

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

RESUMEN EJECUTIVO



CONTEXTO

El Grupo de Acción Financiera Internacional (GAFI) define como financiamiento de la proliferación (FP) el “acto de proveer fondos a 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 su Recomendación N°1, el GAFI establece que los países deben identificar, evaluar y entender los riesgos de FP.

En este contexto, durante el año 2023, las instituciones miembros de la Mesa Intersectorial sobre Prevención y Combate al Lavado de Activos y al Financiamiento del Terrorismo (MILAFT) decidieron ampliar su ámbito de acción hacia la lucha contra el FP, para lo cual emprendieron la tarea de elaborar una Estrategia Nacional para Prevenir y Combatir el Lavado de Activos y el Financiamiento del Terrorismo y el de la Proliferación, con un Plan de Acción a desarrollar entre los años 2023 y 2027.

Asimismo, resolvieron actualizar la ENR de LA/FT 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).

¿QUÉ ES UNA EVALUACIÓN NACIONAL DE RIESGOS DE FP?

La ENR-FP actúa como una aproximación al fenómeno de la proliferación y su financiamiento en relación con Chile, 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.

¿CÓMO SE IDENTIFICARON LOS RIESGOS DE FP EN EL PAÍS?

La ENR-FP 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 para abordar la ocurrencia de este fenómeno.

CONCEPTOS: ARMAS DE DESTRUCCIÓN MASIVA, SUS SISTEMAS VECTORES Y MATERIALES CONEXOS

Armas atómicas explosivas, armas de material radioactivo, armas químicas y biológicas letales y otras.



PRINCIPALES RESULTADOS

AMENAZAS DEL FP

Para identificar las amenazas de FP en Chile se consideraron documentos elaborados por el GAFI, el Royal United Services Institute (RUSI) y el Grupo de Expertos que apoya al Comité de Sanciones 1718 que supervisa las sanciones impuestas por el CSNU a la República Popular Democrática de Corea (Corea del Norte).

Dado que el régimen de sanciones impuesto por el CSNU a Irán se encuentra en pausa bajo el compromiso del cumplimiento del Plan de Acción Integral Conjunto, la ENR-FP solo considera las actividades y operaciones realizadas por Corea del Norte que han sido identificadas en los reportes del Grupo de Expertos, y a las que Chile podría quedar eventualmente expuesto.

Las amenazas establecidas son aquellas asociadas a (1) productos y servicios financieros relacionados con el comercio de bienes sensibles a la proliferación, (2) actividades de obtención de fondos (lícitas e ilícitas) para financiar programas de ADM y (3) infraestructura financiera y corporativa que apoye las actividades mencionadas en (1) y (2).

Con base en la información disponible y el análisis de los reportes del Grupo de Expertos se identificaron las operaciones que podrían ser clasificadas en alguna de las categorías mencionadas y que, a su vez, constituirían amenazas para Chile, resultando lo siguiente:

TIPO AMENAZA RELACIONADA CON:	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).	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

(*) 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 2021. Es posible señalar que Chile no registró actividad de comercio exterior con la RPDC en el periodo.

(**) Cabe aclarar que estas cifras informadas por el Grupo de Expertos 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.

VULNERABILIDADES RELACIONADAS CON EL FP

Las vulnerabilidades son materias, contextos (económicos, sociales, políticos, tecnológicos, entre otros) y pueden 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.

Respecto del FP, las vulnerabilidades de Chile se asocian principalmente con:

1. Comprensión del riesgo de FP:

El Informe de Evaluación de Chile, 2021, del Grupo de Acción Financiera de Latinoamérica 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 Anti LA/FT/FP

2. Implementación de las Sanciones Financieras Dirigidas (SFD) de FP:

Dadas ciertas deficiencias normativas del país, 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 permitirían eludir la aplicación de SFD.

3. Infraestructura TI, ciberseguridad y actividades de comercio:

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.

4. Nuevos productos y servicios de pago:

Los atributos de nuevos productos y servicios de pago, que involucran tanto a los activos virtuales como las tarjetas de prepago y los servicios de

pago online, derivan en vulnerabilidades del Sistema Nacional ALA/CFT. Esto, debido a que personas/entidades designadas o vinculadas a la proliferación podrían realizar actividades de FP, y utilizar estos productos y servicios.

MITIGANTES RELACIONADOS CON EL FP

Los mitigantes son 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 FP.

Los principales mitigantes identificados en Chile son:

1. Monitoreo de las SFD por parte del sector financiero:

Las entidades obligadas a reportar operaciones sospechosas a la Unidad de Análisis Financiero tienen el deber de revisar permanentemente los listados del CSNU. En el evento de detectar a alguna persona, empresa o entidad enlistada tratando de realizar algún acto, transacción u operación, deben informar de inmediato dicho hallazgo a la UAF, a efectos de que este Servicio pueda proceder a tomar la medida de congelamiento de activos establecida en el artículo 38 de la Ley N°19.913.

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.

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 RPDC.

RIESGOS DEL FINANCIAMIENTO DE LA PROLIFERACIÓN

[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, 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.

Dado lo anterior, **EL RIESGO ESTIMADO DE FP EN CHILE ES BAJO**, 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.