PADTEC HOLDING SA

CORPORATE RISK MANAGEMENT POLICY

1. Purpose

This Corporate Risk Management Policy ("Policy") of Padtec Holding SA ("Company") aims to stipulate the guidelines, principles, roles and liabilities in the management of corporate risks, as well as the development, dissemination and implementation of the of Risks management culture, by guiding the processes for identifying, analyzing, assessing, treating, monitoring and communicating the mapped Risks, aiming at promoting continuous improvement for the Company's processes and obtaining better results.

2. Scope

This Policy applies to all macroprocesses, business operations and areas of the Company, and its compliance by Management and all employees is mandatory.

3. Definitions

"Action Plan" - is the organized form, according to a certain methodology previously defined by the Internal Controls and Internal Audit areas, as the case may be, which describes goals and objectives, as well as the activities that must be carried out for the treatment of a certain identified Risk to avoid it, accept it, reduce it, eliminate it or transfer it.

"Company" - is Padtec Holding SA and its subsidiaries, especially Padtec SA.

"Controls" - are the actions taken by the Company aiming at reducing the risks inherent to the activities carried out by the business units and other areas, and these activities may be periodic or continuous. These actions will assist the respective bodies of the Company and its employees, as the case may be, in monitoring the exposure levels of each of these Risks.

"Event" - is the occurrence or change in a specific set of circumstances that result in the materialization of a Risk.

"Management" - Board of Directors and Executive Board of the Company.

"Probability" - indicates the possibility of a given event occurring. It can be expressed in quantitative terms, such as: percentage, frequency of occurrence, or other numerical metric, or in qualitative terms, such as: high, medium, low.

"Risk(s)" - are the factors and/or events that may cause negative impacts, compromising the Company's ability to achieve its strategic objectives and the effective creation and protection of its value.
"Risk Analysis" **-** is the process of understanding the nature of a certain risk and determining the Probability of its materialization, resulting in how much the Company would be exposed to that particular risk.

"Risk Appetite" - is the level of Risk exposure that the Company is willing to accept in order to achieve its objectives within the limits established by the Management.

"Risk Assessment" - is the process of comparing the results obtained in the Risk Analysis with the criteria established by the Management, in accordance with this Policy, to determine whether the Risk and/or its magnitude are acceptable or tolerable by the Company.

"Risk Management" - is the set of coordinated and structured activities in order to align the Risk Appetite with the strategic decision-making cycle in the search for risk mitigation and optimization of the results to be achieved by the Company.

"Risk owner" - has the definition in "Step 2" of item 7.

"Risk Treatment" - is the process of modifying the Risk, which may be the action of (i) avoiding the Risk by deciding not to initiate or discontinue the activity that gives rise to the Risk; (ii) assume or increase the Risk, in order to seek an opportunity for the Company; (iii) removal of the Risk Source; (iv) changing the Probability; (v) changing the expected consequences; (vi) sharing the Risk with other party(ies); and/or (vii) the retention of the Risk due to a conscious choice by the Company.

"Source of Risk" - are the elements that, individually or in combination, have the intrinsic potential to give rise to a given Risk.

4. Duties and Liabilities

FUNCTION	LIABILITIES
Board of Directors	• To establish general Risks guidelines in line with the business context and the strategic planning cycle of the Company; • To establish, through the capacity and tolerance of the Company, the acceptable limits of Risk Appetite; • To assess, deliberate and approve the matrix of strategic and prioritized risks, in line with the Company's Risk Appetite; • To define and review the Risk Management criteria and strategies; • To assess, annually, the sufficiency of the structure and budget of the Internal Audit area for the performance of its functions, as recommended by the Audit Committee; • To assess and deliberate on the reports made by the Internal Audit, through the Audit Committee; • To review and approve the general definitions of Risk Management strategies;

	• To ensure the Audit Committee operational autonomy, to approve its own budget to cover expenses with its operation; • To approve and modify this Policy, its future developments and revisions.
Audit Committee	• To monitor the activities of the Internal Audit area and the Company's Internal Controls area; • To assess and monitor the Company's risk exposures; • To propose to the Board of Directors the definitions and guidelines to compose the Company's Risk Management model; • To propose to the Board of Directors the tolerance levels for exposure to the identified risks; • To monitor and support the Risk Management process in defining the prioritized risks in line with the business context and the guidelines of the Board of Directors; • To supervise Risk Management activities in compliance with current legislation and the Company's internal policies, rules and procedures; • To periodically evaluate, monitor and inform the Board of Directors about the prioritized Risks identified by the Risk Owners' reviews in the Risk Management process, assisting in the evaluation of action plans and preparation of recommendations; • To evaluate, approve and monitor the execution of the treatment and monitoring of risks; • To evaluate, approve and recommend to the Management the correction or improvement of the Company's internal policies; • To assess the Company's quarterly information, interim statements and annual financial statements; • To present to the Board of Directors, for deliberation, the reports made by the Internal Audit; • To make recommendations, annually, to the Board of Directors, on the sufficiency of the structure and budget of the Internal Audit area.
Executive Board	• To promote the integration and culture of Risks, in the Company and in the strategic planning cycles; • To ensure the implementation of an efficient Risk Management model, in line with the Company's objectives and targets. To apply the general guidelines established by the Board of Directors to assign the level of Risk Appetite acceptable by the Company; • To monitor the Risks managed at the level of each process and ensure the effectiveness of the Control measures; • To participate in the Company's Risks validation and prioritization rituals with the Audit Committee; • To evaluate and monitor the Risks Treatment in line with the execution of the Company's strategic planning; • To assess, in a timely manner, the effectiveness and applicability of the guidelines of this Policy; • To evaluate and support the adaptations of the structure destined to the Risk management process, considering human, financial and technological resources; and • To monitor, evaluate and supervise the activities of the 1st and 2nd Lines of Defense.
Compliance Area	• To guide the analysis of third party risks, in order to mitigate possible risks of corruption, fraud, conflicts of interest and negative media, ensuring compliance with current anti-corruption laws and regulations, according to the priority risk matrix; • To monitor the risk analysis carried out based on the degree of risk classification; • To assist in the preparation and adaptation of rules, policies and procedures in order to reduce exposure to business risks; and • To disseminate the Compliance culture, through training and communications, ensuring compliance with existing laws and regulations and internal rules, seeking to mitigate the identified Risks.
Risk Management and Internal Controls Area	• To implement Risk Mapping and Controls; • To review of Controls with the business areas; • To conduct tests to assess the efficiency of Risk Management; • To support other areas in the implementation of the Action Plans and in the remediation of points identified in the Risk Management process; • To assist external auditors; • To assist in the development of rules, policies and procedure manuals; • To map and evaluate adherence to the Rules and Procedures and adapt the processes to the best market practices; • To do monitoring and follow-up control of the main aspects reported (Internal Audit, Internal Controls and Risk Management);

	• To support other areas in the improvement of Controls and processes.
Leaders in support and business areas (back office and front office)	• To identify, classify and manage the Risks of their respective areas according to the mitigation strategies, together with the Internal Controls area; • To appoint the professional who will respond as a Risk Management facilitator with the Internal Controls area; • To report the levels of exposure, the Action Plans and the indicators that describe the status of the Risks to which it is responsible; • To retain the technical knowledge of the processes in which the Risks are inserted; • To be responsible for updating information on the mapping and treatment of the Risks of his/her business unit; • To keep the information updated in a timely manner, respecting the planning calendar of the Risk Management cycle; • To monitor the status of the Action Plans with those responsible for implementing the Controls devices.
Internal Audit Area	• To assess the quality and effectiveness of the Company's Risk Management, control and governance processes; • To identify and point out opportunities for improvement in the Internal Control and Risk Management processes; • To periodically report to the Audit Committee, the body to which the Internal Audit area is functionally linked, and to its audited clients the results of independent, impartial and timely assessments of the effectiveness of Risk Management in the Company; • To prepare the planning and ensure the operationalization of Risk Management; • To develop and operationalize the Internal Audit plan, by Company's sector, according to the risks previously mapped and prioritized; • To evaluate the efficiency of the Internal Controls, with the measurement of the potential impact and probability of eventual failure of the Controls; • To evaluate and propose Control strategies; • To support other areas in the improvement of Controls and processes.
All employees	• To ensure the operationalization of Risk Management, being part of the identification, evaluation and measurement process, and implementing preventive and corrective actions; • To participate in training that allows the dissemination, in a conscious way, of the Risk Management culture.

The Company's Risk management structure will be conducted by the following areas/persons, in addition to having the effective participation of the members of the Audit Committee, the Executive Board and the Board of Directors:

- Compliance: this function is performed by the legal area, reporting to the legal manager and the Board of Directors;
- Internal Audit: the person in charge is the manager of the Corporate Quality area, reporting directly to the Audit Committee and the Board of Directors;
- Risk Management and Internal Controls: this role is performed by the Strategic Planning area, reporting to the person responsible for the Controllership area.

5. Company Guidelines and Lines of Defense

This Policy has as its general guideline the commitment to the Company's value proposal, which, in line with the other corporate policies and the Code of Ethics and Conduct, seeks to create an efficient and integrated Risk Management culture,

involving Management and all employees in the process of identifying, assessing and mitigating the identified risks.

Risk Management is part of the Company's corporate governance structure, integrates the decision-making process and contributes to the execution of its strategy. Risks are identified and treated in order to ensure compliance with the goals established for each strategic planning cycle.

Therefore, the Risk Management structure considers the joint performance of the corporate governance and management bodies, in accordance with the concept of the three lines of defense, according to the competencies described below:

- **1st Line of Defense (Leadership - *front and back offices*)**

→ Includes Operational Management, represented by the Executive Officers, managers and other employees of the business units allocated in day-to-day operations and tasks.

→ Employees working in the 1st Line of Defense have ownership over the Risks and are responsible for implementing corrective actions in order to resolve deficiencies in Control and processes, mitigating the Risks related to the activities they perform.

→ These employees play a crucial role in supporting the 2nd Line of Defense in the process of identifying risk mapping, as well as in the process of executing the Action Plans defined by the Risk Management and Internal Controls area or by the Internal Audit area.

→ Managers are responsible for managing the Risks inherent to the processes under their responsibility from the identification, assessment, monitoring and treatment of these Risks, with the participation of the other areas to be involved, according to the division of competences provided for in this Policy.

→ Report to the 2nd Line of Defense (Risk Management and Internal Controls area) about the Risks inherent in the activities carried out by the 1st Line of Defense that are not yet covered by Controls that mitigate their probability of occurrence and/or impact.

→ Implementation and monitoring of Action Plans to address deficiencies identified in the respective processes.

→ Report of the occurrence of materialization of Risks to the 2nd Line of Defense (Risk Management and Internal Controls area) immediately for treatment and preparation of Action Plans.

- **2nd Line of Defense (Risk Management, Internal Controls and Compliance areas)**

→ The 2nd Line of Defense has a preventive status in relation to Risks, with an emphasis on internal controls and compliance with laws and regulations applicable to the Company, as well as in relation to controllership aspects, with the monitoring of financial risks and financial reporting issues.

→ It must guide, monitor and evaluate the adherence to the defined standards and policies and support the 1st Line of Defense to achieve the objectives established by the Company.

→ It must advise the 1st Line of Defense on the aspects of internal controls, procedures, rules, and support management policies, define roles and responsibilities, identify changes in the Company's Risk Appetite, assist in the construction of processes, Controls and procedures.

→ Facilitation, communication and monitoring of Risk Management practices and assistance in the identification of Risks according to the Risk Appetite established by Management.

→ Assessment of the vulnerability of the Controls environment of the Company's processes through effectiveness tests.

→ Monitoring the implementation of the Action Plans for the identified failures.

- **3rd Line of Defense (Internal Audit area)**

→ It provides the Company's Management and governance bodies with structured assessments of the mapped Risks, based on the events and related consequences, independently and objectively within the Company.

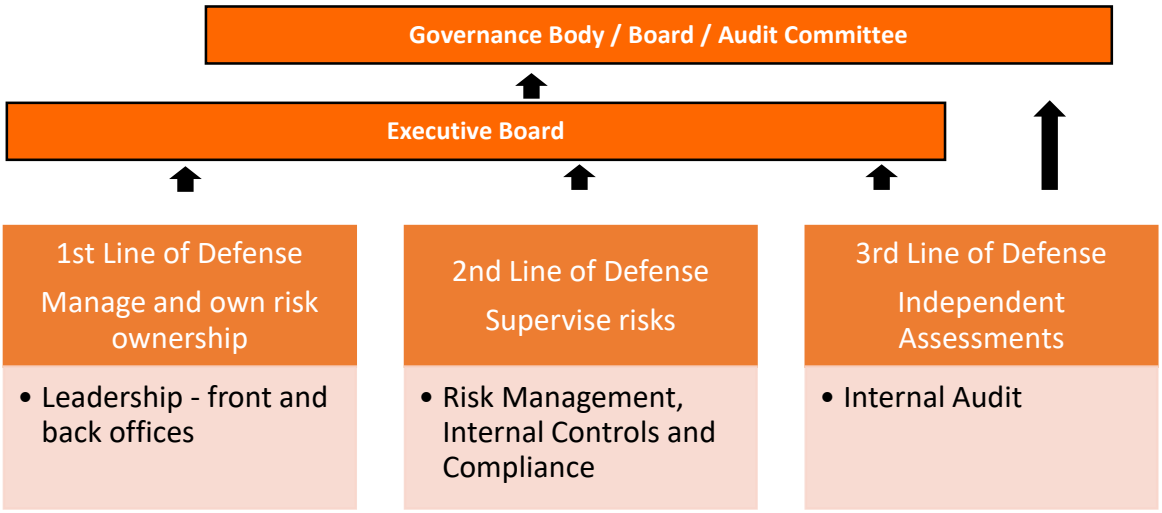
→ In a detective way, it provides assessments on the status of governance, structured internal controls and how this scenario impacts the Company's objectives, having in its scope the assessment of efficiency and effectiveness of the operation, safeguarding assets, reliability of information, integrity processes, adherence to laws, regulations, policies and procedures, and analysis of processes in the Company's business and support areas.

→ Elaboration of the Risk Management planning, together with the Risk Management and Internal Controls area.

→ Elaboration and operationalization of the internal audit plan, by Company area, according to the Risks previously mapped and prioritized.

→ Evaluation of the efficiency of the internal controls, with the measurement of the potential impact and probability of the eventual failure of the Controls.

Below, follows the model of three lines of defense adopted by the Company:



6. Risk Categorization

The Risks to which the Company is exposed are categorized in order to standardize internally and externally the references to the various Risks that may impact its activities. The categorization of Risks facilitates to organize the division process according to the respective natures, due also to the segments in which the Company operates that are affected by the Events in a different way.

Accordingly, the Company categorizes its Risks as follows:

RISK CATEGORY	DESCRIPTION OF THE RISK CATEGORY
STRATEGIC	Risks associated with decision-making by the Company's Management whose materialization may generate a substantial loss of economic value, capital or market share of the Company, as a consequence of flawed planning and/or decisions, usually related to business strategies/market share, investments, succession, innovation and competition. They are, therefore, Risks that can damage the core of the Company's business model. They challenge the logic of strategic choices, threaten competitiveness and impair the ability to achieve or maintain exceptional performance.
FINANCIALS	These are Risks that may adversely affect the Company's finances, associated with the exposure of financial operations. They arise from changes in the values of assets and liabilities in the market, non-compliance with financial obligations of counterparties, high cost or inability to meet financial obligations, inefficiency in the allocation of capital or failures in financial reporting.
OPERATIONAL	These are Risks resulting from the failure of processes and Controls, lack of consistency and adequacy of information systems, as well as arising from errors or

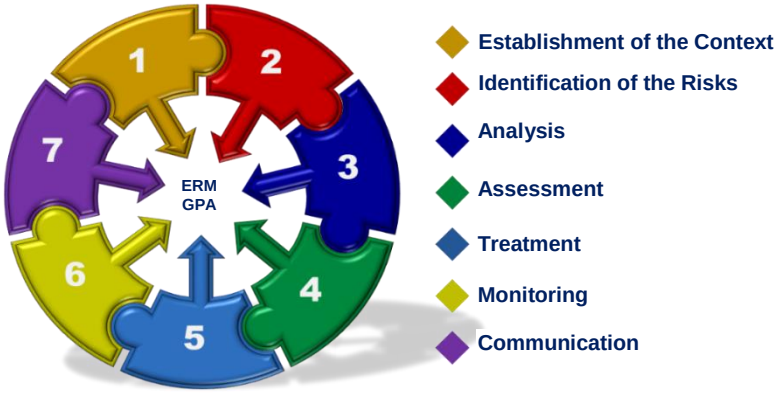
RISK CATEGORY	DESCRIPTION OF THE RISK CATEGORY
	fraud that hinder or prevent the exercise of the Company's activities. Operational risks generally entail a reduction, degradation or interruption, in whole or in part, of the Company's activities, with possible negative reputational impact, in addition to the potential generation of contractual, regulatory and environmental liabilities.
REGULATORY	Risks related to legal or regulatory sanctions, financial loss or reputation, which the Company may eventually suffer as a result of failure to comply with the application of laws, agreements and regulations of any nature, including labor, tax, contractual, environmental, regulatory and civil.
CYBERNETICS	Risks that can expose the Company's information assets to known or unknown threats through cyber attacks by *hackers*. These Risks can be represented by failures, unavailability or obsolescence of equipment and installations, as well as computerized control, communication, logistics and operational management systems, which impair or impede the continuity of the Company's regular activities, along its value chain (customers, suppliers, partners and regional units, among others).

Still, it is worth mentioning that in certain situations, Risks may fall into two or more categories concurrently.

7. Risk Management Process

The Company's Risk Management process was defined based on the guidelines of the COSO - Committee of Sponsoring Organizations of the Treadway Commission and the ISO 31000: 2018 - Risk Management Principles and Guidelines.

In this context, the Risk Management process is an integral part of the development of the Company's activities, incorporated into the organizational culture and practices and adapted to the business processes, consisting of the following subsequent and dependent steps:



Step 1: Establishing the context

Initial phase of the ongoing Risk Management process, which articulates the Company's strategic objectives with the external and internal parameters that will be taken into account, establishing the scope and the Risk criteria for the rest of the process.

It seeks to understand the business scenario and context considering factors linked to the short and long term strategic planning of the Company and its business units, in line with the environment in which these objectives are inserted.

It is a fundamental step to ensure that the Risk Management process is aligned with the Company's management and strategic planning cycles, to align its acceptable levels of Risk Appetite.

In order to establish the scenarios that should support this step, the influencing factors of both the External Context and the Internal Context are considered.

External Context

The External Context is the external environment in which the Company seeks to achieve its objectives. It includes, but is not limited to: (a) cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; (b) key factors and trends that have an impact on the organization's objectives; and (c) relationships with external stakeholders and their perceptions and values.

Generally, the Company is unable to intervene directly on the External Context, having a predominantly reactive action. However, following the guidelines of this Policy, the Company must seek to mitigate any impacts of Events materialized in the External Context.

Internal Context

It consists of the Company's internal environment, based on the Company's organizational culture, processes, structure and strategies, at the following levels, but not limited to: (a) culture; (b) rules, guidelines and models adopted by the Company; (c) governance, organizational structure, roles and responsibilities; (d) policies, objectives and strategies implemented to achieve them; (e) capabilities, understood in terms of resources and knowledge (for example, resources, time, people, processes, systems and technologies); (f) information systems, information flows and decision-making processes (formal and informal); (g) relations with internal stakeholders, and their perceptions and values; and (h) contractual relationships.

The attention to the Internal and External Contexts can help to ensure that Risk Management is appropriate to the circumstances, the Company and the Risks that truly impact considering the real scope of its strategic objectives.

Step 2: Risks Identification

The Risk identification approach is top-down, based on interviews with the main executives of the business units, in view of the main processes for which they are liable.

The product generated in this step is a comprehensive list of Risks based on events that may identify vulnerabilities and threats that put the achievement of the Company's strategic objectives at risk.

In this step, the owner and the person responsible for each of the identified Risks (Owner of the Risk) must also be defined, as well as a description that will guide the next steps of the mapping.

Still at this step, all the Risks associated with the Company's activities are mapped, whether these are under its Control or not.

Step 3: Risk Analysis

After the completion of Step 2 of identification of Risks, these are analyzed in detail, with the objective of obtaining greater clarity and qualitative and quantitative support that generate variables that will assist in the classification of Risks so that the Company can act more assertive in its Action Plans and in prioritizing these identified Risks.

In this step, the causes or Risk factors are defined, among others, as well as their possible effects in the event of a specific Event materializing. In addition, the Company classifies the aggravating factors for each of the identified Risks to ensure the assertiveness of its Controls.

In this way, information is collected in order to obtain data that can describe the probability and impacts of the identified Risks, thus generating a qualitative matrix to describe in an executive manner the universe of Risks based on their classifications. Within the qualitative matrix, Risks are classified according to the following criteria:

IMPACT	QUALITATIVE ASPECTS	VULNERABILITY	QUALITATIVE ASPECTS
EXTREME	- Financial losses that can compromise the profitability of the business (above 20% of revenue);	**EXTREME**	The organization's lines of defense are insufficient to minimize risk, due to the

IMPACT	QUALITATIVE ASPECTS	VULNERABILITY	QUALITATIVE ASPECTS
	- Loss of key customers or *market share*; - Payment of high fines or severe penalties with an impact on the image and reputation of the company; - Loss of large investments or much lower return than expected		absence of key controls or recurrence of problems
HIGH	- Significant financial losses (between 11% and 20% of revenue); - Loss of customers or a large number of transactions; - Payment of high fines or severe penalties; - Loss of great business opportunities or investments with an indefinite return period	**HIGH**	The organization's lines of defense are insufficient to minimize risk, due to the absence of key controls or recurrence of problems.
AVERAGE	- Considerable financial losses (between 5% and 10% of revenue); - Customer dissatisfaction, which may result in loss of transactions; - Payments of fines or other penalties; - Loss of business opportunity; - Non-compliance with internal procedures, laws and regulations	**AVERAGE**	Existing controls do not operate in a standardized manner or are inefficient and may not minimize the risk
LOW	- Immaterial financial losses (below 5%); - Customer dissatisfaction; - Payments of fines or other minor penalties.	**LOW**	Existing controls minimize risks

Thus, the Risk analysis involves developing an understanding of the Risks mapped in Step 2. Based on this understanding, Step 4 of Risk Assessment is reached and decisions are made about which treatments to be adopted, as well as which strategies and methods are most appropriate for their management.

Step 4: Risk Assessment

The Risks mapped and analyzed are evaluated according to their potential materialization impacts in order to achieve the Company's objectives.

In this sense, the Company's Management, Risk Owners and process leaders jointly assess the Events from the perspective of Probability, frequency and impacts. In the Risk assessment process, variables are sought to combine qualitative and quantitative methods. Thus, variables are considered, among others, for the classification of impacts that help in the better classification of Risks, using the extreme, high, medium and low gradient for each variable.

Finally, combining all the evaluation variables, the criticality of the identified Risks is defined, which allows the construction of a prioritization map, starting from the Risks with the highest exposure to those with the least exposure.

This map helps the Company and its business units to obtain a greater degree of alignment of strategic planning with the acceptable level of Risk Appetite of the Company.

In this sense, Step 4 is crucial in assisting the Company's Management in making decisions regarding the risks that should or should not be prioritized.

In addition, a general assessment of the Company's Risks is carried out annually, led by the Board of Directors, with the participation of the Executive Board and the members of the Audit Committee, through meetings and interviews, whose objective is to carry out the diagnosis of the Company's structure, identify the Risks, define the prioritization in the treatment of the identified Risks, prepare a new Risk map, define the Risk management strategy and, consequently, the human and financial resources necessary to operationalize the Company's Risk Management structure.

However, despite the periodicity of the general assessment described above, the Risk map is subject to adjustments at any time (exclusion, modification and addition of Risks and priorities), if changes are observed in the reality of the Company that justify such adaptability.

Step 5: Risk Treatment

The Risk Treatment phase involves identifying the existing Control devices within the process for analyzing the effectiveness of these Controls as preventive measures and as factors that reduce the degree of exposure (Mitigating Factor), in order to arrive at Residual Risk.

For processes that require a greater degree of effectiveness of the Controls or that do not have effective mitigation factors, the Risk will be treated by the Risk Management and Internal Controls area together with the area responsible for the 1st Line of Defense of this Risk, through the implementation of one or more Action Plans that aim to mitigate the exposure to the Risk and/or the impacts in the event of materialization of an Event associated with it.

For each Action Plan, those responsible and the implementation schedules are assigned to ensure the effectiveness and efficiency of the Plans and thus reduce the level of Residual Risk.

In this process, the Risk Treatment actions that can be taken by the Company are:

→ Avoid: do not take risks, determining the discontinuation of the activities that generate them, whether due to the production of a specific good, the maintenance of a line of business or company processes. This alternative should be applied when there is no viable or sufficient alternative to reduce the impact or the Probability of the occurrence of a Risk that may have relevant and/or irreversible consequences, justifying its discontinuation.

→ Accept: do not take any action to reduce the Probability or the impact of the Risk. This alternative should be applied when the cost of management/mitigation does not compensate, if compared to the assumed impact, within the acceptable level of Risk Appetite defined by the Company. In this case, the Risk must be monitored continuously, in order to guarantee a new appropriate treatment if there is a change in the situation that may increase the impact and/or probability of the Risk - generating a change in its criticality.

→ Eliminate: adopt actions that alter or eliminate a process or a project, protecting the business objectives from the impacts of a given Risk.

→ Reduce or mitigate: determine measures to reduce the likelihood of the Risk materializing and/or its impact in the event of materialization. This alternative should be applied when the reduction in Probability or impact is sufficient to make the risk assumable, according to the Company's Risk Appetite.

→ Share and/or Transfer: take actions that reduce the Probability and/or the impact of the Risk by the total transfer or by sharing a part of the Risk with third parties, whether through insurance, hedge, associations, outsourcing of activities and others.

When opting for a specific action in the Risk treatment process, the responsible executives and managers must analyze the cost benefit of the action, considering the costs involved, efforts and implementation, as well as studying the benefits resulting

from the action in the financial, legal and reputational scope, among others. The treatment plan must identify the order of priority in which each treatment should be implemented.

After determining together with the liable and/or affected areas the treatment strategies to be adopted, the Action Plan will be documented and communicated to the areas involved, to ensure the timely implementation of the determined measures.

The Risk Management and Internal Controls area will support the areas in the preparation of Action Plans to correct the control failures identified in the root cause and mitigate the identified Risks.

Step 6: Monitoring

The Company's monitoring processes are intended to ensure that Risk Controls are effective and efficient in their implementation, with the achievement of the intended results and strategies designed by Management and the Lines of Defense.

Through the monitoring process, it is possible to obtain information that can better guide the phases of Risk assessment, analysis of Events, changes, trends, successes and failures, detection of changes in the Internal and External Contexts, and identification of emerging Risks. The results of the monitoring must be recorded and reported to those responsible for Risk Management and Internal Controls in the Company.

In this scenario, the monitoring of Risks is constituted in a dynamic and continuous cycle, being fundamental to guarantee in a timely, preventive and reactive manner actions that help to minimize impacts in case of materialization of Risks.

Monitoring must be carried out by the 1st Line of Defense, seeking to continuously evaluate the effectiveness of its controls and the improvement in the management of its Risks. The Risk Management and Internal Controls area (2nd Line of Defense) will support the business areas in the monitoring of risks, with the objective of contributing to the achievement of the objectives and goals of the Company.

Thus, the employees involved in each area must have the capacity and competence to identify, assess, prioritize, monitor and manage the Risks of their responsibility, considering all changes within the internal and external environment of the Company, so that they can obtain a higher degree of control of their processes and, consequently, so that they can achieve the objectives established during the Risk Management.

The monitoring process is also linked to the implementation of the Action Plans, which will be prepared and put into practice by the business units in accordance with the responsibilities and periodicity defined by the owners of the Risks and by the areas of Internal Audit and Risk Management and Controls Company's internal staff.

Step 7: Communication

Risks must be communicated in a clear and objective manner, with all relevant information possible, to all affected and/or responsible parties, and, mainly, to the parties responsible for determining and implementing measures for their treatment.

Likewise, once the measures to be adopted to deal with the Risks have been determined, they must be communicated in a precise and rapid manner to the areas responsible for implementing the determined measures.

8. Duration and Review

This Policy is effective as of its approval by the Company's Board of Directors, which took place on February 23, 2021, and should be revised whenever necessary.

9. References

- ABNT NBR ISO 31.000 / 2009: Gestão de Riscos – Princípios e diretrizes.
- As três linhas de defesa no gerenciamento eficaz de riscos e controles, IAA (*The Institute of Internal Auditors*) 2013.
- Código de Ética e Conduta da Companhia.
- COSO – ERM: *Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework*.
- Guia de Orientação para Gerenciamento de Riscos Corporativos IBGC (Instituto Brasileiro de Governança Corporativa) 2007.