718 del CSNU, se han promulgado (y publicado) seis Decretos del Ministerio de Relaciones Exteriores que dan cumplimiento a dichas Resoluciones, entre los años 2012 y 2019. En cuanto a la Resolución 2231 del CSNU sobre Irán, se promulgó el decreto correspondiente en enero de 2020. Estos pueden ser consultados en el Anexo 2.
Cabe señalar que los Decretos Supremos dictados por el Minrel, en relación con las Resoluciones del CSNU relativas al financiamiento de la PADM, son parte integrante del ordenamiento jurídico chileno, haciendo obligatoria dichas normas a toda la población, lo que es complementado con los procedimientos establecidos en el artículo 38° de la Ley N°19.913 y las circulares 49, 54 y 60 de la UAF.
19. Los que poseen características similares con aquellos implementados por motivo del FT.
20. Para cumplir con el rol de punto de contacto y enlace, el Minrel podrá solicitar y recibir desde otros órganos del Estado, y dentro de sus atribuciones legales, la información pertinente para la cooperación con otros países, organizaciones o entidades extranjeras.

21. Al respecto, queda pendiente el Reglamento que permite la implementación de la Ley. El organismo encargado del cumplimiento de la Ley corresponde a la DGMN, la que se encarga de las funciones de coordinación y enlace con la Organización para la Prohibición de Armas Químicas (OPAQ) y con la Oficina de las Naciones Unidas para Asuntos de Desarme (UNODA), así como con otros organismos internacionales relacionados con los demás Estados respecto de las materias abordadas. Dichas coordinaciones deben ser efectuadas a través del Minrel, con la colaboración y asistencia de la Subsecretaría de Defensa.
22. En el próximo apartado se profundizará este procedimiento.
23. Boletín N°14773-02: <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15272&prmBOLETIN=14773-02>
24. Tal como lo indica el inciso final del artículo 3°: "En todo caso, ninguna persona podrá poseer o tener armas denominadas especiales, que son las que corresponden a las químicas, biológicas y nucleares".
25. Tal como lo contempla el artículo 8°, inciso primero, del Decreto 400: "los que organizaren, pertenecieren, financiaren, dotaren, instruyeren, incitaren o indujeren a la creación y funcionamiento de milicias privadas, grupos de combate o partidas militarmente organizadas, armadas con algunos de los elementos indicados en el artículo 3°, serán sancionados con la pena de presidio mayor en cualquiera de sus grados".
26. Entre las instituciones se encuentran, además de la UAF, el Banco Central de Chile, Comisión para el Mercado Financiero, ministerios del Interior y Seguridad Pública, de Hacienda y de Relaciones Exteriores, Ministerio Público, direcciones generales del Crédito Prendario y del Territorio Marítimo y Marina Mercante de Chile, Servicio de Impuestos Internos, Servicio Nacional de Aduanas, superintendencias, policías y el Poder Judicial.
27. Para mayor detalle, consultar las Circulares UAF N°49, 54 y 60.
28. La UAF orienta la búsqueda respecto de las listas por medio de su sitio web direccionado a las Resoluciones del CSNU. Puede ser consultado en el siguiente enlace: https://www.uaf.cl/asuntos/consulta_onu.asp
29. Esta Guía se encuentra disponible en la página web de la UAF.
30. Entre las medidas que se podrán ordenar se entenderán incluidas la prohibición de transferencia, conversión, disposición o movimiento de fondos u otros bienes durante el plazo de vigencia de la medida.
31. Entre las instituciones se encuentran, además de la UAF, el Banco Central de Chile, Comisión para el Mercado Financiero, ministerios del Interior y Seguridad Pública, de Hacienda y de Relaciones Exteriores, Ministerio Público, direcciones generales del Crédito Prendario y del Territorio Marítimo y Marina Mercante de Chile, Servicio de Impuestos Internos, Servicio Nacional de Aduanas, superintendencias, policías y la Contraloría General de la República.
32. Parcialmente cumplida corresponde a que existen deficiencias moderadas (GAFI, actualización octubre 2021, pág. 154).
33. De acuerdo con GAFI, la frase sin demora significa: "idealmente, en una cuestión de horas luego de una designación por el CSNU o sus Comités de sanciones" (GAFI, actualización octubre 2021, pág. 133). En este sentido, se considera un plazo de "sin demora" dentro de 24 horas (GAFI, 2021, pág. 105).
34. Un nivel moderado corresponde a que el resultado inmediato se ha logrado en gran medida, por lo que pocas mejoras son necesarias. (GAFI, actualización octubre 2021, pág. 162).
35. La fuente de la información de estos reportes corresponde a los Estados Miembros que la entregan al Grupo de Expertos, además de reportes de prensa e investigación del mismo Grupo.
36. Se considera este periodo con el objetivo de analizar información más actualizada.
37. Este informe del Grupo de Expertos se encuentra publicado en: <https://undocs.org/es/S/2021/211>
38. Tal como se establece en la Resolución 2231 sobre Irán, todos los Estados podrán participar y permitir actividades con Irán, previa aprobación del CSNU, y caso por caso, relacionadas con transferencias y actividades asociadas con energía nuclear (canales de compras), misiles balísticos, armas, otras prestaciones relacionadas de diversa índole (asistencia técnica, asesorías, servicios financieros, de intermediación, inversiones, entre otras materias).
39. Los informes del Grupo de Expertos se encuentran publicados en los siguientes enlaces:
<https://undocs.org/es/S/2019/691>
<https://undocs.org/es/S/2019/171>
<https://undocs.org/es/S/2021/211>
40. En relación a Irán, el GAFI solicitó a todas las jurisdicciones robustecer la supervisión para las sucursales y subsidiarias de las instituciones financieras con sede en Irán. También solicitó tener mecanismos mejorados de reportes relevantes, o un informe sistemático de las transacciones financieras, entre otras materias. El GAFI manifestó que Irán se mantendría como país de alto riesgo (en lista negra), hasta que cumpla con su Plan de Acción y ratifique las convenciones de Palermo y de FT.
41. Clasificación propuesta por el RUSI en el documento «Guide to Conducting a National Proliferation Financing Risk Assessment» (RUSI, 2019).
42. Categoría según definición de amenaza de RUSI, descrita anteriormente.
43. La Resolución 1718 del CSNU en su párrafo 8, inciso tercero estableció una prohibición para la venta o transferencia de este tipo de artículos a la RPDC. En el caso de las bebidas alcohólicas, no todos los Estados Miembros las clasifican como bienes de lujo. Cabe señalar que los artículos de lujo incluidos en los anexos de las Resoluciones 2094 (2013), 2270 (2016) y 2321 (2016) no incorporan a las bebidas alcohólicas bajo esta categoría.
44. Conjunto de técnicas utilizadas para obtener datos confidenciales, infectando computadores con malware o acceder a enlaces de sitios infectados.
45. También utilizarían el denominado "cripto secuestro", utilizando programa malicioso para infectar (o "secuestrar") una computadora y utilizarla para la minería de activos virtuales.
46. El Grupo de Expertos también tuvo información de que un grupo ligado a la RPDC era capaz de establecer infraestructura de phishing que imitaba aplicaciones y sitios web conocidos (por ejemplo, Microsoft Outlook), con el objetivo de engañar a las víctimas para obtener sus credenciales de acceso.
47. Los ataques perpetrados contra las casas de cambio de activos virtuales habrían producido mayores ganancias que aquellos realizados contra instituciones financieras, dada la mayor robustez de la infraestructura de tecnología de la información de estas últimas. El Grupo de Expertos incentiva a los Estados Miembros a aplicar las normas del GAFI, enfatizando en la Recomendación N°15, dado que para gestionar y mitigar los

- riesgos asociados a los activos virtuales "los países deben velar por que los proveedores de servicios de activos virtuales estén regulados a efectos de la lucha contra el blanqueo de dinero y la financiación del terrorismo y cuenten con licencias o estén registrados y sometidos a sistemas eficaces de vigilancia y garantía del cumplimiento de las medidas pertinentes previstas en las recomendaciones del GAFI".
48. P2P: Corresponde a la forma de compartir todo tipo de material entre usuarios de internet.
49. La información disponible sobre este caso proviene, principalmente, de fuentes de información pública de medios de comunicación, dado que no se encuentran en el dominio público reportes oficiales respecto de este ataque en particular, ni desde organismos gubernamentales ni de instituciones financieras.
50. Cabe señalar que, producto de las restricciones producidas por la pandemia de Covid-19, se redujeron las exportaciones de carbón y otras mercancías, indicadas anteriormente, durante los últimos dos años del periodo analizado.
51. Ropa de esquí.
52. Whisky, vodka, vino, cerveza, coñac y brandy.
53. Los envíos de bebidas alcohólicas a la RPDC prácticamente se detuvieron desde inicios de 2020 y no estuvieron disponibles en el mercado interno debido a las restricciones por la pandemia de Covid-19.
54. Según información entregada por el Servicio Nacional de Aduanas a fuentes de prensa, luego de revisar registros de años anteriores se detectaron errores por parte de agentes de aduana, en particular de codificación, por lo que podría suceder que luego de revisiones posteriores se corrijan las cifras erróneas.
55. Cabe señalar que el párrafo 8 de la Resolución 2397 (2017) del CSNU exige a los Estados Miembros que repatrien a todos los ciudadanos de la RPDC que obtengan ingresos dentro de su jurisdicción, y a todos los agregados gubernamentales de supervisión de la seguridad que vigilan a los trabajadores de la RPDC en el extranjero, en un plazo de 24 meses a partir del 22 de diciembre de 2017.
56. En el área TI, se estimó que el salario mensual rondaba los USD 3.000-5.000, y alrededor de un tercio se destinaba a la RPDC. Se ha informado que la RPDC ha enviado trabajadores relacionados a la informática a diferentes países de Europa, Asia, África y Medio Oriente, utilizando empresas en el país de destino dirigidas por desarrolladores de la RPDC, o identidades falsas.
57. Dado el escenario de pandemia, se reportó que ciudadanos de la RPDC han permanecido en terceros países debido al cierre de fronteras.
58. Información corresponde a la Nota verbal del 7 de abril de 2017 dirigida a la Presidencia del Comité por la Misión Permanente de Chile ante las Naciones Unidas.
59. El párrafo 31 de la Resolución 2321 (2016) indica que "Decide que los Estados Miembros deberán adoptar las medidas necesarias para cerrar las oficinas de representación, filiales o cuentas bancarias que tengan en la RPDC en un plazo de 90 días, a menos que el Comité determine en cada caso que esas oficinas, filiales o cuentas son necesarias para el suministro de asistencia humanitaria o para las actividades de las misiones diplomáticas en la RPDC, o para las actividades de las Naciones Unidas o de sus organismos especializados o de organizaciones conexas o para cualquier otro fin compatible con los objetivos de la presente resolución".
60. Supervisor prudencial para bancos, valores y seguros.
61. Categoría según definición de amenaza del RUSI, descrita anteriormente.
62. La Resolución 1718 en su párrafo 8, inciso tercero, estableció una prohibición para la venta o transferencia de este tipo de artículos a la RPDC. En el caso de las bebidas alcohólicas, no todos los Estados Miembros las clasifican como bienes de lujo. Cabe señalar que los artículos de lujo incluidos en los anexos de las resoluciones 2094 (2013), 2270 (2016) y 2321 (2016) no incorporan a las bebidas alcohólicas bajo esta categoría.
63. En un periodo anterior al utilizado para el análisis en este documento, reportes del Grupo de Expertos relacionados con Irán (anterior al PAIC), identificaron personas/entidades designadas que realizaron actividades restringidas o prohibidas, a través de terceros países, en otras regiones, países los cuales poseían capacidades para desarrollar tecnología relacionada con ADM.
64. A la fecha de la Evaluación Mutua de Chile, los comerciantes de piedras y metales preciosos no estaban considerados como sujetos obligados a reportar a la UAF. A contar de mayo de 2023, estos fueron incorporados como sujetos obligados (Ley N°21.575) al mencionarseles expresamente en el artículo 3° de la Ley N°19.913.
65. De acuerdo con el GAFI, la frase "sin demora significa, idealmente, en una cuestión de horas luego de una designación por el CSNU o sus Comités de sanciones". (GAFI, actualización octubre 2021, pág. 133). En este sentido, se considera un plazo de "sin demora" dentro de 24 horas. (GAFI, 2021, pág. 105).
66. Este reporte se basa, principalmente, en los resultados de la Encuesta de Percepción de Riesgos Globales, realizada anualmente por el FEM. Según la metodología descrita en dicho reporte, esta encuesta es completada por más de 650 miembros de las comunidades de líderes del FEM. Además, el Comité Asesor de Riesgos Globales del FEM supervisa la elaboración de este reporte y provee información durante el proceso de redacción.
67. Los ciberataques (a gran escala) son descritos en este reporte como: "Ataques cibernéticos a gran escala o malware que causan grandes daños económicos, tensiones geopolíticas o una pérdida generalizada de confianza en Internet". Según indica este reporte, los ciberataques pueden ser diversos, e ir desde el robo de datos, uso de ransomware, hasta la toma de poder de los sistemas con consecuencias a gran escala, potencialmente dañinas.
68. La interrupción a la infraestructura de TI (riesgo global tecnológico) es descrito en este reporte como: "El deterioro, saturación o cierre de infraestructuras/servicios físicos y digitales críticos como consecuencia de una dependencia sistémica de las redes cibernéticas y/o tecnología: sistemas intensivos en Inteligencia Artificial, internet, equipos portátiles, servicios públicos, satélites, etc".
69. Dado a conocer en agosto de 2021.
70. Según indica la información publicada en la página web de la International Data Corporation (IDC), esta es "la principal empresa mundial en inteligencia de mercado, servicios de consultoría, y eventos para los mercados de Tecnologías de la Información, Telecomunicaciones y Tecnología de Consumo".
71. Según indica la IDC, este estudio analizó dos grupos de empresas: las grandes empresas y las corporaciones. Se consultó a 154 ejecutivos pertenecientes a empresas de distintas industrias nacionales, que facturan desde USD 4 millones anuales. Las empresas se clasificaron en distintos niveles de

madurez en relación con la ciberseguridad, mediante una evaluación en 5 dimensiones: visión, gestión de riesgos, capital humano, procesos y tecnologías de seguridad. Esta clasificación inició en la categoría "Inexperto" (implementan medidas básicas de seguridad conforme surgen necesidades) hasta el nivel "Profesional predictivo" (pueden predecir y tomar acciones efectivas contra ciberataques). Mayor detalle puede ser consultado en: <https://www.idc.com/getdoc.jsp?containerId=prLA48174321>

72. El Capítulo 20-10 de la RAN, consideró como definición de "seguridad de la información" a "el conjunto de acciones para la preservación de la confidencialidad, integridad y disponibilidad de la información de la entidad". A su vez, consideró la definición de ciberseguridad como: "el conjunto de acciones para la protección de la información presente en el ciberespacio y de la infraestructura que la soporta, que tiene por objetivo evitar o mitigar los efectos adversos de sus riesgos y amenazas inherentes, que puedan afectar la seguridad de la información y la continuidad del negocio de la institución".
73. El Capítulo 20-10 de la RAN, entiende como "activos críticos de ciberseguridad" a aquellos "activos de información lógicos que son considerados críticos para el funcionamiento del negocio, incluidos los componentes físicos tales como hardware y sistemas tecnológicos que almacenan, administran y soportan estos activos, los que, de no operar adecuadamente, exponen a la entidad a riesgos que afecten la confidencialidad, integridad y disponibilidad de la información".
74. El Capítulo 20-10 de la RAN, definió "incidente de seguridad de la información" como: "acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información de la entidad".
75. En enero de 2022 ingresó al Congreso Nacional el proyecto de ley Boletín N°14773-02 que crea la Comisión de Comercio Estratégico y regula la exportación de material de uso dual y de defensa y otras materias que indica. A través de este cuerpo legal se lograrían implementar dos de los instrumentos internacionales relacionados con el FP, a saber, la Resolución 1540 del CSNU (complementaría la normativa ya emitida por el país en base a esta resolución, regulando otros aspectos del fenómeno) y el Tratado sobre Comercio de Armas (este Tratado entró en vigencia en agosto de 2018). Según el Informe de Impacto Regulatorio del proyecto, esta ley sometería a regulación la operatoria con material de uso dual, es decir, "la exportación, tránsito y corretaje internacional de equipos, materiales y tecnología utilizados comúnmente en la industria civil que podrían ser utilizados para producir y fabricar armas nucleares, químicas y biológicas". La normativa también incluiría las armas convencionales, sus piezas y componentes. Para exportar este tipo de productos, la ley exigiría una autorización previa basada en el nivel de riesgo representado por el país/entidad de destino (regulación flexible), lo que sería determinado por una Comisión de Comercio Estratégico. Por lo tanto, podría exportarse a países sin autorización previa mediante el otorgamiento de permisos, por un plazo determinado. También sería tipificado como delito usar el territorio nacional para intentar desviar materiales regulados en

Chile hacia países/entidades que presenten sanciones de las Naciones Unidas (Cabe señalar que Chile no es productor de este tipo de elementos que serían sometidos a control, sino más bien importador).

Como indica el Informe de Impacto Regulatorio del proyecto de ley, la competitividad de la industria nacional se vería perjudicada por la ausencia de una legislación de este tenor, dado que los países que tienen regulada la exportación de este tipo de elementos, cuentan con restricciones para su transferencia hacia aquellos donde no existe normativa al respecto. En ese escenario la reexportación desde países sin regulación sugiere un riesgo para la seguridad internacional. Por otra parte, también afectaría a aquellas empresas interesadas en desarrollar negocios a nivel internacional relacionados con estos elementos (fabricación bajo licencia, por ejemplo), dado que implicaría tener acceso a ellos. Boletín N°14773-02: <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmiD=15272&prmiBOLETIN=14773-02>

76. En enero de 2023 se publicó en el Diario Oficial la Ley N°21.521 que "Promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros" (también denominada Ley Fintec). Su objetivo es establecer un marco general para incentivar la prestación de servicios financieros a través de medios tecnológicos, que realicen los proveedores regidos por ella. Entre otras materias, el proyecto incluye como sujetos obligados (artículo 3°, Ley N°19.913) a "**quienes estén inscritos en el Registro de Prestadores de Servicios Financieros y en el Registro de Proveedores de Servicios de Iniciación de Pagos mantenido por la Comisión para el Mercado Financiero (CMF) y presten los servicios de plataforma de financiamiento colectivo, sistemas alternativos de transacción, custodia de instrumentos financieros, intermediación de esos instrumentos; e iniciación de pagos. Idéntica obligación de reporte tendrán las demás personas naturales o jurídicas que en virtud de cualesquiera de sus giros estén sometidas a la fiscalización de la CMF y que voluntariamente hayan solicitado su inscripción en el registro (...)**".
77. En caso de incumplimiento de estas obligaciones se pueden aplicar sanciones que podrían incluir multas de hasta USD 206.000 (en casos reiterados, podría llegar hasta los USD 618.000).
78. Chile no mantiene relaciones diplomáticas con la RPDC desde septiembre de 1973 (información del documento; "Relaciones bilaterales entre Chile y la Corea del Norte", extraído desde la Biblioteca del Congreso Nacional).
79. Información extraída desde portales: Embassypages.com (enlace: <http://embassypages.com/coreademocratica>) y Northkoreaintheworld.org (<https://northkoreaintheworld.org/diplomatic/dprk-embassies-worldwide>)
80. Para más información revisar: <https://www.iaea.org/es/temas/convenciones-sobre-seguridad-fisica-nuclear>

CRÉDITOS

La Evaluación Nacional de Riesgos del Financiamiento de la Proliferación (ENR FP) es una publicación de la Mesa Intersectorial sobre Prevención y Combate al Lavado de Activos y Financiamiento del Terrorismo (MILAFT), producto del trabajo realizado por las entidades públicas que participan en su Mesa Técnica de Riesgos (MT Riesgos) y el equipo del Área de Difusión y Estudios de la Unidad de Análisis Financiero (UAF), y se clasifica como de "conocimiento público".

Se agradece la participación de las siguientes instituciones invitadas a participar en las mesas técnicas de trabajo de la MILAFT:

INSTITUCIONES INVITADAS

- Agencia Nacional de Inteligencia
- Banco Central de Chile
- Consejo de Defensa del Estado
- Contraloría General de la República
- Ministerio Público
- Dirección General del Crédito Prendario
- Gendarmería de Chile
- Instituto de Salud Pública
- Servicio Agrícola y Ganadero
- Ministerio de Economía, Fomento y Turismo
- Ministerio de Justicia y Derechos Humanos
- Poder Judicial
- Tesorería General de la República

Diseño y diagramación: Fredy Castillo V. / División de Gobierno Interior / Subsecretaría del Interior.
Año 2023, Santiago. Región Metropolitana. Chile.

Imagen de wirestock en Freepik (Portada)

CONDICIONES DE USO

Se autoriza su uso o reproducción total o parcial, bajo condición de que se mencione la fuente (la MILAFT) y no se afecte la imagen ni reputación institucional de las entidades involucradas o la del Estado.

La MILAFT no asume responsabilidad desde el punto de vista legal o de otra índole, por la precisión, oportunidad, contenidos o usos (acción y omisión) que se dé a la información contenida en este documento.

De esta manera, todo eventual uso abusivo de la ENR FP es y será de exclusiva responsabilidad de quien (quienes) la utilice(n) o reproduzca(n) total o parcialmente.



EVALUACIÓN NACIONAL DE RIESGOS FINANCIAMIENTO DE LA PROLIFERACIÓN 2016-2021

MILAFT

Mesa Intersectorial sobre Prevención
y Combate al Lavado de Activos y
al Financiamiento del Terrorismo

