

CORPORATE POLICY ON COMBATING MONEY LAUNDERING, CONCEALMENT OF ASSETS, RIGHTS AND PROPERTY, AND FINANCING OF TERRORISM AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (AML/CFT)

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

CONTENTS

1	PURPOSE.....	3
2	SCOPE.....	4
3	REFERENCES.....	4
4	CONCEPTS	6
5	GUIDELINES	7
6	RESPONSIBILITIES	9
7	FORESEEN SANCTIONS.....	15
8	FINAL PROVISIONS	15
9	CHANGE LOG.....	15

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

1 PURPOSE

B3 collaborates with government authorities on combating money laundering, concealment of assets, rights and property, and financing of terrorism and proliferation of weapons of mass destruction (AML/CFT), pursuant to Article 9, Sole Paragraph, Indent (I), of Law 9,613/1998, as amended by Law 12,683/2012, and to Articles 3 and 4 of CVM Resolution No. 50, dated August 31, 2021.

In compliance with best AML/CFT practices, B3 drafted this Corporate Policy, through an Internal Committee created for this purpose to establish the Program on Anti-Money Laundering, Preventing Concealment of Assets, Rights and Property, and Countering Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT Program).

To prevent and combat the use of the financial system, and the markets managed by B3 in particular, to launder money, conceal assets, rights and property, and finance terrorism and the spread of weapons of mass destruction (ML/CFT), this document is made known to the Company's executive officers, employees, interns, relevant service providers, suppliers and partners, who commit to comply with its guidelines and determinations.

Through this Policy, which is reviewed and approved by the Board of Directors each year, B3 undertakes to develop and maintain effective AML/CFT processes and controls that reflect best local and international practices for peer service providers.

Pursuant to Article 22, Paragraph 3, of CVM Resolution No. 50, dated August 31, 2021, B3 reports to the Council for Financial Activities Control (COAF) any detected situation or transaction liable to constitute serious ML/CFT evidence, within 24 (twenty-four) hours of completion of the analysis that characterized the unusualness of the transaction or proposal, or even the atypicality of the situation detected or declared by the AML/CFT Internal Committee, as a suspicious activity.

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

Through a risk-based approach and transaction monitoring, B3 selects the unusual transactions and suspicious situations, with the purpose of performing all the procedures associated with their assessment and reporting flow to COAF, if applicable, within 30 (thirty) days of the date of the transaction or situation.

This Policy establishes controls, principles and guidelines for B3's AML/CFT Program, based on legal and regulatory requirements applicable to the Company, and also on international best practices. The purpose of the AML/CFT Program is to prevent products and services provided by the Company, and the markets it manages, from being used in tortious acts connected with ML/CFT and similar or prior crimes.

2 SCOPE

This Policy applies to all executive officers, employees, interns, relevant service providers, suppliers and partners of B3 S.A. – Brasil, Bolsa, Balcão, its subsidiaries abroad, as well as of BSM Market Supervision, Cetip Info Tecnologia S.A, B3 Social and other associations (Company), except for Banco B3 S.A., which has its own Policy.

3 REFERENCES

This Policy must be read and construed in conjunction with the following documents:

- Brazilian Federal Law No. 9,613, dated March 3, 1998, and amendments;
- Brazilian Federal Law No. 13,260, dated March 16, 2016;
- Brazilian Federal Law No. 13,810, dated March 8, 2019;
- Brazilian Federal Law 13,709, dated August 14, 2018;
- Brazilian Federal Decree No. 5,640, dated December 26, 2005;
- Brazilian Federal Decree No. 9,825, dated June 5, 2019;

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

- Brazilian Council for Financial Activities Control (COAF) Resolution No. 36, dated March 10, 2021;
- Brazilian Securities and Exchange Commission (CVM) Resolution No. 50, dated August 31, 2021;
- Central Bank of Brazil (BCB) Circular No. 3,978, dated January 23, 2020(*);
- BCB Circular No. 4,005, dated April 16, 2020(*);
- BCB Circular Letter No. 4,001, dated January 29, 2020(*);
- BCB Resolution No. 44, dated November 24, 2020(*);
- List of Politically Exposed Persons – Reputational AML;
- Consolidated United Nations Security Council Sanctions List;
- Wolfsberg Anti-Money Laundering Principles; and
- Financial Action Task Force (FATF) Recommendations.

(*). Although not applicable to B3, the provisions of this normative document have been adopted as best practice and should be read as such in this Policy.

As an organized market administrator and as a clearinghouse considered systemically important by the Central Bank of Brazil, B3 regulates the operation of the markets it manages through rules, regulations and procedures manuals, which establish the rights and duties of B3 and its participants.

Furthermore, B3 declares that all personal data processing activities it performs, including those deriving from processes provided for in this Policy, observe and adhere to the following: (i) The underpinnings, principles and legal bases stipulated by Brazilian Federal Law No. 13,709, dated August 14, 2018 (General Data Protection Law, or LGPD), (ii) The Personal Data Protection Notice for B3 Employees, (iii) The Personal Data Protection Statement, available on the B3 portal at www.b3.com.br/pt_br/termos-de-uso-e-protecao-de-dados/declaracao-de-protecao-de-dados-pessoais/, and (iv) B3's Information Retention and Disposal Rules.

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

4 CONCEPTS

In legal terms, the crime of money laundering consists of concealing or disguising the nature, source, location, disposition, movement or ownership of assets, rights or property originating, directly or indirectly, from a penal offense. In this sense, it could be said that the crime of **money laundering** employs legal or illegal means to convert illicit money into licit money. When employing legal means, defrauders take advantage of weaknesses in internal controls and of insufficient mechanisms for the identification of abnormalities, in order to perpetrate the act.

The crime of money laundering is usually committed through a set of commercial or financial transactions that seek to incorporate into the economy, in a temporary or permanent way, illicitly originated funds, assets and property. This incorporation occurs through a dynamic process that involves, theoretically, three separate stage, which frequently occur simultaneously.

- **Placement:** The first stage of the process is the placement of money in the economic system. Seeking to hide its origin, criminals try to move it through countries with laxer rules and less-regulated financial systems. Placement is performed through cash deposits or purchase of tradable instruments or assets. To make it difficult to identify the source of money, criminals apply sophisticated and increasingly dynamic techniques, such as splitting the funds that pass through the financial system and using business establishments that generally work with hard cash.
- **Layering:** The second stage of the process consists of making the accounting tracking of illicit funds as difficult as possible. The purpose in this case is to break the evidentiary chain in a possible investigation into the source of money. Criminals seek to move funds electronically, transferring assets to anonymous accounts, preferably in countries covered by bank secrecy laws, or making deposits into third-party accounts, usually by submitting fake registration documentation.
- **Integration:** In this last stage, assets are formally incorporated into the economic system. Criminal organizations seek to invest in enterprises

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

that facilitate their activities, with businesses providing services to each other. Once this chain has been created, it becomes increasingly easier to legitimize funds from illicit sources.

Financing terrorism and the spread of weapons of mass destruction may be defined as the financial support, by any means, to terrorism and proliferation of weapons of mass destruction, or to those who encourage, plan or commit such acts.

Therefore, financing terrorism and spreading weapons of mass destruction seek to provide funds or capital to terrorist activity and other similar and related practices. This fundraising may take several forms, even by legal means, such as membership contributions, donations, or profits from a range of business activities, as well as from criminal sources, such as drug trafficking.

5 GUIDELINES

This Policy is based on the following guidelines:

- The Company must permanently develop and disseminate AML/CFT knowledge and culture to its executive officers, employees, interns and relevant service providers;
- The Company must clearly define the roles and responsibilities of executive officers, employees, interns and relevant service providers in connection with AML/CFT;
- The Company must have a risk-based approach to continually assess the products and services it provides in order to identify whether they are

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

being unduly used in ML/CFT practices, taking the necessary measures to mitigate such risks;

- The Company must formalize and perform proper analyses, through the application of a risk-based approach, designed to continuously know and classify risks and monitor active customers, suppliers, partners, executive officers, employees, interns and relevant service providers, undertaking to identify and rate potential ML/CFT risks and other similar cases;
- The Company must produce each year or more frequently, if necessary, in addition to an annual report containing the internal assessment of ML/CFT risks, an evaluation of the effectiveness of the criteria adopted for risk classification and monitoring of the products and services it provides and of the analyses designed to continuously know and classify risks and monitor and update the registration data of active customers, suppliers, partners, executive officers, employees, interns and relevant service providers;
- The Company must develop and maintain robust monitoring processes to detect transactions, either executed or proposed, deemed unusual and/or suspicious and liable to constitute evidence of ML/CFT, and, whenever appropriate, report such transactions to the competent authorities, pursuant to the applicable legislation and regulations;
- The Company must store and keep available for CVM, BCB, self-regulatory entities and other competent authorities, pursuant to the provisions of the law and B3's Information Retention and Disposal Rules, all information gathered and analyses performed in cases where executed or proposed transactions, deemed unusual and/or suspicious, might constitute evidence of ML/CFT, under the terms of the legislation and regulations in force; and

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

- The Company must draft and issue a report containing an internal ML/TF risk assessment, to be submitted to the senior management bodies specified in this Policy, by the last business day of April of the following year. This report must remain available to CVM, BCB, self-regulatory entities and other competent authorities, according to law.

6 RESPONSIBILITIES

6.1 AML/CFT Internal Committee (Committee)

The Committee is a permanent decision-making body, whose powers are granted by B3's Executive Board, governed by its own rules and consisting of B3's staff members also appointed by the Executive Board.

The Committee is responsible for:

- Reviewing this Policy and submitting it to the Executive Board and, subsequently, to the Board of Directors for approval;
- Approving rules, procedures and actions associated with B3's AML/CFT Program, and assuring their compliance with the applicable regulations;
- Establishing roles and duties for the Company's areas whose activities are affected by the AML/CFT Program's implementation;
- Approving the models, criteria and parameters used by the Company to monitor and detect executed or proposed transactions, deemed suspicious and/or unusual, that might constitute evidence of ML/CFT, and assessing the performance of such models, criteria and parameters, in accordance with the applicable legislation and regulations in force, at least once a month;
- Assessing the executed or proposed transactions deemed suspicious and/or unusual, as detected by the Company's monitoring processes, that might constitute evidence of atypicality not captured by the quantitative criteria referred to in the previous bullet and, based on the

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

laws and regulations in force, report them to the competent authorities; and

- Carrying out any other evaluations and passing resolutions deemed necessary for AML/CFT purposes.

6.2 Officer in Charge

In consonance with Article 8 of CVM Resolution No. 50, dated August 31, 2021, B3 designates its Chief Operating Officer – Issuers, Depository and OTC as responsible for the implementation and enforcement of the rules established in this Policy.

6.3 Chief Operating Officer – Issuers, Depository and OTC

The following responsibilities of the Chief Operating Officer – Issuers, Depository and OTC are distributed among several subordinate areas, as detailed in the AML/CFT Rules, which must maintain processes and controls for AML/CFT purposes, subject to their respective authorities and the guidelines defined by the Committee:

- Answering for AML/CFT initiatives at B3, as required by CVM Resolution No. 50;
- Coordinating the Committee;
- Reporting transactions, deemed suspicious or unusual, that might constitute evidence of ML/CFT practices as detected by the Company's monitoring processes, to COAF and BSM Market Supervision, pursuant to the legislation and regulations in force;
- Keeping a record of all communications made to COAF and BSM Market Supervision, as well as their justifications;
- Generating, controlling and making monitoring lists available;

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

- Reporting the communications made to COAF to the Audit Committee and Board of Directors, in a consolidated manner, also disclosing the most relevant cases;
- Filing risk-based analyses and annual reports issued and made available to CVM and potentially to BCB, in addition to centrally filing risk-based analyses of products, services, active customers, suppliers, partners, executive officers, employees, interns and relevant service providers, in accordance with B3's Information Retention and Disposal Rules;
- Defining the best performance strategy for the monitoring area of OTC and depository transactions, establishing processes for the creation and periodic review of filter methodologies intended to identify atypical transactions in relation to similar trades, applying procedures stipulated in B3's rules and regulations and reporting them to the regulatory bodies;
- Also in the OTC segment, implementing and managing the following: (i) Controls to mitigate the risk of centralized asset depository services and OTC trade registration provided by B3 and liable to be used in ML/CFT activities, and (ii) Monitoring processes to detect suspicious or atypical transactions associated with centralized deposit and OTC trade registration processes that might constitute evidence of ML/CFT;
- Managing and controlling the participant and customer registration platforms in the Listed and OTC segments, pursuant to the applicable legislation and regulations; and

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

- Reporting, on a timely basis, to public administration bodies – COAF, Ministry of Justice and Public Security (MJSP), BCB and CVM – any sanctions imposed by resolutions passed by the United Nations Security Council (UNSC), or by assignment of its sanctions committees, determining the unavailability of assets or funds, resulting from events directly or indirectly associated with such assets, held by individuals, legal entities or other entities, when duly identified, pursuant to Law No. 13,810/2019, CVM Resolution No. 50/2021, BCB Circular No. 3,942/2019, Decree No. 9,825/2019, and BCB Circular 3,978/2020, also referring such determinations of unavailability to those responsible for their enforcement.

6.4 Chief Product and Client Officer

The following responsibility of the Chief Client and Product Officer is distributed among subordinate products areas:

- Classifying products and services of the infrastructure of markets managed by B3 in order to assess any risks of misuse of such products, services and technologies in ML/CFT practice.

This responsibility is carried out jointly with the Chief Operating Officer – Issuers, Depositary and OTC.

6.5 Chief Financing Infrastructure Unit Officer

Is responsible for implementing and managing, at the Finance Unit, monitoring processes designed to detect suspicious or unusual transactions in the registration system for collateral consisting of vehicle and real estate that might constitute evidence of ML/CFT practices.

The Chief Financing Infrastructure Unit Officer is also responsible for rating ML/CFT risks for the Finance Unit's active customers, , products and services by using the scoring model contained in the Quantitative Criteria Manual (QCM/AML/CFT).

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

6.6 Electronic Trading Department

Is responsible for implementing and managing the following: (i) Controls designed to mitigate the risk of B3's electronic trading platforms being used in ML/CFT and (ii) Monitoring processes aimed at detecting suspicious or atypical transactions performed in the electronic trading platforms that might constitute evidence of ML/CFT.

6.7 Settlement Department

Is responsible for implementing and managing the following: (i) Controls designed to mitigate the risk of B3's settlement, position management and securities lending registration services being used in ML/CFT, and (ii) Monitoring processes aimed at detecting suspicious or atypical transactions associated with settlement, position management and securities lending registration processes that might constitute evidence of ML/CFT.

6.8 Risk Management Department

Is responsible for implementing and managing the following: (i) Controls designed to mitigate the risk of the central counterparty services provided by B3 being used in ML/CFT and (ii) Monitoring processes aimed at detecting suspicious or unusual transactions in connection with collateral posting, withdrawal and liquidation processes that might constitute evidence of ML/CFT.

6.9 Governance, Integrated Management and Cyber Security Department

Is responsible for the Company's compliance processes to assure the enforcement of legal and regulatory requirements involving AML/CFT, among other requirements.

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

6.10 People, Branding, Communication, Sustainability and Social Investment Department

Is responsible for (i) Maintaining, updating and storing the registration documentation of B3's executive officers, employees and interns, for as long as the Company's contractual relationship with each party remains in effect and during at least 10 (ten) years after the end of each contractual relationship, subject to the guidelines of B3's Information Retention and Disposal Rules; (ii) Initiating every process by submitting the registration data of executive officers, employees and interns, their names and documents to Participant and Investor Registration, which is responsible for applying the risk-based approach (KYE); and (iii) Providing the registration data of potentially new executive officers, employees and interns, who are participating in a selection process for monitoring and classification process.

This department is also responsible for implementing training within the scope of the AML/CFT Program, subject to the guidelines established by the Committee.

6.11 Audit Department

Is responsible for monitoring the Company's compliance with this Policy.

6.12 Legal Department

Is responsible for managing the Company's legal and administrative processes, and for providing legal counsel in decision-making to ensure compliance with the legal and regulatory requirements within the scope of the AML/CFT Program.

6.13 Administration and Facilities Department

Is responsible for applying the risk-based approach, with the subsequent classification of ML/CFT risks, to all B3's suppliers and partners, according to the diligence stipulated in B3's Suppliers Risk Assessment Procedure, in the Purchasing Rules and in the Partner Risk Assessment Rules.

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

7 FORESEEN SANCTIONS

Failure to comply with regulatory requirements may subject the Company's executive officers, employees, interns, relevant service providers and partners to administrative and criminal penalties for money laundering and concealment of assets, rights and property.

Negligence and voluntary fault (intentional or knowing involvement in illicit activities or transactions backed up by funds originating from tortious acts, such as structuring or advising others to structure transactions with the purpose of bypassing the obligation to report them to regulatory authorities) are considered violations of this Policy and B3's Code of Conduct and Ethics, when applicable, subjecting offenders to the disciplinary measures specified in the Company's normative documents, without prejudice to the relevant act being reported to the competent government bodies.

8 FINAL PROVISIONS

The above provisions apply to the entire Company as of October 1, 2021, the date on which the provisions set forth in CVM Resolution No. 50 take effect.

9 CHANGE LOG

Validity: As of December 8, 2023.

1st draft: October 23, 2013.

Areas responsible for this document:

Responsible for	Area
Drafting	Participant and Investor Registration
Revision	Governance, Integrated Management and Cyber Security Department Legal Department Countering Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction Internal Committee
Approval	Board of Directors

PUBLIC INFORMATION

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)



Updates:

Version	Changed section	Change	Reason	Date
1	First draft	NA	NA	October 23, 2013
2	4.2 Roles and Responsibilities	Combination of CSD and OTC Departments' responsibilities	Adjustment to Company's structure	February 21, 2014
3	Inclusion of the Counterterrorism provision 4.2 Roles and Responsibilities	Inclusion of counterterrorism measures and responsibilities of the Product Engineering Department and Legal Department	Complement	April 30, 2015
4	2.2 Related documents 4.2 Roles and Responsibilities	Inclusion of legal provisions and reference to Consolidated UNSC Sanctions List Changes to Risk and Credit Management (name) and responsibilities Inclusion of reporting to the Audit Committee and Board of Directors the communications made to COAF Inclusion of responsibilities for the Operations, Settlement, CSD and OTC Registration, and Risk Management departments to perform controls using internal, national and international lists	Update of references Adjustment to Company's organizational structure	March 15, 2016
5	4.2.3.4 CSD and OTC Department 4.2.3.5 Customer Relationship Department 4.2.5 Products Department	Exclusion of reference to responsibility for participant registration, now under the responsibility of the Customer Relationship Department Name change and inclusion of responsibility for participant registration Exclusion of subsection	Adjustment to Company's structure	
6	4.2.3.5 Operations Department (UTVM) 4.2.6 Technology and Operations Department (UFIN)	Inclusion of Operations (UTVM) and Technology and Operations (UFIN) Departments' responsibilities and changes to corporate name and structure	Adjustment to Company's structure	August 11, 2017
7	6.4 Operations Department (BM&F and BOVESPA segments)	Name change	Adjustment to Company's structure	

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)



	6.8 CSD and OTC Department	Changes to department's name and responsibilities, now encompassing CETIP UTVM segment and participant and investor registration	Adjustment to Company's organizational structure	September 20, 2018
	6.9 Operations Department (CETIP – UTVM)	Exclusion of subsection, as department's responsibilities now under DDOB's responsibility, as described in subsection 6.8	Adjustment to Company's organizational structure	
	6.10 Customer Relationship Department	Name change and exclusion of participant and investor registration, now under DDOB's responsibility, as described in subsection 6.8	Adjustment to Company's organizational structure	
	6.11 International Clients Relationship Department	Inclusion of subsection	Adjustment to Company's organizational structure	
	6.12 Product Engineering Department	Exclusion of subsection	Adjustment to Company's organizational structure	
	6.13 Technology and Operations Department (CETIP – UFIN)	Department's name change	Adjustment to Company's organizational structure	
	Introduction	Reference to Law 12683/2012		July 26, 2019
	3 References	Replacement of Law 13,170/2015 with Law 13,810/2019 Replacement of Circular Letters CVM/SMI/SIN 04/2015 and 05/2015 with Circular Letter CVM/SMI/SIN 03/2019 Replacement of BCB Circular 3,780/2016 with BCB Circular 3,942/2019 Inclusion of Decree 9,825/2019	Update of references to Law	
	6.7 Data Department	Inclusion of subsection	Adjustment to Company's structure	
8	3 References	Replacement of CVM Instruction 301/1999 by CVM Instruction 617/2019	Update of references to Law	
	4 Scope	Adjustment regarding subsidiaries	Scope change	
	3 References	Replacement of BCB Circular 3,461/2009 and BCB Circular Letter 3,542/2020 with BCB Circular 3,978/2020 and BCB	Update of references to Law	

Corporate Policy on Combating Money Laundering, Concealment of Assets, Rights and Property, and Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CFT)

[B]³

		Circular Letter 4,001/2020, respectively Exclusion of revoked COAF Resolution 015/2007		September 24, 2020
	6.11 Finance Unit Department	Name change	Adjustment to Company's structure	
	6.7 Data Department	Inclusion of communication regarding cases identified by UNSC	Alignment with normative documents	
	Entire Policy	Formatting	Alignment with new template	
	2 Scope	Inclusion of foreign subsidiaries and BSM, Cetip Info Tecnologia and B3 Social and exclusion of Banco B3	Updates	
	1 Purpose	Inclusion of deadlines for reporting and analysis	Alignment with normative documents	
	3 References	Inclusion of reference to AML/CFT Rules		
	4 Guidelines	Inclusion of risk-based approach		
	6.7 Data Department	Adjustment of person responsible for managing and controlling participant and customer registration platforms	Adjustment to Company's structure	
9	Entire Policy	Adjustment to person in charge and roles of AML/CFT areas	Adjustment to Company's structure	September 29, 2021
	3. References in entire Policy	Inclusion of reference to Anti-Terrorism Law and changes to CVM, BCB and COAF normative documents	Alignment with normative documents	
	2. References in entire Policy	Alignment with CVM Resolution No. 50/2021		
		Inclusion of reference to General Data Protection Law (Law 13,709/2018)		
	6.9.1 AML/CFT and Operations Modeling	Inclusion of the MJSP contact for UNSC communications	Formatting	
10	6. Responsibilities	Adjustment of responsibilities and roles of AML/CFT areas	Adjustment to Company's organizational structure	December 8, 2023