ÍNDICE

1. OBJETIVO

Este documento estabelece diretrizes gerais e responsabilidades para identificar, avaliar, tratar, monitorar e reportar os principais riscos das atividades da organização. O objetivo é apoiar os objetivos estratégicos, reduzir incertezas, ampliar oportunidades e garantir alinhamento ao apetite de risco definido pelo Conselho de Administração.

2. ABRANGÊNCIA

Esta Política abrange todas as áreas, unidades, e operações de negócio do Assaí e seus respectivos processos e atividades.

3. DIRETRIZES

3.1 DIRETRIZES GERAIS

3.1.1. Nossas diretrizes gerais são o compromisso com a proposta de valor da Companhia e o Código de Ética e Conduta, para criar uma cultura de gestão de riscos entre todos os colaboradores.

3.1.2. A gestão de riscos integra a governança corporativa e o processo decisório da Companhia, contribuindo para a execução da estratégia. Os riscos são identificados e tratados para assegurar o cumprimento das metas estratégicas e o alinhamento ao apetite ao risco.

3.1.3. A estrutura de Gestão de Riscos envolve a atuação conjunta dos órgãos de governança e gestão, conforme o conceito das três linhas.

3.1.4. Os riscos devem ser monitorados continuamente nas atividades diárias, com revisões formais periódicas ao longo do ano, ou de forma imediata após eventos de impacto significativo ou mudanças relevantes no ambiente regulatório, competitivo ou tecnológico.

3.1.5. As matrizes de riscos devem ser analisadas criticamente, no mínimo uma vez ao ano, levando em conta todos os fatores que possam afetar os riscos existentes, incluindo o contexto interno e externo, a estratégia da Companhia e seu apetite ao risco.

3.1.6. Fragilidades e falhas identificadas devem ser comunicadas à Gestão de Riscos para análise e incorporação nas matrizes de riscos existentes. Essas fragilidades podem

ser detectadas por avaliações de áreas como Segurança da Informação, TI, Auditoria, Compliance, Controles Internos ou pelas próprias áreas de negócio da organização.

3.2. DIRETRIZES ESPECÍFICAS

3.2.1. Modelo de Três Linhas

3.2.1.1. **1ª Linha**: Áreas de negócio da Companhia responsáveis pela gestão de riscos no dia a dia, implementando controles e ações.

3.2.1.2. **2ª Linha**: Responsável por apoiar a 1ª linha, fornecendo metodologias, conhecimentos e ferramentas para gestão de riscos, controles internos, compliance e conformidade regulatória, garantindo a aplicação adequada de processos e controles.

3.2.1.3. **3ª Linha**: Auditoria Interna, atua de forma independente e objetiva avaliando a eficácia da governança e da gestão de riscos da Companhia.

3.2.1.4. **Avaliações Externas**: Ex: Auditoria Externa Independente que avalia a qualidade dos controles internos relacionados à preparação das demonstrações financeiras.

3.2.2. Papeis e responsabilidades

3.2.2.1. **Conselho de Administração**: Estabelecer as diretrizes gerais de riscos alinhadas à estratégia da Companhia. Define e aprova o apetite ao risco, avalia e aprova a matriz de riscos priorizados e promove a cultura de riscos. Avalia anualmente a estrutura da gestão de riscos e auditoria interna.

3.2.2.2. **Comitê de Auditoria (COAUD)**: Acompanhar as atividades de Controles Internos, Gestão de Riscos e Auditoria Interna, monitorar os principais riscos da Companhia e a execução do tratamento dos riscos, incluindo os indicadores, avaliar a conformidade regulatória e reportar periodicamente ao Conselho de Administração. Também propor melhorias nas políticas e avaliar informações financeiras e demonstrações contábeis da Companhia.

3.2.2.3. **Presidência Executiva / Comitê Executivo (COMEX) / DirEx (Diretoria Executiva)**: São responsáveis por gerenciar os riscos da sua área de atuação, designar pontos focais, garantir a aplicação adequada dos controles e planos de ação, manter os

registros atualizados e incorporar a gestão de riscos nas decisões de negócio. Devem prestar contas nos fóruns de governança sobre os riscos sob sua responsabilidade.

3.2.2.4. Área de Gestão de Riscos: Estabelecer a Política de Gestão de Riscos e desenvolver e aprimorar a metodologia interna. Conduzir o ciclo de gestão de riscos assessorando as áreas na identificação, avaliação e monitoramento dos riscos conforme o apetite ao risco estabelecido e acompanhando a aplicação das atividades mitigatórias. Comunicar o status da matriz de riscos nos principais fóruns, reportar riscos significativos ao CoAud e ao Conselho e notificar variações aos responsáveis.

3.2.2.5. Controles Internos: Apoiar a revisão de processos e controles, avaliar sua eficácia, conduzir testes de conformidade, acompanhar planos de ação, apoiar na elaboração de políticas e ajustar os processos conforme as melhores práticas.

3.2.2.6. Dono do Risco / responsável: Identificar, categorizar e gerenciar os riscos em conjunto com a Gestão de Riscos, assegurando a implementação dos planos de ação, a execução de atividades mitigatórias e o acompanhamento de indicadores. Indicar um ponto focal para gestão de riscos, prestar contas sobre a exposição e o status dos riscos residuais nos fóruns de governança.

3.2.2.7. Ponto focal da área: Atuam como elo entre as áreas e a Gestão de Riscos. São responsáveis por atualizar tempestivamente as informações nas ferramentas de riscos e controles, acompanhar a implementação dos planos de ação e comunicar eventos, mudanças ou novos riscos.

3.2.2.8. Área de Auditoria Interna: Avaliar de forma independente os processos de gestão de riscos, controles internos e governança. Conduzir auditorias com base nos riscos priorizados, emite recomendações e acompanha sua implementação. Reportar os resultados ao Comitê de Auditoria e ao Conselho de Administração.

3.2.2.9. Colaboradores(as): Devem atuar de acordo com as políticas da Companhia, contribuir para a execução dos controles estabelecidos e comunicar qualquer risco, falha ou irregularidade observada em suas atividades.

3.2.3. Etapas da gestão de riscos

A gestão de riscos da Companhia é orientada pelos princípios da norma ISO 31000:2018 e pelas diretrizes do COSO – Committee of Sponsoring Organizations of the Treadway Commission. O processo segue um ciclo estruturado composto por sete etapas interdependentes:

3.2.3.1. Estabelecimento do Contexto: Compreender o cenário interno e externo da Companhia, incluindo o ambiente regulatório, econômico e estratégico. Esta etapa define os critérios para avaliação dos riscos e alinha o processo de gestão de riscos aos objetivos organizacionais.

3.2.3.2. Identificação dos Riscos: Identificar e mapear os principais riscos, oportunidades e vulnerabilidades junto aos executivos e gestores. Gerar uma lista estruturada de riscos com descrição, responsável e ponto focal, classificados entre Riscos de Negócio e Riscos ESG (Ambientais, Sociais e Governança). Para os riscos emergentes, deve-se realizar o monitoramento contínuo de sinais fracos (early warnings), como mudanças regulatórias, novas tecnologias (ex. Inteligência Artificial), questões socioambientais ou tendências de mercado, que possam indicar riscos potenciais e demandar atualização imediata dos riscos priorizados.

3.2.3.3. Análise de Riscos: Avaliar os impactos e ocorrência de cada risco, utilizando critérios qualitativos e/ou quantitativos. Os riscos são categorizados em 8 tipos principais:

a) Estratégicos: Relacionados à definição e execução da estratégia da Companhia, incluindo decisões de investimento, posicionamento competitivo e inovação.

b) Financeiros: Ligados à gestão de recursos financeiros, como fluxo de caixa, crédito, câmbio, investimentos e tributos.

c) Operacionais: Decorrentes de falhas em processos, sistemas, pessoas ou infraestrutura, que podem afetar a continuidade das operações.

d) Reputacionais: Associados à imagem e credibilidade da Companhia perante seus públicos de interesse.

e) Compliance: Relacionados ao cumprimento de normas legais, regulatórias e políticas internas.

f) Meio Ambiente e Sustentabilidade: Decorrentes de impactos ambientais e do não atendimento às exigências legais e normativas ambientais.

g) Fiscal: Relativo a obrigações tributárias e eventuais passivos fiscais

h) Social: Relacionado a aspectos sobre direitos humanos, condições de trabalho e impactos sociais.

3.2.3.4 Avaliação de riscos: Avaliar os riscos com base em sua ocorrência e impacto, utilizando métodos qualitativos e quantitativos. Realizar essa avaliação com o suporte da Alta Administração, executivos e líderes de processos, dentro das dimensões consideradas, permitindo a classificação do risco entre Alto, Médio e Baixo. Com base nessas classificações, construir o mapa de riscos priorizados, que orienta a tomada de decisão e o alinhamento com o apetite ao risco e o planejamento estratégico da Companhia

3.2.3.5 Tratamento de Riscos: Definir a resposta mais adequada para cada risco entre as alternativas: **eliminar**, **mitigar**, **transferir** ou **aceitar**. A Companhia prioriza a mitigação de seus riscos por meio da criação, identificação e avaliação dos controles existentes, considerando seu desenho, maturidade e efetividade. Quando necessário, é proposto a implementação de planos de ação com responsáveis definidos (Membro da diretoria executiva), prazos e cronogramas de execução, buscando reduzir o risco residual.

3.2.3.6. Monitoramento e Revisão: Monitorar continuamente os riscos através das medidas de controles e o acompanhamento dos planos de ação. Verificar a efetividade das ações implementadas e identificar mudanças nos riscos existentes ou surgimento de novos riscos. Utilizar indicadores para sinalizar variações na exposição e avaliar a eficácia das respostas adotadas.

3.2.3.7. Comunicação e Consulta: Estabelecer uma rotina contínua de alinhamento com os principais fóruns da Companhia, como o Conselho de Administração, Comitês e lideranças executivas. Promover ações de comunicação e engajamento, como workshops, treinamentos e sessões de prestação de contas com os donos dos riscos para disseminar a cultura de riscos e garantir o entendimento dos processos e responsabilidades em toda a organização.

3.2.4. Assunção de Riscos

A assunção de riscos ocorre exclusivamente por decisão formal e consciente da Alta Administração**, quando determinado risco residual** permanece acima do apetite ou tolerância definidos**, mas sua manutenção é considerada aceitável em função de** justificativas estratégicas, operacionais ou econômicas**.**

A decisão de assunção deve ser **precedida de análise técnica** da área de Gestão de Riscos e, quando aplicável, de Compliance e Auditoria Interna, contendo:

a) descrição do risco e dos controles existentes;

b) motivos para não eliminação, mitigação ou transferência;

c) avaliação de impacto e exposição residual;

d) prazo e condições para reavaliação;

A decisão deve ser **documentada e aprovada conforme as alçadas competentes**, devendo constar em **ata ou sistema corporativo de registro de riscos**.

O **descumprimento de planos de ação ou controles dentro dos prazos estabelecidos** não caracteriza assunção de risco, mas **falha de execução**, sujeita a reporte imediato e tratamento corretivo.

3.2.4.1. Comunicação e Acompanhamento

Os riscos assumidos devem ser **formalmente comunicados ao Comitê de Auditoria e ao Conselho de Administração** pela área de Gestão de Riscos, com apoio da Auditoria Interna, **incluindo justificativa, responsável e prazo de vigência**.

A **prestação de contas** sobre riscos assumidos cabe aos **Diretores Executivos responsáveis**, que deverão **reportar o status e a eventual necessidade de revisão ou encerramento da assunção** nos fóruns competentes.

Esses riscos devem constar em **relatório específico de riscos assumidos**, monitorado periodicamente pela área de Gestão de Riscos e **revisado ao menos semestralmente**.

4. PENALIDADES

Todo(a) administrador(a) ou colaborador(a) que presenciar ou tiver conhecimento de descumprimento desta Política tem o dever de comunicar imediatamente ao Canal de Denúncias. O anonimato será assegurado e é vedada qualquer forma de retaliação. O descumprimento poderá configurar falha grave, sujeitando o infrator às sanções disciplinares cabíveis, sem prejuízo das responsabilidades cíveis e/ou criminais que poderão ser aplicadas, conforme a gravidade do caso e em consonância com o Código de Ética e Conduta da Companhia.

5. ANEXOS

N/A

6. REFERÊNCIAS

Fazem parte desta Política:

6.1. Código de Ética e Conduta.
6.2. Política Regimento de Auditoria Interna.

7. DEFINIÇÕES

7.1. Alta Direção ou Alta Administração: Conselho de Administração e Diretoria Executiva.
7.2. Apetite ao risco: É o nível de risco que a Companhia está disposta a aceitar para atingir seus objetivos, considerando os possíveis benefícios, perdas e a capacidade de resposta aos impactos.
7.3. Risco Alto: Representa uma ameaça significativa à Companhia, com alta probabilidade de ocorrência e/ou impacto severo. Exige ação imediata, priorização e forte acompanhamento por parte da liderança
7.4. Risco Médio: Representa um risco relevante, com impacto moderado e/ou probabilidade controlável. Requer monitoramento frequente e ações corretivas conforme necessidade, sem urgência imediata.

7.5. Risco Baixo: Representa uma ameaça limitada, com baixo impacto e baixa probabilidade. Pode ser aceito sem necessidade de monitoramento contínuo, desde que esteja dentro dos limites definidos pela Companhia

7.6. Controles ou Medidas Mitigatórias: Ações adotadas para reduzir a probabilidade ou o impacto dos riscos, podendo ser atividades contínuas ou periódicas que contribuem para manter a exposição dentro dos níveis aceitáveis.

7.7. Fatores Externos: Condições fora da Companhia que podem influenciar seus objetivos, como aspectos políticos, regulatórios, econômicos, ambientais, sociais, tecnológicos e relações com partes interessadas ou compromissos contratuais.

7.8. Fatores Internos: Elementos dentro da Companhia que influenciam a gestão de riscos, como cultura organizacional, estrutura, recursos, estratégias, sistemas, dados, governança e relacionamentos internos.

7.9. Gestão de riscos: É o conjunto de ações e práticas adotadas para entender, tratar e acompanhar os riscos da Companhia, de forma organizada e alinhada ao nível de risco que ela está disposta a aceitar.

7.10. Impacto: É o efeito causado se um risco acontecer. Pode afetar as finanças, o negócio, a segurança, o cumprimento de regras, a reputação ou a imagem da Companhia.

7.11. Ocorrência ou Frequência: Indica a chance de um evento acontecer, com base em quantas vezes ele ocorre em um determinado período ou análise qualitativa.

7.12. Risco: Efeito da incerteza sobre os objetivos, podendo resultar em impactos positivos ou negativos.

7.13. Risco Emergente: Risco recém-identificado ou pouco conhecido, com alta incerteza e potencial de impacto significativo devido sua imprevisibilidade e capacidade disruptiva.

7.14. Risco Inerente: Nível de risco existente antes da aplicação de qualquer controle, considerando apenas sua natureza e origem.

7.15. Risco Meta: Nível de risco considerando o conhecimento dos controles implementados e em processo de implementação.

7.16. Risco Residual: Nível de risco remanescente após a implementação adequada e efetiva dos controles e medidas mitigatórias.

7.17. Riscos Priorizados: Riscos selecionados pela Alta Administração por representarem maior potencial de impacto nos objetivos da Companhia, exigindo atenção e gestão estruturada.

7.18. Sinais Fracos: Pequenos indícios, alertas sutis ou informações preliminares, de baixa intensidade, que indicam uma possível tendência, ameaça ou oportunidade futura.

8. REVISÕES E APROVAÇÕES

Registro interno de revisões.

CONTENTS

1. PURPOSE

This document establishes the general guidelines and responsibilities for identifying, assessing, addressing, monitoring, and reporting the main risks of the organization's activities. Its objective is to support strategic objectives, reduce uncertainties, enhance opportunities, and ensure alignment with the risk appetite defined by the Board of Directors.

2. SCOPE

This Policy covers all areas, units, and business operations of Assaí, and their respective processes and activities.

3. GUIDELINES

3.1 GENERAL GUIDELINES

3.1.1. Our general guidelines are a commitment to the Company's value proposition and the Code of Ethics and Conduct, in order to create a risk management culture among all employees.

3.1.2. Risk management is integrated into the company's corporate governance and decision-making process, contributing to the execution of its strategy. Risks are identified and addressed to ensure the achievement of strategic goals and alignment with risk appetite.

3.1.3. The Risk Management structure involves the joint action of governance and management bodies, according to the three-line concept.

3.1.4. Risks should be monitored continuously in daily activities, with periodic formal reviews throughout the year, or immediately following events of significant impact or important changes in the regulatory, competitive, or technological environment.

3.1.5. Risk matrices must be critically analyzed at least once a year, taking into account all factors that may affect existing risks, including the internal and external context, the Company's strategy, and its risk appetite.

3.1.6. Identified weaknesses and failures should be reported to the Risk Management for analysis and incorporation into the existing risk matrices. These weaknesses can be detected through assessments from areas such as Information Security, IT, Audit, Compliance, Internal Controls, or by the organization's own business areas.

3.2. SPECIFIC GUIDELINES

3.2.1. Three-Line Model

3.2.1.1. 1st Line: Company business areas responsible for day-to-day risk management, implementing controls and actions.

3.2.1.2. 2nd Line: Responsible for supporting the first line, providing methodologies, knowledge, and tools for risk management, internal controls, compliance, and regulatory compliance, ensuring appropriate application of processes and controls.

3.2.1.3. 3rd Line: Internal Audit, operates independently and objectively, assessing the efficacy of the Company's governance and risk management.

3.2.1.4. External Assessments: Ex.: Independent External Audit that assesses the quality of internal controls regarding the preparation of financial statements.

3.2.2. Roles and responsibilities

3.2.2.1. Board of Directors: Establishes general risk guidelines in line with the Company's strategy. Defines and approves risk appetite, assesses and approves the prioritized risk matrix, and promotes a risk culture. Annually, it assesses the risk management and internal audit structure.

3.2.2.2. Audit Committee ("COAUD"): Monitors the activities of Internal Controls, Risk Management and Internal Audit, as well as the Company's main risks and the execution of risk treatment, including indicators. It assesses regulatory compliance and reports periodically to the Board of Directors. It also proposes improvements to policies and assesses the Company's financial information and accounting statements.

3.2.2.3. Executive Presidency / Executive Committee (COMEX) / DirEx (Executive Board): Responsible for managing the risks in their area of operation, designating focal points, ensuring the proper application of controls and action plans, maintaining up-to-date records, and incorporating risk management into business decisions. In governance forums, they give an account of the risks under their responsibility.

3.2.2.4. Risk Management Area: Establish the Risk Management Policy and develop and improve the internal methodology. Conduct the risk management cycle, advising areas on the identification, assessment, and monitoring of risks according to the established risk appetite, and monitoring the application of mitigating activities. Communicate the status of the risk matrix in key forums, report significant risks to the Audit Committee and the Board, and notify variations to those responsible.

3.2.2.5. Internal Controls: support the review of processes and controls, assess their effectiveness, conduct compliance tests, monitor action plans, assist in the development of policies, and adjust processes according to best practices.

3.2.2.6. Risk Owner/Person Responsible: Identify, categorize, and manage risks together with the Risk Management area, ensuring the implementation of action plans, execution of mitigating activities, and monitoring of indicators. Appoint a focal point for risk management, and report on the exposure and status of residual risks in governance forums.

3.2.2.7. Area Focal Points: They act as a link between the areas and Risk Management. They are responsible for promptly updating information in risk and control tools, monitoring the implementation of action plans, and communicating events, changes, or new risks.

3.2.2.8. Internal Audit Area: Independently assess risk management processes, internal controls, and governance. Conduct audits based on prioritized risks, issue recommendations, and monitor their implementation. Report the results to the Audit Committee and the Board of Directors.

3.2.2.9. Employees: They must act in accordance with Company policies, contribute to the application of established controls, and report any risk, failure, or irregularity observed in their activities.

3.2.3. Risk management steps

The Company's risk management is guided by the principles of ISO 31000:2018 standard and the guidelines of COSO - Committee of Sponsoring Organizations of the Treadway Commission. The process follows a structured cycle comprised of seven interdependent steps:

3.2.3.1. Establishing the Context: Understanding the Company's internal and external environment, including the regulatory, economic, and strategic context. This step defines the criteria for risk assessment and aligns the risk management process with organizational objectives.

3.2.3.2. Risk Identification: Identification and mapping of the main risks, opportunities, and vulnerabilities together with executives and managers. Generation of a structured risk list with description, person responsible, and focal point, classified between Business Risks and ESG (Environmental, Social, and Governance) Risks. For emerging risks, continuous monitoring of weak signs (early warnings) should be carried out, such as regulatory changes, new technologies (e.g., Artificial Intelligence), socio-environmental issues, or market trends, which may indicate potential risks and require immediate updating of prioritized risks.

3.2.3.3. Risk Analysis: Assess the impacts and occurrence of each risk, using qualitative and/or quantitative criteria. Risks are categorized into 8 main types:

a) **Strategic:** Related to defining and performing the Company's strategy, including investment decisions, competitive positioning, and innovation.

b) **Financial:** Related to the management of financial resources, such as cash flow, credit, foreign exchange, investments, and taxes.

c) **Operational:** Resulting from failures in processes, systems, people, or infrastructure, which may affect the continuity of operations.

d) **Reputational:** Associated with the company's image and credibility before its stakeholders.

e) **Compliance:** Related to adherence to legal, regulatory, and internal policy standards.

f) **Environment and Sustainability:** Resulting from environmental impacts and failure to comply with legal and regulatory environmental requirements.

g) **Tax:** Relating to tax obligations and potential tax liabilities.

h) **Social:** Related to human rights, working conditions, and social impacts.

3.2.3.4 Risk Assessment: Evaluate risks based on their occurrence and impact, using qualitative and quantitative methods. Conduct this assessment with the support of Senior Management, executive officers, and process leaders, within the considered dimensions, allowing for risk classification as High, Medium, and Low. Based on these classifications, building a map of prioritized risks, which guides decision-making and alignment with the company's risk appetite and strategic planning.

3.2.3.5 Risk Treatment: Define the most appropriate response for each risk among the alternatives: **eliminate**, **mitigate**, **transfer**, or **accept**. The Company prioritizes mitigating its risks through the creation, identification, and evaluation of existing controls, considering their design, maturity, and effectiveness. When necessary, the implementation of action plans with defined responsible parties (Member of the executive board), deadlines, and execution schedules is proposed, seeking to reduce residual risk.

3.2.3.6. Monitoring and Review: Continuously monitor risks through control measures and follow-up on action plans. Verify the effectiveness of implemented actions and identify changes in existing risks or the emergence of new risks. Use indicators to show variations in exposure and evaluate the effectiveness of the responses adopted.

3.2.3.7. Communication and Consultation: Establish an ongoing routine of alignment with the Company's key forums, such as the Board of Directors, Committees, and executive leadership. Promote communication and engagement initiatives, such as workshops, training sessions, and accountability sessions with risk owners, to disseminate a risk culture and ensure understanding of processes and responsibilities across the organization.

3.2.4. Assumption of Risks: The assumption of risks occurs exclusively through a formal and conscious decision by Senior Management, when a given residual risk remains above the defined appetite or tolerance levels, but its maintenance is deemed acceptable due to strategic, operational, or economic justifications.

The decision to assume a risk must be preceded by a technical analysis conducted by the Risk Management department and, when applicable, by Compliance and Internal Audit, containing:

- a description of the risk and the existing controls;
- the reasons for not eliminating, mitigating, or transferring the risk;
- an assessment of the impact and residual exposure; and
- the timeframe and conditions for re-evaluation.

The decision must be duly documented and approved in accordance with the applicable authority levels and recorded in meeting minutes or within the corporate risk management system.

Failure to implement action plans or controls within the established deadlines does not constitute an assumption of risk, but rather an execution failure, subject to immediate reporting and corrective measures.

3.2.4.1. Communication and Monitoring: Assumed risks must be formally communicated to the Audit Committee and the Board of Directors by the Risk Management department, with the support of Internal Audit, including the justification, responsible party, and validity period.

Accountability for assumed risks lies with the Executive Directors responsible, who must report on the status and any need for review or termination of the assumption in the appropriate forums.

Such risks must be included in a specific Assumed Risks Report, to be periodically monitored by the Risk Management department and reviewed at least on a semiannual basis.

4. PENALTIES

All managers and employees who witness or become aware of a breach of this Policy have a duty to immediately report it to the Whistleblowing Channel. Anonymity is guaranteed, and any form of retaliation is prohibited. Non-compliance may constitute a serious offense, and the offender will be subject to the applicable disciplinary sanctions, without prejudice to civil and/or criminal liabilities that may be applied, depending on the severity of the case and in accordance with the Company's Code of Ethics and Conduct.

5. ATTACHMENTS

Not applicable field.

6. REFERENCES

This Policy includes:

6.1. Code of Ethics and Conduct.

6.2. Internal Audit Policy and Regulations.

7. DEFINITIONS

7.1. Senior Management: Board of Directors and Executive Board.

7.2. Risk appetite: This is the level of risk the Company is willing to accept to achieve its objectives, considering the potential benefits, losses, and ability to respond to impacts.

7.3. High Risk: Represents a significant threat to the Company, with high probability of occurrence and/or severe impact. Requires immediate action, prioritization, and close monitoring by leadership.

7.4. Medium Risk: Represents a significant risk, with moderate impact and/or controllable probability. Requires frequent monitoring and corrective actions as needed, without immediate urgency.

7.5. Low Risk: Represents a limited threat, with low impact and low probability. It can be accepted without the need for continuous monitoring, as long as it remains within the limits defined by the Company.

7.6. Controls or Mitigation Measures: Actions taken to reduce the likelihood or impact of risks, which may be continuous or periodic activities that contribute to keeping exposure within acceptable levels.

7.7. External Factors: Conditions outside the Company that may influence its objectives, such as political, regulatory, economic, environmental, social, technological aspects, and relationships with stakeholders or contractual commitments.

7.8. Internal Factors: Elements within the company that influence risk management, such as organizational culture, structure, resources, strategies, systems, data, governance, and internal relationships.

7.9. Risk management: Set of actions and practices adopted to understand, address, and monitor the Company's risks, in an organized manner and in line with the level of risk it is willing to accept.

7.10. Impact: This is the effect caused if a risk occurs. It can affect the Company's finances, business, security, regulatory compliance, reputation, or image.

7.11. Occurrence or Frequency: Indicates the likelihood of an event occurring, based on how many times it happens in a given period or through qualitative analysis.

7.12. Risk: This is the effect of uncertainty on objectives, and it may result in positive or negative impacts.

7.13. Emerging Risk: A newly identified or poorly understood risk, with high uncertainty and potential for significant impact due to its unpredictability and disruptive capacity.

7.14. Inherent Risk: Level of risk that exists before the application of any controls, considering only its nature and origin.

7.15. Target Risk: Risk level considering knowledge of implemented controls and those in the process of implementation.

7.16. Residual Risk: Level of risk remaining after the proper and effective implementation of controls and mitigation measures.

7.17. Prioritized Risks: Risks selected by Senior Management because they represent a greater potential impact on the Company's objectives, requiring attention and structured management.

7.18. Weak Signs: Small indications, subtle warnings, or preliminary information of low intensity that suggest a possible future trend, threat, or opportunity.

8. REVIEWS AND APPROVALS

Internal record of revisions.