



**BUSINESS CONTINUITY POLICY**

## BUSINESS CONTINUITY POLICY

### 1 Introduction

The Board of Directors of MAPFRE, SA (the “ **Company** ”) is the competent body to define the general strategy and establish the basis for adequate and efficient coordination between the Company and the other companies integrated into the group of companies of which MAPFRE, SA is the dominant entity in the sense established in article 42 of the Commercial Code (the “ **Group** ” or the “ **MAPFRE Group** ”).

In exercising these powers, it approves and updates the corporate policies that govern the actions of the Company and establishes the guidelines and basic principles that inspire, govern or are the basis of mandatory compliance with the rules that the other companies of the Group approve within the scope of the decision-making capacity and responsibility of each of them.

Furthermore, in accordance with the current regulations applicable to the Company regarding operational and digital resilience and with the requirements arising from the Solvency II regulations, the Board of Directors must approve a business continuity policy.

In this regard, the Board of Directors of the Company has approved this *Business Continuity Policy* (the “Policy”), which forms part of the corporate governance system of the MAPFRE Group.

### 2 Qualification

This standard is a corporate policy in accordance with the classification set out in the *Corporate Policy on the development and organization of the standards that make up the corporate governance system of the MAPFRE Group*.

### 3 Purpose

This *Policy* establishes the overall framework for the development, documentation, implementation, testing, review and continuous improvement of Business Continuity Plans at MAPFRE and its management systems, including elements related to the continuity of activity in ICT matters and following a risk-based approach.

### 4 Scope of application

This *Policy* is mandatory for all companies within the MAPFRE Group. It also applies, where appropriate and in accordance with the relevant shareholder agreements, to the various alliances and joint ventures in which Group companies participate.

Without prejudice to the foregoing, the governing bodies of the Group's insurance and reinsurance entities shall approve a policy similar to this one, incorporating the necessary adaptations that, where applicable, are strictly required to (i) make it compatible with the particularities of the business of said entities and (ii) comply with

any sectoral rules or those derived from applicable legislation or the requirements of supervisors in the countries in which they carry out their activity.

These adaptations will be subject to prior review by the Operational Resilience and GRC Area of the Corporate Security Division.

## 5 General principles

The *Policy* is based on the set of principles and commitments set out below:

- a) The protection and safety of people is the first premise and the top priority objective, both in normal situations and in crisis situations.
- b) Business continuity plan owners must appoint representatives from different areas with the appropriate experience and knowledge to actively participate in the development, documentation, implementation, testing, review, updating, and continuous improvement of business continuity plans and their management systems.
- c) The development and implementation of business continuity plans by the Group's companies will consider internal areas and departments, as well as providers and services, employing appropriate and proportionate systems, resources, and procedures. These business continuity plans will include specific, appropriate, and documented provisions, plans, procedures, and mechanisms designed to ensure the continuity of ICT activities, structured through the recovery strategies associated with the unavailability of technology unavailability.
- d) Leveraging the synergies generated and the lessons learned in the development and implementation of business continuity plans and any other plans in the field of security in the Group entities, taking into account the common means and resources available to them.
- e) The adoption of reasonable measures for the operational continuity of processes and activities, including digital operational resilience, is based on the criticality established by the Group.
- f) The inclusion of security, privacy and reliability criteria that reasonably guarantee the continuity of critical services provided by third parties.
- g) The incorporation of appropriate crisis communication procedures into business continuity plans, ensuring the timely and relevant transmission of information. These procedures will take into account and must comply with the provisions of the *Corporate Communication Policy* and must cover:
  - Internal communication to all staff, differentiating messages directed to those involved in the response and recovery, from messages for the rest of the staff.
  - External communication, as well as the timely provision of information to relevant stakeholders (which include, but are not limited to, shareholders,

employees, intermediaries, customers, suppliers, supervisors and regulatory authorities, as well as other key players for business continuity).

- h) Communicating the responsibilities and procedures for Group personnel with expertise in business continuity through awareness and training. The content to be disseminated will include procedures for escalating incidents, taking into account both their nature and the potential downtime they could cause. This *Policy* will also be communicated to Group personnel.
- i) Under the coordination of the Operational Resilience and GRC Area of the Corporate Security Division, a framework will be established to set business continuity objectives within a management system that, complying with legislative and regulatory requirements and the main applicable standards, includes periodic reviews, tests, and updates of business continuity plans. These reviews and updates will take into account lessons learned from past crises and incidents and will be carried out (i) in response to significant changes in the technological infrastructure, (ii) as a result of findings obtained after the execution of tests, or (iii) following the emergence of new threats. All of this will be part of a process that allows for the regular evaluation of the effectiveness of the implemented continuity measures and ensures the continuous improvement of the Group's operational resilience capabilities.
- j) The constant willingness to collaborate with the authorities in the event of a disaster or need, as part of the spirit of service that permeates all the actions of the Group and of the responsibility towards the societies in which it carries out its activity.

## **6 objectives regarding business continuity**

Plans and their associated management systems will be developed in accordance with the provisions of this *Policy*, in such a way that:

- a) Through Business Impact Analysis (BIA), a preliminary estimate can be made of the potential repercussions, damages, and losses that a disruptive incident affecting the company's business processes could cause. The BIA will allow for the evaluation of the potential impact of such incidents using quantitative and qualitative criteria, considering the functions identified as critical and the resources that support them.
- b) Enable an appropriate and timely response to the materialization of a security risk of catastrophic characteristics, which causes a scenario of lack of availability of any of the basic components of the Group's activity (people, buildings and offices, technology, information and providers).
- c) Minimize the impact of potential disasters on business activities by ensuring that essential data and functions are preserved or, if this is not possible, that such data or functions are recovered in a timely and progressive manner until normality is restored.

- d) Following a disruptive incident, ensure the recovery of critical functions and the resumption of all other normal business activities, meeting the recovery time and point objectives identified in the Business Impact Analysis (BIA). These objectives may vary depending on the nature of the incident and the criticality of the affected operations.
- e) Ensure that, in the event of an incident of the characteristics described, activities can be operated adequately for a sufficient period, according to the needs of the business and until normal operation has been restored.
- f) Contribute to the continuous improvement of the operational resilience capabilities of the MAPFRE Group, by carrying out annual tests to verify the correct functioning of the implemented strategies and that help to identify areas for improvement.

## **7 Responsibilities**

The Group's Security, Crisis, and Resilience Committee is the body responsible for promoting and coordinating the development, implementation, evolution, and continuous improvement of business continuity plans across the Group's entities. It is also responsible for deciding on and coordinating the implementation, maintenance, and improvement of the business continuity management system associated with each business continuity plan. These actions provide protection, reduce the likelihood and impact of disasters or catastrophes, and facilitate preparedness, response, and recovery from disruptions, including those affecting the ICT environment.

Based on the potential impact estimated by the Security, Crisis, and Resilience Committee after evaluating the incident, the Committee will decide whether to activate the relevant business continuity plans and other complementary action plans without delay, including crisis communication plans. All of this is aimed at providing a centralized, timely, and effective response to incidents and limiting their potential adverse effects.

Likewise, this Committee will assume leadership and control of crisis management involving several entities of the Group or that, due to their characteristics, exceed the scope contemplated in the business continuity plans of the various entities, whether by affecting several companies of the Group or more than one region, requiring extraordinary economic investments that exceed the scope of the entities or business units, or having the potential to significantly affect the competitive position and/or reputation of the MAPFRE Group.

Furthermore, the Security, Crisis and Resilience Committee will determine when the crisis is considered resolved and normality is restored, which may be done progressively, depending on the impact and effectiveness of the measures taken.

The Security, Crisis and Resilience Committee will report on its activities to the Company's Executive Committee and will inform it of the actions taken and the measures adopted in crisis situations that require the activation of business continuity plans.

The remaining roles and responsibilities associated with business continuity management are detailed in *MAPFRE's Crisis and Business Continuity Management Governance Framework* approved by the Corporate Security, Crisis and Resilience Committee.

## **8 Supervision, dissemination and monitoring of this *Policy***

The Corporate Security Directorate is the Promoter of this *Policy*, as defined in the *Corporate Policy on the development and organization of the rules that make up the corporate governance system of the MAPFRE Group*.

For its part, the Group's Security, Crisis and Resilience Committee is the body responsible for promoting the development and implementation of this *Policy*.

Notwithstanding the foregoing, the management and governing bodies of the Group companies, at the corporate, regional, and local levels, are responsible for disseminating and ensuring compliance with this *Policy* within their respective companies. To this end, they must adopt the necessary measures and, where applicable, report any non-compliance or partial compliance through the established channels.

This *Policy* will be reviewed at least annually and may be amended at any time by the Board of Directors of MAPFRE, SA, following a report from the Risk, Sustainability and Compliance Committee, to adapt it to any significant changes affecting its content. To this end, they will consider the information provided by the Security, Crisis and Resilience Committee and by the *Policy's Promoter* regarding the results of tests performed, recommendations arising from audit controls, or any reviews that may be conducted by supervisory bodies.

As part of the Company's commitment to its stakeholders, this *Policy* will be published on the corporate website.

## **9 Approval and entry into force of this *Policy***

This *The Policy* was initially approved by the Company's Board of Directors on December 20, 2021, and last amended on December 22, 2025, repealing and replacing the previously valid version.