Business Continuity Policy

Table of Contents

Business Continuity Policy

1. Purpose

The purpose of the Business Continuity Policy is to set out the general principles and guidelines that enable Grupo Dia to implement a response process for disruptive incidents in order to minimise their impact and limit their propagation, as well as recovering the affected services to adequate operational levels.

The guidelines must be described in a set of Standards and Procedures which will supplement this policy.

Moreover, the Policy aims to make Management's commitment to business continuity clear, in permanent compliance with applicable legislation.

2. Scope

The Business Continuity Policy applies to all companies belonging to Grupo Dia and has the following scope:
- Corporate information of any nature and in any format.
- Personal information of employees and third parties (suppliers and customers).
- IT assets.
- Employees.
- Third parties (suppliers and subcontractors).
- Premises (e.g. offices, warehouses, stores, data centres, etc.).
- Processes and activities that support the business.

2.1. Distribution and Control

The Business Continuity Policy must be disseminated, distributed and provided to all employees and/or external collaborators in an official Grupo Dia repository.

2.2. Policy Maintenance

A review must be carried out on an annual basis or when there are relevant changes in the Group and/or the environment (e.g. operational, legal, technological, regulatory, etc.).

3. General Principles

Governance and capacity: At Grupo Dia we rely on the Business Continuity Management System (hereinafter BCMS), which is composed of the set of people, processes and resources (e.g. technology, documents, etc.) assigned to achieve the objective of continuity of services and operations in case of disruptive events.

The Management of Grupo Dia must:

- Designate a Business Continuity Manager for leading and overseeing the proper implementation, operation, and maintenance of the BCMS.
- Provide the Business Continuity Manager and/or the BCMS with the necessary resources to ensure the correct implementation and maintenance of the system.
- Carry out regular supervision in order to ensure compliance with the objectives of the BCMS.

Responsibilities: The Business Continuity Manager (relying on the BCMS) must establish rules and procedures that define the responsibilities of the different stakeholders involved in the process (prior to, during, and after the disruptive event) in order to ensure compliance with response and recovery objectives.

Additionally, the Business Continuity Manager must maintain and update this Policy.

Integrity and Security – The BCMS must:

- ensure the protection and security of its employees, external staff, suppliers and any person present or providing a service on its premises, both in normal circumstances and in crisis situations resulting from an emergency or disaster.
- protect Grupo Dia's processes, particularly because of the importance of the Group's work with the public.

Guarantee and proportionality: the BCMS must consider the mechanisms needed to prevent and/or mitigate relevant business continuity risks in accordance with tolerance, risk appetite and the current regulatory framework, as well as maintaining and updating them to guarantee continuous improvement.

Minimal impact: the BCMS must attempt to minimise any impact on critical services and their level of service provision (e.g. operational capacity, performance, etc.) that could result from a disruptive event.

Collaboration and coordination: the BCMS must be developed and implemented effectively, taking into account all critical areas, resources, suppliers and services within its scope, and ensuring that everyone commits to achieving BCMS objectives. Moreover, all Grupo Dia employees (internal and/or external) must always be willing to collaborate with the authorities in the event of a disaster or when needed.

Communication: the BCMS must identify and implement tools for collaboration and communication between the different functions and offices involved and ensure the commitment of each and every one of them.

4. General Guidelines

The Dia Group BCMS should consider at least the following general guidelines:

Identification of critical processes and assets
All critical processes and any critical assets that support them (physical, digital and/or human resources) must be identified, including the information necessary for their inventory, classification, management, etc.

Identification of business needs
The minimum recovery needs (in time and form) of a process and/or asset should be identified in the event of a disruptive event.

Assessment of disruptive events
Possible disruptive events associated with Grupo Dia's critical processes and assets must be analysed, identifying those that entail major disruption for the Group, so as to prioritise the associated actions and resources.

Disruptive event management strategy
A disruptive event management strategy must be produced to ensure correct incident prevention measures are in place before and after the incident.

a) Disruptive event prevention
Protection mechanisms must be implemented to prevent and/or reduce the likelihood of disruptive events occurring, as well as to speed up and facilitate any response and recovery work for the Group's critical processes and assets.

b) Business continuity plans (response and recovery)
For critical processes and assets, response plans must be produced for any potential disruptive events, establishing the responsibilities, operations and resources needed to respond to the event in a coordinated and effective manner, minimising the impact of the event and limiting its spread.

Furthermore, disaster recovery plans must be produced to restore critical processes and assets to the minimum levels accepted by business.

BCMS Training and testing
All users involved in the BCMS must be trained on an ongoing basis to ensure their full and effective participation.

Regular testing plans must be produced for business continuity and response and recovery procedures to validate their effective implementation, knowledge and operation.

Continuous improvement
As a result of training and testing, as well as managing disruptive events, points of improvement must be identified for the BCMS, with the aim of producing action plans that ensure weaknesses are corrected.

Continuous maintenance and update

The BCMS, and all of its supporting documentation, must be updated, reviewed and approved on a regular basis, ensuring it is constantly updated and aligned with the business, and adjusted to new trends, risks and regulatory changes in processes, technologies, organisational structure, etc.

5. Exceptions and Breaches

Any exceptions to the guidelines of the Policy and the associated Standards must be approved by the Business Continuity team and/or Group Management (depending on their criticality/risk).

Any breach of the Policy and/or associated Standards may be punishable in accordance with the agreements, disciplinary regime and applicable legislation in force.

This Policy has been approved on 12 December 2024 by the Board of Directors of Distribuidora Internacional de Alimentación S.A. and is applicable until the Board of Directors approves its update, review or repeal.