ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 A Publicly-Held Company NIRE 35300010230

CORPORATE POLICY FOR THE PREVENTION OF UNLAWFUL ACTS

1. OBJECTIVE

This Policy for the Prevention of Unlawful Acts consolidates the principles and guidelines of the Itaú Unibanco Conglomerate for the Prevention and Combat of Money Laundering, the Financing of Terrorism, the Proliferation of Weapons of Mass Destruction (AML/CFT), and of fraud and claims, in line with current legislation and regulations and with the best national and international market practices.

2. TARGET AUDIENCE

This policy applies to the Itaú Unibanco Conglomerate and its companies in Brazil and abroad.
The requirements of local policies and legislation, where foreign representations are located, must be evaluated individually and will follow the guidelines determined by internal procedure.

3. INTRODUCTION

Financial institutions play a fundamental role in the Prevention of Unlawful Acts, which are all conscious human actions or omissions directed towards the practice of criminal illicit acts, notably money laundering, terrorist financing, corruption, fraud and claims.

Money laundering consists in the concealment or dissimulation of the nature, origin, location, disposition, movement or ownership of goods, rights or sums arising, directly or indirectly, from a criminal offence.

Financing of terrorism is when someone, directly or indirectly, by any means, provides financial support, provides or gathers funds with the intention of being used or knowing that they will be used, in whole or in part, by terrorist groups for the practice of terrorist acts. On the other hand, Financing the Proliferation of Weapons of Mass Destruction is constituted when someone, directly or indirectly, by any means, provides financial support, provides or gathers funds with the intention of being used for the proliferation of weapons of mass destruction, which may be biological, chemical and nuclear.

Corruption consists of suggesting, offering, promising, granting, requesting, demanding, accepting or receiving, directly or indirectly, upon demand or not, to/from people or companies in the public or private sectors or third sector organizations, as well as between people, companies or organizations from different countries, undue advantages of any nature (financial or otherwise) in exchange for carrying out or omitting acts inherent to their duties, operations or activities for the Conglomerate or aiming at benefits for themselves or third parties.

Fraud refers to any illegal activities, attitudes or actions that have the purpose of deceiving or illuding someone, using bad faith for their own benefit or that of third parties. Examples are: omission/manipulation of information, appropriation of values, tampering with documents, records and financial statements.

Claim/accident refers to atypical events that result in losses or disasters for Itaú Unibanco, such as: robberies of branches and customers, extortion through kidnapping, theft, accidents, break-ins, among others.

Embargo is the total or partial prohibition of carrying out commercial operations with a given country, established by a jurisdiction or by an international organization in retaliation for certain actions taken by the embargoed jurisdiction, of an economic, political, social or military nature. Some jurisdictions or international bodies also place restrictions on certain persons or companies that engage in illegal activities.

The great challenge is to identify and curb increasingly sophisticated operations that seek to hide or disguise the nature, authorship, origin, location, disposition, movement or ownership of goods, rights and/or sums arising directly or indirectly from illegal activities.

Itaú Unibanco dedicates an exclusive board to deal with the topic and establishes this policy with the aim

of avoiding its intermediation in illicit activities, and to safeguard and protect its name, reputation and image before employees, customers, strategic partners, suppliers, outsourced service providers, regulators and society, through a governance structure oriented towards transparency, strict compliance with rules and regulations and cooperation with police and judicial authorities. It also seeks to continuously align itself with the best national and international practices for the prevention of unlawful acts, through investments and continuous training of its employees.

4. RESPONSIBILITIES

Board of Directors (CA)
Approves the Institution's guidelines for the prevention of unlawful acts and their respective amendments, with a commitment to the effectiveness and continuous improvement of the subject. Additionally, the Board receives the Internal Risk Assessment, the Effectiveness Assessment Report, as well as the action plans developed to resolve deficiencies, and their respective Monitoring Report for acknowledgment.

Audit Committee (CAUD)
It supervises the Corporate Program for the Prevention of Unlawful Acts based on information compiled and presented by the departments, as well as other mechanisms at its disposal. Additionally, the Committee receives the Internal Risk Assessment, the Effectiveness Assessment Report, as well as the action plans developed to resolve deficiencies, and their respective Monitoring Report for acknowledgment.

Superior Operational Risk Commission – CSRO:
- Defines and proposes to the Board of Directors the Institution's guidelines for the prevention of unlawful acts;
- Analyzes the results of the processes and activities of the illicit acts prevention program; and
- Decides on situations not provided for in this Policy.

Risk and Capital Management Committee (CGRC)
Supports the Board of Directors in carrying out its duties related to risk and capital management at Itaú Unibanco. Additionally, it receives the Internal Risk Assessment for acknowledgment.

Money Laundering Prevention Board (DPLD)
- Ensures the implementation of the AML/CFTP Program of the Itaú Unibanco Conglomerate and its companies in Brazil and abroad;
- Prepares Itaú Unibanco's Internal Risk Assessment;
- Improves the quality and effectiveness of its processes and responsibilities for the AML/CFTP processes of Itaú Unibanco, verifying compliance with the policy, as well as correcting any deficiencies found;
- Conducts prior assessment of money laundering and terrorist financing risks in new products and services, including the use of new technologies;
- Defines the guidelines and minimum criteria for classifying money laundering and terrorist financing risks for customers, employees, business partners, suppliers and outsourced service providers;
- Elaborates and monitors the implementation of the risk-based approach in the processes, formalizing them in internal procedures, together with the criteria established for the generation of effectiveness indicators;
- Monitors and diagnoses the different types of money laundering, in order to anticipate trends and propose preventive and combating solutions;
- Validates AML/CFTP procedures of Itaú Unibanco mentioned in the business unit documents;
- Periodically reports to the Audit Committee relevant facts regarding Itaú Unibanco's AML/CFTP.
The AML/CFTP Director is also responsible for the following duties:
- Manage AML/CFTP risks through information received through Committees and, depending on the risk, cases submitted to their approval authority level;
- Approve the Internal Risk Assessment of Itaú Unibanco;
- Delegate to the appropriate authorities the approvals of procedural rules aimed at knowing your customer, employees, commercial partners and outsourced service providers, as well as monitoring, selection and analysis;
- Receive for acknowledgment the partnership contracts with Financial Institutions based abroad, as well as with third parties participating in payment arrangements in which Itaú Unibanco also participates, as established in current regulations;

Corporate Security Board (DSC)
- Manages Itaú Unibanco’s Unlawful Acts Prevention Program in Brazil and abroad;
- Improves the quality and effectiveness of its processes, ensuring the integrity, availability and confidentiality of information; the physical security of employees, customers and executives, of the patrimony; and the responsibilities on the processes of Prevention of Unlawful Acts;
- Conducts prior assessment of fraud risks in products and services, including the use of new

technologies;
- Defines the guidelines and minimum criteria for classifying fraud risks for customers, employees, business partners, suppliers and service providers;
- Monitors and diagnoses the different types of illegal acts, in order to anticipate trends and propose preventive and combat solutions;
- Validates the procedures for the Prevention of Unlawful Acts mentioned in the documents of the business units;
- Periodically reports relevant facts of illegal acts to the Audit Committee;
- Manages extreme, unique and rare events that threaten the organization's strategy, objective and viability, its image and/or reputation.

Business and Support Units in Brazil and abroad
- As the first line of governance, define and implement procedures and controls that adhere to this policy with the guidance of the DPLD – AML and DSC, considering the assessment of risks at the beginning and maintenance of relationships with natural and legal entities (whether customers, employees, business partners, suppliers, service providers or other relationships), in those processes that are executed and are under its direct responsibility;
- Ensure that employees undertake PLD/CFTP, Fraud and Claims training.

Legal Department
- Analyzes legal and regulatory requirements for AML/CFTP and their respective impacts on business;
- Helps business managers to develop action plans for implementing AML/CFTP controls;
- Supports the assessment of risks and necessary measures to deal with occurrences of transactions or operations suspected of money laundering, fraud and claims, from a legal point of view.

Operational Risk Board
Certifies the effectiveness of the control environment, through monitoring programs, evaluation of control effectiveness tests, reporting residual risk and monitoring independently verified deficiencies, as defined in Integrated Operational Risk Management and Internal Controls Policy and prepares an Effectiveness Report as well as a Monitoring Report, submitting it for approval and acknowledgment to those responsible, following, at least, the deadline established by regulation.

Internal Audit
As a third line of governance, the scope of internal auditing covers the examination and assessment of the adequacy and effectiveness of the organization's governance, risk management and internal controls, the quality of execution of assigned responsibilities to achieve the goals established by the organization, as per defined in Internal Audit Policy.

5. INTERNAL RISK ASSESSMENT

Itaú Unibanco annually prepares its Internal Risk Assessment, a document that aims to identify, measure and mitigate the risk of using its products and services in the practice of money laundering and terrorist financing.

Based on this Assessment, a risk-based approach is applied, a methodology that ensures that the measures to prevent and mitigate money laundering and terrorist financing are proportionate to the identified risks, because where the risks are higher, strengthened measures will be adopted to manage and mitigate such risks and, where the risks are minor, simplified measures will be used.

The details of the guidelines that underlie the risk-based approach are formalized in internal procedure.

6. EFFECTIVENESS ASSESSMENT

Itaú Unibanco prepares an Effectiveness Report annually, in order to evaluate the effectiveness of AML/CFTP policies, procedures and internal controls. Action plans aimed at solving the deficiencies identified, through the aforementioned Assessment, must be followed up by means of a Monitoring Report. Additionally, the Effectiveness Assessment must contain, at a minimum, information that describes the adopted methodology; the tests applied; the qualification of the evaluators and the deficiencies identified.

7. CORPORATE PROGRAM FOR THE PREVENTION OF UNLAWFUL ACTS

In order to ensure compliance with the guidelines of this policy and prevent its products and services from being used in illegal activities, Itaú Unibanco established a Program for the Prevention of Unlawful Acts. Such program must be applied, independently and autonomously, in Brazil and in the International Units, as defined in internal procedure. It must contain at least:

7.1. Preventing and Combating Money Laundering and the Financing of Terrorism

Policies and Procedures

Itaú Unibanco has structured policies, rules and procedures to determine its guidelines for combating illegal acts, which comply with local laws and regulations, as well as with the risk profiles of customers; of the institution; operations, transactions, products and services; and employees, business partners and third-party service providers. These documents are periodically reviewed and approved according to the previously established scope and are available to all employees.

Customer Identification

This is a set of actions that must be taken to identify and qualify customers, as well as their administrators and representatives, covering the capture, verification and validation of their information, with the aim of knowing their true identity . The registration data obtained must be updated and stored in accordance with the established deadlines.

Additionally, in order to perform a complete identification and qualification of the client, the procedures defined in internal policies must be followed for obtaining information, which allows verification of their status as a Politically Exposed Person (PEP), as well as analyzing the chain of ownership interest until the identification of the natural person characterized as the final beneficiary.

Itaú Unibanco does not allow the opening and maintenance of anonymous accounts.

The rules that detail these items are described in internal policy.

Know Your Customer - KYC

This is a set of actions that must be adopted to ensure the identity and economic activity of clients, as well as the origin and constitution of their assets and their financial resources. The collection of this information should allow the assessment of the client's financial capacity. The more accurate the information collected and recorded at the beginning of the relationship, the greater the ability to identify illegal acts.

Based on a risk-based approach to AML/CFT, for clients classified as having the highest risk and for cases that require Special Attention, such as the relationship with PEPs and clients where it was not possible to identify the final beneficiary, rigorous specific analysis procedures are adopted.

It is mandatory to assess the interest in starting or maintaining a relationship with natural persons or legal entities classified as PEPs by a person holding a position or role at a higher hierarchical level than the person responsible for authorizing the relationship, as defined internal procedure.

The guidelines that address this item are in internal document.

Your Partner - KYP

Partners are considered to be Legal Entities that enter into commercial agreements or associations with one or more companies of the Itaú Unibanco Conglomerate and that meet the requirements established in Business Partnership Governance Policy.

This pillar includes a set of rules, procedures and controls that must be adopted to adequately identify and qualify commercial partners, including correspondents in the country and abroad. These partners must be classified into risk categories considering the activities they carry out.

The objective is to prevent doing business with unreputable counterparties or those suspected of involvement in illicit activities, as well as ensuring that they have adequate AML/CFTP procedures, as defined in internal procedure.

Itaú Unibanco does not accept relationships with so-called Shell Banks, that is, banks incorporated in a jurisdiction where there is no physical presence and which are not part of any regulated financial group.

The guidelines that address this item are in document internal procedure.

Know Your Supplier (KYS)

It is a set of rules, procedures and controls that must be adopted to properly identify and qualify suppliers and outsourced service providers. These agents must be classified into risk categories considering the activities they carry out.

The objective is to prevent doing business with untrustworthy counterparties or parties suspected of being involved in illegal activities.

For **customers**, **commercial partners**, **suppliers** and **outsourced service providers** that present greater risk associated with illicit acts, stricter identification and due diligence criteria are applied, with the approval of the relationship by a higher hierarchical level.

The procedures that deal with this item are in the internal documents.

Know Your Employee - KYE

It is a set of rules, procedures and controls that must be adopted to identify and adequately qualify employees and/or candidates, in order to support their selection and hiring, as well as monitoring situations that may characterize some type of risk or deviation, for the purposes of preventing money laundering, terrorist financing and other illicit acts. These employees must be classified into risk categories considering the activities performed by them.

The guidelines that address this item are in internal procedure.

Assessment of New Products and Services;

New products and services, including the use of new technologies, when applicable, must be previously evaluated, from the perspective of AML/CFTP, in accordance with the guidelines established in Product Assessment Policy.

Compliance with Sanctions

It is a set of rules, procedures and controls related to sanctions, embargoes and political and economic restrictions that may be applicable to commercial operations with people, institutions and countries/regions involved in terrorism, drug trafficking, military conflicts, violation of human rights or other improprieties and illegalities in line with current legislation and regulations and best practices.

In accordance with internal procedure, Itaú Unibanco establishes guidelines for total embargoes on countries and follows restrictive lists imposed by sanction-issuing authorities.

Monitoring, Selection and Analysis of Suspicious Operations or Situations;

All financial transactions and operations, including proposals, carried out by customers, employees or not, must be monitored to determine situations that may constitute evidence of money laundering or terrorist financing. Monitoring considers the profile, origin and destination of funds and the financial capacity of customers.

According to the risk-based approach, for clients with greater exposure to AML/CFT, a more stringent set of rules or parameters should be applied, or even more frequent or in-depth monitoring of their activities.

Additionally, the Monitoring, Selection and Analysis process must occur independently and autonomously in the AML/CFTP department, which must be segregated from the commercial department, in accordance with legal and regulatory provisions.

Reporting Suspicious Transactions to Regulatory Bodies

The transactions, situations or proposals that contain evidence of money laundering or terrorist financing must be reported to the competent regulatory bodies, when applicable, in compliance with legal and regulatory requirements. Good faith communications do not entail civil or administrative liability to Itaú Unibanco, nor to its administrators and employees.
Information about these communications is restricted and should not be disclosed to customers and/or third parties.

The guidelines that address this item are in internal procedure.

Training

The AML/CFTP training program promotes continuous training and disseminates the culture of the topic, thus achieving learning and awareness of its importance, as well as the deepening and recycling of knowledge. The training must be applied to administrators, all eligible commercial partners and employees. Said program aims to:
- Deepen knowledge of legal and regulatory requirements and responsibilities, as well as corporate AML/CFTP guidelines;
- Train on the best way to identify, prevent, treat and communicate risk situations or with indications of money laundering or terrorist financing in the business carried out;
- Promote the organizational culture of prevention of money laundering and the financing of terrorism, the proliferation of weapons of mass destruction.
The application of the program must take place through institutional actions and in the business units, and may include classroom or distance courses (e-learning), lectures, teleconferences, audio-conferences, campaigns, announcements, publications, among other modalities and shapes.

The guidelines that address this item are in internal procedure.

7.2. Combat and Prevention of Fraud

The prevention and fight against fraud is the responsibility of all employees. Frauds can be classified as:
a) Disciplinary Infractions and Violations of the Itaú Unibanco Code of Ethics and the Corporate Integrity and Ethics Policy, committed in groups or individually:
- Adoption of practices not authorized by the company;
- Behavioral deviations;
- Breach of confidentiality and conflict of interest.
b) Non-compliance with Legal and Regulatory Standards:
These are all situations identified as a result of non-compliance with legal and regulatory norms, which jeopardize the Organization's image, assets or continuity.
c) Unlawful Acts of Any Nature:
These are all types of unlawful acts (crimes or criminal misdemeanors) provided for in the Brazilian Criminal Legislation, or local in the case of International Units, as applicable, and that may cause damage, direct or indirect, to the Bank, its employees, customers or third parties. Some examples are:
- Counterfeiting;
- Stellionate (in all its forms, including by electronic means);
- Misappropriation;
- Theft;
- Breach of bank secrecy;
- Robbery;
- Extortion through kidnapping.

Model of Action in Preventing and Combating Fraud

Risk Assessment at the Beginning of the Relationship

The processes for contracting services and products must include procedures to prevent and mitigate the risk of fraud at the beginning of the relationship with proponents.

Preventing and Combating Internal Fraud

Itaú Unibanco adopts specific measures to prevent the occurrence of fraud involving its employees, through guidelines and control procedures for the prevention and detection of irregular activities.

The guidelines that address this item are in internal procedure.

Preventing and Combating Accounting Fraud

Itaú Unibanco adopts specific measures to prevent the occurrence of fraud involving its employees, through control guidelines and procedures for the prevention and detection of irregular activities.

Risk Assessment in New Products and Services

New products and services must be previously evaluated, from the perspective of fraud prevention, in accordance with the guidelines established in internal document.

Transaction Monitoring

The products and services contracted by the clients must be monitored for the detection and determination of atypical situations or suspected fraud or other unlawful acts.

Handling of Events

Situations under suspicion or confirmed must be dealt with to determine responsibilities and necessary measures.

The procedures and decisions taken during the handling of occurrences must be formalized with a view to generating subsidies for legal proceedings.

Training and Awareness

The training program on Prevention of Fraud and Claims is continuous and must be applied to all eligible employees, aiming to:
- Deepen the knowledge that administrators and employees have of external and internal regulatory requirements for preventing and combating fraud and claims/accidents;
- Train administrators and employees to identify, prevent, deal with and report suspicious situations or situations related to fraud and other illegal acts.
The application of the program must take place through institutional actions and in the business units, and may include distance courses (e-learning) and face-to-face courses, lectures, teleconferences, audio conferences, campaigns, communiqués, publications, among other modalities and shapes.

8. MAINTENANCE AND STORAGE OF INFORMATION AND RECORDS

All information related to the pillars described above, as well as records of operations and services provided must be kept in their original form or in electronic files, according to deadlines and responsibilities established by current legislation.

9. TRANSPARENCY IN CUSTOMER RELATIONSHIP

Itaú Unibanco's customers have access, through various channels, to their financial information, including invested funds, contracted products and limits granted. With this, the client itself is a strong and active partner in the prevention of Illicit Acts.

Itaú Unibanco also continually alerts its customers, through its relationship channels, about the possibilities of Unlawful Acts and the actions and precautions that must be taken to prevent them.

10. CHANNELS FOR REPORTING UNLAWFUL ACTS

Itaú Unibanco's managers, employees, partners and outsourced service providers must, within the limits of their attributions, immediately communicate the proposals or occurrences of situations or operations with indications or evidence of illegal acts, identified in the prospection, negotiation or during the relationship using the following established channels, by physical or electronic means:

Situations Related to Money Laundering or Financing of Terrorism
In Brazil, communications must be sent to the DPLD - AML Department
Phone: +55 (11) 2757-6753
- Internal email: MONEY LAUNDERING PREVENTION.
- Website:https://www.itau.com.br/atendimento-itau/para-voce/denuncia/

In international units, communications must be forwarded to the local channels or "*Compliance Officers* " of the Unit.

Situations Related to Fraud and Other Unlawful Acts
In Brazil, communications must be forwarded to the Superintendence of Inspection and Fraud Prevention or to the Audit Committee:

Superintendence of Inspection and Fraud Prevention:
- External phone number: 0800-723-0010;
- Internal phone number: 0300 100 0341
- Website: www.itau.com.br/atendimento-itau/para-voce/denuncia;
- Internal e-mail: Inspection box;

- External e-mail: inspetoria@itau-unibanco.com.br and fornecedor_relatos@itau-unibanco.com.br;
- Interoffice mail: recipient: Inspection Management/São Paulo;
- Mailing address:
Att. Inspetoria
Av. Dr. Hugo Beolchi, 900 floor -1 – Torre Eudoro Villela – São
Paulo (SP) – CEP 04310-030
In international units, communications must be forwarded to local channels or *"Unit Compliance Officers"*

Audit Committee:
- Internal email: AUDIT COMMITTEE box.
- External email: comitê.auditoria@itau-unibanco.com.br
- Mailing address:
Att Audit Committee of Itaú Unibanco Holding SA
Alfredo Egydio de Souza Aranha Square, 100
Olavo Setubal Tower - PM Floor
CEP 04344-902 – SP – São Paulo

In the international units, communications can be sent to the channel established by the local Audit Committee, if any, or to the channel of the Audit Committee of Itaú Unibanco detailed above.

These channels must be publicized and can also be used by customers, service providers and the general public.

11. PROTECTION FOR WHISTLEBLOWERS

Managers and employees may not perform acts of Retaliation against those who, in good faith report or express a complaint, suspicion, doubt or concern regarding possible violations to the guidelines of this Policy; and provide information or assistance in investigations regarding possible violations.

Managers and Employees must preserve information confidentiality related to the investigation of possible violations to the guidelines of this Policy.

The Whistleblower Channels accept anonymous reports and preserve the whistleblowers' anonymity. Disciplinary sanctions will be applied to managers or employees who attempt or retaliate against anyone who, in good faith, reports possible violations of this Policy's guidelines.

Sanctions should also be applied to managers or employees who are proven to be in bad faith when reporting possible violations of this Policy's guidelines or reporting facts known to be false.

12. EXPECTED SANCTIONS

Failure to comply with legal and regulatory provisions subjects administrators and employees to sanctions ranging from administrative to criminal penalties, for money laundering, terrorist financing, fraud, corruption and other illegal acts.

Negligence and Voluntary Failure are considered non-compliance with this policy, the Code of Ethics and the Corporate Integrity, Ethics and Conduct Policy, being subject to the application of disciplinary measures provided for in internal policy.

13. INFORMATION EXCHANGE

When applicable and in accordance with the information security guidelines determined in Corporate Information Security and Cyber Security Policy information may be exchanged between its control departments to comply with the guidelines established here.

14. RELATED REGULATIONS

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

Circular Letter No. 4001/2020 of the Central Bank of Brazil;
Circular No. 3691/2013 of the Central Bank of Brazil;
Circular No. 3680/2013 of the Central Bank of Brazil;
Circular No. 3,978/2020 of the Central Bank of Brazil and respective amendments;
Circular No. 612/2020 of the Superintendence of Private Insurance and its amendments;
Decree-Law No. 2,848/1940 - Brazilian Penal Code;

Instruction No. 34/2020 of the Brazilian National Supplementary Pension Superintendence;
Law No. 12,846/2013;
Law No. 9,613/1998 and respective amendments;
Law No. 13,810/2019 and its correlates;
SARB Self-Regulation Norm No. 011/2013 of the Brazilian Federation of Banks;
Recommendations from the Financial Action Task Force (FATF);
Resolution No. 021/2012 of the Financial Activities Control Council;
Resolution No. 50/2021 of the Securities and Exchange Commission and respective amendments;
Resolution No. 4,567/2017 of the National Monetary Council; and
Resolution No. 4,753/2019 of the National Monetary Council;
Wolfsberg Anti-Money Laundering Principles.

15. GLOSSARY

Unlawful Acts: are all conscious human actions or omissions directed towards the practice of criminal offenses - money laundering, terrorist financing, corruption and fraud.
Close Collaborators: Natural person known for having any type of close relationship with a politically exposed person, including for: i) having joint participation in a legal entity governed by private law; ii) appear as an agent, even if by private instrument of the person mentioned in *item i)* ; or iii) have joint participation in unincorporated arrangements; and Natural person who has control of legal entities or unincorporated arrangements known to have been created for the benefit of a politically exposed person.
Shell Banks: a bank incorporated in a jurisdiction where there is no physical presence and which is not part of a regulated financial group.
Final Beneficiary: is the individual who ultimately holds control of the legal entity or on behalf of which a transaction is being conducted. It is also considered the final beneficiary the representative, including the attorney and the agent, who exercise the de facto command over the activities of the Legal Entity customer.
.
Special Attention: Situations that require enhanced monitoring are those involving, but not limited to:
- I - proposals for starting relationships and operations with Politically Exposed Persons;
- II - evidence of circumvention of identification and communication procedures;
- III - customers and operations in which it is not possible to identify the final beneficiary;
- IV - transactions from countries that insufficiently apply the recommendations of the Financial Action Group - FATF; and
- V - situations in which it is not possible to keep the customer registration information updated.

Voluntary Failure: it is the intentional act of engaging in illegal acts, such as, for example, structuring or advising others to structure operations with the purpose of circumventing communications to regulatory bodies, or knowingly engaging in transactions whose proceeds come from unlawful acts.
Itaú Unibanco: Itaú Unibanco Holding S.A.
Politically Exposed Persons (PEPs): public officials who perform or have performed, in the last five years, in Brazil or in foreign countries, territories and dependencies, positions, jobs or relevant public functions, as well as their representatives, direct family members or collaterals up to the second degree, the spouse, partner, companion, stepson, stepdaughter, as well as the Close Employees. Also considered PEPs are legal entities whose representatives or controllers, directly or indirectly, are PEPs.
AML/CFTP: Preventing Money Laundering and Combating the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction.
Focal Points: administrators or employees appointed by the business unit Executive to ensure compliance with corporate AML/CFT guidelines by the business unit.
Retaliation: act of persecution, retaliation or revenge against administrators or employees who express their doubts, suspicions or findings. Examples of retaliation are: threats, demotion, inclusion in a "black list", application of suspension, termination, etc.
Accidents/Claims : atypical events that result in losses or disasters for Itaú Unibanco, such as: robberies of branches and customers, extortion through kidnapping, theft, accidents, break-ins, etc.

Approved by the Board of Directors on 2024, July.