

1. OBJECTIVE

This Policy was prepared by M. Dias Branco Indústria e Comércio de Alimentos SA (“M. Dias Branco” or “Company”) for employees and third parties who work in critical processes or who are involved in committees with the aim of ensuring the business continuity of the company, providing guidance and support to M. Dias Branco in accordance with business requirements and relevant laws and regulations, in order to:

- Protect employees, customers, vital information and financial assets of M. Dias Branco;
- Define guidelines for identifying, preventing, monitoring and treating business continuity risks;
- Improve the organization's ability to recover from disruption or interruption of its ability to supply its products;
- Define the methodology and governance of the Business Continuity Management System during planning, preparation and response to situations impacting your business;
- Define those responsible and functions for Business Continuity Management and others involved in the defined committees;
- Enable the continuity and recovery of operations within defined objectives, considering the highest priorities for recovery and associated business impacts.

2. APPLICATION

Applicable to M. Dias Branco units.

3. RESPONSIBLE MANAGERS

Vice Presidency of Legal, Governance, Risks and Compliance
Risk Management
Statutory Board
Non-Statutory Board
ESG Committee
Audit Committee
Administrative Council

4. DESCRIPTION

4.1. Introduction

The Business Continuity Management Policy (GCN) (“Policy”) is a central component of corporate governance and an integral part of the organization's Risk Management Structure, being in line with the Risk Management Policy of M. Dias Branco SA Food Industry and Commerce.

This policy defines the guidelines and principles for structuring, implementing, and maintaining a Business Continuity Management System (SGCN) in accordance with best market practices and adhering to ISO 22.301 standards.

4.2. Business Continuity Management Governance Framework

The Business Continuity Management Governance structure is divided into three parts: Guidelines, Standards and Procedures, as shown in Figure 1.

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ

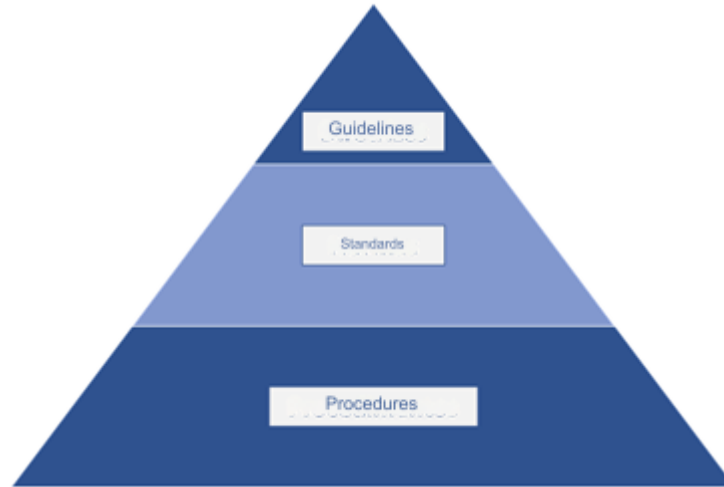


Figure 1 - Business Continuity Management Governance Framework

Guidelines: These are documents of a strategic nature that correspond to strategic determinations and guidelines, with regard to Business Continuity Management.

These documents are called Policies and provide guidance for the creation of work standards and procedures, in accordance with the company's main requirements and best market practices.

This Business Continuity Management Policy document fits into this item of the structure;

Standards: These are tactical documents aimed at regulating the management plan, clarifying responsibilities, as well as providing specific guidance on how the corporation will be structured. The components of this structure item are the Business Continuity Plan and the Crisis Management Plan;

Procedures: These are operational documents, with instructions for Business Continuity on specific processes and resources, guiding the execution of tasks. The Operational Continuity Plans (PCOs) and the Disaster Recovery Plan (PRD) are part of this structural classification of GCN governance.

4.3. Business Continuity Management System

The Business Continuity Management System (SGCN) is made up of interrelated elements to establish policies, objectives, procedures, responsibilities and organizational structure for the assessment, planning, preparation, response and recovery in situations of interruption to your business, impacts to the life, heritage or brand of M. Dias Branco.

This system provides a structure so that organizational resilience can be developed and the Company can respond effectively, safeguarding the interests of interested parties, its reputation and its activities. M. Dias Branco's SGCN covers the main phases: Business Mapping and Assessment, Planning and Preparation, Response and Recovery, Involvement and Maintenance and Monitoring.

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ



Figure 2 - Phases of the Business Continuity Management System

Business Mapping and Assessment

The business mapping and assessment phase is essential for identifying the Company's situation, through understanding processes, collecting information, and analyzing data. Given this information, it is possible to identify risks, vulnerabilities, dependencies, and possible contingency alternatives for the business and allow the development of the following steps.

Business Impact Analysis (AIN/BIA): *Business Impact Analysis (BIA)* aims to identify the criticality of business processes and consequently the order in which their recovery is prioritized, as well as the impact caused by situations of unavailability on them. The analysis is carried out by mapping processes and dependencies with those responsible within the Company to identify the following periods in each process and system:

- ✓ MTPD (*Maximum Tolerable Period of Time*): Maximum acceptable period of unavailability after interruption;
- ✓ RTO (*Recovery Time Objective*): recovery time objectives (RTO) with deadlines for returning to activities and acceptable capacity. Time after an incident when products, services and activities must be resumed or resources recovered.
- ✓ RPO (*Recovery Point Objective*): recovery point objectives (RPO) with acceptable losses or point of activity resumption. It is the point at which the information used by an activity must be restored to allow the activity to operate upon resumption.

To evaluate the impacts of the interruption of these activities, the evaluation context was established, impact criteria were defined (Financial, Legal/Regulatory, Image, Operational and Customers) and related in relation to their unavailability time, being classified in the following order of relevance for the Company: Vital (Extreme), Critical (High), Important (Moderate) and Necessary (Low).

Business Continuity Risk Analysis : Business Continuity Risk Analysis allows you to assess the exposure of M. Dias Branco and its processes to threats, contributing to preventive and preparatory action for more critical

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ

risks. Risk Assessment must follow the same procedures and assessments defined by the Company's Risk Management Policy.

Assessments and responses to all Risks must be carried out by the Vice-Presidency of Legal, Governance, Risks and *Compliance*, to whom Risk Management reports, with the monitoring of the Audit Committee and/or ESG Committee, according to hierarchical levels defined in the Risk Management Policy. Any acceptance of risks must also respect the same governance.

4.3. 2. Planning and Preparation

After the Business Mapping and Assessment phase, it is necessary to define a strategy, actions and person responsible for each stage to mitigate impacts that allow an effective response to critical events, enabling a rapid resumption of operations.

4.3.2.1. Business Continuity Plan (PCN)

The Business Continuity Plan (PCN) consists of a set of pre-defined measures depending on time and which must be carried out if unacceptable interruptions occur in business activities, with or without the participation of third parties or partners. Its objective is to maintain critical processes and activities in their minimum operation and minimize impacts generated on the business. The evaluation of strategies and definition of prioritized actions must be evaluated by the Risk Management together with the areas responsible for their execution and the ESG Committee and/or Audit Committee, according to the responsibilities defined in this policy.

This plan establishes the Business Continuity Committee (CCN) with its members and responsibilities.

4.3.2.2. Crisis Management Plan (PGC)

The Crisis Management Plan consists of a set of pre-defined actions to respond to severe incidents that may affect M. Dias Branco, directly or indirectly related to the interruption of its operations, such as impacts on the brand and reputation. Its objective is to respond to its stakeholders, appropriately establishing effective communication and carrying out actions to reduce impacts on the business.

This plan establishes the Image Management Committee with its members and responsibilities, aligned with the definitions of the ESG Committee.

4.3.2.3. Disaster Recovery Plan (PRD)

The Disaster Recovery Plan is responsible for reestablishing critical systems and technology components that were affected by an incident, in addition to meeting the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) times defined in the impact analysis. Its objective is to recover the affected systems, directing the steps to be carried out by the Disaster Recovery Team (ERD). This plan establishes the ERD with its members and responsibilities.

4.3.3. Response and Recovery

The Response and Recovery phases are only initiated in the event of an incident that causes a prolonged interruption or a crisis situation. Those responsible for each activity are defined in the Planning and Preparation stage. In this case, the activities defined in each subphase must be carried out:

4.3.3.1. Response

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ

During the resumption period, the plans and actions developed in the Planning and Preparation phase must be used by those responsible, with support from Risk Management, or by defined focal points. Throughout this period, all activities must be formalized through plans and minutes, ensuring knowledge management and the possibility of evaluation after the deactivation of your plans.

4.3.3.2. Recovery

During the Response subphase, recovery activities can be evaluated. The committees involved must evaluate priorities and define processes and plans for returning activities. This process must be gradual according to the scenarios and indicators of each return stage.

4.3.3.3. Post-Incident

At the end of the Response and Recovery subphases, the deactivation of plans and committees must be assessed in addition to carrying out the following activities:

- ✓ Backlog analysis : critical analysis of all demands that were not met during the interruption and that need to be normalized after recovery;
- ✓ Lessons Learned : document that brings together the main information about the event, actions taken and perception of the reaction of everyone involved. It must be prepared within 30 days after the end of the crisis;
- ✓ Assessment of improvements to the SGCN: based on the Lessons Learned and experiences evaluated throughout the response phase, a review of the documents related to this Policy mentioned in the Planning and Preparation phase must be prepared.

4.3.4. Involvement

Interaction between the areas involved is important so that the committees and members defined in the "Preparation and Planning" phase are able to apply this Policy and its aforementioned Plans. This ensures preparation and greater agility in decision-making in the event of an incident, as well as the return to normal operations.

4.3.4.1. Trainings

The Company, through the Organizational Development area, must maintain a periodic and constant communication and training plan for all Employees (observing the degree of participation of each one in business continuity activities and defined committees). Risk Management, with the assistance of the Organizational Development area, must establish a specific plan for updating and improving the technical and behavioral skills necessary for the adequate development of its responsibilities. Evidence of training execution must be stored for at least 5 years or in accordance with current regulations.

4.3.4.2. Tests and Simulations

Testing and simulation exercises are necessary to evaluate the applicability of the strategies and initiatives defined in the plans of this SGCN. They must be carried out internally with their own employees, and may involve third parties who carry out critical activities.

Risk Management must define a periodic testing plan considering all the elements defined in this Policy, with the participation of the members defined for the committees, and which must be carried out at least once a

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ

year. Evidence of test execution must be stored for at least 5 years or in accordance with current regulations.

4.3.5. SGCN Maintenance and Monitoring

4.3.5.1. Maintenance

The SGCN, as well as its elements, must be reviewed periodically, based on improvements detected through testing and simulation exercises and/or whenever changes occur in any sphere related to its application, not limited to, but including:

Immediately, for regulatory reasons;
Relevant organizational changes;
Up to 30 days after the closure of the interruption or crisis incident;
Changes to critical systems or suppliers; or,
Every 24 months - if none of the above events occur.

4.3.5.2. Monitoring

Risk Management must periodically present to the Audit Committee and the ESG Committee the indicators and parameters for monitoring the activities carried out to maintain and adapt this Policy, considering:

- ✓ Element update indicators as defined in this policy;
- ✓ Employees and/or third parties trained in the established plans;
- ✓ Awareness-raising actions during the period of validity of this Policy;
- ✓ Carrying out tests and simulations and their execution evidence.

M. Dias Branco must periodically organize or conduct internal audits, by areas not related to the management of this document or by independent companies, to assess compliance related to the application of the requirements defined in this Policy by the organization or to adapt to current regulations. The results of this assessment must be reported to the Audit Committee, the ESG Committee and, when applicable, the Board of Directors.

4.4. Governance and Responsibilities

The SGCN has teams and employees from all spheres of M. Dias Branco to ensure its continued success in accordance with specific objectives and activities.

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ

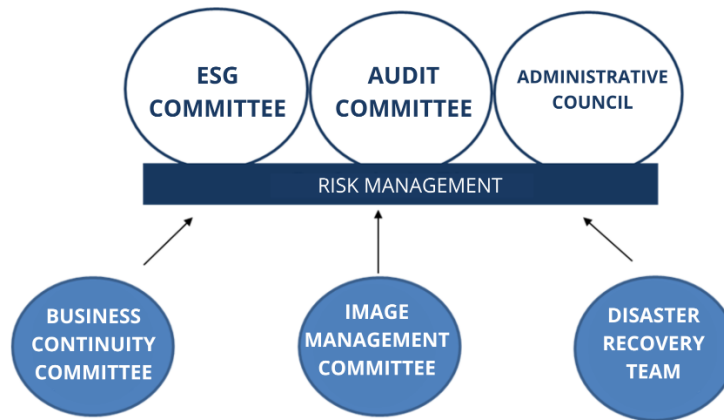


Figure 3 - Governance Structure of the Continuity Management System

4.4.1. Administrative Council

- ✓ Establish the culture of Business Continuity Management in the Company's activities, setting the tone through example, active participation, sponsorship and encouragement.
- ✓ Define the Company's strategic objectives that will guide the work of identifying risks and impacts to the business. Monitor continuity risks, dependencies and business priorities for strategic initiatives and projects.
- ✓ Monitor the work of the Audit Committee and the ESG Committee in reviewing methodologies, approaches, tools, evaluation, classification, and reporting applied to Business Continuity Management.
- ✓ Monitor business continuity management activities according to the Company's business direction.
- ✓ With the support of the Audit Committee and the ESG Committee, identify, evaluate, monitor and manage the risks, impacts and dependencies to which the Company is exposed.
- ✓ Approve any changes and revisions to this Policy.
- ✓ Regulate the cases omitted from this Policy.
- ✓ Process non-compliance with the obligations and rules established in this Policy and resolve on it, as applicable.
- ✓ Define, Support and Disseminate the Business Continuity Management culture in the Company.

4.4.2. Audit Committee

- ✓ Analyze and review annually and monitor the risk matrix, which encompasses the Company's business continuity, in accordance with their respective duties.
- ✓ Review structure, processes, methodologies, approach, tools, evaluation, classification and reporting of business continuity management, according to their respective duties.
- ✓ Send to the Board of Directors an annual activity report containing the main risks, dependencies and strategies defined for business continuity, as well as the training and tests carried out, in accordance with their respective responsibilities.
- ✓ Approve and monitor the activities of the Risk Management, including the annual work plan, according to business continuity themes.
- ✓ Review this Policy and propose any changes.

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ

4.4.3. ESG Committee

- ✓ Ensure and disseminate the Company's commitment to management based on the pillars of corporate governance, environmental preservation, sustainability and business ethics, including, but not limited to, corporate risk management and business continuity.
- ✓ Promote, monitor and ensure the adoption of best corporate governance, environmental preservation and sustainability practices, as well as coordinate the process of implementing and maintaining such practices in the Company, including business continuity processes, proposing changes, updates and improvements when necessary .
- ✓ Analyze and issue recommendations when preparing and updating reports that demonstrate the Company's performance in ESG matters, which include business continuity, to interested parties (stakeholders)
- ✓ Submit to the Board of Directors its recommendations on issues within its competence and report its activities periodically to the Board of Directors, which must guide the Committee regarding the level of risk tolerance in the processes and activities carried out at different levels of the Company, including continuity issues of business.
- ✓ Monitor the execution of its recommendations, meeting periodically with the Company's Board of Directors and managers, according to business continuity topics.
- ✓ Review this Policy and propose any changes.

4.4.4. Risk Management

- ✓ Establish the Company's business continuity management structure, as well as coordinate, assist and monitor its implementation.
- ✓ Establish the Business Continuity Management Process, as well as coordinate, assist and monitor its implementation.
- ✓ Develop Business Continuity Management methodologies that can be applied efficiently by the Company and that adhere to internal policies and procedures and applicable laws and regulations.
- ✓ Develop business continuity management strategies together with business areas
- ✓ Support the Audit Committee in the continuous assessment of the Business Continuity Management structure and process.
- ✓ Support Employees in the Business Continuity Management of their respective activities.
- ✓ Support the communication plan and periodic training, in accordance with this Policy.
- ✓ Support the promotion of the Business Continuity Management culture in the Company.
- ✓ Conduct the process of assessing continuity risks and analyzing the business impact of the Company's areas, observing the methodology, strategy and schedule approved by the Audit Committee.
- ✓ Validate the results of Business Continuity Management analyzes with Employees from the areas involved and assist in defining business continuity strategies (business continuity plans, reduction of dependencies, alternative processes, testing, etc.).

4.4.5. Collaborators

- ✓ Pay attention to continuity risks, evaluate internal dependencies, propose and implement workaround measures and ensure and monitor the implementation of Business Continuity Management processes related to their respective areas of activity.
- ✓ Provide and facilitate access to Risk Management to all information relevant to Business Continuity Management, ensuring its integrity and correctness.
- ✓ Ensure and monitor the implementation of action plans defined to address risks and business continuity.
- ✓ Support, encourage and participate in Business Continuity Management communication, dissemination and training and testing initiatives.

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ

- ✓ Report to Risk Management any and all relevant continuity risks identified, whether materialized or not, in order to maintain the appropriate Risk Management process.
- ✓ Participate in and execute business continuity activities as directed by defined committees during periods of interruption or crisis.

4.4.6. People, Management and Sustainability Department

- ✓ Develop and implement the periodic communication plan.
- ✓ Develop and implement the periodic training plan.
- ✓ Keep documented all training and initiatives that corroborate the application of this Policy by the Company.

4.4.7. Business Continuity Committee

- ✓ The Business Continuity Committee is responsible for leading response and decision-making measures related to the Business Continuity Plan (BCP) and Operational Continuity Plans (PCOs) during a period of disruption, as well as operational feasibility analysis and financial. Its duties and members will be defined in the Committee's Internal Regulations, to be approved by the Statutory Board.

4.4.8. Image Management Committee

- ✓ The Image Management Committee is responsible for leading response measures and decision-making during a crisis. Its responsibilities and members are detailed in the Committee's Internal Regulations.

4.4.9. Disaster Recovery Team

- ✓ The Emergency Response Team is responsible for leading and executing response and recovery activities for systems and equipment in cases of unavailability of critical systems and equipment. Its responsibilities and members are defined in the Disaster Recovery Plan (PRD).

5. GLOSSARY

- Business Impact Analysis (BIA) - Business Impact Analysis aims to identify the criticality of the Company's processes and the order of prioritization of their recovery, as well as the impacts caused by their unavailability.
- Crisis - a high-impact and/or visible incident that can drastically affect an organization's profitability, reputation, ability to operate and even survival.
- Committee(s) - Group of people with decision-making power who will be appointed to manage an outage, business continuity, disaster recovery or crisis management.
- Risk Management - process applied to defining and executing strategy, designed to identify potential events that could affect the Company.

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ

- Business Continuity Management - management process that identifies potential threats to an organization and the possible impacts on the continuity of operations and business if these threats materialize.
- MTPD (Maximum Tolerable Period of Disruption) - Maximum acceptable period of unavailability after interruption;
- Business Continuity Plan - documented procedures that guide organizations to respond, recover, resume and restore to a pre-defined level of operation following disruption;
- Process - group of related or interactive activities that transform inputs into outputs;
- Resources - all assets, people, skills, information, technology, locations, supplies and information that the Company must have available for use in order to operate and achieve its objectives.
- RTO (Recovery Time Objective) - recovery time objectives (RTO) with deadlines for returning to activities and acceptable capacity. Time after an incident when products, services and activities must be resumed or resources recovered.
- RPO (Recovery Point Objective) - recovery point objectives (RPO) with acceptable losses, or point of activity resumption. It is the point at which the information used by an activity must be restored to allow the activity to operate upon resumption.
- Business Continuity Management System (SGCN) - continuous management and governance process supported by Senior Management that appropriately receives resources to implement and maintain business continuity management.
- Disaster Recovery Institute International (DRI-I) - International Institute for Disaster Recovery
- Business Continuity Institute (BCI) - Good Practices Guidelines - Business Continuity Institute - Best Practices Guidelines
- Stakeholder - people or organization who can affect or be affected by a decision or activity.

6. CHANGE HISTORY

Revision	Latest Changes
0	MIGRATION TO THE GED - PHASE 1 - DOCUMENT WITHOUT CHANGE

PREPARED BY:

Gabriela Pessoa Fernandes

APPROVED BY:

DANIEL MOTA GUTIERREZ