

CONTENTS

1. PURPOSE.....	2
2. GUIDELINES	2
3. REFERENCES.....	21
4. DEFINITIONS.....	21



1. PURPOSE

To establish the risk management principles, process guidelines and responsibilities of Sendas Distribuidora S.A. (hereinafter "Company"), as well as to guide the identification, assessment, treatment, monitoring and communication of risks that are inherent to the activities, incorporating the risk vision to strategic decision-making in accordance with the market best practices; contributing to the protection of the Company's value; supporting the fulfillment of business objectives; reducing uncertainty in a preventive manner; and increasing the identification of opportunities.

2. GUIDELINES

- 2.1. Our general guidelines are commitment to the Company's value proposition, in line with our Code of Ethics so we can create a risk management culture that reaches all employees.
- 2.2. Risk Management is part of the Company's corporate governance process, being an integral part of the decision-making process and contributing to the execution of its strategy. Risks are identified and treated to ensure that the goals set in the strategic planning are met.
- 2.3. To that end, the Risk Management structure takes into account the joint action of corporate governance and management bodies, in accordance with the concept of the four lines, as described in table 1 below:

First Line	Second Line	Third Line	Fourth Line
- Operational Management, represented by the directors, managers and other employees in all business areas (stores, DCs, regional offices and	- Specialized areas, control areas and support functions, represented by the Risk Management and Business Continuity Area, which analyzes	- The assurance functions, represented by the Internal Audit Area, responsible for auditing and reviewing Risk Management and Internal Control	- Independent External Audit functions, whose professional mission is to assess the quality of internal controls aimed at

<p>headquarters) that deal with day-to-day tasks and operations.</p> <ul style="list-style-type: none"> - They must manage the performance and the assumed risks in accordance with the provisions of this Policy. - They implement control systems, action plans and render account in a timely manner of the information regarding Risk Management. - The responsibility for risk management is still an essential part of first-line functions, and in the scope of their management. 	<p>the effectiveness of risk assessments conducted by the Operations Management, and may require assistance from other internal areas of the Company responsible for, among other matters, Legal, Tax, Personal Data Protection, Projects Office, Compliance, Internal Controls, Information Security, Sustainability etc.</p> <ul style="list-style-type: none"> - They must guide, monitor and assess adherence to defined standards and policies, and support the first line in achieving 	<p>practices, as well as the effectiveness of governance, identifying problems and opportunities for improvement with independence, objectiveness and power for the recommendations.</p> <ul style="list-style-type: none"> - The Internal Audit provides independent and objective assessment and advisory on the appropriateness and efficacy of governance and risk management, through the competent application of systematic and disciplined process Reports its conclusions to the senior management and 	<p>preparing financial statements. In this role, the Independent External Audit is also one line among the four lines, as it must report to the company the shortcomings of these controls, if they find any.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	the Company's objectives. - Facilitate, communicate and monitor risk management practices and help identify risks.	the governance body in order to promote and facilitate continuous improvements, also in the risk management process (including internal controls).	
--	-----------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------	--

Table 1: 4-The four lines model

- 2.4.** Risks must be continuously monitored during the performance of your routines, and they must also be reviewed on a quarterly basis, or occasionally, in the occurrence of an event that generates significant impact.
- 2.5.** Risk matrices must be critically analyzed once a year, considering all elements that affect the existing risks, and the internal and external context and organizational strategy.
- 2.6.** Identified weaknesses and failures must be informed to Risk Management, so that they can be analyzed and reflected in the existing risk matrices. Weaknesses can be identified in the analysis of sectors such as Information Security, IT, Audit, Compliance, Internal Controls, or the organization's business areas.

2.7. Roles and responsibilities

- We describe all stakeholders within the life cycle of the Risk management process, along with their respective responsibilities.

Function	Responsibilities
Board of Directors	<ul style="list-style-type: none"> • Establishing general risk guidelines in line with the business context and the strategic planning cycle; • Assessing, deliberating and approving the strategic and prioritized risk matrix;

Function	Responsibilities
	<ul style="list-style-type: none"> • Influencing and sponsoring Prioritized Risks monitoring within the management forums; • Influencing and sponsoring the Risk culture within the Company; • Conducting an annual assessment of whether the Risk Management and Internal Audit Area's structure and budgets are adequate for the performance of their functions; • Reviewing and approving general definitions of the Risk Management strategies; • Approving the budget intended for the Audit Committee, aiming at ensuring its operational autonomy and covering its operating expenses.
Audit Committee (COAUD)	<ul style="list-style-type: none"> • Following the activities of the Company's Internal Controls, Risk Management, and Internal and External Audit areas; • Following the Company's risk exposures; • Assessing the eligibility of forums, definitions and guidelines to compose the risk management model within the Company; • Following the risk indicators applicable to the business context and the Board of Directors' guidelines; • Checking the regular performance of Risk Management activities, following compliance with legislation, as well as the Company's internal policies, norms and standards; • Assessing, monitoring and periodically informing the Board of Directors of Prioritized Risks identified in the reviews conducted by the

Function	Responsibilities
	<p>Risk Management area, helping with the assessment of the action plans and fulfillment of recommendations;</p> <ul style="list-style-type: none"> Assessing, approving and following the execution of Prioritized Risks treatment and monitoring; Assessing, approving and recommending to administration the corrections and/or improvements related to Company's internal policies; Assessing the Company's quarterly information, interim statements and financial statements;
Corporate Governance and Sustainability Committee	<ul style="list-style-type: none"> Planning and ensuring the operationalization of Risk Management, taking into account all dimensions of the defined structure, including the Company's strategic, tactical and operating activities; Advising the Board of Directors when applying the Company's Risk Management methodology; Supporting the Board of Directors when defining the Company's prioritized risks; Supporting the Company in the analysis and approval of the Risk Management strategy; Advising the Audit Committee and the Board of Directors on Risk exposure levels; Assessing the Company's Risk Management process; Identifying risks arising from the Company's strategic and direction changes decided by the Board of Directors.

Function	Responsibilities
<p>Chief Executive Office / <u>COMEX</u> / <u>DirEx (Executive Board)</u></p>	<ul style="list-style-type: none"> • Promoting integration and risk culture in the Company and in strategic planning and management cycles; • Approving the Risk Management Policy and supporting the initiatives of the Risk Management and Business Continuity area, aiming at contributing to the efficacy of their actions; • Promoting the implementation of an efficient Risk Management model, in line with business objectives and business goals. Applying general guidelines established by the Board of Directors; • Monitoring risks managed at the level of each process and operations in order to ensure the effectiveness of control measures; • Taking part in the Company's Risk identification, validation and prioritization processes; • Monitoring KRIs and KPIs and the mitigation strategy for Prioritized Risks; • Assessing and monitoring the treatment of business Risks, in line with the execution of strategic planning; • Assessing in a timely manner the effectiveness and applicability of this Policy's guidelines; • Assessing and supporting adjustments to the structure aimed at the management process, taking into consideration human, financial and technological resources; • Responsible for the Company's relevant risk management, concentrating all efforts required

Function	Responsibilities
	<p>to mitigate the risks deemed to have significant impact on the fulfillment of business objectives;</p> <ul style="list-style-type: none"> Assuming and authorizing risks that are above accepted levels and, thus, justify strategic initiatives and corporate decisions.
Risk Management Area	<ul style="list-style-type: none"> Establishing the Risk Management Policy and Procedures; Encouraging the adoption of good risk management practices, considering the Company's business needs; Fostering training programs and awareness campaigns about Risk Management and Business Continuity; Defining, establishing and improving the Risk Management methodology, in line with the value chain, and integrated into the strategy, tactics and operations of the Company; Managing the Company's Risk Management process cycle, jointly with the areas and respective business activities of the Company; Conducting the management of information flow within all business areas and activities, in line with concepts, methodology and deadlines established for each cycle of Risk Management; Supporting all business areas and activities in the cycle of risk identification, assessment, treatment and monitoring in order to assist them in reducing the level of risk exposure;

Function	Responsibilities
	<ul style="list-style-type: none"> Managing the Risks Matrix, communicating in the main management forums their status and levels of exposure; Assisting the business areas in identifying and assessing the risks' impact. Reporting/Informing the status of the most significant risks to the Audit Committee of Assaí in a timely manner; Analyze potential risks based on the vulnerabilities informed by business areas, audit, security, internal controls or compliance; Notify risk owners about significant changes in risk under their responsibility; Support the Senior Management in the process of approval of risks that are above the acceptance levels established.
Compliance Area	<ul style="list-style-type: none"> Assist Risk Management with the identification and assessment of third parties' risk, in order to mitigate possible risks of corruption, fraud, conflicts of interest and negative media, among others, ensuring compliance with current anticorruption and antifraud laws and regulations, and in accordance with the matrix of prioritized risks; Monitoring risk assessments conducted based on the level of risk; Supporting prepare and adjust standards, policies and procedures so as to reduce the business's risk exposure;

Function	Responsibilities
	<ul style="list-style-type: none">• Assisting the preparation of policies, processes, standards and procedures manuals; and• Spreading Compliance culture through training and communication, ensuring compliance with existing laws and regulations as well as internal norms, aiming to mitigate identified risks.
Internal Controls Area	<ul style="list-style-type: none">• Reviewing controls in the SOx matrix together with the business areas;• Conducting SOx tests;• Supporting areas in the implementation of action plans and remedying identified issues before and after the stages of the SOx audit process;• Meeting the requests of the external audit;• Supporting with preparation of procedures policies, processes, norms and manuals;• Mapping and assessing adherence to Policies, Norms and Procedures and adjusting processes to the best market practices;• Follow up on and controlling the main reported aspects (external and internal audit, internal controls and risk management);• Supporting the Risk Management and Business Continuity area in mapping the risks relating to non-compliance to SOx requirements;• Provide support to other areas in order to improve the internal controls environment of the processes.

Function	Responsibilities
Information Security Area	<ul style="list-style-type: none">• Identifying information security vulnerabilities and risks;• Maintaining effective communication with the Risk Management team on possible vulnerabilities, threats, failures, abnormalities, violations and new security measures;• Promptly informing the Information Technology area about violations, failures, anomalies and other conditions that may put the Company's information and assets at risk;• Monitoring access to technology information and assets (systems, databases, network resources), respecting to the Information Security' policies and procedures;• Implementing and keeping security controls and standards defined for technology assets in operation;• Defining controls for treating risks, vulnerabilities, threats and non-compliances identified by Information Security processes;• Proposing methodologies and processes referring to information security, such as classification of information, risk assessment and analysis of vulnerabilities;• Classifying and reclassifying the level of access to information whenever necessary;• Establishing and maintaining the Information Security Policy;• Establishing, controlling, implementing, disclosing and updating the Information

Function	Responsibilities
	<p>Security Policy, other policies, and the Information Security norms and standards applicable;</p> <ul style="list-style-type: none">• Developing and implementing, with the engagement of the Internal Communication area, awareness programs and training on Information Security;• Conducting vulnerability analyses, aimed at ensuring the level of security of the information systems and other environments that store, process or transmit information of interest to the Company;• Treating risks and vulnerabilities identified in assets, systems or processes under the responsibility of the area or of interest to the Company;• Conducting the management of Information Security incidents, including investigations to determine the causes and those responsible, as well as communicating the facts;• Proposing corrective actions for Information Security incidents;• Requesting information to other areas of the Company and conducting security tests and assessments aimed at verifying compliance and adherence to the Information Security Policy whenever necessary;• Conducting project assessment in Assaí's business areas and IT, making the necessary

Function	Responsibilities
	<p>security observations for implementing/hiring Software/Service/Solution;</p> <ul style="list-style-type: none"> Proposing projects and initiatives to improve Assaí's level of Information Security; Proposing investment related to Information Security aimed at minimizing risks;
Risk Owner / Person Responsible	<ul style="list-style-type: none"> Identifying, classifying and managing risks in the areas in accordance with mitigation strategies, together with the Risk Management Area; Appointing the professional who will be the area's focal point in Risk management process jointly with the Risk Management area. Ensuring the implementation of action plans and monitoring of KRIs and KPIs; Rendering account of the levels of exposure, the action plans and the indicators that describe the residual risk status to the governance and management forums; Notifying the Risk Management area about the risks, similar events, or changes in the current context of risks that have been identified in work routines.
Area's focal point	<ul style="list-style-type: none"> Having the technical knowledge of processes where there are Risks; Being responsible for updating the information on the mapping and treatment of Risks in their business area/unit (stores, DCs, regional offices, headquarters' areas);

Function	Responsibilities
	<ul style="list-style-type: none"> • Keeping information up to date in a timely manner, respecting the Risk Management cycle's planning calendar; • Monitoring the status of action plans before those responsible for implementing control mechanisms; • Notifying the Risk Management area about any risks or similar events that have been identified in work routines.
Internal Audit Area	<ul style="list-style-type: none"> • Assessing the quality and effectiveness of the Company's risk management control and governance processes; • Identifying and pointing out opportunities to improve the processes of Internal Control and Risk Management; • Auditing information and controls regarding KRIs and KPIs developed and monitored by the functioning areas; • Periodically reporting to COAUD, body to which the internal audit area is linked, and to its audited clients the results of independent, impartial and timely assessments on the effectiveness of the Company's Risk Management.
Employees	<ul style="list-style-type: none"> • Ensuring the operationalization of Risk Management, being part of the identification, assessment and measuring processes and implementing preventive and corrective actions;

Function	Responsibilities
	<ul style="list-style-type: none">• Preparing and fulfilling the action plans intended to appropriately address the risks under their responsibility;• Notifying the Risk Management area about similar risks or events identified in their work routines.

Table 2: Roles and responsibilities

2.8. Risk Management process

The Company's Risk Management process was defined based on the guidelines of COSO - Committee of Sponsoring Organizations of the Treadway Commission and the ISO 31000 standard: 2018: Risk Management Principles and Guidelines. The process's life cycle has 7 subsequent and dependent stages which we execute annually.

2.9. Stages of the Company's Risk management process

- **Stage 1 - Definition of the Context:**
 - Understanding the business scenario and context, taking into account factors linked to the Company's and its business areas' short and long-term strategic planning, in line with the environment where these objectives are found.
 - This is a crucial stage to ensure that the Risk Management process is in line with the Company's management and strategic planning cycles in order to align its acceptable levels.
 - It comprises an annual cycle of executive alignments with process owners, risk owners and Senior Management to build a reference map that in the next stages will help identify risks, emergent risks and opportunities that are in line with the business context.
 - In order to establish the scenarios that should support this stage, we take into account two influencing factors, namely:
 - **External Factors:** They may include, among others:

- social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, in the international, national, regional or local level;
- key drivers and trends affecting the organization's objectives;
- relationships, perceptions, values, needs and expectations of external stakeholders;
- contractual relationships and commitments;
- complexity of relationship networks and dependencies.
- **Internal Factors:** They may include, among others:
 - Vision, mission and values;
 - Governance, organizational structure, roles and responsibilities;
 - Strategy, objectives and policies;
 - Organizational culture;
 - Norms, guidelines and models adopted by the organization;
 - Capacities understood in terms of resources and knowledge (for example, capital, time, people, intellectual property, processes, systems and technologies);
 - Data, information systems and information flows;
 - Relationships with internal stakeholders, considering their perceptions and values;
 - Contractual relationships and commitments;
 - Interdependencies and interconnections. Infrastructure, Human Resources, Processes, Governance and Technology.
- **Stage 2 - Identification of Risks:**
 - A top-down risk identification approach, beginning with an interview with the main executives in all areas of the Company, in light of the main processes for which they are responsible.
 - The product generated in this stage is a broad list of Risks, Emerging Risks and Opportunities based on the events that may identify vulnerabilities, threats putting the achievement of the Company's strategic objectives at

risk, and opportunities that provide an advantage in reaching these objectives.

- In this stage, the owner and the focal point of each one of the Risks and Opportunities identified must be appointed, as well as the description that will guide the next stages of the mapping process.
- A primary key classification of risks and opportunities is as follows: i) “traditional” and ii) environment, social and governance.

▪ **Stage 3 - Analysis:**

- We carry out a more detailed analysis of the identified Risks, including important attributes for clarity and qualitative and quantitative support, in order to generate variables that can classify the risks universe, so we can act more assertively in their prioritization.
- We define, among others, risk causes and factors, as well as their effects, classifying aggravating factors so we can create a broad and relevant list of risks to carry on with the mapping process.
- We raise information in order to obtain data that may quantify and describe the probability and impact of risks, thus generating an assessment map to describe in an executive manner the risks universe based on their classification, as described in Figure 1.

Impacto	Catastrófico	5	10	15	20	25	<table><tr><td>Risco Baixo</td><td>de 1 a 4</td></tr><tr><td>Risco Médio</td><td>de 5 a 12</td></tr><tr><td>Risco Alto</td><td>de 15 a 25</td></tr></table>	Risco Baixo	de 1 a 4	Risco Médio	de 5 a 12	Risco Alto	de 15 a 25
	Risco Baixo	de 1 a 4											
	Risco Médio	de 5 a 12											
	Risco Alto	de 15 a 25											
	Crítico	4	8	12	16	20							
Importante	3	6	9	12	15								
Médio	2	4	6	8	10								
Baixo	1	2	3	4	5								
		Excepcional	Raro	Ocasional	Provável	Frequente							
Ocorrência													

Legend:

Impact
Catastrophic
Critical
Important
Medium
Low
Occurrence
Exceptional
Rare
Occasional

Probable
Frequent
Low Risk from 1 to 4
Medium Risk from 5 to 12
High Risk from 15 to 25

Figure 1: Assessment Map – Risk Severity

- We rate Risks in this assessment map according to the following criteria:
 - **High Rating or High Risk (Red):** They represent a potential threat to the Company's business and priority actions must be taken in order to reduce or eliminate the risk component.
 - **Medium Rating or Medium Risk (Yellow):** They represent a threat and can be monitored and managed through preventive control measures that can keep the level of exposure or risk acceptance.
 - **Low Rating or Low Risk (Green):** They represent an acceptable threat with lower levels of impact, thus no continuous monitoring is necessary and the risk is acceptable.
- **Stage 4 - Assessment:**
 - We assess inherent and residual risks (at the moment of the assessment) and their potential impacts of their materialization on the achievement of the Company's objectives.
 - With the support of Senior Management, executives and process leaders, we assess the events from the perspectives of occurrence (likelihood of occurrence of the risk) and impacts. We look for variables to combine qualitative and quantitative assessment methods.
 - We take into account, among others, variables for classification of impacts that help with better classification of risks, using quantifications and scales that provide a gradient of high, medium and low for each variable.
 - Finally, we combine all assessment variables, define the criticality of identified risks, which allows us to build a prioritization map, from risks of higher exposure to those of lower exposure.
 - This map helps the Company to obtain a higher level of alignment of the Company's strategic planning with the acceptable Risk level.

▪ **Stage 5 - Treatment:**

- The risk treatment stage involves control mechanisms existing within the process for us to classify its effectiveness as a preventive measure and as a measure that reduces the level of exposure (Mitigating Factor), which will help calculating the residual risk.
- For processes that require a higher level of effectiveness of controls or that do not have effective mitigating factors, we formalize the implementation of one or more action plans to mitigate risk factors in this stage.
- For each action plan, we appoint a risk owner (a member of the Company's Executive Board) and the different persons responsible for actions and implementation timelines in order to ensure the effectiveness and efficiency of the plans, thus reduce the level of residual risk and looking for our target residual risks.
- Within this process, we apply possible risk responses, as shown in Table 2:

Eliminate	Reduce or Mitigate	Transfer	Accept
Taking actions that change or eliminate the risk source, whether through the discontinuance of a product, process or project, in order to protect business objectives from the impacts of this risk.	Adopting control measures to reduce the impact and/or occurrence of a risk to an acceptable level.	<p>Taking actions that reduce the impact and/or occurrence of the risk by transferring or sharing part of the risk.</p> <ul style="list-style-type: none">• Note: The transferred risk owner continues to be the main manager of the risk, since	No measure is adopted to affect the impact and/or occurrence of the risk.

		the transfer is not absolute.	
--	--	----------------------------------	--

Table 2: Possible risk responses

▪ **Stage 6 - Monitoring:**

- Systematic and continuous activity that is crucial to maintain the efficacy of actions taken to mitigate risks in a preventive manner, in order to reduce the impacts or the occurrence.
- Employees involved in each area must have the ability and competence to identify, assess, prioritize, monitor and manage their risks, taking into account all changes in the internal and external environment so they can achieve a high level of control of their processes, in order to meet targets set in risk treatment (see Table 2).
- The risk monitoring process is composed of two main fronts, namely:
 - **Action Plans:** Must be conducted by the areas under the leadership of the process/risk owner, according to the responsibilities defined by the risk owners, with a frequency that may vary between monthly, bimonthly, quarterly, half-yearly and up to annually, depending on the Risk Management needs.
 - **Control Measures:** We use metrics and indicators that we call KRIs and/or KPIs. These metrics and indicators are related to risk factors, preventive measure factors and/or performance indices relating to the level of implementation of the action plans established to mitigate risks. During the risk treatment stage, we identify these metrics according to control mechanisms, making a relationship among financial and non-financial variables that enable us to timely follow the development and/or deviations that may materialize risks, so that triggers may be set for the business areas to take reverse actions on the events and, consequently, the impacts, and also according to the capacity to deliver the action plans established.

▪ **Stage 7 - Communication:**

- We carry out a frequent alignment process aimed at spreading the Risk Management culture through workshops, training and/or accountability

processes with risk owners and the Company's main management forums, such as the Board of Directors, the Executive Committee and the Audit Committee, among others.

In order to carry out this communication process, we set a plan that develops communication formats according to the target audience, where we describe the frequency, those involved and the responsibility within that context. These are key activities in keeping and improving Assaí's Risk Management culture.

- **Risk Rating:** We have adopted 4 main risk ratings in this process, namely:
 - **Strategic:** Risks that affect the Company's strategy or strategic objectives. They are linked to uncertainty and/or opportunity scenarios and are the priority focus of Senior Management.
 - **Operational:** Risks arising from inadequacy or failure in the management of internal processes, of people or technologies that can hinder or prevent the achievement of objectives.
 - **External:** Risks arising from events outside the company and are beyond its influence or control. They are linked to external factors, such as the economic environmental, sanitary crises, regulatory environment, consumer habits and others.
 - **Corporate Social Responsibility:** Risks related to any matters of an environmental, social and/or governance nature, and linked to the reputation and/or image of the Company.

3. REFERENCES

3.1. The following are part of this Policy:

3.1.1. Code of ethics.

4. DEFINITIONS

- 4.1. **Senior Executives or Senior Management:** Person or group of persons in the highest level that run and control an organization, represented by the Board of Directors and the Executive Board.

- 4.2. Risk Cause:** Risk factors that contribute for the risk to materialize, increasing its impacts through related consequences.
- 4.3. COAUD:** Audit Committee.
- 4.4. COMEX:** Executive Committee.
- 4.5. Risk Consequences:** Aggravating factors of an event's results and impacts, which can positively or negatively affect the Company's ability to achieve its objectives.
- 4.6. Controls or Mitigation Initiatives:** Actions carried out to reduce inherent risks, which can be periodic or continuous activities in the business units to help monitor the levels of risk exposure.
- 4.7. DIREX:** Executive Board, which represents the Senior Management.
- 4.8. Event:** An occurrence or set of occurrences that can generate impact, either positively or negatively affecting results.
- 4.9. Risk source:** Element that, individually or combined, has an inherent potential to originate the risk.
**NOTE: A risk source can be tangible or intangible.*
- 4.10. Risk Management:** Systematic application of policies, procedures and management practices in activities linked to communication, inquiries, definition of context, and identification, analysis, assessment, treatment, monitoring and critical analysis of risks.
- 4.11. Impact:** Aggravating factors or consequences in case the risk materializes, which can be classified as Financial, Business, Physical Security, Food Security, Compliance, Reputational and Image Impacts.
- 4.12. Mitigation Initiatives or Controls:** Actions carried out to reduce inherent risks, which can be periodic or continuous activities in the business units to help monitor the levels of risk exposure.
- 4.13. Key Performance Indicator (KPI):** Metrics used to measure and monitor the performance and results of processes, as well as the level of development and performance of action plans established to mitigate risks, and they can be used to monitor Risks.
- 4.14. Key Risk Indicator (KRI):** Metrics used to measure and monitor exposure to risks. They are related to the causes of the risk help the Company act

preventively in order to reduce the impacts of risk materialization, also being a control and good practice mechanism in Risk Management.

4.15. Mitigation: Option for treatment of risks, intended to reduce risks through controls and actions that are taken in a **tolerable level**.

4.16. Opportunity: Risk identified based on a positive source that allows to obtain gains or advantages through an effective action.

4.17. Risk Management Policy: Declaration of an organization's intentions and general guidelines relating to risk management.

4.18. Probability of Occurrence or Frequency: Measure on the probability of an event, expressed as the number of events or results occurred during a defined time unit.

4.19. Risk: effect of uncertainty on the objectives.

***NOTE 1:** "Effect" is a deviation relating to the expectations – positive and/or negative.*

***NOTE 2:** The objectives may have different aspects (such as financial, health and safety, and environmental targets), and they may be applied in different levels (such as strategic, across the organization, project, product and process).*

***NOTE 3:** Risks are often characterized by their reference to potential events and consequences, or both.*

***NOTE 4:** Risks are often expressed in terms of a combination of consequences of an event (including changes in circumstances) and the related occurrence probability.*

***NOTE 5:** "Uncertainty" is the state, even partial, of the information gaps relating to an event, the understanding thereof, its knowledge, its consequences or its probability.*

4.20. Emerging Risk: Any risk recently identified with a possible long-term impact on the Company's business, although, in some cases, it may already have started to impact the Company's business today.

4.21. Inherent Risk: Property in which the risk is always present in an intrinsic manner, both in its potential or residual condition, as long as its source exists.

4.22. Potential Risk: Pure or gross risk; risk that does not have treatment measures or controls that could reduce its impact or probability of occurrence.

4.23. Residual Risk*: Level of risk after taking into account all controls and actions identified to reduce its impacts or probability of occurrence.

Note*: *This is the level of risk that the Company will have after the end of the period in question, once the established actions plans have been implemented, and the Company's existing control activities have been maintained.*

4.24. Prioritized Risks (Top Main Risk – TMR): List of risks deliberately defined by Senior Management. which describes the levels of exposure that can enhance high impacts for the business. Their management must be a structured priority.

4.25. Handling Risks: Process to modify risks.

NOTE 1:

The handling of risks may involve:

- actions to avoid risks through the decision of not starting or interrupting the activity that originates the risk;*
- undertaking our increasing the risk in order to search for an opportunity;*
- elimination of the risk source;*
- change in probability;*
- change in consequences;*
- sharing the risk with another party or parties (including contracts and risk financing); and*
- knowingly retaining the risk.*

NOTA 2: *The treatment of risks relating to negative consequences is often referred to as “risk mitigation”, “elimination of risks”, “risk prevention” and “risk reduction.”*

NOTE 3: *The handling of risks may result in new risks or change the existing risks.*

4.26. Vulnerability: Intrinsic properties that result in the susceptibility to a risk source that may lead to a consequence.

ATACADISTA