

NATIONAL RISK ASSESSMENT OF **PROLIFERATION FINANCING** 2016-2021



MILAFT

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





NATIONAL RISK ASSESSMENT OF **PROLIFERATION FINANCING** 2016-2021

MILAFT

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



CONTENTS

04 INTRODUCTION

08 CHAPTER I: CONCEPTUAL FRAMEWORK AND METHODOLOGY FOR NATIONAL PF RISK ASSESSMENT

- 08 Conceptual Framework of the proliferation of weapons of mass destruction and its financing
- 12 Methodology

16 CHAPTER II: INTERNATIONAL STANDARDS, CONTEXT OF THE PROLIFERATION AND ITS FINANCING IN CHILE

- 16 International Standards related to PF
- 17 National regulatory framework and implementation of UNSC resolutions
- 20 Functioning of the National AML/CTF System regarding Proliferation Financing

25 CHAPTER III: DIAGNOSTIC OF THE PROLIFERATION FINANCING PHENOMENON IN CHILE

- 25 National Strategy for Preventing and Combating ML/TF and 2018-2020 Action Plan
- 26 Results of Gafilat's Mutual Evaluation of Chile
- 28 Analysis of the reports made by the Group of Experts that support the 1718 Sanctions Committee and mention Chile in matters of Proliferation Financing

31 CHAPTER IV: THREATS OF PROLIFERATION FINANCING

40 CHAPTER V: IDENTIFICATION OF VULNERABILITIES RELATED TO PROLIFERATION FINANCING

- 40 Vulnerabilities associated with the understanding of PF risk
- 40 Vulnerabilities associated with the implementation of PF TFSs
- 41 Vulnerabilities associated with IT infrastructure, cybersecurity and foreign trade activities
- 45 Vulnerabilities associated with new products and payment services

48 CHAPTER VI: IDENTIFICATION OF MITIGANTS RELATED TO PROLIFERATION FINANCING

- 48 Monitoring of TFSs by the financial sector
- 48 Oversight of reporting entities' compliance with TFSs measures
- 49 Non-existence of diplomatic relations between the DPRK and Chile

51 CHAPTER VII: ASSESSMENT OF THE RISKS OF PROLIFERATION FINANCING IN CHILE

53 ATTACHMENTS

- 53 ANNEX 1: Other Conventions, Treaties or Agreements in which Chile participates related to WMD
- 54 ANNEX 2: Table with Minrel decrees that have provided for compliance with the UNSC Resolutions on the subject of PF

56 BIBLIOGRAPHY

58 FOOTNOTES



INTRODUCTION

INTRODUCTION

United Nations Security Council (UNSC) Resolution 1540 on the Non-Proliferation of Weapons of Mass Destruction of April 28, 2004, establishes obligations for all Member States to develop and enforce appropriate legal and regulatory measures against the proliferation of chemical, biological, radiological and nuclear weapons and their means of delivery, in particular, to prevent the spread of weapons of mass destruction to non-state actors.

This resolution establishes that all States should abstain from providing any form of support to non-state actors who attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes. The resolution obliges all States to adopt and enforce effective laws to this end, as well as adopt other effective measures to prevent the proliferation of these weapons and their means of delivery to non-state actors, particularly for terrorist purposes.

Weapons of mass destruction and their means of delivery are of constant concern to the international community because of the catastrophic consequences of their use. In this regard, the Financial Action Task Force (FATF) recommends that the countries take appropriate steps to identify, assess and understand the risks of money laundering, terrorism financing and proliferation financing of weapons of mass destruction (ML/TF/PF), on an ongoing basis, as well as to manage and mitigate the risks identified (Recommendation N°1).

In 2012, the FATF incorporated Recommendation N°7, which calls on countries to implement targeted financial sanctions regimes to comply with the UNSC Resolutions on preventing, suppressing and disrupting the proliferation of weapons of mass destruction and its financing (PF).

These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by or under the authority of the UNSC under Chapter VII of the UN Charter, to prevent funds/assets from being made available to those who commit or attempt to finance proliferation.

Since 2020, the FATF has expanded its focus to the need for countries to comprehensively understand these threats, in order to develop public policies and implement relevant measures to combat them in both the private and public sectors.

Since 2013, the country has had a National Strategy to Prevent and Combat ML/TF, whose action plans (2014-2017 y 2018-2020) have been developed and implemented by over twenty public agencies coordinated by the Financial Analysis Unit (UAF, by its acronym in Spanish), with the support of the Intersectoral Roundtable on Preventing and Combating ML/TF (MILAFT).

MILAFT is a permanent Commission whose mission is to advise the President of the Republic in coordinating the actions, plans and programs of the different institutional actors in matters of the prevention, detection and prosecution of ML/TF.

Created through Decree N°1.724, of 2016, of the Ministry of Finance, the Roundtable must also follow up on the progress of the objectives set out in the National Strategy.

Its 15 permanent members are:

- Ministry of the Interior and Public Safety
- Ministry of Foreign Affairs
- Ministry of Finance
- Ministry General Secretariat of the Presidency
- Carabineros de Chile (through the Department O.S.7 of Drugs, Department O.S.9 of Investigation of Criminal Organizations and the Intelligence Directorate (Dipolcar)).
- Financial Market Commission
- General Directorate of Maritime Territory and Merchant Marine of the Chilean Navy (DIRECTEMAR)
- Investigative Police (through the money laundering (BRILAC) and organized crime (BRICO) investigation brigades).
- Internal Revenue Service
- National Customs Service
- National Service for the Prevention and Rehabilitation of Drug and Alcohol Abuse
- Superintendency of Casinos
- Superintendency of Pensions
- Superintendency of Social Security
- Financial Analysis Unit (acting as Executive Secretariat).

In 2023, MILAFT invited the following to participate in its technical working groups:

- National Intelligence Agency
- Central Bank of Chile
- State Defense Council
- Office of the Comptroller General of the Republic of Chile
- General Directorate of Pledge Credit
- Gendarmerie of Chile
- Institute of Public Health
- Public Prosecutor's Office
- Agriculture and Livestock Service
- Civil Registry and Identification Service
- Ministry of Economy, Development and Tourism
- Ministry of Justice and Human Rights
- Judiciary (Supreme Court)
- General Treasury of the Republic

In line with international standards, in March 2017, Chile, through the UAF, in its capacity as coordinator of the National Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) System, presented to the community the National Risk Assessment of Money Laundering and Terrorism Financing (NRA-ML/TF).

The purpose of the document was to analyze the country's economic and legal threats and vulnerabilities to ML/TF, and their consequent impact, so that the authorities can design essential measures and policies to combat them, and prioritize and allocate resources in an efficient manner.

However, given the updates of the international standard regarding the spread of weapons of mass destruction and its financing, the threat it entails and the strategic vision that it's needed to face the phenomenon, during 2023, the institutions part of the National Strategy for Preventing and Combating ML/TF, coordinated by the UAF, with the support of MILAFT, worked on an update of the NRA, separating it into three volumes: NRA of money laundering (NRA-ML), NRA of terrorism financing (NRA-TF) and NRA of proliferation financing (NRA-PF).

This broadens the scope of action of the National AML/CTF System to include the country's risks to the PF and the need to implement measures to prevent and mitigate them.

This NRA-PF acts as an approximation to the phenomenon of proliferation and its financing concerning Chile. This document intends to create and expand knowledge of PF in the National AML/CTF System, since it addresses the key concepts associated with it and identifies possible threats, vulnerabilities and mitigating factors, positioning itself as the first NRA-PF.

To assess Chile's risks regarding PF, threats, vulnerabilities and mitigants were analyzed for the period 2016-2021, taking as a basis the methodology implemented in 2017, but adjusted to the most recent FATF recommendations.

Thus, the guidelines included in the **"Proliferation Financing Risk Assessment Guidance"** of June 2021 have been considered, in which the FATF sets out the following objectives and scope (FATF, 2021, p. 7).

- a. Provide guidance to help the public and private sectors apply the new requirements to identify, assess and understand their PF risk.
- b. Provide guidance to assist the public and private sectors in implementing the requirement to mitigate the PF risks they identify.
- c. Provide additional guidance to supervisors/self-regulatory bodies (SRBs) on the supervision or monitoring of PF risk assessment and mitigation.

In order to provide information on the country's PF risk assessment, this document is divided into seven sections: the first details the methodology used to prepare the NRA and provides the concepts involved in this matter; the second contextualizes the phenomenon of proliferation and its financing in Chile, considering the functioning of the National AML/CTF System and the existing legal regulatory framework, as well as international standards in this area; the third section makes a diagnosis of PF in the country. The fourth, fifth and sixth sections address the threats, vulnerabilities and mitigating factors identified in the country. The seventh and final section presents the risks and conclusions related to PF in Chile.

In line with NRA-ML and NRA-TF, this instrument is continuously reviewed and updated. The latter to the extent that new threats and vulnerabilities are identified and evaluated, according to the evolution of the national and international context, as well as situations or actions that act as mitigating factors.



CHAPTER I: CONCEPTUAL FRAMEWORK AND METHODOLOGY FOR NATIONAL PF RISK ASSESSMENT

CHAPTER I: CONCEPTUAL FRAMEWORK AND METHODOLOGY FOR NATIONAL PF RISK ASSESSMENT

CONCEPTUAL FRAMEWORK OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION AND ITS FINANCING

This section identifies the main concepts associated with the proliferation phenomenon and its financing.

WEAPONS OF MASS DESTRUCTION, DELIVERY SYSTEMS AND RELATED MATERIALS

The United Nations Commission on Conventional Armaments provided, in August 1948, the first formal definition applicable to the concept of **Weapons of Mass Destruction (WMD)**: "Atomic explosive weapons, weapons of radioactive material, lethal chemical and biological weapons, and any weapons developed in the future which have characteristics comparable, in destructive terms, to atomic or other weapons mentioned above".¹

In general terms, according to the United Nations Office for Disarmament Affairs (UNODA), WMD have the potential to kill, in an instant, "millions of people, endanger the environment, and fundamentally alter the world and the lives of future generations given their catastrophic effects" (UNODA, 2022).

The UNSC defines **delivery systems** as "missiles, rockets and other unmanned systems capable of delivering nuclear, chemical or biological weapons, specifically designed for that purpose". **Related materials** are those "materials, equipment and technology covered by relevant treaties and multilateral mechanisms or included in national control lists, which could be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery".

FATF (2008) complemented the definition of related materials by stating that they correspond to various goods such as components of a weapon or inputs for its production. As an example, machinery used for a lawful purpose, but which can be used in the construction of components for a WMD vector system.

PROLIFERATION OF WMD

Proliferation of WMD, hereinafter referred to as Proliferation, means the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials. It could include, among others, technology, goods, software, services or expertise (FATF, 2008).

PROLIFERATION FINANCING OF WMD

It is important to note that for proliferation financing (PF) there is still no internationally agreed definition. Therefore, for the purposes of this document we will consider the references provided by the FATF in 2008 and 2010, regarding the joint work carried out by various experts in the field.

Financing the proliferation of WMD, hereinafter proliferation financing (PF), shall be understood as (FATF, 2010):

WHAT IS THE FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION?

"the act of providing funds or financial services that are used, in whole or in part, for the manufacture, purchase, possession, development, export, transshipment, brokering, transport, transfer, storage or use of nuclear, chemical or biological weapons, as well as their means of delivery and related materials (including dual-use technologies and goods used for illegitimate purposes). All this in breach of each country's regulations, or when applicable, of international obligations".



Complementarily, in 2010, the FATF noted that the PF could contribute to global instability and loss of human life due to the use of WMD, as it facilitates the movement and development of proliferation-sensitive elements. It was also indicated that proliferators tend to use cash, or abuse the formal and informal sectors of the international financial system to trade useful goods for proliferation. In this way, financial institutions may involuntarily act as facilitators of these acts.

ROLE OF THE UNSC IN THE PREVENTION OF THE PROLIFERATION OF WMD AND ITS FINANCING

The UN² Charter gives the UNSC³ the power to determine the existence of any threat to the peace, breach of the peace or act of aggression, and may make recommendations or take decisions on what measures to take to maintain or restore international peace and security.⁴

In the context of the PF, the UNSC has the power to impose sanctions to maintain international peace and security. For the development of this document, the focus will be on sanctions related to economic and/or trade measures, arms embargoes and financial restrictions, which do not require the use of armed force.⁵

Since 1966, the UNSC has established 30 regimes of sanctions that have not implicated the use of armed force. Of these, 15 are active and focus on political conflict resolution, non-proliferation of nuclear weapons and the fight against terrorism (UNSC, 2022).

Using the faculties described above, the UNSC, in the matter of the prevention of proliferation and its financing, has approached from two perspectives. The former comprises a global application approach materialized through Resolution 1540 (2004), while the latter has a specific approach, that is, through the application of financial sanctions imposed against certain States, and which today takes the form of Resolutions 1718 and 2231.

It is important to consider that any resolution issued by the UNSC is mandatory for every State part of the United Nations, even if these States have not ratified the treaties on which the resolutions are based.⁶

UNSC RESOLUTIONS AND THE PREVENTION OF PROLIFERATION OF WMD AND ITS FINANCING

In order to prevent, repress and interrupt proliferation and its financing, **the UNSC Resolutions** in this area are the following:

• Comprehensive approach:

► **Resolution 1540 (2004):** On April 28, 2004, the UNSC unanimously adopted Resolution 1540, which affirms that the proliferation of nuclear, chemical and biological weapons and their means of delivery constitutes a threat to international peace and security. In this regard, it provides broad disposition in relation to:

- Export controls.
- Prohibiting the financing of proliferation-related activities carried out by non-State actors.
- In terms of the provision of funds and financial services related to the export and transshipment of goods that may contribute to proliferation, it requests countries to establish, develop, review and maintain adequate controls in this regard.

Resolution 1540 is the first international instrument to expressly mention PF and the need for States to implement the necessary controls to prevent it. This Resolution is the fundamental precedent for the work that the FATF subsequently developed within the framework of the incorporation of it into its standards in 2008 and, subsequently, in 2012 through Recommendation N°7.

• Restrictive approach:

These correspond to specific resolutions issued against States, groups, entities or individuals. In the use of its faculties, in these cases, the UNSC concluded that certain actions provoked by them threaten international peace and security.

Therefore, out of 15 sanctions regimes in force, 1 includes measures to prevent the proliferation of WMD and its financing. In this case, the objective is to restrict the Democratic People's Republic of Korea (DPRK or North Korea) from actions that would allow it to generate trade relations with its peers, groups, entities and individuals, by means of limitations on its imports, exports, or trade bans, among others. Within this regime, sanctions specifically focused on preventing the collection of resources are known as targeted financial sanctions (TFS or SFD in Spanish).

Iran is another case that is under a special regime. Unlike the previous one, the sanctions regime imposed by the UNSC is terminated under the commitment of compliance with the Joint Comprehensive Plan of Action (JCPOA), signed in July 2015 (Resolution 2231 (2015)), between that country and the United States, United Kingdom, Russia, France and China (the five permanent members of the UNSC), in an attempt to prevent Iran from acquiring nuclear weapons.

► **Resolution 1718 (2006) and its successors:** These are sanctions directed against the DPRK, as a result of repeated violations of UNSC Resolutions.

► **Resolution 2231 (2015):** Targets Iran, and formalizes the implementation of the Joint Comprehensive Plan of Action (JCPOA) that puts on hold the sanctions regime that had been in place since 2006. The JCPOA changed the way the UNSC viewed the Iranian nuclear issue, since through this Resolution Iran undertook several commitments to monitor the peaceful use of its nuclear program,

allowing it to restart cooperative, economic and commercial relations. Notwithstanding the above, the Resolution added new restrictions and maintained TFS to some individuals and entities in the country. In the event of Iran's non-compliance with the JCPOA, the Resolutions prior to this one will resume their validity⁷. The JCPOA has a 10-year implementation period, provided that Iran complies with the terms. Upon expiration of the term, the Plan will cease to have effect, as well as the Resolutions that apply the sanctions regime.⁸

TARGETED FINANCIAL SANCTIONS (TFS)

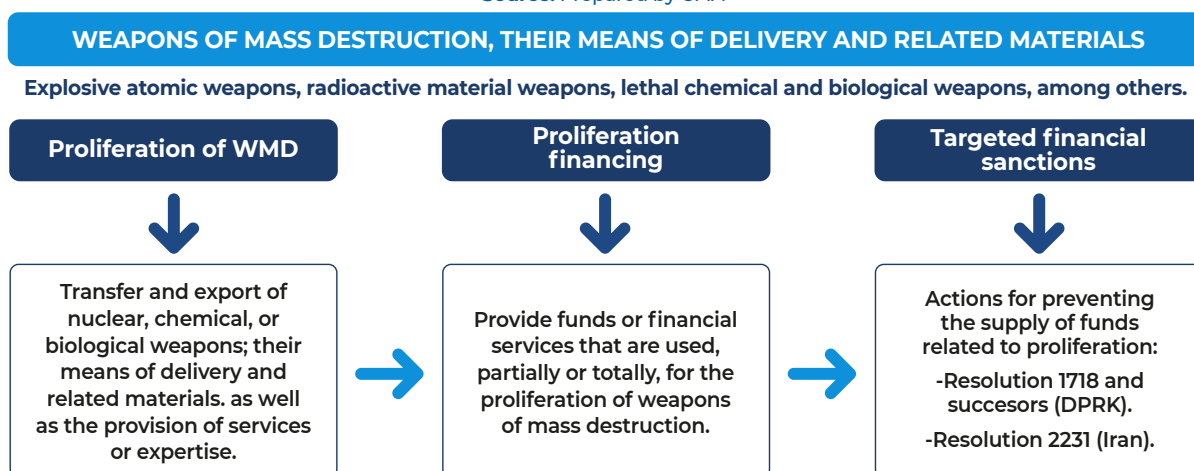
TFS are applied to prevent the use of funds for proliferation-related activities. In this regard, the FATF indicates that these correspond to "both asset freezing and prohibitions to prevent funds or other assets from being provided, directly or indirectly, for the benefit of designated persons and entities" (FATF, October 2021 update).

The UNSC Resolutions that provide for TFS related to the PF are Resolution 1718 (2006) and its successors, and Resolution 2231 (2015) both described above.

ILLUSTRATION 1

Summary of concepts related to proliferation and its financing

Source: Prepared by UAF.



METHODOLOGY

This first National PF Risk Assessment prepared by Chile in order to characterize the phenomenon, bases its methodology on the collection of qualitative information available nationally and internationally, to analyze the context of the period 2016-2021. This is because the country does not have sufficient quantitative information to address the occurrence of PF.

In this context, the methodology used is in line with proposals formulated by international organizations: FATF, based on its global guidelines and recommendations for countries to implement an adequate and effective fight against ML/TF/PF, and The Royal United Services Institute (RUSI), a group of experts dedicated to research in defense and international security.

In this sense, a process of information gathering was established that includes national and foreign sources, to complement the analysis and conclusions on the PF phenomenon.

The activities carried out for this purpose are detailed below, as well as the documents considered in the identification and review of threats, vulnerabilities and mitigants, which will be discussed later in this document.

1. Information gathering: A process of review, analysis and verification of the bibliography related to PF in the country was done, which included, among other matters:

a. Reports of the Panel or Group of Experts supporting the UNSC 1718 Sanctions Committee on the Democratic People's Republic of Korea⁹: Information contained in 10 reports prepared by the Group of Experts in the period from 2015 to 2021 was analyzed.

b. Documents published by international entities: FATF Recommendations and reports related to this matter, guides and reports

prepared by non-governmental institutions specialized in the subject (for example, the RUSI), reports on proliferation typologies and international PFs, and cases of export control violations, among other publicly available information, were considered. A review of PF risk assessments developed by countries that are benchmarks in the field was carried out as well.

c. Chile Mutual Evaluation Report (MER, IEM by its acronym in spanish): Published in September 2021 by the Latin American Financial Action Task Force (Gafilat). This input analyzes Chile's level of compliance with the FATF 40 Recommendations and the degree of effectiveness of the National AML/CTF System.

d. International standards: The relevant conventions, international treaties and UNSC Resolutions that set the scope or range of action of nations at the global level, and establish standards in relation to proliferation and its financing, were reviewed.

e. At the national level: Various types of information were used (e.g., commercial and financial), mainly from the National Customs Service, the Ministry of Foreign Affairs, the police (Investigative Police, Carabineros and the General Directorate of Maritime Territory and Merchant Marine of the Navy (Directemar), and the Financial Analysis Unit, among others, which, at the aggregate level, facilitate the identification of threats, vulnerabilities and mitigating factors. Information related to the country's regulatory framework, foreign trade data and other publicly available information was also reviewed.

f. Working groups with subject matter experts: The results of the roundtables with people who, given their experience, knowledge, and expertise, constitute a point of reference with respect to the understanding of the PF phenomenon, and have been identified to obtain their opinion, were considered.

Within the framework of MILAFT's Technical Roundtable (MT) on ML/TF/PF Risks, the background information on proliferation and its financing was reviewed in 2023.

This MT was attended by representatives of institutions that deal with these matters, both directly and indirectly, including the National Intelligence Agency (ANI), the police (Carabineros de Chile and the Investigative Police) and other institutions with permanent participation such as the Public Prosecutor's Office and the Ministry of the Interior and Public Security, among others.

2. Identification of PF risks: After analyzing the information collected, the potential threats, vulnerabilities and mitigants of the actions/activities that could impact the country were determined, from which it was proceeded to:

a. Determine current threats: In order to identify threats that the country could face regarding PF, a compilation and analysis of the information recorded in the reports published by the Group of Experts and the RUSI document "Guide to Conducting a National Proliferation Financing Risk Assessment" was carried out, which classifies and defines PF threats in three categories:

i. Products and financial services related to trade in proliferation-sensitive goods:

Correspond to those that can be used directly or in a modified form in the development of WMD, their delivery systems and related materials. They also include financial products/services related to foreign trade operations and their transportation.

ii. Fundraising activities (licit and illicit):

Generate revenue to eventually finance the acquisition or development of WMD or their delivery systems.

iii. Financial and corporate infrastructure supporting financial and goods movement:

Any type of financial or corporate infrastructure supporting the activities mentioned in the two previous categories. Includes the provision of financial assets or services to persons/entities subject to direct financial sanctions of PF.

b. Determine vulnerabilities: In general, vulnerabilities are matters, contexts (economic, social, political, technological, among others) or other situations that can be exploited by threats or exploited to facilitate and support threats. In this case, vulnerabilities should be understood as characteristics of the country itself, susceptible to being exploited not only by persons or entities designated for the PF, but also in maneuvers that violate or evade the SFD or by related third parties acting as intermediaries or controllers, in disregard of the provisions contained in the UNSC Resolutions on the matter.¹⁰

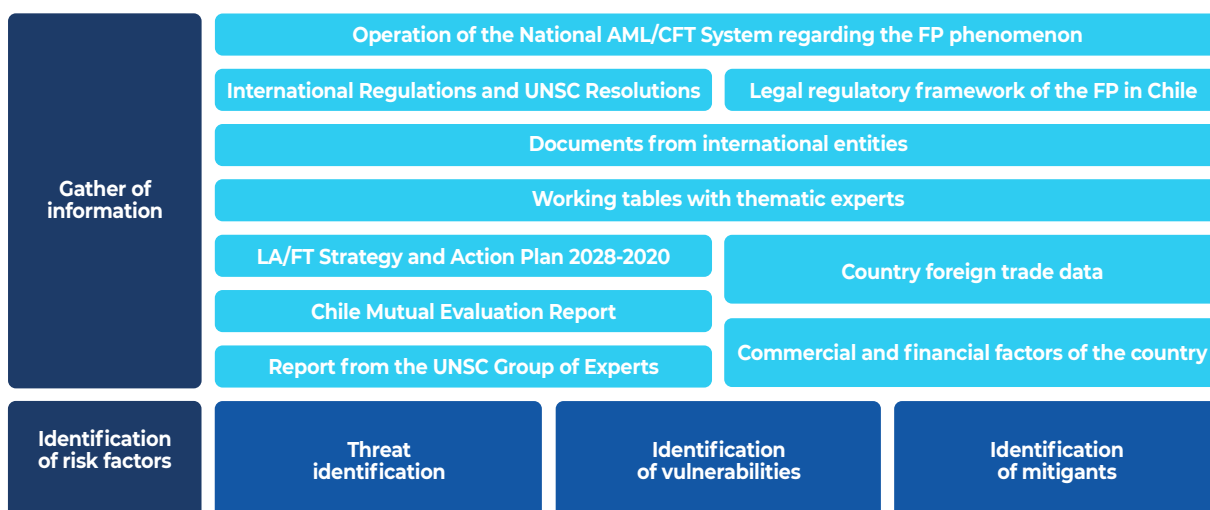
To identify vulnerabilities, the current regulatory framework related to the matters identified in the activities considered as PF threats was reviewed, as well as the information recorded in Chile's MER, which revealed, among other things, the strengths and weaknesses of the National AML/CTF System with respect to the PF phenomenon.¹¹

c. Determine mitigants: Mitigants were considered to be those economic or demographic factors that act as a structural and/or natural defense against the presence of hazards. These factors make it possible to reduce the probability of occurrence of harmful or undesired events in the PF context.¹²

In order to determine and identify the main mitigants, the information used comes mainly from the information recorded in Chile's MER by Gafilat, which evaluated, among other matters, the regulations related to PF TFS in the country. In addition, relevant information related to information security, cybersecurity and foreign trade, among others, was included.

ILLUSTRATION 2
Summary. Methodology for the National Risk Assessment of PF of Chile

Source: Prepared by UAF.





CHAPTER II: INTERNATIONAL STANDARDS, CONTEXT OF THE PROLIFERATION AND ITS FINANCING IN CHILE

CHAPTER II: INTERNATIONAL STANDARDS, CONTEXT OF THE PROLIFERATION AND ITS FINANCING IN CHILE

This chapter addresses the functioning of the National AML/CTF System regarding PF the current national regulatory framework, and the implementation of UNSC Resolutions.

INTERNATIONAL STANDARDS RELATED ON PF

Preventing and combating proliferation and its financing are part of an international effort, promoted by a series of intergovernmental organizations specialized in the field.

UNSC Resolution 1540 (2004), in addition to integrating international treaties and conventions on the subject into one document, obliges UN member countries, signatories or not of these treaties, to take concrete actions against proliferation and its financing.

FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an intergovernmental body created in Paris, France, in 1989 by the Group of Seven (G7) to set standards and promote the effective application of legal, regulatory, and operational measures to combat money laundering (ML), the financing of terrorism (TF) and other threats to the integrity of the international financial system.

To this end, it issues a series of Recommendations, recognized as the international standard for combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction (ML/TF/PF).

One milestone is the incorporation of international PF standard setting into the FATF mandate in 2008. Since 2012, the FATF incorporated Recommendation N°7 which establishes the implementation of TFSs to comply with the UNSC Resolutions related to the prevention, repression and interruption of proliferation and its financing.¹³

Additionally, in 2020, the FATF incorporated the obligation to assess the risks associated with Recommendation N°7. The FATF recognizes the close connection between PF, terrorism, and its financing, a phenomenon that has begun to be comprehensively addressed in the country.

Chile has generated regulations to prevent and repress PF, in line with compliance with international standards. This is aimed at the implementation of treaties, conventions, and UNSC resolutions related to proliferation and its financing. The country has also worked on measures to comply with the FATF Recommendations.¹⁴

Non-proliferation committee pursuant to Resolution 1540 (2004)

On April 28, 2004, the UNSC unanimously adopted Resolution 1540 (2004) under Chapter VII of the UN Charter. The Resolution affirms that the proliferation of nuclear, chemical and biological weapons and their means of delivery constitutes a threat to international peace and security. Since 2006, the UNSC has extended the Committee's mandate to strengthen cooperative relations with the international community in order to facilitate the implementation of Resolution 1540 by all States.

NATIONAL REGULATORY FRAMEWORK AND IMPLEMENTATION OF UNSC RESOLUTIONS

REGULATIONS AND INITIATIVES FOR THE IMPLEMENTATION OF UNSC RESOLUTIONS IN CHILE

Ministry of Foreign Affairs

Through supreme decrees of the Chilean Ministry of Foreign Affairs (Minrel, by its acronym in Spanish), the Resolutions issued by the UNSC on proliferation and its financing have been incorporated into the national legal system. The implementation of these can be summarized as follows:

In order to prevent and repress PF, the UNSC Resolutions binding on Chile in this area are:

- **Resolution 1540 (2004).**
- **Resolution 1718 (2006) concerning North Korea and its successors.**
- **Resolution 2231 (2015) concerning the Iran nuclear issue.**

1. Implementation of UNSC Resolution 1540 (2004) in Chile

This process is led by Minrel, which since 2004 has implemented various milestones for its execution:

- Creation of the Interministerial Committee for the Implementation and Compliance of UNSC Resolutions, 2012. This Committee acts as coordinator in the implementation and compliance with these Resolutions, as well as those issued by subsidiary bodies to the UNSC, by advising the Ministries.

During 2017, the 1540 Sub-Committee was created, the purpose of which is to implement the provisions of Resolution 1540. It is composed of different public institutions, including the National Customs Service, the UAF and the National Intelligence Agency (ANI) (Minrel, 2017, p. 3).¹⁵

- In September 2016, Minrel Decree N°145 was issued, which provides for compliance with Resolution 1540, and establishes that the authorities and State bodies ensure that, within the scope of their functions, the provisions contained therein are executed.
- In August 2017, the Permanent Mission of Chile to the United Nations presented the National Action Plan for the Implementation of UNSC Resolution 1540 (PANIR 1540) to the UNSC Committee the 2017-2021, jointly developed between Minrel and ANI. PANIR 1540 included five areas of work: (1) legislation, (2) capacity building and training, (3) international cooperation, (4) institutional strengthening, and (5) awareness raising in the public and private sectors, civil society and academia. Three of these five areas include specific or explicit measures related to proliferation financing (Minrel, 2017, pp. 6-13).¹⁶

2. Implementation of Resolutions and TFSs related to the PF in Chile

The Permanent Mission of Chile to the UN submitted, in November 2011, a report on the measures adopted under UNSC Resolution 1718, in accordance with its paragraph 11 (UNSC, 2011). In this document, it was reported that:

- The country took the decision to terminate all cooperative relations, both technical and commercial, with the DPRK (UNSC, 2011, p. 2).¹⁷
- Supreme Decree N°366 of the Minrel, published in 2007, contains the decision of the Government of Chile to comply with UNSC Resolution 1718, through the adoption of measures against the DPRK. In addition, it

indicates that the authorities and State agencies must ensure compliance with the provisions of UNSC Resolution 1718, within the framework of their functions (UNSC, 2011, p. 2).¹⁸

- In Chile, Law N°17.798 on arms control subjects to control the materials indicated in paragraph 8, letter a) subparagraphs **i)** and **ii)** of Resolution 1718, with the General Directorate of National Mobilization (DGMN) being responsible for the oversight and control of arms, explosives, among other goods in the country. (UNSC, 2011, p. 2)
- Regarding UNSC Resolution 2231 on the Islamic Republic of Iran, concerning the Iran nuclear issue, in August 2019, Minrel Decree N°128 was issued, which recorded the decision of the Government of Chile to comply with UNSC Resolution 2231. In addition, it states that the authorities and State agencies must ensure compliance with the provisions of UNSC Resolution 2231, within the framework of their functions.

2.1 Targeted Financial Sanctions imposed by the UNSC under Resolutions 1718 (DPRK) and 2231 (Iran): In relation to the TFSs imposed by the UNSC, under Resolutions 1718 (DPRK) and 2231 (Iran), Chile has a regulatory framework and a mechanism that executes the implementation of such TFSs under the terms required by the Resolutions.¹⁹

Minrel, through Decree N°214 (2020), established the measures implementing the UNSC Resolutions for the prevention and repression of the financing of activities affecting international peace and security, in particular the financing of terrorism (including Resolution 1373) and proliferation financing. With this decree, information was disseminated regarding the lists, implementation of measures and TFSs, together with information exchange and international cooperation.

The role of government agencies was also defined:

- **Ministry of Foreign Affairs:** It will be the point of contact and liaison with the UNSC and its Committees, as well as with other organizations or entities related to these regulations. It is also the actor in charge of receiving information on the updates sent by the UNSC regarding the persons/entities designated by the UNSC Committees on TF and PF, which are then forwarded to the UAF.²⁰
- **Financial Analysis Unit:** After receiving the information from Minrel, and within its legal powers, it may request or adopt measures to prevent and suppress PF, in addition to requesting and collecting relevant information in order to identify, under certain criteria, persons/entities susceptible to be included or eliminated from the lists designated by the respective UNSC Committees on TF and PF. Subsequently, the UAF will have to forward the information on identified persons/entities to Minrel, on a confidential basis, recommending their inclusion/deletion from these lists.

Annex 2 of this document includes the Minrel Decrees that have provided for compliance with UNSC resolutions related to proliferation and PF.

National regulatory framework for proliferation and proliferation financing

The main legal instruments governing proliferation issues in Chile are related to the security control of activities that may contribute to the illicit trade of strategic goods associated with chemical, biological, radiological or nuclear threats. These regulations correspond to:

- Law N°17.798, on arms and explosives control.
- Law N°18.302, on nuclear safety.
- Law N°21.250, which implements the Chemical and Biological Weapons Convention.²¹

These regulations address issues related to the manufacture, acquisition, possession, development, transport, transfer, use, participation as an accomplice in the aforementioned activities and assistance with means of delivery (means of delivery: missiles, rockets and other unmanned systems capable of carrying nuclear, chemical or biological weapons that are specially designed for such use).

In this area, one of the institutions in charge of overseeing and implementing controls on strategic trade is the National Customs Service, which, upon detecting any irregularity, must report it to the corresponding agencies for the investigation of crimes related to the proliferation of WMD, or, failing that, may submit a Suspicious Transaction Report to the Financial Analysis Unit.²²

In this regard, a bill is in the legislative process that creates the Strategic Trade Commission and regulates the export of dual-use and defense material, as well as other matters indicated.²³

In relation to arms control in Chile, Decree N°400 (2022) consolidated, coordinated and systematized the text of Law N°17.798, which deals with the matter. This body of law includes WMD among its components, establishing the prohibition of their possession²⁴. Infringement of this prohibition is punishable by a minimum to medium term of imprisonment. There is also a sanction when financing paramilitary groups that could use this type of weaponry.²⁵

It is necessary to consider that PF is not criminalized in Chilean legislation.

FUNCTIONING OF THE NATIONAL AML/CTF SYSTEM REGARDING PROLIFERATION FINANCING

Law N°19.913 constitutes a regulatory structure of the National AML/CTF System, composed of three fundamental pillars: prevention, detection and prosecution-punishment.

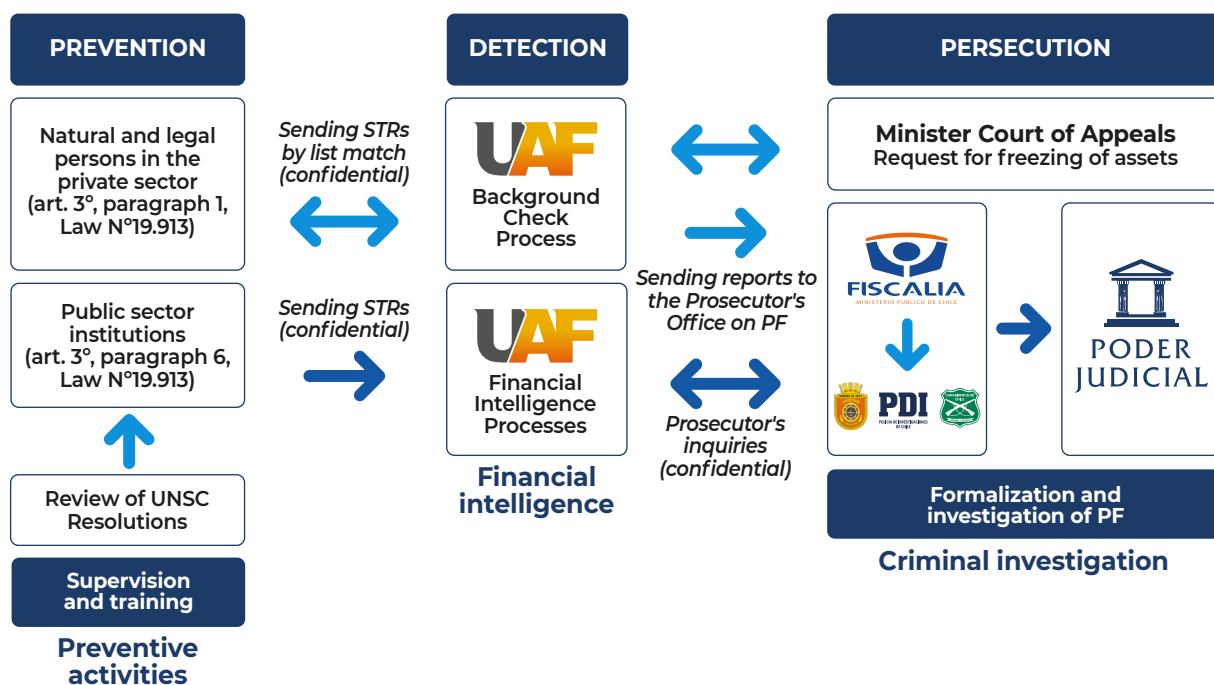
The System is made up of public institutions that regulate, supervise and prosecute ML/TF, in addition to all reporting entities (SO by its acronym in Spanish) to report suspicious transactions to the UAF (expressly indicated in Article 3° of Law N°19.913), through a Suspicious Transaction Report (STR).²⁶

The following is a summary of the functioning of the National AML/CTF System regarding the phenomenon of PF in the country.

ILLUSTRATION 3

Summary. Functioning of the National AML/CTF System regarding the PF phenomenon

Source: Prepared by UAF.



PREVENTION

The country's regulatory agencies and the natural and legal persons of the public and private sectors act in this area, as expressly indicated in Article 3° of Law N°19.913 (regulated entities).

These entities must implement ML/TF prevention and detection policies and procedures in accordance with their own organizational characteristics and risk matrices, all of which must be set out in a Prevention Manual (UAF Circulars N°49, 54 and 60).

In order to prevent PF, the country has a regulatory framework and a mechanism that implements the application of TFSs, in the terms required by the UNSC resolutions. The regulations in force in this area are based on Law N°19.913 and the circulars issued by the UAF, which must be complied with by all regulated entities.

Regarding the detection of natural or legal persons listed in the UNSC Resolutions, it is established that the regulated entities, in the circumstance of ***"detecting any person, company or entity that is mentioned in any of the lists of the UNSC Resolutions that sanction the financing of terrorism and the financing of the proliferation of weapons of mass destruction (...), shall send to the UAF, immediately, a STR reporting such finding, so that the UAF may proceed to take the asset freezing measures established in Article 38° of Law N°19.913"*** (Circulars N°49, 54 and 60).²⁷

Regarding compliance with the obligations to review the lists of UNSC Resolutions by the regulated entities, the regulations establish the duty to carry out these consultations through the implementation of specific procedures, which must be included in a Prevention Manual and effectively implemented. For this, UAF provides the necessary information for compliance with these measures by regulated entities through its website.²⁸

Likewise, it is established as an obligation to have procedures, in the respective Prevention Manuals, that ensure the permanent and timely review and checking of the lists of the UNSC Sanctions Committees, and there are means of verification that allow accrediting compliance with such obligations.

It should be noted that the public sector institutions responsible for the implementation of Resolution 1540 (Minrel, Customs, DGMN, among others) are obligated entities of the UAF and, therefore, must submit to this Service any suspicious transactions detected in the exercise of their functions, through a STR.

Dissemination and training activities

The UAF has a Training Plan aimed at both the private and public sectors, which develops content for the prevention and detection of ML/TF/PF, and guides the use of red flags on the subject and the implementation of procedures that allow the timely and confidential submission of STRs.

The training activities place special emphasis on the obligation of reporting entities to permanently review and check their clients on the lists issued by the UNSC Resolutions on TF and PF.

In addition, since the second half of 2019, PF-related subjects are part of the permanent contents of the training activities carried out by UAF, both in its in-person and remote format (e-Learning courses, free of charge).

The training activities place special emphasis on the obligation of reporting entities to permanently review and check their clients on the lists issued by the UNSC Resolutions on TF and PF.

In addition, in order to provide guidance to reporting entities and the general public regarding situations that should be considered as suspicious of ML/TF/PF, the UAF prepared and issued an updated version of its Red Flags Guide,

which describes the behaviors or characteristics of certain persons or transactions that could lead to the timely detection of a "suspicious transaction" of PF.²⁹

DETECTION

1. Suspicious Transaction Report for matching UNSC listings

The regulated entities must permanently review the lists of the UNSC Resolutions on TF and PF, and report immediately to the UAF, without prior analysis, through a STR, in case of finding any coincidence in the list, so that the UAF may proceed to take the asset freezing measure established in Article 38° of Law N°19.913.³⁰

Within 24 hours after receiving information (through a STR) that proves that the natural or legal persons identified in the lists drawn up by the UNSC intend to carry out a financial act, transaction or operation, the UAF must request a minister of the Court of Appeals of Santiago to adopt the necessary measures to prevent the use, exploitation, benefit or destination of any kind of goods, securities or money involved in the act, transaction or operation, without prior notice to the affected party and for a specified period of time. The validity of the measures decreed by the Minister of the Court may not exceed thirty days, which may be extended by a well-founded resolution.

2. Suspicious Transaction Report linked to possible PF activities

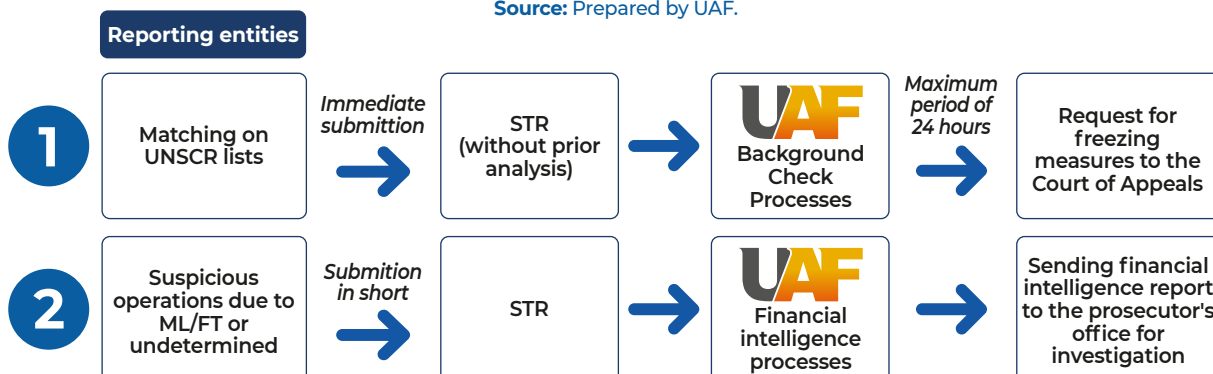
When any of the natural or legal persons expressly indicated in Article 3° of Law N°19.913 notices, in the exercise of their activity or functions, any act, operation or transaction that, according to the regulations, meets the criteria of "suspicion" of PF, they have the legal obligation to immediately submit this information to the UAF through a STR.

For this purpose, regulated entities must analyze the transactions and determine, according to their policies and procedures of their own ML/TF prevention systems, whether they are in the presence of a suspicious transaction that must be reported to the UAF.

Once the STR is received, the UAF activates its financial intelligence processes, with the sole objective of detecting initial signs of ML, TF or undetermined. If any, the UAF prepares and sends a confidential and timely Financial Intelligence Report to the Public Prosecutor's Office, the only institution responsible for investigating and criminally prosecuting those responsible for a crime.

ILLUSTRATION 4 Ways of reporting a STR to the UAF and its analysis process

Source: Prepared by UAF.



PERSECUTION AND SANCTION

The investigation and prosecution of possible offenses related to PF should be conducted exclusively by the Public Prosecutor's Office. Specialized police units, whose personnel participate under the direction of the prosecutor of the case, may collaborate.

IMPORTANT

It is important to note that PF is not criminalized in most jurisdictions at the international level, including Chile. On the other hand, other crimes that could be indirectly related to the PF are criminalized in the country, which could be committed with the aim of obtaining funds (drug trafficking, cybercrime, among others) and using them to finance proliferation.



CHAPTER III: DIAGNOSTIC OF THE PROLIFERATION FINANCING PHENOMENON IN CHILE

CHAPTER III: DIAGNOSTIC OF THE PROLIFERATION FINANCING PHENOMENON IN CHILE

In Chile, no investigations, prosecutions and/or formalized cases have been identified for crimes that could be related to proliferation activities and its financing. In line with this, UAF has also not received any suspicious transaction reports associated with PF.

During the period under analysis, no matches with the names of persons listed by the UNSC have been detected in the country, nor have there been cases of freezing of assets related to UNSC Resolutions regarding financial sanctions directed at the PF.

The following section identifies the PF phenomenon in Chile, integrating, mainly, information regarding:

- The National Strategy to Prevent and Combat ML/TF, which incorporates private and public sector approaches;
- Gafilat's Mutual Evaluation Report on Chile and its recommended actions;
- Mentions of the country in the reports of the Group of Experts on PF.

NATIONAL STRATEGY FOR PREVENTING AND COMBATING ML/TF AND 2018-2020 ACTION PLAN

With the aim of protecting the country from serious damage caused by ML/TF crimes, in December 2013 the Government of Chile launched a National Strategy to prevent and combat both crimes, with an Action Plan that was developed between 2014 and 2017.

During 2018, the second version of the National AML/CTF Strategy was built as an instance of integration, organization and interinstitutional coordination in the areas of prevention, detection and criminal prosecution of ML/TF, in order to strengthen the integrity of the country's financial and non-financial sectors.

In order to protect the national economy from the threats posed by these illicit acts, work was carried out on the implementation of anti-ML/TF/PF measures to strengthen the integrity of the country's financial and non-financial sectors.

The 2018-2020 Action Plan was the result of the work of 17 public institutions, supported by MILAFT, which was oriented to six strategic lines identified by the National Strategy member entities: **(1)** Updating of AML/CTF regulations, **(2)** Risk-based supervision, **(3)** Asset investigation and increased forfeiture, **(4)** Strengthening of capacities and skills for preventing and combating ML/TF (Training), **(5)** Inter-institutional cooperation and coordination, and **(6)** Financing of terrorism and that of the proliferation of weapons of mass destruction.³¹

This Plan contemplated the FT and PF problem as one of the strategic axes to strengthen the regulation, detection and sanction system, in particular, strategic line N°6 "Financing of terrorism and proliferation".

Two fundamental aspects were addressed through this axis:

- 1.** Evaluate and formulate proposals for legal reforms necessary for the incorporation of international regulations on TF and PF, and full compliance with international standards: To fulfill this purpose, in July 2019, Law N°21.163 was published in the Official Gazette, which incorporated the UNSC Resolutions on TF and proliferation in Article 38° of Law N°19.913.
- 2.** Make operational and coordination adjustments among the institutions in charge of preventing, detecting and prosecuting TF and PF: During the period, meetings were held to coordinate operational aspects of prevention, detection and prosecution of TF and PF.

In 2023, the members of the National Strategy, with the support of MILAFT began working on the development of a new Action Plan, with a view to the years 2023-2027, through 5 permanent technical roundtables on: Legislative Update, ML/TF/PF Risks, Supervision and Regulation, Criminal Prosecution and Financial Intelligence.

RESULTS OF GAFILAT'S MUTUAL EVALUATION OF CHILE

The Financial Action Task Force of Latin America (Gafilat, formerly Gafisud) is a regionally based intergovernmental organization that promotes the implementation and continuous improvement of policies to combat ML/TF/PF.

It was formally created on December 8, 2000 in Cartagena de Indias, Colombia, under the FATF model; therefore, it adheres to its 40 Recommendations and, in addition, supports its members in implementing them, through training measures and mutual evaluations.

Chile's evaluations correspond to the years 2006, 2010 and 2019-2021. The latter was carried out within the framework of the IV Round of Mutual Evaluations. The period evaluated comprised the actions taken by our country between 2015 and 2019, both years inclusive, to prevent and combat ML/TF, according to the new FATF Methodology (approved in 2012), which comprises criteria for reviewing technical compliance with the FATF 40R (the country's regulatory framework) and the actual effectiveness of the National AML/CTF System, based on a risk approach (measured through 11 Immediate Outcomes). During the evaluation process, and in its capacity as Chile's representative to Gafilat, the UAF acted as coordinator and liaison point.

In July 2021, the Plenary of Representatives of Gafilat approved the Final Report of the Mutual Evaluation of Chile, which was published in September of that year. Of the 40 R's, the country achieved 12 Compliant, 18 Largely Compliant,

9 Partially Compliant and none Not Compliant. Regarding the effectiveness of the National AML/CTF System, the country was rated in 3 Immediate outcomes as Substantial, 7 Moderate and 1 Low. With these levels of compliance, the Plenary decided to subject the country to an enhanced follow-up process, which means that Chile must report every six months the progress made to overcome the deficiencies detected (Gafilat, 2021).

Regarding PF, Gafilat's findings and recommended actions are as follows:

<p>Technical Compliance Recommendation N°7: Targeted Financial Sanctions Related to Proliferation</p>	<p>Recommendation N°7 (Targeted financial sanctions related to proliferation) Partially Compliant.³²</p> <p>The country has a framework for implementing TFSs measures for PF. However, the regime has the following shortcomings:</p> <ul style="list-style-type: none"> (i) There are doubts whether the system allows for the implementation of TFSs without delay.³³ (ii) The implementation of the freezing measures may be ordered only with respect to reporting entities (RE) of Law N°19.913 and not with general scope. (iii) There are doubts as to whether the freezing measure of Article 38° of Law N°19.913 could be revoked beyond cases of homonymity or removal from the list. (iv) The regulatory framework does not require that the obligation to apply TFSs fall on all natural and legal persons in the country. (v) There are limitations as to the scope of the assets subject to freezing under Law N°19.913. There is no evidence that public knowledge procedures have been implemented to submit requests for delisting from the UNSCRs of PF, as required by the criterion, and therefore no procedures are foreseen to allow listed individuals and entities to submit a delisting request to the Focal Point, in accordance with UNSC Resolution 1730.
<p>Effectiveness Immediate Outcome 11: "Individuals and entities involved in the proliferation of weapons of mass destruction are prevented from raising, transferring and using funds, in line with relevant United Nations Security Council Resolutions."</p>	<p>Immediate Outcome 11 (PF Financial Sanctions) Moderate Level.³⁴</p> <p>Main findings:</p> <ul style="list-style-type: none"> • Chile has regulations that allow it to impose TFSs related to PF. However, in certain cases, the prompt implementation of the measures could be affected by the stages foreseen in the respective procedure and by the deficiencies identified, although it should be noted that the most material sectors of the financial sector generally have the possibility to act promptly. • The country, through the UAF, disseminates in a timely manner the UNSC lists and their updates, which can be consulted on its website by all the financial RE of Law N°19.913. • The RE of Law N°19.913 seems to have an accurate level on the obligations related to the implementation of TFS in PF. However, the Designated Non-Financial Businesses and Professions (DNFBP) sector has opportunities for improvement. <p>Recommended actions:</p> <ul style="list-style-type: none"> • Reform the regulatory framework to ensure prompt implementation of TFS by PF by all RE without delay of Law N°19.913. In particular: amend the regulations so that TFSs can be implemented without delay, broaden the scope of freezing measures so that they are applied generally and not only to the RE that submitted the STR to the UAF, establish a general prohibition on the provision of funds or other assets to or for the benefit of designated persons or entities, extend the time period, and address the other technical deficiencies identified in relation to Recommendation N°7. • Issue additional guidelines and create awareness and training mechanisms for the RE of Law N°19.913, especially for DNFBPs, to promote permanent consultation of the UNSC lists. The work with non-financial RE should be deepened, so that they understand the importance of their role in the prevention of PF, as well as that already carried out with ML and TF crimes. • Ensure that all RE of Law N°19.913 are subject to permanent monitoring and sanctions for violations of their obligations regarding the implementation of the UNSC Resolutions on PF. • Establish a system to notify or alert the RE of Law N°19.913 when there is a change in the UNSC lists.

ANALYSIS OF THE REPORTS MADE BY THE GROUP OF EXPERTS THAT SUPPORT THE 1718 SANCTIONS COMMITTEE AND MENTION CHILE IN MATTERS OF PROLIFERATION FINANCING³⁵

For this NRA-PF, information recorded in 10 reports published by the Group of Experts of the UNSC Committee 1718 between 2015 and 2021 was compiled and analyzed.

The content was related to trade and financial activities carried out by the DPRK in an illicit manner, along with the various evasion maneuvers the country attempted to employ to violate the sanctions imposed by the UNSC. Foreign trade with Iran was also considered.³⁶

The following table summarizes the mentions of Chile by the Group of Experts assisting the 1718 DPRK Sanctions Committee, together with the complementary information available:

TABLE 1
Mentions of the Group of Experts and Chile's background regarding PF
Source: Prepared by UAF.

Actions/ Background	Group of Experts	Background information Chile
Commercial operations	Chile is listed as one of the countries that has carried out commercial operations (imports and/or exports) with both the DPRK and Iran in the period under consideration. Such business operations would have been related to luxury goods (wine) and import of commodities (coal/iron) (UNSC, 2018). ³⁷	DPRK: According to official figures from Chilean Customs Service, the country has had no trade with the DPRK in the period under review. The figures reported by the Group of Experts regarding the aforementioned operations correspond to a recording error by the competent national institution in this matter, considering the DPRK as the counterpart country, when in fact it corresponded to South Korea. Iran: There have been commercial transactions between Chile and Iran, mainly exports of forestry products and their derivatives, and other non-mining products. While imports, fundamentally, are those derived from petroleum (CAC, 2020a) (CAC, 2020b). ³⁸
Cyber-attacks or other similar actions	The report of the Group of Experts addressed three cyber-attacks in the country against financial institutions, possibly executed by hacker groups linked to the DPRK. (UNSC, 2019a) (UNSC, 2019b) (UNSC, 2021). ³⁹	Chile has indeed been subject to cyber-attacks against financial institutions, including a bank that in 2018 suffered a data and money hijacking (more than 10 million USD). Through investigations, the bank confirmed the international origin of the attack, an incident that was reported to the corresponding authorities and jurisdictions.

Therefore, given the situations described in the reports, Chile has been identified as a possible source of income for the DPRK, either through restricted or prohibited commercial activities, or as a target of cyber-attacks that would seek to obtain funds from financial institutions, which would have been executed, allegedly, by actors linked to the DPRK.

On the other hand, it is important to clarify the following points regarding Chile's performance in the area of PF. In this regard, in the Group of Experts reports supporting the 1718 Sanctions Committee, Chile:

- It is not identified as a transit country for financial movements made by designated or related persons/entities.
- It is not identified or mentioned in the reports analyzed as a country of transit of restricted or prohibited goods with origin/destination in the DPRK, nor with activities related to correspondent banking, financial operations of diplomats or persons/entities linked to that State.
- It is not associated with the use of legal entities, located in the country, to develop maneuvers of concealment of beneficial owners, nor the use of insurance company products.
- It is not mentioned as a country whose financial or corporate infrastructure has been breached by persons/entities designated or related to PF activities.
- Has not been involved in transactions or use of financial products or services in business transactions involving sensitive or dual-use goods, or other business relationship (e.g., restaurants) linked to DPRK workers.



CHAPTER IV: THREATS OF PROLIFERATION FINANCING

CHAPTER IV: THREATS OF PROLIFERATION FINANCING

In order to identify PF threats in Chile, documents prepared by the FATF, RUSI and the Group of Experts supporting the 1718 Sanctions Committee, which oversees the sanctions imposed by the UNSC on the DPRK, have been considered.

In the period under analysis, the DPRK is indicated as the major focus of proliferation threats and its financing. This is due to its continued development of WMD, despite the various sectoral and financial sanctions to which it has been subjected. In this scenario, Chile could eventually be exposed.

With regard to Iran, given that it is under a special regime, the sanctions regime imposed by the UNSC on Iran are on pause under the commitment of compliance with the JCPOA. In commercial terms, Chile did not carry out trade operations with Iran related to any type of goods associated with nuclear equipment, materials or technology, missiles, ships, combat vehicles, artillery systems, or the provision by its nationals or from its territory, of technical training, financial services, consultancy services related to the supply, sale, transfer, manufacture, maintenance or use of the aforementioned weapons and related materials, among others. It also does not maintain targeted financial sanctions measures against designated persons/entities from this country.⁴⁰

Therefore, the PF threats described in this section have their origin in the activities and operations carried out by the DPRK identified in the reports of the Group of Experts. Threats were identified as described, since Chile has no history of cases or situations related to PF, whether suspicious transactions reports, investigations, convictions, among others. Therefore, the analysis of this information is linked to the potential risks that the country could face.

The identified threats were classified into three categories:⁴¹

1. Products and financial services related to trade in proliferation-sensitive goods:

Correspond to those that can be used directly or modified in the development of WMD, their means of delivery and related materials. They also include financial products/services linked to foreign trade operations and their transportation.

2. Fundraising activities (licit and illicit):

Generate revenue to eventually fund the acquisition or development of WMD or their delivery systems.

3. Financial and corporate infrastructure supporting financial and goods movement:

Any type of financial or corporate infrastructure supporting the activities mentioned in the two previous categories. Includes the provision of financial assets or services to persons/entities subject to direct financial sanctions of PF.

In this regard, an analysis was made of the reports published by the Group of Experts, identifying the set of operations that could be classified in any of the three categories mentioned above and which, in turn, would constitute potential threats to Chile, according to their nature. These actions allowed the DPRK to generate and obtain revenues to eventually finance its WMD, delivery systems or related material development programs, and to access the international financial system through various sanctions evasion maneuvers.

No threats related to the first category, i.e., those associated with financial products and services related to trade in proliferation-sensitive goods, were identified. On the other hand, four threats related to fundraising activities (licit and illicit) were identified, and three associated with the use of financial and corporate infrastructure that supports the movement of finance and goods, as detailed below:

TABLE 2
Identified threats, by category

Source: Prepared by UAF.

Type of threat related to: ⁴²	Threat
Fund raising activities (licit and illicit)	1. Cyber-attacks, use of information technology platforms and operation with virtual assets (among other similar activities).
	2. Exportation/sale of coal, iron, steel, sand, among others.
	3. Luxury goods (particularly, manufacture of sportswear in the DPRK and other clothing for export). Alcoholic beverages (among others). ⁴³
	4. Sending workers abroad or the presence of DPRK nationals (or countries at risk).
Use of financial and corporate infrastructure to support financial and asset movement	1. Use of legal entities (including fictitious ones), for example, to hide information on beneficial owners.
	2. Banking: Representatives of DPRK banks abroad and financial transactions of diplomats and other DPRK officials.
	3. Use of insurance company products.

The following is an overview of the seven identified threats, which include methods used by the DPRK to illicitly obtain revenue and access to the international financial system.

1. Cyber-attacks, use of information technology platforms and operation with virtual assets (among other similar activities)

During the period, as recorded in the reports of the Group of Experts, the DPRK has generated illicit resources to finance its WMD programs, through cyber-attacks targeting financial institutions, mining and virtual asset brokers.

DPRK agents steal such assets for the purpose of laundering the proceeds of evading financial sanctions. There are also links between the DPRK and various cybercrime groups that develop and implement, among other things, a set of malicious tools to carry out cyber-attacks on various institutions.

As of 2019, at least 35 attacks were under investigation in 17 countries (including 2 cases in Chile), in the context of evasion of financial sanctions determined in UNSC resolutions. These had as a target various financial institutions and virtual asset platforms.

The year 2020 saw cyber-attacks against defense industries globally, perpetrated by actors linked to the DPRK. In these, it was attempted to access military technology and extract information for the purpose of generating illicit profits. Attacks on pharmaceutical companies developing vaccines against Covid-19 were also identified.

To obtain cryptoassets illicitly, the methods used by actors linked to the DPRK were:

- The use of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system to make transfers, accessing the banking infrastructure.
- Access to ATM network management infrastructure.

- Mining and theft of virtual assets.
- Social engineering operations.⁴⁴
- Use of malicious software.⁴⁵
- Fake job offers schemes, through various mechanisms, including email phishing.⁴⁶
- Phishing and spear phishing schemes, particularly targeting cryptocurrency intermediaries.

To transform illicitly obtained virtual assets into fiat currency, the DPRK used networks of poorly regulated virtual asset service providers and other unofficial brokerage services⁴⁷. With this in mind, the DPRK continued to focus on OTC (over-the-counter) virtual asset providers, mainly located in China. They also targeted companies that provide P2P⁴⁸ (peer to peer) services or those that do not require customer due diligence (CDD) information.

In Chile, the Group of Experts report addressed two cases that occurred in 2018, and one under investigation in 2020:

- The first involves the theft of USD 10 million from a domestic bank through unauthorized SWIFT transactions, destined mainly to accounts in Hong Kong. To achieve their goal, the criminals distracted the attention of bank officials by disabling around 9.000 computers through a malicious program. According to U.S. information, the perpetrators are reportedly linked to an organization that is part of the DPRK's General Reconnaissance Office.
- The second was executed using social engineering and targeted the "Redbanc" interbank network. Through a social network, the hackers contacted an employee of the company simulating a job offer. They conducted an interview in Spanish via teleconference and once they gained his trust, they got him to download a malicious program (malware). According to the company, this attack had no impact and services were able to continue operating normally.

- The third attack (September 2020) was on another national bank. Based on publicly available information, the Group of Experts indicated that it is investigating alleged attacks involving DPRK-related actors. In this sense, it has been indicated that hackers linked to the DPRK would be involved in this cyberattack, given its sophistication, magnitude and scale. This according to publicly available information, through specialized economic/financial media and cybersecurity companies.⁴⁹

The cyber-attacks that have occurred could be categorized as low impact, both in terms of the amounts involved and the financial/technological infrastructure affected and the operational disruption caused.

Nevertheless, it is not possible to discard the occurrence of the cyber-attacks. Not only regarding the size of the amounts, but also affecting the operational continuity of the associated financial services.

This point is one of the relevant risks that Chile would face with respect to the PF, at the level of IT, institutional and sectoral security.

2. Exportation/sale of coal, iron, steel, sand, among others

Regarding the DPRK, the main goods exported illegally were coal, as well as minerals, iron, sand and textile products. For the period analyzed, the DPRK exported coal along with other prohibited items, mostly to areas or territorial waters under Chinese jurisdiction.

The DPRK changed the way it transported coal by sea, since it was carried out through transshipments between ships. To circumvent the sanctions set forth in the various UNSC resolutions, it transferred cargo from DPRK-flagged or DPRK-controlled vessels to Chinese vessels.⁵⁰

Through various methods, even in their combination, it has sought to conceal the real origin of coal or other traded goods, and to hide its vessels from maritime tracking in databases. These operating patterns have been maintained during the period under analysis, and are characterized as follows:

- Use of intermediary networks through shell or fictitious companies in other countries.
- Misleading navigation routes.
- Manipulation or cessation of vessel location transmission signals.
- Manipulation or adulteration of vessel flags, identity numbers or vessel types.
- Use of false documents.

According to the Group of Experts, in 2017, Chile was listed with imports of around USD 35.000 in coal/iron originating in the DPRK. It should be clarified that these figures reported by the Group of Experts regarding the aforementioned operations correspond to a recording error by the competent national institution in the matter, considering the DPRK as the counterpart country, when in fact it corresponded to South Korea, so it is possible to point out that there was no foreign trade of these goods with the DPRK during the aforementioned period.

3. Luxury goods (particularly, manufacture of sportswear in the DPRK and other clothing for export), alcoholic beverages (among others)

In the period under review, the export/import of goods destined to the eventual direct or indirect financing of WMD programs was identified, including by designated persons/entities. In particular, regarding the transaction of revenue generating goods, the following were recognized:

- At least since 2014, the DPRK has been engaged in the manufacture and export of

luxury sportswear or other apparel. To this end, it uses low-cost labor and generates income from joint ventures with foreign firms.⁵¹

- Alcoholic beverage shipments to the DPRK. Reports indicated sales of these products by some European countries and Chile.^{52 53}

Regarding this last item, from June 2016 to August 2017, the Group of Experts recorded sales of alcoholic beverages by Chile, particularly wine, for an approximate amount of USD 290.000. However, according to official foreign trade figures published by the Chilean Customs, no trade with the DPRK was recorded in the period analyzed between 2016 and 2021.⁵⁴

Considering the above, Chile did not register any foreign trade activity with the DPRK, at least since 2012, according to statistical figures of the National Customs Service.

Therefore, there is no exposure from Chile to the DPRK as a counterparty in terms of commercial activities restricted or prohibited by UNSC resolutions. In this way, the country is complying with the various sectoral and trade sanctions set forth in the UNSC Resolutions against the DPRK.

4. Sending workers abroad or the presence of dprk nationals (or countries at risk)

Sending workers abroad to generate income is another form of DPRK fundraising identified in the reports of the Group of Experts⁵⁵. The DPRK workers would be employed in different fields, such as information technology (IT), construction, art, health, sports, hospitality, textiles, electronics and agriculture. DPRK restaurants were also identified in various Southeast Asian countries that, in some cases, operated after the repatriation deadline.⁵⁶

For example, in Ecuador, acupuncture professionals and translators whose contracts in the country expired in May 2020, were registered. Ecuador reported that measures were

implemented to terminate the contracts of these workers and repatriate them to the DPRK. In other cases, health professionals have been detected in countries in Asia and Africa.

One of the methods used is to enter countries as tourists or on student visas, a situation that has been identified in Russia and, eventually, in China. It was also noted that the national legislation of several countries allows for the generation of income for these workers, under certain circumstances.⁵⁷

In the case of Chile, through its Permanent Mission to the UN, it was reported that, in the period from 2005 to 2014, the country delivered 63 visas subject to contract to DPRK nationals. Of these, none are in force as of June 2020 and from 2015 onwards no such visas have been granted to DPRK nationals.

Regarding scientific/technical cooperation with individuals or groups, sponsored by the DPRK, such activities are suspended under the provisions of UNSC Resolution 2321 of 2016. In this regard, in April 2017, the Permanent Mission of Chile indicated that it does not maintain this type of programs or cooperation with the aforementioned individuals or groups sponsored by, or officially representing, the DPRK.⁵⁸

Considering the above, Chile does not register in its territory citizens of the DPRK as tourists, students or workers. In this sense, considering the various sanctions provided for in the UNSC Resolutions regarding the DPRK and its persons/entities, Chile presents a lower probability of occurrence of entry of DPRK nationals through legal or formal channels without proper registration and plausible reasons for entry.

In addition to the above, there is a lower probability of illegal entry, particularly due to their geographic remoteness, and few reasons for entry related to family roots, studies, or associated with commercial activities, given the lack of such activities.

Finally, Chile does not maintain diplomatic missions or facilities of the DPRK in the country that would justify the entry/exit of such citizens to the national territory.

5. Use of correspondent banking and legal entities to hide information on beneficial owners

Information received by the Group of Experts indicates that the DPRK has accessed the international financial system to make payments to suppliers and conceal information on beneficial owners in its operations. Among the methods used are shell companies, joint ventures, use of the name of foreign associates, crypto-asset services, use of correspondent banking, offshore bank representatives, off-shore accounts, among others.

It has been found that, unintentionally, corporate service companies such as financial institutions through correspondent banking services, have provided support or advice to persons and/or entities linked to the DPRK, for the development of prohibited activities. In this regard, it was found that DPRK companies and diplomatic missions opened bank accounts and provided the same services that a financial institution would provide.

These concealment methods and techniques target States with weak financial oversight standards, rules and/or regulations. According to one of the reports of the Group of Experts, "the illicit revenues generated by sanctions evasion activities and laundered through these networks support both, directly and indirectly, the DPRK's WMD and ballistic missile programs".

Regarding correspondent banking relationships in Chile, these institutions have a legal framework that allows them to deal with correspondent banking relationships, among other matters, with transnational banks, obtain information for a better understanding of the business, verify the reputation and quality of their supervision, and evaluate policies and procedures for the detection of suspicious ML/TF operations.

6. Banking: Representatives of DPRK banks abroad and financial transactions of diplomats and other DPRK officials

These activities allow the DPRK to evade sanctions by conducting business operations contrary to the UNSC Resolutions provisions.

Representatives of DPRK banks control bank accounts and conduct transactions involving large amounts of cash. The main evasion techniques employed by DPRK proxies operating internationally to open bank accounts included the use of foreign third parties, shell companies and, in some cases, using embassies themselves for their banking operations.

In addition, the Group of Experts, investigation revealed deficiencies in the CDD of some foreign financial institutions. Triangulation of payments through representatives of DPRK overseas banks was also observed in financial transactions related to coal and oil trade.

It was also attempted to access funds in frozen accounts, through embassy officials and false/suspicious documentation. To avoid sanctions such as freezing assets or limiting bank accounts, they use family members, shell companies and operate in other jurisdictions to open accounts. When opening these accounts, they also use different addresses, fictitious company names or names of different family members, different versions of a name, and so on.

DPRK diplomats have also been found to be purchasing prohibited items on behalf of companies related to designated entities. For this purpose, they use third countries to evade sanctions and send the goods to the DPRK, or use another country's citizen identification to accomplish this goal.

Through the verbale note of April 2017, the Permanent Mission of Chile to the UN informed that there were no banking institutions, branches or representations of banks of the DPRK in Chile, in compliance with the provisions of paragraph 31 of UNSC resolution 2321 (2016).⁵⁹

In this specific area, the exposure of the Chilean banking system is low due to the non-existence of banking institutions, branches or representations of banks of the DPRK. Therefore, in the country, the risk of PF activities through this direct channel of operations of financial institutions linked to the DPRK is non-existent.

In terms of requirements to enter the domestic financial market, the operation of most financial institutions in the country is authorized by their prudential supervisors. For example, the Financial Market Commission (CMF, by its acronym in Spanish), together with the Superintendency of Casinos, have procedures for licensing the operations of entities under their prudential regulation. In addition, all financial institutions must be registered with the UAF, which has the power to accept or deny registration (almost in its entirety, because the natural or legal person does not exercise the line of business expressly indicated in Article 3° of Law N°19.913).⁶⁰

In particular, in the case of the banking industry, licensing has three stages: provisional authorization, existence authorization and operating authorization. Entities must submit various documents evidencing solvency information, minimum capital requirements, company bylaws, structure, procedures and controls, among other areas.

7. Use of insurance company products

According to the information provided by the Group of Experts, there have been cases in which insurance companies have granted coverage to vessels carrying prohibited goods and/or savings products or life insurance to individuals. In some cases, the identity theft of vessels related to the DPRK was found to have taken place; as a result, insurance companies provided coverage without knowledge of such facts.

On another occasion, it was reported that a DPRK diplomat opened bank accounts in European institutions, using various evasion techniques, and then took out life insurance with savings, which the diplomat was able to withdraw later.

In this regard, according to the reports of the Group of Experts, the country has not been named in situations related to this matter.

SUMMARY OF PF THREATS ASSOCIATED WITH CHILE

Based on the information provided by the Group of Experts, the following threats faced by Chile and their level of incidence have been identified:

TABLE 3

Summary. Threats identified for the country according to the reports of the Group of Experts

Source: Prepared by UAF using information obtained from the reports of the Group of Experts.

(*) The status of these transactions was explained above in the corresponding section.

Type of threat related to: ⁶¹	Threat	Chile's Participation	Estimated level of incidence
Fund raising activities (licit and illicit)	1. Cyber-attacks, use of information technology platforms, and operation with virtual assets (among other similar activities).	Yes: 2018: Two cyber-attacks targeting financial institutions (ransomware and social engineering methods). 2020: A cyber-attack targeting a financial institution (ransomware method).	High
	2. Luxury goods (particularly, manufacture of sportswear in the DPRK and other clothing for export). Alcoholic beverages (among others). ⁶²	Yes: 2017: Sale of alcoholic beverages (wine) to persons/entities in the DPRK (USD 290.000) (*).	Medium
	3. Exportation/sale of coal, iron, steel, sand, among others.	Yes: 2017: Coal imports from the DPRK (USD 35.000) (*).	Low
	4. Sending workers abroad or the presence of DPRK nationals (or countries at risk).	No	Low
Use of financial and corporate infrastructure to support financial and asset movement	5. Use of legal entities (including fictitious ones), for example, to hide information on beneficial owners.	No	Low
	6. Banking: Representatives of DPRK banks abroad and financial operations of diplomats and other DPRK officials.	No	Low
	7. Use of insurance company products.	No	Low

Based on the above, the estimated level of incidence was assigned according to the following criteria:

- **High:** It is associated with activities or events (cyber-attacks) in which the country has actually been involved, or the operations have been named in the reports of the Group of Experts. Although the activities recorded have had a minor impact, both regarding the entities involved and the financial system as a whole, it is not possible to discard that more significant events could arise in the future, both at the individual level in relation to certain entities and at the systemic level, to the domestic financial system.
- **Medium:** Although the country has been mentioned in activities related to commercial operations (import or export) with the DPRK, it has been exposed to a lesser extent to these operations, both in terms of activities and associated amounts. Likewise, as mentioned above, according to data from Chilean Customs, there was no trade with the DPRK during the aforementioned period, which contrasts with the information recorded by the Group of Experts in their reports.
- **Low:** Regarding activities or operations mentioned, the country did not show exposure in these matters, as recorded in the reports of the Group of Experts. However, it is not possible to rule out a future occurrence of any of these events, given the nature of such activities, particularly those in which geographic remoteness is not relevant, for example, related to the use of fictitious legal entities to hide the beneficial owner of certain financial transactions.



CHAPTER V:

IDENTIFICATION OF VULNERABILITIES RELATED TO PROLIFERATION FINANCING

CHAPTER V: IDENTIFICATION OF VULNERABILITIES RELATED TO PROLIFERATION FINANCING

According to the FATF, designated persons/entities explore new and diverse ways to evade PF TFSs, where geography is not a limiting factor for DPRK and Iran. The reports of the Group of Experts reported movements in African and European countries, and identified financial operations in countries with weak AML/CTF/CPF controls to conceal the flow of funds.⁶³

Vulnerabilities could eventually be exploited for the purpose of violating or evading sanctions imposed by UNSC Resolutions, by designated persons/entities or other related parties.

This section identifies the country's main vulnerabilities based on the results of Chile's Mutual Evaluation Report (MER), and reports that address the country's foreign trade, cybersecurity and information technology (IT) infrastructure, new products and payment services. Vulnerabilities are mainly associated with:

1. Understanding the risk of PF.
2. Implementation of PF TFSs.
3. IT infrastructure, cybersecurity and trading activities.
4. New products and payment services.

1. VULNERABILITIES ASSOCIATED WITH THE UNDERSTANDING OF PF RISK

Chile's MER detected the existence of gaps on the knowledge of PF risks, the frequency and/or automatization in the review of UNSC sanctions by reporting entities in some economic sectors, and the non-inclusion of reporting entities in certain sectors relevant to the National AML/CTF/CPF System.

Regarding obligations related to PF TFSs, the MER indicated that while financial entities have an acceptable level of compliance, reporting

entities in certain DNFBP sectors show a lower level of understanding in these matters, so there are greater challenges and opportunities for improvement in this regard.

In this way, the Chile MER registered that although certain sectors belonging to the DNFBPs showed a periodic review of the lists of UNSC designations, this is not done with the frequency deemed necessary, which could eventually result in difficulties for asset freezing actions to be carried out without delay, in the case that there are coincidences in lists.

Also, some DNFBPs, such as notaries and real estate management companies, do not have automated systems or processes that issue alerts when there are changes in the lists of designations. This would facilitate early detection of name matches in lists and continuous verification, which would result in faster reporting of such activities.

Chile's MER also identified as a deficiency the non-inclusion of reporting entities of companies exporting dual-use materials and any other actor involved in this area, as well as international brokerage of sensitive material. Along with these, the MER pointed out that the law also does not consider lawyers, accountants, corporate service providers and precious stones and metals dealers of as reporting entities to the UAF.⁶⁴

Therefore, the various deficiencies mentioned above constitute a vulnerability for possible PF activities or operations not to be prevented, detected or investigated in the country.

2. VULNERABILITIES ASSOCIATED WITH THE IMPLEMENTATION OF PF TFS

Regarding the prompt implementation of PF TFS measures, Article 38° of Law N°19.913 allows for the freezing of assets of designated persons/entities derived from UNSC Resolutions related to PF.

In general terms, the mechanism involves the UAF requesting the Court of Appeals for asset freezing measures within 24 hours of receiving the information from the regulated entities.

At the same time, the Court must resolve the request within a period lesser than 24 hours, while the duration of the measures adopted is a maximum of 30 days, which may be extended by means of a well-founded resolution. Once these asset freezing measures have been decreed, the UAF notifies the reporting entity of the actions taken, so that they are implemented within a period lesser than 24 hours.

Regarding the implementation of PF TFSs, the MER indicated that the country's anti-PF regime could exceed the "without delay" notion of the standard, due to the time that would pass between the verification of the UNSC lists by the reporting entity, the sending of the associated STR and the subsequent application of asset freezing measures ordered by the courts of law.⁶⁵

Scope of PF TFS measures:

The MER indicated that in Chile there are no provisions in the legislation that the freezing of assets can be applied, as indicated in the standard to:

- All assets owned or controlled by the designated persons/entities.
- Assets owned/controlled wholly or jointly, directly or indirectly, by designated persons/entities.
- Assets deriving from other assets owned/controlled, directly or indirectly, by designated persons/entities.
- Assets of persons/entities acting on behalf of or under the direction of designated persons/entities.

Regarding the scope of the TFSs, the MER indicated that the obligation to apply these measures applies only to reporting entities included in the legislation,

and is not applicable to all natural and legal persons operating in the country.

Likewise, asset freezing measures are ordered only regarding the entity that reported the operation and not with a general scope (e.g., the entire financial system).

In this manner, Chilean law provides the possibility of appeal, in order to revoke the freezing measures. In this regard, the MER expressed doubts about the revocation of the freezing of assets in situations other than homonymy or removal from the lists of PF designations.

As noted by the MER, the country also has no regulatory provisions prohibiting all persons in the national territory from providing assets to designated persons/entities.

The aforementioned situations constitute a vulnerability to the National AML/CTF/CPF System, due to the country's regulatory deficiencies. Consequently, possible PF activities may not be detected in time, or freezing measures may be applied only on some assets of the designated person/entity. This could give rise to PF schemes that allow the possibility to avoid the application of TFSs by the country's entities.

3. VULNERABILITIES ASSOCIATED WITH IT INFRASTRUCTURE, CYBERSECURITY AND FOREIGN TRADE ACTIVITIES

CYBERSECURITY AND TECHNOLOGICAL INFRASTRUCTURE OF THE FINANCIAL SYSTEM IN CHILE

The annual Global Risk Reports published by the World Economic Forum (WEF)⁶⁶ over the past five years have successively included large-scale cyber-attacks⁶⁷ among the top 10 global risks in terms of likelihood of occurrence, and in three of

the five years in the top 10 in terms of impact. Additionally, between 2019 and 2021, these reports have included IT infrastructure⁶⁸ disruptions in the top 10 risks in terms of impact.

According to these reports, up until 2020 more than half of the global population will have access to the Internet, and approximately 2 out of every 3 people will own a mobile device. Although this generates both economic and social benefits for the population, there are also situations that represent a significant risk, such as the lack of a global technological governance framework, cyber insecurity and unequal access to the Internet, among other issues. Geopolitical and geoeconomic uncertainty are also mentioned as risks, which would threaten the development potential of new technologies.

According to these WEF reports, cyber-attacks on critical infrastructure have been frequent in the energy, healthcare and transportation sectors, affecting even entire cities. In the United States, a low probability of detection and prosecution was estimated at about 0.05%. In addition, it was estimated that there would be more than 21 billion technological devices globally, while attacks associated with these devices increased by around 300% in the first half of 2019. Damages from cyber-attacks could reach USD 6 billion, according to cybersecurity firm Cybersecurity Ventures.

According to the Cybersecurity Maturity Study in Chile⁶⁹ conducted by International Data Corporation (IDC)⁷⁰, which analyzed the state of cybersecurity in large Chilean companies and corporations, by measuring progress in this area⁷¹, 61% of these companies advanced towards higher levels of maturity, particularly in the dimensions of IT security processes and technologies, while over 40% still face the challenge of strengthening the skills of their human capital, the capabilities associated with risk management and strategic vision, as well as strengthening the culture related to shared responsibility associated with cybersecurity. The study also indicated that national corporations made greater progress in IT security maturity than large companies.

It should be noted that the three cyber-attacks registered in Chile during the period under review involved attacks using ransomware and social engineering, which compromised the IT systems and processes of the financial institutions affected.

Regarding the aforementioned, in relation to the domestic banking sector, in December 2020, the update of information security and cybersecurity standards came into force, whose adherence is considered in the evaluation of management and solvency performed by the CMF (Financial Market Commission) to banks, in relation to operational risks. In this regard, Chapter 20-10 was incorporated to the Updated Compilation of Standards (RAN, Chapter 20-10), which included the minimum guidelines for banks for an adequate management of risks related to information security and cybersecurity.⁷²

This regulation considers, among other matters, general management elements, information security and cybersecurity risk management, protection of critical cybersecurity assets and detection of threats and vulnerabilities, as well as response and recovery of activities in the event of incidents.^{73 74}

Within the framework above, the supervisor evaluates the relevance of the management system of the banking entity, according to certain elements such as: the existence of an organizational structure with personnel specialized in information security and cybersecurity; approval of policies for the management of these risks; an approved level of minimum availability in the delivery of services through technological platforms; determination of critical cybersecurity assets; identification of threats that may damage information assets, their vulnerabilities and consequences related to the loss of confidentiality, integrity and availability, among other aspects.

FOREIGN TRADE AND EXPORT CONTROL

In terms of foreign trade, in the 2016-2020 period, in particular regarding the means of transport in which this commercial exchange is generated, it is found that Chile, in terms of cargo (in tons), 96.6% of exports and 90.6% of imports were

carried out by sea, followed by land. In terms of amounts, 88.7% of those associated with exports (Free On Board amounts) and 76.6% of those related to imports (CIF amounts) were associated with maritime transport, followed by air transport, in both cases.

FIGURE 1
Part. % exports and imports (tons), by type of transport. 2016-2020

Source: Prepared by UAF, with data from the Chilean Customs.

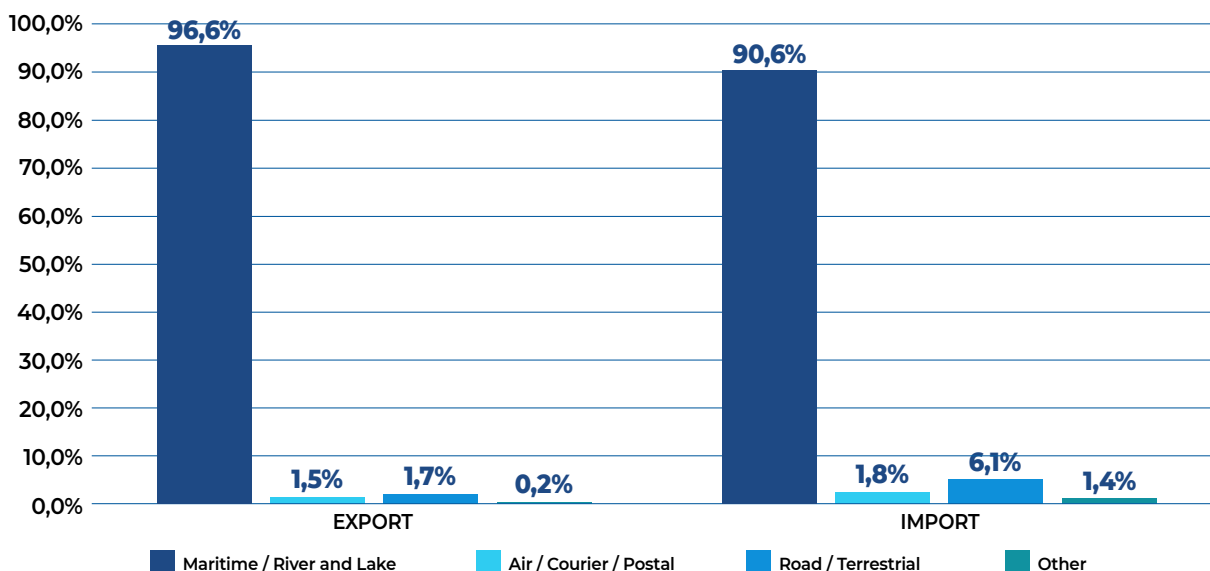
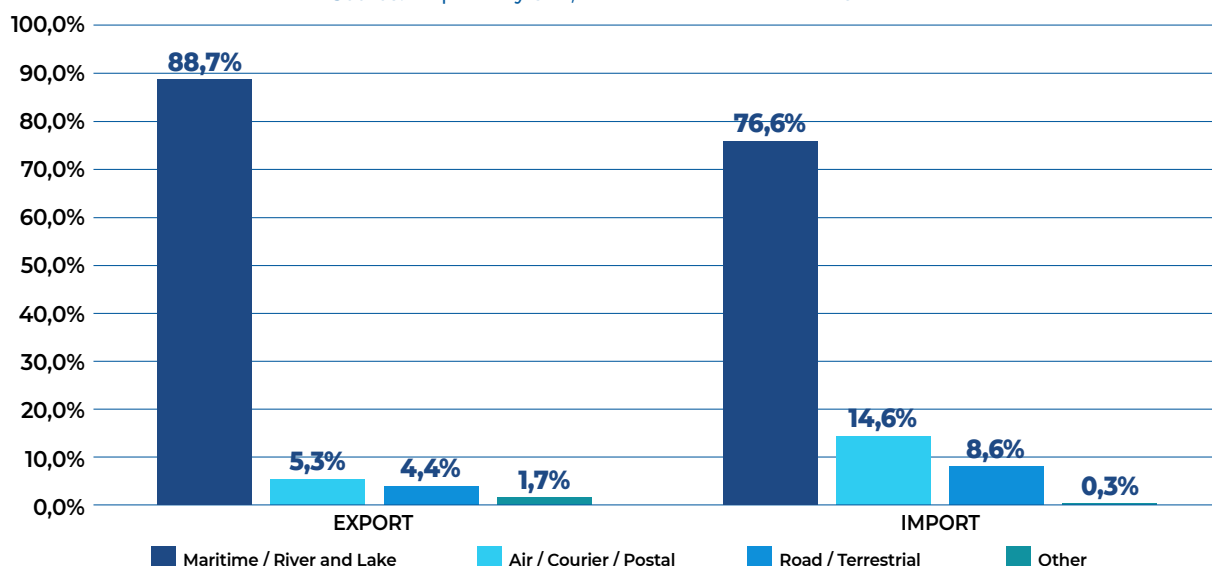


FIGURE 2
Part. % exports and imports (amounts), by type of transport. 2016-2020

Source: Prepared by UAF, with data from the Chilean Customs.



Interdiction and transportation measures:

In Chile, maritime interdiction operations are carried out by Directemar, a Chilean Navy agency whose purpose is to ensure compliance with the laws and international agreements in force, and to supervise maritime activities within the country's jurisdiction, among other matters. For this type of operation, there is also inter-institutional coordination between Chilean Customs and the police.

Chile, in 2015, through the Chilean Customs adopted amendments to a set of provisions related to smuggling of goods, which support compliance with the interdiction and transportation measures required by UNSC Resolution 2270 of 2016.

In relation to trade in prohibited goods, this offense is contemplated in Chilean regulations. Article 168° of the Customs Ordinance states that the crime of smuggling is committed by anyone **"who brings into or takes out of the national territory goods whose importation or exportation, respectively, are prohibited"**. This offense is also incurred by **"whoever removes goods from the country through unauthorized places or without presenting them to Customs"**.

This Ordinance also establishes penalties of imprisonment and a fine when there is a malicious false declaration, whether of origin, weight, quantity or content of the export goods. The above also applies to those who falsify certifications or analyses (either materially or ideologically) used to establish the origin, weight, quantity or content of export goods. It also establishes that consignors of goods leaving the country **"who present false, adulterated or partialized documents to serve as the basis for the preparation of the declarations, determining through them the classification or value of the goods"** will be sanctioned. (Customs Ordinance, 2005)

It is important to note that the dual-use materials regulated in Chile are those categorized as hazardous, which represent an imminent risk to the population, such as weapons, explosives, among others. Most of other sensitive goods are innocuous, and correspond, for example, of parts, components, pieces of equipment, that are not regulated as dual-use goods in Chile.

Chile has no regulations related to strategic trade controls, which constitutes a vulnerability in this regard.⁷⁵

The set of situations described above, regarding deficiencies associated with the cybersecurity situation in Chile (public and private sector institutions), with particular attention to those in the financial sector (due to their potential impact), in addition to the absence of regulations governing strategic trade, constitute vulnerabilities that could be exploited by the threats identified.

In the first case, these vulnerabilities could make certain sectors attractive as targets for cyber-attacks, either to illegally steal funds or to hijack data and demand payment for its release. In the second case, the absence of a related regulation with dual-use goods or materials, could create incentives to use the country as a transit route to commercialize and send certain dual-use parts or components abroad with poor traceability.

4. VULNERABILITIES ASSOCIATED WITH NEW PRODUCTS AND PAYMENT SERVICES

One of the vulnerabilities is related to new payment products and services that have emerged globally, in line with new technologies, whose characteristics make them attractive to ML/TF/PF.

The FATF report "Emerging Terrorist Financing Risk", published in October 2015, indicates that new electronic and online payment methods present an emerging vulnerability, which could increase as their use increases or becomes more widespread. Some of the characteristics that these products and services have in common are:

- They can be accessed globally, without border barriers, resulting in faster transfer of funds from one country to another.

- Difficulty in identifying the final beneficiary of these transactions, regardless of whether they can be traced.

In this regard, among the products and services analyzed in this report, the following stand out:

- **Virtual assets:** Designed to transmit value online. Their main characteristics are that they offer anonymity for transferring funds internationally (both at the user and transaction levels) and allow funds to be moved quickly from one country to another, which is why virtual asset-based payment products and services have attracted the attention of criminal groups and present ML/TF/PF risks.
- **Prepaid cards:** Correspond to cards that are preloaded with a fixed amount of money or electronic value. According to this report, the prepaid cards of greatest concern are open-loop cards, which allow withdrawing money from ATMs.
- **Internet payment services:** Provide the client with online mechanisms to access pre-funded accounts, which can be used to transfer funds to other accounts of the same provider. Recipients of funds may not have an obligation to register with the provider to receive the funds.

Regarding the deficiencies detected in these matters, Chile's MER indicated that there is no identification and evaluation of risks related to the development of *"new products and commercial practices, and to the use of new technologies or technologies under development for new or existing products"*.

In addition, it was pointed out that although provisions were identified for some financial activities, there is no legal framework applicable to the financial sector as a whole, with the objective of having them carry out risk assessments prior to the launch or use of such products, practices and/or technologies.⁷⁶

Therefore, the attributes of these new payment products and services, which involve virtual assets as well as prepaid cards and online payment services, result in vulnerabilities for the National AML/CTF/CPF System. This is due to the fact that persons/entities designated or linked to the proliferation could carry out PF activities and use these products and services, taking advantage of **1)** their anonymity characteristics to hide the origin/destination of the funds and the final beneficiary, **2)** the speed in the movement of funds to complicate their traceability and **3)** the non-existence of border barriers and intermediaries (in the case of virtual assets) to move the funds through different jurisdictions, or with the eagerness to hinder the traceability of the funds, which would make it difficult to prevent, detect and/or stop this flow of illicit assets.



CHAPTER VI:

IDENTIFICATION OF MITIGANTS RELATED TO PROLIFERATION FINANCING

CHAPTER VI:

IDENTIFICATION OF MITIGANTS RELATED TO PROLIFERATION FINANCING

According to the FATF, the key elements for a PF risk mitigation, to constitute a robust system for the implementation of TFSSs, are:

- A national risk assessment (at country and institutional levels).
- Effective regulatory framework.
- Broadcasting of sanctions to all relevant entities.
- Effective information exchange, cooperation and national coordination.
- Compliance monitoring and enforcement.
- Regular and in-depth training (conducted by the public and private sectors) on the topics of risks and obligations regarding PF TFSSs.

The following is a description of the main mitigating factors identified, mostly related to the current regulatory framework for PF in Chile.

1. MONITORING OF TFSS BY THE FINANCIAL SECTOR

Reporting entities have a duty to review the UNSC listings on an ongoing basis. They are also obliged to inform the UAF of all acts, transactions or operations carried out (or attempted to be carried out) by the persons/entities designated in the UNSC Resolutions related to PF, upon detection or existence of coincidences in the lists with this type of persons/entities. The UAF, upon analyzing the data received, may request the implementation of the freezing of assets of these designated persons/entities to the Minister of the Court of Appeals, a procedure described in detail in Article 38° of Law N°19.913.

In this regard, the Chile's MER indicated that reporting entities, especially those belonging to the financial sector, are aware of their duty to permanently verify the list of designated

persons/entities established by the UNSC. In fact, financial institutions perform automatic monitoring of these listings. It also pointed out that, in general, reporting entities carry out these reviews through their systems and that they have external suppliers and/or automatized tools that allow them to verify operations. It was also noted that in most of the ML/TF Prevention Manuals reporting entities have included obligations to review these UNSC lists, with respect TF and PF.

2. OVERSIGHT OF REPORTING ENTITIES' COMPLIANCE WITH TFSS MEASURES

The UAF has the power to supervise compliance by reporting entities with the measures related to the TFSSs of PF and, in case of non-compliance, to sanction them according to the Law.

In relation to the implementation of UNSC Resolutions, the authorities that ensure their compliance correspond to the Ministry of Foreign Affairs, which receives UNSC notifications through its Permanent Mission to the UN, which is responsible for their dissemination to the competent national entities.

According to Chile's MER, the UAF is the main supervisor in charge of verifying compliance with these measures by reporting entities. The UAF also verifies the obligation of reporting entities to review the UNSC lists and the ML/TF Prevention Manuals.⁷⁷

Between 2015 and 2019, the UAF detected 339 non-compliances when reviewing and checking the lists of the UNSC Resolutions by reporting entities, which resulted in 268 sanctioning processes ending with a sanction, which is equivalent to 79.1% of the total number of non-compliances being sanctioned by the UAF in the period.

Additionally, as part of the UAF's financial intelligence and monitoring processes, various technological systems and products are used. In particular, there's the Strategic Monitoring System, that corresponds to a system of detection, continuous and recursive search of patterns and typologies of ML/TF/PF risks, generating automatic alerts to the process of operational analysis, being able to analyze, in a massive way, records and transactions through various algorithms. The use of machine learning technology is a central part of these processes.

In summary, UAF's monitoring systems enable a robust prioritization-allocation process and, if applicable, a complete value-added analysis process. Furthermore, the UNSC lists are incorporated, and also integrate the information that the UAF reviews through an internal analysis tool.

3. NON-EXISTENCE OF DIPLOMATIC RELATIONS BETWEEN THE DPRK AND CHILE

As of 2023, the DPRK does not register an Embassy in Chile and Chile does not have an Embassy in the DPRK either.⁷⁸

At the Latin American level, five countries register DPRK embassies in their territories: Brazil, Cuba, México, Perú and Venezuela, while three of them have embassies in North Korean territory (Brazil, Cuba and Venezuela).⁷⁹

This results in a low incidence of DPRK diplomats with a permanent presence in the country, which eliminates any associated activity that could be considered a PF threat; however, it does not terminate the possibility of transit from neighboring countries with embassies.



CHAPTER VII: ASSESSMENT OF THE RISKS OF PROLIFERATION FINANCING IN CHILE

CHAPTER VII: ASSESSMENT OF THE RISKS OF PROLIFERATION FINANCING IN CHILE

Regarding the threats, vulnerabilities and mitigating factors identified throughout this document, no activities directly related to PF have been detected in Chile. In this regard, the country has no history of cases or situations related to the PF, whether suspicious transactions reports, investigations, convictions, among others.

However, financial institutions in the country have been the target of cyber-attacks, allegedly perpetrated by DPRK-linked actors, with the potential aim of financing WMD proliferation activities. In the period analyzed, three cases were recorded (two cases occurred in 2018 and one in 2020), which could be categorized as low impact, both for the amounts involved and for the financial/technological infrastructure affected along the operational disruption caused.

In this sense, it is not possible to rule out the occurrence of cyber-attacks that may have a greater impact or greater consequences, both in terms of the amounts involved and in terms of affecting the operational continuity of the associated financial services. Therefore, this particular threat, given the exploitation of certain vulnerabilities, such as the level of understanding of PF risk by reporting entities, IT infrastructure, new payment products/services (including virtual assets), among others, place cyber-attacks, mainly, as one of the relevant risk factors for Chile.

On the contrary, no other activities were identified that could take advantage of the mentioned vulnerabilities, such as foreign trade operations of commodities such as coal, iron or other minerals, presence of DPRK nationals with employment contracts in Chile, use of legal entities and/or related banking activity to move funds through the country, or use of insurance company products.

Given the above, **the estimated PF risk in Chile is low**, mainly determined by the cyber-attack activities registered in the country, which could take advantage in the future, mainly those vulnerabilities related to the understanding of PF

risk, IT infrastructure, cybersecurity and new payment products/services (including transactions with virtual assets), whose impact, although in the past has not been relevant at the operational level or in the affectation of the financial/technological infrastructure involved, it is not possible to rule out a greater impact in possible future events.



ATTACHMENTS

ATTACHMENTS

ANNEX 1: OTHER CONVENTIONS, TREATIES OR AGREEMENTS IN WHICH CHILE PARTICIPATES RELATED TO WMD

- **International Convention for the Suppression of Acts of Nuclear Terrorism:** It was adopted by the United Nations in 2005 and entered into force in July 2007, after 22 countries became parties to it. It was ratified by Chile on September 27, 2010, and published in the Official Gazette in April 2011 under Decree 252° of the Ministry of Foreign Affairs, which promulgated the Convention. This instrument punishes anyone who "unlawfully and intentionally" possesses radioactive material, or manufactures or possesses related devices with the objective of causing death or damage, including to property and the environment. It also punishes the (credible) threat using this type of material or device, and the unlawful solicitation under threat thereof, participation as an accomplice, organizer/instigator or contributor in the aforementioned acts.
- **Convention on the Physical Protection of Nuclear Material:** In 1980 this Convention was opened for signature by the States, entering into force in 1987 when 21 States had ratified it. Chile deposited the instrument of accession on April 27, 1994. Through the publication in the Official Gazette of Decree 1.121° of the Ministry of Foreign Affairs, it entered into force in our country on October 17, 1994. In July 2005, the States Parties to the Convention adopted an amendment to the Convention, which entered into force in May 2016. *Whereas the physical protection obligations under the Convention covered nuclear material in international transport, the Amendment (2005) established a legally binding obligation on States Parties to protect nuclear facilities and nuclear material in peaceful domestic use, storage and transport.*

It also provides for enhanced cooperation among States in taking prompt action to locate and recover stolen or smuggled nuclear materials, mitigate any radiological consequences of sabotage, and prevent and combat related crimes. The Convention and its amendment are the only internationally legally binding international instruments in the field of physical protection of nuclear materials.⁸⁰

Our country's acceptance of said amendment was deposited on March 12, 2009 and became part of our legislation in February 2017, through the publication in the Official Gazette of Decree 132° of the Ministry of Foreign Affairs.

- **Comprehensive Nuclear-Test-Ban Treaty:** 25 years after its adoption in 1996, this treaty has not yet entered into force, despite the signature of 185 States. This is because to enter into force it must be ratified by at least the 44 States listed in Annex 2 of this treaty, present at the time of its approval, 8 of which have not yet ratified it (United States, China, Iran, Israel, Egypt, India, Pakistan and North Korea). In particular, this Treaty prohibits carrying out, inciting, participating in or permitting nuclear tests in the territory of the States Parties, among other matters. Chile is one of the 36 States listed in Annex 2 of the treaty that have signed and ratified this instrument. This is because Chile signed the Treaty on September 24, 1996, and ratified it on July 12, 2000.
- **Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (Geneva Protocol):** A Protocol for the Prohibition of the Use of Chemical and Biological Weapons in Warfare, which entered into force on February 8, 1928 in response to the catastrophic results of World War I, when for the first time the modern use of chemical weapons was witnessed. It was signed by Chile on June 17, 1925 and ratified on July 2, 1935.

- **The Hague Code against the Proliferation of Weapons of Mass Destruction Ballistic Missile Delivery Systems (HCoC):** Aimed at strengthening disarmament and non-proliferation objectives and mechanisms, in particular, ballistic missile systems capable of delivering WMD. This code, together with the Missile Technology Control Regime (MTCR), are the only multilateral instruments focused on preventing the spread of ballistic missiles capable of carrying WMD. The Code came into force in 2002 and was developed outside the United Nations. Notwithstanding this, there are several UN resolutions that support it. At the moment, 143 States have signed it, including Chile (on November 25, 2002).

ANNEX 2:

TABLE WITH MINREL DECREES THAT HAVE PROVIDED FOR COMPLIANCE WITH THE UNSC RESOLUTIONS ON THE SUBJECT OF PF

TABLE 4
Chile: Decrees implementing UNSC Resolutions on PF

Source: Prepared by UAF.

Decree	Detail	Promulgation	Publication
Decree 366°	It complies with UNSC Resolution 1.718 of 2006, which adopts measures against the DPRK.	09-11-2006	20-06-2007
Decree 127°	It complies with UNSC Resolutions 1.874 of 2009 and 1.928 of 2010, which adopt measures against the DPRK.	27-09-2011	21-02-2012
Decree 30°	It implements UNSC Resolution 2.094 of 2013, which imposes measures on the DPRK.	04-04-2013	17-10-2013
Decree 9°	It implements UNSC Resolutions 2.087 (2013), 2.270 (2016) and 2.321 (2016), adopted by the UNSC, concerning the DPRK.	10-01-2017	15-07-2017
Decree 116°	Provides for compliance with UNSC Resolution 2.356 (2017) and its Annexes i and ii, adopted by the UNSC, concerning the DPRK.	22-06-2017	09-11-2017
Decree 186°	Provides for compliance with UNSC Resolutions 2.371 (2017) and its Annexes i and ii, and 2.375 (2017) and its Annexes i and ii, adopted by the UNSC, concerning the DPRK.	02-10-2017	29-03-2018
Decree 100°	Provides for compliance with UNSC Resolution 2.397 (2017) and its Annexes i and ii, adopted by the UNSC, concerning the DPRK.	02-04-2018	08-07-2019
Decree 128°	Provides for compliance with Resolution 2.231 (2015), adopted by the UNSC, regarding the Iran nuclear issue.	08-08-2019	09-01-2020
Decree 214°	Establishes measures implementing UNSC Resolutions for the prevention and repression of direct and indirect financing of activities affecting international peace and security.	17-12-2019	11-09-2020



BIBLIOGRAPHY

BIBLIOGRAPHY

- UNSC. (November 30, 2011). *United Nations Security Council. Note verbale dated 18 November, 2011 from the Permanent Mission of Chile to the United Nations addressed to the Chairman of the Committee. Security Council Committee established pursuant to resolution 1718.* Retrieved from <https://undocs.org/es/S/AC.49/2011/15>
- UNSC. (2016). *United Nations Security Council. Note verbale dated July 8, 2016 from the Permanent Mission of Chile to the United Nations addressed to the Chairman of the Committee.* United Nations. New York. Retrieved from https://www.un.org/ga/search/view_doc.asp?symbol=S/AC.49/2016/40
- UNSC. (March 5, 2018). *UN Security Council, Final Report of the Panel of Experts established pursuant to resolution 2345 (2017). S/2018/171.* United Nations. New York. Retrieved from <https://undocs.org/es/S/2018/171>
- UNSC. (August 30, 2019a). *United Nations Security Council. Mid-term report of the Panel of Experts established pursuant to resolution 2464 (2019). S/2019/691.* United Nations. New York. Retrieved from <https://undocs.org/es/S/2019/691>
- UNSC. (March 5, 2019b). *United Nations Security Council. Final Report of the Panel of Experts established pursuant to resolution 2407 (2018). S/2019/171.* United Nations. New York. Retrieved from <https://undocs.org/es/S/2019/171>
- UNSC. (March 4, 2021). *United Nations Security Council. Final Report of the Panel of Experts established pursuant to resolution 2515 (2020).* Retrieved from <https://undocs.org/es/S/2021/211>
- UNSC. (2022). *United Nations Security Council. Sanctions.* Retrieved from <https://www.un.org/securitycouncil/es/sanctions/information>
- FATF. (June 18, 2008) *Financial Action Task Force. Proliferation Financing Report.* Retrieved from <https://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>
- FATF. (February 2010). *Financial Action Task Force. Combating Proliferation Financing.* Retrieved from <https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf>
- FATF. (August 2021). *Financial Action Task Force. Anti-money laundering and counter-terrorist financing measures, Japan. Mutual Evaluation Report.* Retrieved from <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-japan-2021.html>
- FATF. (June 2021) *Financial Action Task Force. Proliferation Finance Risk Assessment and Mitigation Guidance (Guía para la evaluación y mitigación de riesgo de financiamiento de la proliferación).* Retrieved from <https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/traducciones/4104-guia-del-gafi-para-la-evaluacion-y-mitigacion-de-riesgo-de-financiamiento-de-la-proliferacion>
- FATF. (updated October 2021). *Financial Action Task Force. International Standards on Combating Money Laundering and Terrorist Financing, and the Financing of the Proliferation of Weapons of Mass Destruction (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.)* Retrieved from https://www.uaf.cl/descargas/legislacion/internacionales/GAFI_Recomendaciones_102021.pdf
- Gafilat. (September 2021). *Grupo de Acción Financiera de Latinoamérica. (Gafilat) Mutual Evaluation Report of the Republic of Chile.* Retrieved from <https://www.gafilat.org/index.php/es/noticias/145-informe-de-evaluacion-mutua-de-la-republica-de-chile>
- Law N°19.913 (December 18, 2003). *Ministry of Finance Creates the Financial Analysis Unit and modifies several provisions on money laundering and money laundering. Articles 19° and 20°.* Retrieved from <https://www.bcn.cl/leychile/havegar?idNorma=219119>
- Minrel. (August 18, 2017). *Ministry of Foreign Affairs 2017-2021 National Action Plan for the Implementation of United Nations Security Council Resolution 1540 (Plan de Acción Nacional 2017-2021 para la Implementación de la Resolución 1540 del Consejo de Seguridad de las Naciones Unidas).* Retrieved from https://www.un.org/es/sc/1540/national-implementation/pdf/chile_action_plan_es.pdf
- Customs Ordinance (2005). *Approves the consolidated, coordinated and systematized text of the decree with force of law of the Treasury N°213, of 1953, on customs ordinance.* Retrieved from <https://www.bcn.cl/leychile/havegar?idNorma=238919&idParte=>
- RUSI. (May 2019) *Royal United Services Institute. Guide to Conducting a National Proliferation Financing Risk Assessment.* Retrieved from <https://rusi.org/explore-our-research/publications/special-resources/guide-conducting-national-proliferation-financing-risk-assessment>
- SNA. (2020a). *Chile Aduanas Customs Exports by country and products Chile.* Retrieved from <https://www.aduana.cl/exportaciones-por-pais-y-producto/aduana/2020-05-19/105505.html>
- SNA. (2020b). *Chile Aduanas Customs Imports by country and products. Chile.* Retrieved from <https://www.aduana.cl/importaciones-por-pais-y-producto/aduana/2020-05-15/100754.html>
- UNODA. (2022). *United Nations Office for Disarmament Affairs.* Retrieved from <https://www.un.org/disarmament/>



FOOTNOTES

FOOTNOTES

1. This definition was adopted by the United Nations General Assembly through Resolution 32/84 on the prohibition of the development and manufacture of new types of weapons of mass destruction and new systems of such weapons. Part B, item 3. 100th Session, December 12, 1970.
2. In 1945, at the origin of the United Nations Organization, and specifically in the Fundamental Charter that created it, six main bodies are established, among which is the UNSC. Article 7° of the UN Charter establishes as the principal bodies of the United Nations: General Assembly, Security Council, Economic and Social Council, Trusteeship Council, International Court of Justice and the Secretariat.
3. ***"In order to ensure prompt and effective action by the United Nations, its Members confer on the UNSC primary responsibility for the maintenance of international peace and security, and recognize that the Council acts on their behalf in carrying out the functions assigned to it by that responsibility"*** Article 24° N°1 of the Charter of the United Nations.
4. See Article 39° of the UN Charter.
5. These sanctions are established in Article 41° of Chapter VII of the Charter of the United Nations, stating that: ***"The Security Council may decide what measures not involving the use of armed force shall be employed to give effect to its decisions, and may call upon the Members of the United Nations to apply such measures, which may include the total or partial interruption of economic relations and of rail, sea, air, air, postal, telegraphic, radio, and other means of communication, as well as the severance of diplomatic relations"***.
6. Article 25° of the UN Charter: The Members of the United Nations agree to accept and carry out the decisions of the UNSC in accordance with this Charter.
7. Resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), 1929 (2010) and 2224 (2015).
8. Paragraphs 8 and 9 of Resolution 2231 (2015) UNSC.
9. Hereinafter referred to in this document as the "Group of Experts".
10. Such as its economic, social and regulatory structures, the security of the technological infrastructure of its institutions, among other matters.
11. Regarding PF, the country obtained partially compliance with Recommendation N°7, which assessed technical compliance associated with proliferation-related TFSs, and a Moderate level of effectiveness in Immediate Outcome N°11, with respect to PF financial sanctions.
12. In this case, they correspond to actions of infringement, non-implementation and/or evasion of the TFSs of PF, as well as the carrying out of restricted and/or prohibited activities by the DPRK, which allow them to obtain resources to eventually finance WMD programs and/or access the international financial system and move their funds in a less restrictive manner.
13. The standards promoted by the FATF are contained in the 40 Recommendations, issued in February 2012 and last updated in February 2023.
14. Other international instruments in which Chile participates are included in Attachment 1 of this document.
15. The Resolution 1540 Subcommittee is chaired by the International and Human Security Directorate (DISIN) of the Ministry of Foreign Affairs, through its Non-Proliferation and Arms Control Unit (DISIN-NPCA). Among the main activities of this Unit are the following: Chairing the Coordination Table on Illicit Arms Trafficking; representing authorities in various commissions or committees related to the export of war material; implementation of UNSC Resolutions; and participating in the Radiological Emergency Safety Commission. It also participates in updating the regulations of Law N°17.798 (arms control) and Law N°21.250 (implementation of Chemical and Biological Weapons Conventions); and identifies the interdiction of strategic goods and WMD that is aimed at the agencies responsible for border security, for which it plans these tasks in conjunction with the Chile Aduanas Customs and the Chilean Nuclear Energy Commission (CChEN).
16. Submitted in accordance with paragraph 8 of Resolution 1977 (2011) and paragraph 5 of Resolution 2325 (2016), both successors to Resolution 1540, which encourage States to prepare national action plans on a voluntary basis, indicating their priorities and plans to implement the provisions of Resolution 1540, and subsequently submit such a plan to the 1540 Committee. This Plan was also supported by experts from the United Nations 1540 Committee and the Inter-American Committee against Terrorism of the Organization of American States (OAS).
17. In line with the second paragraph of Article 5° of the Political Constitution of the Republic, among other matters, it is the duty of the organs of the State to respect "the international treaties ratified by Chile and which are in force".
18. It should be emphasized that, if the UNSC Resolutions contain coercive measures applicable in the jurisdiction of the Member State, these must be previously incorporated into the domestic legal system. In this regard, and in relation to the 9 successor Resolutions to UNSC Resolution 1718, six Decrees of the Ministry of Foreign Affairs have been issued (and published) that give effect to such Resolutions, between the years 2012 and 2019. As for UNSC Resolution 2231 on Iran, the corresponding decree was issued in January 2020. These can be consulted in Attachment 2. It should be noted that the Supreme Decrees issued by the Minrel, in relation to the UNSC Resolutions related to proliferation financing, are an integral part of the Chilean legal system, making these norms obligatory for the entire population, which is complemented by the procedures established in Article 38° of Law N°19.913 and UAF Circulars 49, 54 and 60.
19. Those with similar characteristics to those implemented for TF purposes.
20. In order to fulfill its role as point of contact and liaison, Minrel may request and receive from other State bodies, and within its legal powers, the relevant information for cooperation with other countries, organizations or foreign entities.
21. Regulations for the implementation of the Law are still pending. The agency in charge of compliance with the Law is the DGMN, which is responsible for coordination and

- liaison functions with the Organization for the Prohibition of Chemical Weapons (OPCW) and the United Nations Office for Disarmament Affairs (UNODA), as well as with other international organizations related to the other States with respect to the matters addressed. Such coordination must be carried out through Minrel, with the collaboration and assistance of the Undersecretariat of Defense.
22. This procedure will be discussed in more detail in the next section.
23. Bulletin N°14.773-02:
<https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15272&prmBOLETIN=14773-02>
24. As stated in the final paragraph of Article 3°: "In any case, no person may possess or possess special weapons, which are those corresponding to chemical, biological and nuclear weapons".
25. As stated in Article 8°, first paragraph, of Decree 400°: "those who organize, belong to, finance, equip, instruct, incite or induce the creation and operation of private militias, combat groups or militarily organized parties, armed with any of the elements indicated in Article 3°, shall be punished with the penalty of prison mayor in any of its degrees".
26. The institutions include, in addition to the UAF, the Central Bank of Chile, the Financial Market Commission, the Ministries of the Interior and Public Security, Finance and Foreign Affairs, the Public Prosecutor's Office, the General Directorates of Pledged Credit and Maritime Territory and Merchant Marine of Chile, the Internal Revenue Service, the National Customs Service, superintendencies, the police and the Judiciary.
27. For further details, see UAF Circulars N°49, 54 and 60.
28. The UAF guides the search for the lists through its web site directed to the UNSC Resolutions. It can be consulted at the following link: https://www.uaf.cl/asuntos/consulta_onu.asp
29. This Guide is available on the UAF website.
30. The measures that may be ordered shall include the prohibition of the transfer, conversion, disposition or movement of funds or other assets during the term of the measure.
31. The institutions include, in addition to the UAF, the Central Bank of Chile, the Financial Market Commission, the Ministries of the Interior and Public Security, Finance and Foreign Affairs, the Public Prosecutor's Office, the General Directorates of Pledged Credit and Maritime Territory and Merchant Marine of Chile, the Internal Revenue Service, the National Customs Service, superintendencies, the police and the Office of the Comptroller General of the Republic.
32. Partially compliant corresponds to moderate deficiencies (FATF, October 2021 update, p. 154).
33. According to FATF, the phrase without delay means: "ideally, within hours of a designation by the UNSC or its Sanctions Committees" (FATF, October 2021 Update, p. 133). In this sense, a "without delay" deadline is considered to be within 24 hours (FATF, 2021, p. 105).
34. A moderate level corresponds to the fact that the immediate result has been achieved to a large extent, so that few improvements are necessary. (FATF, October 2021 update, p. 162).
35. The source of the information in these reports corresponds to the Member States that provide it to the Group of Experts, in addition to press and research reports from the Group itself.
36. This period is considered in order to analyze updated information.
37. This report of the Group of Experts is available at:
<https://undocs.org/es/S/2021/211>.
38. As established in Resolution 2231 on Iran, all States may engage in and permit activities with Iran, subject to UNSC approval, on a case-by-case basis, related to transfers and activities associated with nuclear energy (procurement channels), ballistic missiles, weapons, other related services of various kinds (technical assistance, consultancy, financial services, brokering, investment, among others).
39. The reports the Group of Experts are published in the following links:
<https://undocs.org/es/S/2019/691>
<https://undocs.org/es/S/2019/171>
<https://undocs.org/es/S/2021/211>
40. In relation to Iran, the FATF called on all jurisdictions to strengthen supervision for branches and subsidiaries of financial institutions based in Iran. It also requested to have improved relevant reporting mechanisms, or a systematic reporting of financial transactions, among other matters. The FATF stated that Iran would remain a high-risk country (blacklisted) until it complies with its Action Plan and ratifies the Palermo and TF Conventions.
41. Classification proposed by the RUSI in the document "Guide to Conducting a National Proliferation Financing Risk Assessment" (RUSI, 2019).
42. Category according to the RUSI threat definition described above.
43. UNSC Resolution 1718 in its paragraph 8, paragraph 3 established a prohibition on the sale or transfer of such items to the DPRK. In the case of alcoholic beverages, not all Member States classify them as luxury goods. It should be noted that luxury items included in the annexes of Resolutions 2094 (2013), 2270 (2016) and 2321 (2016) do not incorporate alcoholic beverages under this category.
44. A set of techniques used to obtain confidential data by infecting computers with malware or accessing links to infected sites.
45. They would also use so-called "crypto hijacking", using malware to infect (or "hijack") a computer and use it for virtual asset mining.
46. The Group of Experts also had information that a group linked to the DPRK was able to set up phishing infrastructure that mimicked well-known applications and websites (e.g. Microsoft Outlook), with the aim of tricking victims into obtaining their login credentials.
47. The attacks perpetrated against virtual asset exchange houses would have produced higher profits than those against financial institutions, given the greater robustness of the latter's information technology infrastructure. The Group of Experts encourages Member States to implement the FATF standards, emphasizing in Recommendation N°15, given that to manage and mitigate the risks associated with virtual assets "countries should ensure that virtual asset service providers are regulated for anti-money laundering and combating the financing of terrorism purposes and

- are licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures set out in the FATF recommendations".
- 48.P2P: Corresponds to the way of sharing all kinds of material among Internet users.
- 49.The information available on this case comes mainly from public information sources in the media, since there are no official reports in the public domain regarding this particular attack, neither from government agencies nor from financial institutions.
- 50.It should be noted that, as a result of the restrictions caused by the Covid-19 pandemic, exports of coal and other commodities, mentioned above, were reduced during the last two years of the period analyzed.
- 51.Ski clothing.
- 52.Whisky, vodka, wine, beer, cognac and brandy.
- 53.Shipments of alcoholic beverages to the DPRK practically stopped since the beginning of 2020 and were not available in the domestic market due to the restrictions due to the Covid-19 pandemic.
- 54.According to information provided by the Chilean Customs to press sources, after reviewing records from previous years, errors were detected by customs agents, particularly in coding, so it could happen that after subsequent revisions the erroneous figures are corrected.
- 55.It should be noted that paragraph 8 of UNSC Resolution 2397 (2017) requires Member States to repatriate all DPRK nationals earning income within their jurisdiction, and all government security monitoring attachés monitoring DPRK workers abroad, within 24 months from 22 December 2017.
- 56.In the IT area, it was estimated that the monthly salary was around 3.000-5.000 USD, with about one third going to the DPRK. The DPRK has reportedly sent IT-related workers to different countries in Europe, Asia, Africa and the Middle East, using companies in the destination country run by DPRK developers, or fake identities.
- 57.Given the pandemic scenario, it was reported that DPRK citizens have remained in other countries due to border closures.
- 58.Information corresponds to the Note verbale of April 7, 2017 addressed to the Chair of the Committee by the Permanent Mission of Chile to the United Nations.
- 59.Paragraph 31 of Resolution 2321 (2016) states that "Decides that Member States should take the necessary steps to close any representative offices, subsidiaries or bank accounts they have in the DPRK within 90 days, unless the Committee determines on a case-by-case basis that such offices, subsidiaries or accounts are necessary for the provision of humanitarian assistance or for the activities of diplomatic missions in the DPRK, or for the activities of the United Nations or its specialized agencies or related organizations or for any other purpose consistent with the objectives of this resolution."
- 60.Prudential supervisor for banking, securities and insurance.
61. *Category according to the RUSI threat definition described above.*
62. *Resolution 1718 in its paragraph 8, third clause, established a prohibition for the sale or transfer of this type of articles to the DPRK. In the case of alcoholic beverages, not all Member States classify them as luxury goods. It should be noted that luxury items included in the annexes of Resolutions 2094 (2013), 2270 (2016) and 2321 (2016) do not incorporate alcoholic beverages under this category.*
- 63.In a period prior to the period used for the analysis in this document, reports by the Group of Experts related to Iran (prior to the JCPOA) identified designated persons/entities that conducted restricted or prohibited activities, through third countries, in other regions, countries which possessed capabilities to develop WMD-related technology.
- 64.At the date of Chile's Mutual Evaluation, dealers in precious stones and metals were not considered obligated to report to the UAF. As of May 2023, these were incorporated as regulated entities (Law N°21.575) when they were expressly mentioned in Article 3° of Law N°19.913.
- 65.According to the FATF, the phrase "without delay means, ideally, within hours of a designation by the UNSC or its Sanctions Committees". (FATF, October 2021 update, p. 133). In this sense, a "without delay" deadline is considered to be within 24 hours. (FATF, 2021, p. 105)
- 66.This report is based primarily on the results of the Global Risk Perception Survey, conducted annually by the WEF. According to the methodology described in the report, this survey is completed by more than 650 members of the WEF leadership communities. In addition, the WEF's Global Risk Advisory Committee oversees the preparation of this report and provides input during the drafting process.
- 67.(Large-scale) cyber-attacks are described in this report as: "Large-scale cyber-attacks or malware that cause major economic damage, geopolitical tensions or a widespread loss of confidence in the Internet". According to this report, cyber-attacks can be diverse, ranging from data theft, to the use of ransomware, to the takeover of systems with large-scale, potentially damaging consequences.
- 68.IT infrastructure disruption (global technology risk) is described in this report as: "The deterioration, saturation or shutdown of critical physical and digital infrastructure/services as a consequence of systemic dependence on cyber networks and/or technology: AI-intensive systems, internet, laptops, utilities, satellites, etc."
- 69.Released in August 2021.
- 70.According to information published on the International Data Corporation (IDC) website, IDC is "the world's leading provider of market intelligence, consulting services, and events for the Information Technology, Telecommunications and Consumer Technology markets".
- 71.According to IDC, this study analyzed two groups of companies: large enterprises and corporations. A total of 154 executives from companies in different domestic industries, with annual sales of 4 million USD or more, were consulted. The companies were classified into different levels of maturity in relation to cybersecurity, through an evaluation in 5 dimensions: vision, risk management, human capital, processes and security technologies. This classification started at the

"Inexpert" category (they implement basic security measures as needs arise) up to the "Predictive Professional" level (they can predict and take effective action against cyber-attacks). Further details can be consulted at:

<https://www.idc.com/getdoc.jsp?containerId=prLA48174321>

72. Chapter 20-10 of the RAN defines "information security" as "the set of actions to preserve the confidentiality, integrity and availability of the entity's information". In turn, it considered the definition of cybersecurity as: "the set of actions for the protection of the information present in cyberspace and the infrastructure that supports it, which aims to avoid or mitigate the adverse effects of its inherent risks and threats, which may affect the security of information and the continuity of the institution's business".
73. Chapter 20-10 of the RAN defines "critical cybersecurity assets" as those "logical information assets that are considered critical to the operation of the business, including physical components such as hardware and technological systems that store, manage and support these assets, which, if not operated properly, expose the entity to risks that affect the confidentiality, integrity and availability of the information".
74. Chapter 20-10 of the RAN defined "information security incident" as: "unauthorized access, attempted access, use, disclosure, modification or destruction of information; an impairment in the normal operation of computer networks, systems or resources; or a violation of the entity's information security policy".
75. In January 2022, the National Congress received a bill, Bulletin N°14.773-02, which creates the Strategic Trade Commission and regulates the export of dual-use and defense material and other matters indicated. Through this legal body, two of the international instruments related to PF would be implemented, namely UNSC Resolution 1540 (it would complement the regulations already issued by the country based on this resolution, regulating other aspects of the phenomenon) and the Arms Trade Treaty (this Treaty entered into force in August 2018).
- According to the bill's Regulatory Impact Report, this law would subject to regulation the operation with dual-use material, that is, "the export, transit and international brokerage of equipment, materials and technology commonly used in civilian industry that could be used to produce and manufacture nuclear, chemical and biological weapons". The regulation would also include conventional weapons, their parts and components.
- To export this type of products, the law would require prior authorization based on the level of risk represented by the destination country/entity (flexible regulation), which would be determined by a Strategic Trade Commission. Therefore, it could be exported to countries without prior authorization through the granting of permits, for a determined period. It would also be a crime to use Chilean territory to attempt to divert materials regulated in Chile to countries/entities that are subject to United Nations sanctions (it should be noted that Chile is not a producer of these types of elements that would be subject to control, but rather an importer).

As indicated in the Regulatory Impact Report of the bill, the competitiveness of the national industry would be adversely affected by the absence of legislation of this nature, given that the countries that regulate the export of this type of elements have restrictions on their transfer to those countries where there are no regulations in this regard. In this scenario, re-export from unregulated countries suggests a risk to international security. On the other hand, it would also affect those companies interested in developing international business related to these elements (manufacturing under license, for example), since it would imply having access to them. Bulletin N°14.773-02: <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmlD=15272&prmlBOLETIN=14773-02>

76. In January 2023, Law N°21.521, which "Promotes competition and financial inclusion through innovation and technology in the provision of financial services" (also known as Fintec Law), was published in the Official Gazette. Its objective is to establish a general framework to encourage the provision of financial services through technological means by the providers governed by it. Among other matters, the bill includes as obligated parties (Article 3°, Law N°19.913) ***"those who are registered in the Registry of Financial Service Providers and in the Registry of Payment Initiation Service Providers maintained by the Financial Market Commission (CMF) and provide the services of collective financing platforms, alternative transaction systems, custody of financial instruments, intermediation of such instruments and payment initiation. The same reporting obligation shall apply to other natural or legal persons who, by virtue of any of their business activities, are subject to the supervision of the CMF and who have voluntarily requested their registration in the registry (...)"***.
77. Failure to comply with these obligations may result in penalties that could include fines of up to USD 206.000 (in repeated cases, up to USD 618.000).
78. Chile has not maintained diplomatic relations with the DPRK since September 1973 (information from the document "Relaciones bilaterales entre Chile y la Corea del Norte", extracted from the Library of the National Congress).
79. Information retrieved from: portals Embassypages.com (link: <http://embassypages.com/coreademocratica>) and Northkoreaintheworld.org (<https://northkoreaintheworld.org/diplomatic/dprk-embassies-worldwide>)
80. For more information, check: <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 (MILAFI), 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 MILAFI:

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 MILAFI) y no se afecte la imagen ni reputación institucional de las entidades involucradas o la del Estado. La MILAFI 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.



NATIONAL RISK ASSESSMENT OF **PROLIFERATION FINANCING** 2016-2021

MILAFT

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



**POLÍTICA
Nacional**
CONTRA EL CRIMEN
ORGANIZADO



PDI | **BRILAC
BRICO**
PROYECTO DE INVESTIGACIÓN
DE RIESGO

**CHILE
ADUANAS
CUSTOMS**

**ARMADA DE CHILE
DIRECTEMAR**

CMF | COMISIÓN
PARA EL MERCADO
FINANCIERO

Sii | Servicio de
Impuestos
Internos

UAF | UNIDAD DE
ANÁLISIS FINANCIERO
GOBIERNO DE CHILE



SCJ | SUPERINTENDENCIA
DE CASINOS DE JUEGO

SUSESO
Superintendencia
de Seguridad
Social
GOBIERNO DE CHILE

SP
Superintendencia de
Pensiones