

Business Continuity Plan





SUMMARY

1. OBJECTIVE.....3

2. INTRODUCTION3

3. SCOPE3

4. DEFINITIONS3

5. GUIDELINES.....6

6. BUSINESS IMPACT ANALYSIS (BIA) AND APPEARANCE FOR INTERRUPTIONS6

7. CONTINUITY PLAN STRATEGY.....7

8. ACTIVATING THE BUSINESS CONTINUITY PLAN.....8

9. CORPORATE PLANS8

9.1. PEOPLE.....8

9.2. SUPPLIERS.....9

9.3. SYSTEMS10

9.4. OPERATIONAL STRUCTURES10

9.5. TECHNOLOGICAL STRUCTURES11

10. COMMUNICATION STRATEGY13

11. DECLARATION OF END OF THE CONTINGENCY14

12. BUSINESS CONTINUITY AND DISASTER RECOVERY TESTS14

13. VALIDITY, REVOCATION AND REVIEW CYCLE14



1. OBJECTIVE

The Business Continuity Plan ("BCP") of XP Group Inc. ("XP") presents a set of fundamental activities that must be developed in order to face scenarios of prolonged interruptions of the physical and/or technological environments.

This document establishes the guidelines, responsibilities and procedures necessary to guarantee the continuity of XP's essential operations, minimizing impacts and ensuring the rapid resumption of activities in situations of disruption or crisis.

The triggering of the BCP is defined on the basis of XP's risk appetite, considering the operational limits and the types of risks the organization is willing to accept. In this way, the plan guides the proper management of these risks during their activation, ensuring that decisions are aligned with the company's risk strategy.

2. INTRODUCTION

XP controls business continuity management in an integrated and independent manner, preserving and valuing the collegiate decision-making environment. The control structure is compatible with the nature of its operations, the complexity of its products and services, activities, processes, systems and the extent of its exposure to risks.

The BCP is aligned with XP's strategic objectives, best market practices and compliance with laws and regulations issued by regulatory bodies.

3. SCOPE

The guidelines set out in this Plan must be observed by all XP Inc. Group employees.

4. DEFINITIONS

Controlling Shareholder: The shareholder or group of shareholders controlling the Company and its Affiliates, bound by a voting agreement or under common control, exercising direct or indirect control over the company, under the terms of Law 6.404/76.

Business impact analysis (BIA - Business Impact Analysis): Process of analyzing activities and the effects that a business interruption could have on them.

Backup: A process by which electronic data is copied in some form so that it can be made available and used if the original data from which it originated is lost, destroyed or corrupted.

Collaborator: All Directors, members of the Audit Board, if any, or other bodies with technical or advisory functions, employees, trainees and representatives.

Associated companies: Companies in which XP Inc. have significant influence (Article 243, Paragraph 1, of Law No. 6,404/76).

XP Prudential Conglomerate: XP Investimentos CCTVM S.A., Banco XP S.A., XP Serviços Financeiros DTVM Ltda. and other companies of the XP Inc. Group, incorporated in Brazil and abroad, which meet the definition set out in CMN Resolution No. 4,950/21.

Subsidiaries: The companies in which XP Inc. is the Controlling Shareholder.



Disaster: It is the result of natural or man-made and/or technological events that affect the normal functioning of operations, causing damage and losses to the Institution.

Adverse Events: Occurrence or change of a particular set of circumstances that may negatively impact operations and business continuity

Critical Tool: Equipment, software or technological resource that is fundamental to the operation of the IT infrastructure and whose failure or unavailability could compromise the continuity of the organization's essential services and processes.

Critical Supplier: Service provider for XP that performs activities with an impact classified as critical by the BIA or a company that XP partners with for mutual benefit in processes classified as critical by the BIA, such as insurers, platforms and any other institutions in which XP can offer the services and/or products of the partners to its customers without generating a single supply contract.

Business Continuity Management (BCM): The institution's ability to continue delivering products or services at a previously defined acceptable level after incidents of interruption.

Critical process manager: Responsible for managing the Critical Process. This is the person who will be contacted to update the information you have filled in annually and in the event of an incident involving your process.

Strategic Group - Level responsible for monitoring crises, evaluating actions, defining strategies and ensuring effective communication for decision-making at XP Inc.

Tactical Group - Level responsible for assessing the impact of the disaster, activating the strategic group, recommending contingency plans, managing the operational team and ensuring communication and allocation of responsibilities to maintain vital services and resume operations.

Operational Group - Level formed by specialists from the impacted areas and support teams, responsible for the practical execution of recovery and resumption of business after an incident.

XP Group Inc ("XP")... Companies Controlled by XP Inc. and its Affiliates, incorporated in Brazil and the United States, taken together.

GTL: General Tech Lead, is the technical reference for the BU/platform, being the functional manager of the technology team and the main point of contact with BU stakeholders. They are responsible for setting up continuity strategies for systems identified as critical and also for carrying out DR tests, where applicable

Impact: Evaluated consequences of a particular event. It can be financial, operational, legal or image.

Incident: Situation that can represent or lead to business interruption, losses, emergencies or crises.

Infrastructure: System of facilities, equipment and services necessary for the operation of the institution.

ITSCM - Infrastructure Expert Team responsible for managing the continuity of technology services.

Onshore: Refers to the operations and units of XP Inc. located in Brazil.

Offshore: Refers to XP Inc. operations and units located abroad.



Critical people: Employees who carry out critical activities in processes or journeys which, if interrupted, cause a significant impact from a financial, customer, regulatory and reputational point of view, and which must be completed on the same day, or in a specific window. These people are defined and/or reviewed annually in the BIA of each process by the manager of the critical process, who communicates that the person has been classified as critical.

Business Continuity Plan ("BCP"): Documented procedures that guide the institution to respond, recover, resume and restore, after the interruption, to a predefined level of operation.

Disaster Recovery Plan (DRP): Structured set of procedures and actions that an organization implements to restore its IT systems after the occurrence of a disaster, whether natural, technical or human. The main objective of the DRP is to minimize the impact of the disaster, guaranteeing the rapid resumption of essential activities and business continuity.

Service Platform - Support and solution of questions, problems and requests from XP Inc. clients.

Critical Processes: Activity or set of activities essential to the functioning and continuity of the business, the interruption of which can cause significant impacts on the organization.

Resilience: This refers to the institution's ability to resume its normal activities after a business interruption event.

RPO - Recovery Point Objective : Point at which the information used by a process must be restored to allow the process to operate on resumption, i.e. it is the secure *checkpoint* of data that can be done via *backup*, data replication, caching or message queuing, necessary for one or more business processes to continue after the contingency or technology resources for continuity have been made available.

RTO - Recovery Time Objective : Target time that the business process or group of processes must be recovered, with its continuity established, partially or totally so that it does not cause corporate impact.

Critical Systems: These are the systems that are essential to the functioning of an organization's critical processes. The unavailability or failure of these systems can have a significant impact on business processes, jeopardizing the continuity of activities and the delivery of services.

Business Continuity Team: Structure of the Corporate Risks team, responsible for the business continuity specialty.

Facilities Team - Expert Facilities Team responsible for managing and maintaining the company's physical facilities, ensuring an efficient working environment for all employees.

People's Team - Expert People Team responsible for activities related to people management.

Information Security (IS) Team - IS Expert Team responsible for protecting the company's digital assets, data and systems from threats, vulnerabilities and security incidents. This team works to guarantee confidentiality, integrity and availability of information, in line with best practices and internal security policies.

5. GUIDELINES

The BCP addresses the contingencies envisaged and actions to be taken, according to various crisis scenarios, so that the services provided, as well as essential/important operational tasks, are maintained in the event of a possible occurrence until they are normal, with the aim of:

- Adhere to current regulations;
- Keeping employees aligned with the organization's needs and strategies;
- Have recovery plans in place to safeguard the lives of our employees.
- Ensure that the proposed contingency arrangements are effective.
- Ensuring customer service and the liquidation of their business.
- Mitigate the reputational impacts of an interruption for XP's brands.
- Define how and what actions should be taken to build organizational resilience capable of safeguarding the business in the event of a disaster.
- Ensure the organization's adequate operational continuity until the return to normality following incidents and/or severe interruptions to processes categorized as critical.
- Promoting an assertive understanding of the group's modus operandi, allowing for opportunities for improvement.
- Describe the main and alternative physical and technological environments.
- Define and apply business continuity and disaster recovery tests.

6. BUSINESS IMPACT ANALYSIS (BIA) AND APPEARANCE FOR INTERRUPTIONS

Business Impact Analysis (BIA) determines and evaluates the potential effects of an interruption to critical business processes as a result of a disaster, accident or emergency. In addition to establishing acceptable downtimes for each process. The BIA also includes identifying the location of operation for critical business processes, as well as the people, systems, applications and suppliers that support these processes.

In order to determine the criticality of the process, the impacts informed by the person responsible for the process are taken into account, which will be weighted by the Business Continuity Team considering the Impact Ruler, available in the Corporate Risk Management and Internal Controls Methodology, defined by the company's management.

These impacts are analyzed by the interruption time that defines the criticality of the process, as shown in the table below:

RTO	Criticality
Up to 1 hour	Very high
Up to 2 hours	High
Up to 4 hours	Average
Up to 8 hours	Low



Up to 24 hours	Very low
Over 24 hours	Not critical

To define the RTO, the first schedule with a high or higher impact declared by the process manager in the BIA is considered. In other words, if it is reported that the first high impact occurs with 2 hours of unavailability, regardless of the type of impact (customer, regulatory, financial or reputational), the RTO of the process will automatically be up to 2 hours. If the person responsible disagrees with the calculated RTO, they can request a change with justification, which will be considered by the Business Continuity Team.

In addition to the RTO, during the BIA the RPO (Recovery Point Objective) is also collected and analyzed, which determines the maximum tolerable point of data loss for each critical process. The RPO guides the backup and recovery strategy for data related to the systems that support these processes, ensuring that essential information is preserved and can be restored as stated in the BIA.

Although the BCP does not explicitly detail these levels, they are incorporated into the continuity strategy through the IT backup and recovery policies, which should be aligned with the BIA results.

The prioritization of processes for business continuity management considers both RTO and RPO, ensuring that operational impacts are minimized and that the most critical data is restored based on the last available backup.

7. CONTINUITY PLAN STRATEGY

XP's business processes will be prioritized for business continuity management based on the processes classified as highly critical (RTO: 2 hours) and Very High (RTO: 1 hour) in the Business Impact Analysis (BIA), considering the impact levels of the Corporate Risk Matrix (financial, regulatory, customer and reputational), in a disruption scenario.

In addition to the processes categorized as critical in the BIA, the following processes will also have their continuity strategies applied as a matter of priority:

- Zeroing out the till;
- Settlement of transactions with clients and with clearings;
- Opening a brokerage house (fixed and variable income brokerage);
- Maintaining customer positions and guarantees;
- Customer service;
- Value transfer (PIX and TED);
- Making bank payments;
- Bank reserve control and management;

During a disaster scenario, the organization will adopt a posture of prudence, which means that the volume of new transactions will have to be monitored. New operations will be carried out according to the



reduced processing capacity during the incident and recovery of operations. Above all, the strategy will be to reduce the number of transactions within a safe processing range.

In addition to the BIA, XP has plans in place to guarantee the continuity of critical business processes. The plans are divided into

- Corporate Plans: aim to meet XP's continuity as a whole or for a group of critical processes and are detailed in this BCP in item 9 of this document with the following Interruption Scenarios:
 - People;
 - Suppliers;
 - Systems;
 - Operational Structures;
 - Technological Structures;
- Specific Plans: these are also known as OCPs (Operational Continuity Plans), which address specific situations within each process and are described in the BIA as alternative solutions for systems and suppliers.

8. ACTIVATING THE BUSINESS CONTINUITY PLAN

The Business Continuity Team may be activated at any time by the heads of the Technology, Information Security, Facilities, People or any other Managers from XP's operational and support areas, upon the occurrence (or high possibility of occurrence) of an adverse event that may impact the continuity of processes and business.

The activation process must take place by instant message via Teams or telephone contact from the Continuity Team described in Annex I.

Once the possibility or occurrence of an adverse event has been identified, in accordance with the scenarios detailed in Item 9, and the Continuity Team has been activated, the magnitude of the impact must be assessed to determine the need to activate the Strategic Group, which will decide on the activation of the corresponding corporate plan."

9. CORPORATE PLANS

9.1. PEOPLE

XP has adopted a hybrid working model for its employees, allowing them to carry out their activities at home or in the office, as determined by each of their respective areas.

Teams must have at least one person as a substitute (*backup*) for the critical person, preferably two backup people, depending on the capacity of the team performing the critical functions. For this strategy to work properly, there needs to be redundancy of routines between team members, i.e. there shouldn't be any critical processes that only one member of staff is capable of carrying out. It is also necessary for teams



to have step-by-step manuals for carrying out their critical processes, in order to make it easier for backup employees to act in case of need.

Adverse Events	Applicable contingency:	People Responsible for Operationalization
Force of nature events (hurricanes, earthquakes, blizzards, floods, epidemics or any other disaster that could endanger the employee's life)	<ol style="list-style-type: none"> 1. Provide means of transportation and accommodation in order to guarantee the personal safety of affected employees, when necessary. 2. Enabling remote working for employees, when possible and/or necessary. 3. Activate teams from other regions to take over critical processes in the event of total unavailability of the affected region, taking advantage of mirror teams and distributed collaborators. 	<ol style="list-style-type: none"> 1. People and Facilities 2. Information Infrastructure and Security 3. Critical Process Manager
Unavailability of the critical person;	Trigger the backup to take over the critical process, if there is no backup in place, make the Operating Procedure for the process available to another employee to be appointed.	Critical Process Manager

9.2. SUPPLIERS

Suppliers that support critical journeys and processes are evaluated during the approval and contract renewal process, so that the risks of interruption are identified and mitigated.

In addition, suppliers can also be identified and assessed as critical in the BIA and, in this process, are reviewed annually, depending on the dependence of the service provided for the critical process. Also in this process, evidence is requested from the supplier demonstrating continuity plans and DR testing in order to ensure that the continuity requirements defined in the BIA are met by the supplier.

Adverse Events	Applicable contingency:	People Responsible for Operationalization
Critical Supplier Unavailability	<ul style="list-style-type: none"> • Activate the supplier for immediate corrections and ensure that it activates its contingency infrastructure, which must have enough redundant equipment and links for the scenario in which its main environment is lost. • Activate a backup provider, previously contracted for contingency use only (this can be a pay-per-use contract), when possible; 	Critical Process Manager



	<ul style="list-style-type: none"> Make available a Process Operating Procedure supported by the supplier, with the aim of internalizing the execution of activities, where possible. 	
--	--	--

9.3. SYSTEMS

Systems strategy is essential to guarantee the availability, integrity and rapid recovery of the technological solutions that support the organization's critical operations. Information systems are fundamental pillars for the execution of business processes, and their unavailability can cause significant impacts, both operational and financial.

Adverse Events	Applicable contingency:	People Responsible for Operationalization
Unavailability of a critical system or tool	<ol style="list-style-type: none"> 1. Trigger the Disaster Recovery Plan (DRP); 2. Use of a parallel system or tool that can perform the activities in a similar way. 3. Use other means to carry out critical process activities (e.g. spreadsheets). 	<ol style="list-style-type: none"> 1. GTL and/or ITSCM 2. Critical Process Manager 3. Critical Process Manager

9.4. OPERATIONAL STRUCTURES

XP has two main sites in São Paulo called SPCT and RLJ, a site in Rio de Janeiro, a site in Miami, a site in New York and one in the Cayman Islands.

XP's offices are equipped with *UPS (nobreaks)* in order to make it possible to supply power in the event of unavailability of the operators.

The address of the offices, the description of the equipment per building and its expected autonomy can be consulted with the Facilities team.

Employees have an XP laptop with access to Palo Alto's Global Protect VPN (Virtual Private Network), meeting the criteria established by Information Security.

However, there is redundancy of VPN access between data centers, allowing the user to access the environment transparently via the secondary connection in the event of problems with the primary connection.

As an alternative to remote access via VPN, or even in cases where the main work equipment (notebooks and/or desktops) is unavailable, employees who support critical processes can request the availability of virtual machines (DaaS).

Adverse Events	Applicable contingency:	People Responsible for Operationalization
----------------	-------------------------	---



Unable to work remotely	Guide the employee to the nearest office. Note: In the case of a critical person, during the period of unavailability, follow the contingency detailed in item 9.1 of this document.	Critical Process Manager
Unavailability of use or access to XP offices	Guide the employee to stay or move to carry out the remote work.	Critical Process Manager

9.5. TECHNOLOGICAL STRUCTURES

XP has two data centers called Equinix SP2 and Equinix SP3, both adhering to Tier 3 standards¹ and each site has its own independent infrastructure. The contracting format with Equinix is Colocation, which is a service that only rents the data center infrastructure to install the servers. The data center service acts as support, providing rack space, electricity, internet connectivity, air conditioning, environmental protection, etc. The servers and equipment are managed by XP's Infrastructure teams.

Data Centers	Address	Structure
DATA CENTER Equinix SP2	Alameda Araguaia, 3641 Tamboré - Barueri/SP.	XP's data center infrastructure.
DATA CENTER Equinix SP3	Avenida Marcos Penteado de Ulhoa Rodrigues, 249 Residencial Três (Tamboré) - Santana de Parnaíba/SP.	XP's data center infrastructure.
Colocation B3 data center	B3 data center.	Infrastructure for trading platforms using robots within the B3 network.

XP's architecture also uses Microsoft Azure cloud services. These services use the provider's best practices to ensure the necessary replication and resilience in the event of a failure. Some services use the local resilience of Brazil (Multi Zone in SP and Private Cloud in SP3) and other services are replicated to another region (East US 2), depending on the classification of the criticality of the services.

We emphasize that the existing data centers act as contingencies for each other, depending on how the replications of services, systems and infrastructure resources (e.g. databases) are configured. The entire environment is monitored with its respective metrics and KPIs using the tool *Dynatrace*.

The physical data centers are connected via an erased fiber ring with a high-speed, low-latency network running MPLS and OSPF protocols. This technology means that any data center has an alternative environment for the electronic processing of a business application in the event of a contingency. The configuration is carried out without a single point of failure, in which the two rings (Ring A - Ufinet and Ring

¹ **Tier 3:** It is a data center where maintenance is carried out without interrupting the system. In this type of structure, IT equipment operates with redundant components, electrical distribution branches, systems and subsystems. Features: **(i)** Cannot be less than 1.6 km from airports; **(ii)** Availability of 99.98% with tolerated annual downtime of 1.6 hours; **(iii)** Electrical distribution branches and other systems and subsystems can be removed without interrupting the system; **(iv)** Redundant UPS modules and generator sets for power supply; etc.



B - Megatelecom) pass through separate paths and the proximity points shown in the image below occur where Ring A is grounded and Ring B is aerial, as well as being installed on opposite sides of the road.

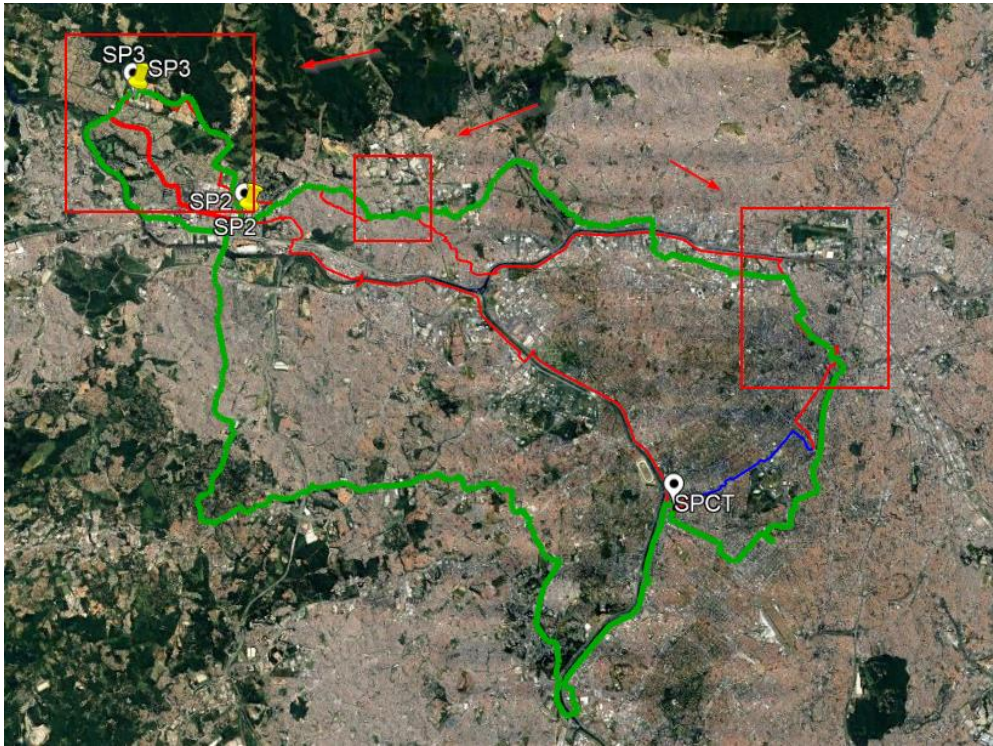


Figure1 - Telecom rings

The server networks are segregated and have their incoming and outgoing traffic controlled by a redundant firewall solution. XP has its own IP blocks (AS), and internet traffic is handled through transit links contracted by various telecommunications operators.

Adverse Events	Applicable contingency:	People Responsible for Operationalization
Datacenter unavailability	Trigger a Disaster Recovery Plan for the affected Data Center.	ITSCM
Unavailability of critical infrastructure and security resources and/or services (Example: Link, telecom equipment, firewall, switch, database, balancer, microservices manager, Active Directory (AD))	Trigger a Disaster Recovery Plan for critical infrastructure and security resources and/or services.	ITSCM and Information Security



Unavailability of the World Wide Web (Internet)	Provide alternative service channels for receiving and executing orders.	Service
---	--	---------

10. COMMUNICATION STRATEGY

The following audiences are provided for in the communication plan and should be identified for immediate contact by XP. It is essential to define spokespeople in advance to communicate with stakeholders.

Public	Communication Channels	Responsible for communication
Press	<ul style="list-style-type: none"> XP's press office through press releases or proactive contact; E-mail / XP website and social media channels; 	<ul style="list-style-type: none"> Martech
Clients	<ul style="list-style-type: none"> XP's institutional e-mail; XP website /Social media; Push notification in the APP; Information banner in the APP; Contact via advisors; XP Call Center; Chatbot; 	<ul style="list-style-type: none"> Service
XP employees.	<ul style="list-style-type: none"> XP corporate e-mail and Teams; Meeting to inform the leadership; 	<ul style="list-style-type: none"> Internal communication
External advisors	<ul style="list-style-type: none"> XP corporate e-mail Contact via XP leadership/employees; 	<ul style="list-style-type: none"> Indirect Distribution
Regulatory bodies / Self-regulators / Committees with external members / Public authorities	<ul style="list-style-type: none"> E-mail from XP's Regulatory Legal Department; Specialized law firms; 	<ul style="list-style-type: none"> Legal
Suppliers	<ul style="list-style-type: none"> E-mail from the area responsible for suppliers 	Manager of the Organizational Unit responsible
Leadership of group companies	<ul style="list-style-type: none"> Contact XP management; 	<ul style="list-style-type: none"> Business Continuity

Public	Communication Channels	Responsible for communication
Experts/opinion leaders	<ul style="list-style-type: none"> XP contacts who have relationships with these sources. 	<ul style="list-style-type: none"> Martech and the Board

The people responsible and the communication channels above must be respected for communication regarding the start and end of the contingency, and communications must be coordinated with the Business Continuity area.

11. DECLARATION OF END OF THE CONTINGENCY

The return to normal operations must be planned by the Operational and Tactical groups within an acceptable timeframe, which must be determined by the Strategic Group.

These are the main tasks/activities to be carried out by the Operational and Tactical groups:

- Identify in detail the damage caused by the incident;
- Identify the insurance policies in force that cover the incident;
- Identify the cause of the incident and ensure that it is properly addressed.

The declaration of the end of the state of contingency will be defined by the strategic group, taking into account the recommendations of the other groups, operational and tactical, if they consider the cause to be extinct.

Communication about the end of the contingency will follow the same process as communication about the start of the contingency.

12. BUSINESS CONTINUITY AND DISASTER RECOVERY TESTS

XP continuously improves the way it carries out tests, with the aim of ensuring that viable recovery strategies and plans are maintained. The test schedule is defined in the Business Continuity Test Plan Procedure.

13. VALIDITY, REVOCATION AND REVIEW CYCLE

The BCP is reviewed annually or in a shorter period of time if necessary, due to changes in legislation, procedures or the environment, submitted for analysis by the Risks and Social, Environmental and Climate Responsibility Committee and approved by the board of directors.

It is the responsibility of the Corporate Risks (Business Continuity) area to keep the contingency plans under its responsibility up to date. The information required for the execution of the operation at the operational contingency site, technological infrastructure, systems, links and data centers must be updated by the areas mentioned in this document whenever significant changes occur in the production environment so that, in the event of a relevant incident and total or partial invocation of the plan, it maintains its effectiveness.

This document will be in force from the moment it is signed and will be disclosed internally and made available to all members and stakeholders of the process.