COMISIÓN NACIONAL DE
ACTIVOS DIGITALES

Guide for Money Laundering and Terrorist Financing Risk Management for the Digital Assets industry

In order to provide specific guidelines for Digital Asset Service Providers (DASPs) regarding the application of articles 21 letter o) of the Digital Asset Issuance Law (DAIL), 19 of the Digital Asset Service Providers Regulation, and other applicable regulations for the management of Money Laundering, Terrorist Financing, and Proliferation of Weapons of Mass Destruction (AML/CFT/CPF) risks, which establish that these supervised entities must maintain a program against Money Laundering, Terrorist Financing, and Proliferation of Weapons of Mass Destruction in compliance with the Anti-Money Laundering Law and international best practices articulated by the Financial Action Task Force (FATF), this guide is issued, comprising the regulatory framework, international standards, and a risk-based approach.

For the issuance of this Guide, the results of the National Risk Assessment on Money Laundering and Terrorism Financing, as well as the National Policy for the Prevention of Money Laundering and Terrorism Financing (2023-2025), have been taken into account.

1. Regulatory Framework

The applicable legal framework for AML/CFT/CPF risk management for DASPs is as follows:

a) Anti-Money Laundering and Asset Laundering Law.
b) Regulation of the Anti-Money Laundering and Asset Laundering Law.
c) Instructions for the Prevention, Detection, and Control of Money Laundering and Asset Laundering, Terrorist Financing, and Proliferation of Weapons of Mass Destruction issued by the Financial Investigation Unit of the Attorney General's Office.
d) Special Law against Acts of Terrorism.
e) United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.
f) United Nations Convention against Transnational Organized Crime.
g) United Nations Convention against Corruption.
h) International Convention for the Suppression of the Financing of Terrorism.
i) Central American Convention for the Prevention and Repression of Money Laundering and Asset Laundering Crimes.
j) Digital Asset Issuance Law and its Regulations.

2. International Standards of the Financial Action Task Force (FATF)

FATF Standards apply to both countries and DASPs, as well as obligated entities providing services related to Digital Assets. In general, DASPs are expected to adopt similar ML/TF/PWMD prevention measures to those of the financial sector insofar as they engage in financial activities covered by FATF Recommendations.

Out of the 40 Recommendations issued by FATF, the following are particularly applicable and relevant to Digital Asset Service Providers:

a) Assessing risks (Recommendation 1).
b) Customer due diligence (Recommendation 10).
c) Record keeping (Recommendation 11).
d) Politically exposed persons (Recommendation 12).

e) Correspondent banking (Recommendation 13).
f) New technologies (Recommendation 15).
g) Wire transfers (Recommendation 16).
h) Reliance on third parties (Recommendation 17).
i) Internal controls and foreign branches and subsidiaries (Recommendation 18).
j) Higher-risk countries (Recommendation 19)
k) Reporting of suspicious transactions (Recommendation 20).
l) Tipping-off and confidentiality (Recommendation 21).

Additionally, all preventive measures must be applied, with two particularities:

a) The designated threshold for an occasional transaction triggering Customer Due Diligence (CDD) by DASPs is US$1,000.00.

b) The electronic transfer standards established in Recommendation 16 apply to DASPs and to transfers of Virtual Assets under the "Travel Rule."

The "Travel Rule," according to Article 84-B, numeral 1, letter e) of the Financial Investigation Unit (UIF) Instruction, includes all records of customers and operations that allow knowing the origin and destination of transactions with Digital Assets. In particular, through the application of the "Travel Rule," it is intended that in the case of a transfer of virtual assets, the originating DASP obtains and maintains the required and accurate information from the originator and the required information from the beneficiary, and that they immediately and securely send this information to the beneficiary DASP or financial institution (if applicable) and make it available to the competent authorities, including this Commission.

The information that may be included in the "Travel Rule" includes: (i) the date of the transaction, (ii) the type and quantity of each virtual currency, (iii) the name of the institution, its address, the nature of its main activity or occupation, and, in the case of an individual, their date of birth, (iv) the name and address of the beneficiaries, (v) the number of each account affected by the transaction, the type of account, and the name of each account holder, (vi) each reference number related to the transaction and serving a function equivalent to an account number, (vii) each transaction identifier, including sending and receiving addresses, and (viii) the exchange rates used and their source.

Under no circumstances should DASPs fail to collect and store information to be used through the "Travel Rule" in Digital Asset transfers, regardless of the transaction amount.

3. Beneficial Ownership

DASPs must exercise special care and diligence in the application of Article 21-A of the Instruction for the Prevention, Detection, and Control of Money Laundering and Asset Laundering, Terrorist Financing, and Proliferation of Weapons of Mass Destruction issued by the Attorney General of the Republic. According to this provision, every DASP, as an obligated entity under the ML/TF/PWMD prevention regulations, must identify and verify the identity of the Beneficial Ownership of individuals or legal structures, obtaining information about the identity of the individual or individuals who ultimately hold the majority shareholding in the legal entity.

Compliance with this regulatory obligation is particularly relevant in transfers or exchanges carried out with Digital Assets.

4. Suspicious Transactions

As a consequence of the proper implementation of Customer Due Diligence (CDD), DASPs must identify, document, and report to the Financial Investigation Unit (UIF) those operations that may be considered irregular, inconsistent, or unrelated to the client's type of economic activity.

The obligation contained in Article 9-A of the Anti-Money Laundering and Asset Laundering Law is emphasized, which establishes that every obligated entity, as is the case for DASPs, must report to the UIF any attempt of suspicious transactions.

5. Risk-Based Approach

Regarding the risk-based management approach, entities supervised by the National Digital Assets Commission (CNAD) are required to implement a risk management system. This system should be understood as a strategic process carried out by the entire entity, whereby they identify, assess, mitigate, monitor, and communicate the various types of risks they are exposed to. This management should be in line with their nature, risk profile, volume and complexity of their activities, business lines, own and third-party resources.

a) Inherent Risk

The risk management system of each PSAD must be capable of mitigating the inherent risks of authorized operations. This is the level of risk inherent to the activity, without taking into account the effect of controls. Therefore, the different levels of exposure to the inherent risk of each activity are presented below, related to Article 19 of the Digital Asset Issuance Law, categorized into four levels ranging from low, moderate, above average to high.

Inherent Risk of AML/CFT/CPF for each authorized activity for PSAD.

Activity	Inherent Risk
a) Exchange of digital assets for fiat money or its equivalent, or for other digital assets, either using one's own capital or that of a third party.	**High Risk**: Transactions between digital assets and fiat money pose a higher risk, as it is necessary to determine the origin of the funds, whether in fiat money or digital assets. This is considered a highly relevant entry filter against AML/CFT/CPF risks and, therefore, an activity with high-risk exposure.

b) Operating a platform for the exchange or trading of digital assets or derivative digital assets.	**High Risk:** Transactions pose a greater risk if they involve a hot wallet. Therefore, their risk level is considered high.
c) Risk and price assessment, as well as the subscription of digital asset issuances.	**Moderate Risk:** Since it involves technical opinion or advisory services, its level of exposure is moderate. Additionally, there are other more relevant entry filters (Certifier and CNAD) that contribute to preventing AML/CFT/CPF risks in the issuance and exchange of digital assets. However, this does not exempt the responsibility of verifying the origin of funds for the clients for whom services are provided.
d) Placing digital assets on platforms or digital wallets.	**Moderate Risk**: Since there are other filters (Certifier and CNAD) to prevent AML/CFT/CPF risks before a PSAD places a third party's issuance on the platform, this activity is considered of moderate risk.
e) Promoting, structuring, and managing all types of investment products in digital assets.	**Moderate Risk:** Since it involves a complementary service and advisory, its degree of exposure is moderate. Additionally, there are other relevant entry filters (Certifier and CNAD) that contribute to preventing AML/CFT/CPF risks in the issuances and exchanges of digital assets.
(f) The following operations when carried out on behalf of and for the benefit of third parties.	

f.1) Transferring digital assets or the means to access or control them, between individuals or legal entities, or among different acquirers, electronic wallets, or digital asset accounts.	**High Risk:** Transactions between digital assets and fiat money pose a greater risk, as it is necessary to determine the origin of the funds, whether in fiat money or digital assets. This is considered a very relevant entry filter in the face of the risks of Money Laundering (LDA), Terrorism Financing (FT), and Prevention of Abuse in Market Development (FPADM), and therefore, an activity with high-risk exposure.
f.2) Safeguard, custody, or administer digital assets or the means to access or control them.	**Above Average Risk:** The existence of controls to determine the origin of assets and prevent illicit funds from entering the system is relevant. However, this activity is considered a secondary filter; therefore, it is rated above average.
f.3) Receive and transmit purchase or sale orders for digital assets or the negotiation of derivative digital assets.	**Above Average Risk:** The presence of controls to determine the origin of assets and prevent illicit funds from entering the system is relevant. However, this activity is considered a secondary filter; therefore, it is rated above average.
f.4) Execute purchase or sale orders of derivative assets.	**Above Average Risk:** The presence of controls to determine the origin of assets and prevent illicit funds from entering the system is relevant. However, this activity is considered a secondary filter; therefore, it is rated above average.

In the previous table, it is highlighted that activities with high risk are characterized by receiving fiat money, virtual assets, or hot wallets, which may originate from sources where it is unknown whether a Money Laundering (LDA)/Terrorism Financing (FT)/Market Development Abuse Prevention (FPADM) risk management process based on international standards has been conducted. Meanwhile, activities such as subscription of issuances, placing assets in wallets, and structuring of digital assets are considered to have a moderate risk. Clients undergoing these processes are required to provide more information to PSADs. For instance, in the structuring of a token for financing a real estate project, the issuer must present financial information, management details, project history, and undergo certification and review processes by CNAD. This is necessary to instill greater confidence in investors acquiring the Digital Assets.

b) Risk Management of AML/CFT/CPF

Within certain aspects that CNAD will evaluate during supervisory visits to PSADs to verify the existence of an effective program against Money Laundering, Terrorism Financing, and the Proliferation of Weapons of Mass Destruction that mitigates inherent risks, in accordance with international standards, include:

1. Board of Directors or equivalent body:

As the principal governing body of the corporate governance of each PSAD, CNAD will verify compliance with all sections of Article 5 of the UIF Instruction.

2. Compliance Officer:

Aspects to be reviewed include registration with the UIF, reports of regulated operations, compliance with the requirements of the titular and substitute Compliance Officer, independence and autonomy of the Compliance Officer from operational areas, use of a risk-based approach in managing the risk of Money Laundering, Terrorism Financing, and Proliferation of Weapons of Mass Destruction, monitoring system, parameterization, and generated alerts.

3. Customer Due Diligence:

During reviews, the effectiveness of standard, enhanced, simplified due diligence processes, transfer travel rule, as well as existing processes for politically exposed persons, definition of high-risk clients, operations with higher-risk countries will be evaluated. For legal entities, the identification process of the ultimate beneficial owner and trusts will also be verified. Additionally, the customer information update policy used by PSADs will be checked.

4. Other Aspects:

The Internal Audit function, Training Plan for the prevention of Money Laundering, Terrorism Financing, and Proliferation of Weapons of Mass Destruction, Institutional Code of Ethics, Information Security Policy, and its safeguarding will also be evaluated.

c) Risk-Based Supervision

The result of identifying all inherent risks resulting from the operations of each PSAD, including the risk of Money Laundering, Terrorism Financing, and Proliferation of Weapons of Mass Destruction, when assessed together with the quality of their management as mitigating factors obtained from supervisory visits, will generate for CNAD the Risk Map of each PSAD. This map is an important internal input to guide available resources towards entities with higher residual risks, upon which supervisory actions will be applied based on the criticality of the determined findings.

The Board of Directors of the National Digital Assets Commission in accordance with the legal powers established in article 9, letter o) of the Law for the Issuance of Digital Assets agrees to approve and publish this guide in a session on December 22, 2023