

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

Business Continuity Policy

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Contents

1. Purpose	2
2. Scope	2
3. Terms and Definitions	3
4. Principles	4
5. Structure of the Continuity Program	4
6. Criticality and Recovery Timeframes	5
6.1. Criticality categories	5
6.2. Rules for timeframes	6
6.3. Minimum acceptable level of operation	7
7. Interruption Scenarios	7
8. Crisis Management	8
9. Communication	8
10. Service Providers and Cloud	9
11. Testing Program	9
12. Review	9
13. Reference Standards	10
14. Effectiveness	10
15. Version Control and History	10

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

1. Purpose

This Policy sets out the principles, guidelines, roles and approval authorities for business continuity management at Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. (the PSAV company), referred to in this document as the Organization, with the aim of ensuring that the critical processes of the provision of virtual asset services are maintained or restored within defined timeframes, and that the control instruments of virtual assets and the financial resources of clients and users remain under the Organization's control during any interruption.

For the Organization, continuity is not a matter of system availability. An interruption that preserves custody but suspends operations is a serious event; an interruption that compromises custody is an irreversible event. This Policy orders priorities in this sequence: first, the integrity of control instruments and client funds; then, the ability to operate; then, convenience.

It is grounded in article 43, IV and paragraph 4, of BCB Resolution No. 520 of November 10, 2025, and in article 3, V, "a", articles 19 and 20 and Chapter III of BCB Resolution No. 85 of April 8, 2021, the scope of which was extended to virtual asset service provider companies by BCB Resolution No. 552 of March 3, 2026. It is aligned with ISO 22301:2019 and with controls 5.29 and 5.30 of ISO/IEC 27001:2022.

This Policy establishes the method and the approval authorities. The recovery timeframes for each process derive from the Business Impact Analysis (BIA) and are set out in the Business Continuity Plan, as provided in Section 6. The operational requirements are detailed in the Business Continuity Management Standard, which this Policy underpins.

2. Scope

This Policy applies to the processes, systems, data, facilities, people and service providers that support the provision of virtual asset services by the Organization, including the technology infrastructure shared with the other companies of the Trace Finance Group, which, for the purposes of this Policy, is treated as a resource of the Organization and is fully subject to its requirements.

It also applies to relevant service providers, in accordance with the Cloud Chapter of the Cybersecurity Policy, and to the other suppliers that support critical processes, in accordance with the Supplier Security Standard.

The continuity management structure is single for the group and is governed by the Business Continuity Management Standard. This Policy adds the requirements specific to the PSAV

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

company and prevails, with respect to it, in the event of any inconsistency.

3. Terms and Definitions

Term	Definition
Critical process	Process whose interruption affects the custody or movement of virtual assets or of clients' and users' financial resources, compliance with a time-bound regulatory obligation, or the full exercise of the rights of a client or user.
Business Impact Analysis (BIA)	Assessment, conducted with process owners, of the impacts of an interruption over time, from which the criticality category, the MTPD, the RTO, the RPO and the minimum acceptable level of operation of each process are derived.
MTPD	Maximum tolerable period of disruption, after which the impact becomes unacceptable for the Organization, for clients or for regulation.
RTO	Recovery time objective: the timeframe set for resuming or normalizing the interrupted process or service, in accordance with article 43, paragraph 4, of BCB Resolution No. 520/2025. It is always shorter than the MTPD.
RPO	Recovery point objective: the maximum acceptable data loss, measured as the interval between the last available recovery point and the interruption.
Business Continuity Plan (BCP)	Document that consolidates, for each critical process, the approved timeframes, continuity strategies, activation criteria, responsible persons and communication scripts.
Disaster Recovery Plan (DRP)	Technical document, maintained by Technology, with the recovery procedures for the systems, data and infrastructure that support critical processes.
Crisis situation	Relevant incident or relevant service interruption that meets the criteria of Section 19.3 of the Cybersecurity Policy, triggering the activation of the Crisis Desk and timely communication to the Central Bank of Brazil.
Crisis Desk	Coordination structure activated in a crisis situation, as provided in Section 8.
Continuity test	Planned exercise that verifies the ability to execute the strategies and plans, in the modalities set out in Section 11.

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

4. Principles

Continuity management observes the following principles, which guide every design, investment and response decision:

- **Custody before operations.** No continuity strategy permits the loss, exposure or unauthorized transfer of virtual asset control instruments. In the event of a conflict between restoring the service and preserving custody, custody prevails.
- **Grounded in the BIA.** No recovery timeframe is set for technical convenience or by infrastructure category. Timeframes derive from the impact assessed with the process owner and are approved by the Compliance Committee.
- **Proportionality.** Strategies are commensurate with the Organization's size and the criticality of each process. Redundancy without grounding in the BIA is a cost; the absence of redundancy in a critical process is a formally accepted risk, never an omission.
- **Security preserved during contingency.** Information security controls remain applicable during the interruption and recovery. Any temporary reduction of controls is authorized, recorded and time-limited, in accordance with the Business Continuity Management Standard.
- **Capacity demonstrated, not presumed.** A plan is only considered effective after a test consistent with its scope. An untested timeframe is a hypothesis and is presented as such in any document, including to the supervisor.
- **Known dependencies.** Every critical process has its dependencies on people, systems, data, facilities and providers mapped, including concentrations in a single provider or region.

5. Structure of the Continuity Program

The continuity program consists of the documents below, in order of precedence. Each derives from the previous one, and none is considered in force without the one that underpins it.

Document	Content
This Policy	Principles, method, roles, approval authorities, minimum scenarios and testing program
Business Continuity Management Standard	Operational requirements for the BIA, strategies, plans, crisis management, communication, suppliers, testing and improvement

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

Document	Content
Business Impact Analysis (BIA)	Critical processes, impacts over time, criticality category, MTPD, RTO, RPO, minimum level of operation and dependencies
Business Continuity Plan (BCP)	For each critical process: approved timeframes, strategies, activation, responsible persons and substitutes, alternative procedures and communication scripts
Disaster Recovery Plan (DRP)	Technical recovery procedures for systems, data and infrastructure, with recovery order and verification criteria
Annual testing program and reports	Schedule, scenarios, results, deviations and actions; includes the restoration tests of the Backup Restoration Testing Process

The BIA is an annex to this Policy, approved by the Compliance Committee and may be updated without a change to the major version, provided that it does not modify the principles, roles or approval authorities established herein. The BCP and the DRP are standalone documents, in accordance with the Document Management Standard. Any change to the category or recovery timeframe of a critical process is always made by revising the BIA, submitted to the Compliance Committee.

6. Criticality and Recovery Timeframes

6.1. Criticality categories

The BIA classifies each process into one of the categories below, defined by the maximum tolerable period of disruption. The category determines the recovery priority, the rigor of the strategies and the minimum testing frequency.

C a t e g o r y	MTPD	Typical processes	Minimum requirement
C r i t i c a l	Up to 4 hours	Custody and movement of virtual assets; client authentication; settlement of transactions; AML monitoring	Automated recovery strategy; annual technical test; scenario included in the annual integrated test

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

C a t e g o r y	MTPD	Typical processes	Minimum requirement
H i g h	Up to 24 hours	Client service; reconciliation; time-bound regulatory reporting	Documented alternative procedure; annual test
M e d i u m	Up to 72 hours	Support processes with deferred financial or contractual impact	Documented alternative procedure; test every two years
L o w	More than 72 hours	Administrative processes with no impact on clients or on time-bound obligations	Recorded in the BIA; no specific plan

The category is assigned according to impact, not according to the system that supports the process. The typical processes indicated are for guidance only; the binding classification is that of the approved BIA.

6.2. Rules for timeframes

The RTO of each process is shorter than its MTPD and is set with a margin for the activation decision, the execution of the recovery and the security check before return. The RPO is set according to the process's tolerance to data loss and is consistent with the recovery capacity actually available under the Backup Policy; any incompatibility between the required RPO and the existing capacity is recorded as a risk and addressed, not adjusted on paper.

The approved timeframes are set out in the BIA, reproduced in the BCP and constitute the timeframes established for the resumption or normalization of activities for the purposes of article 43, paragraph 4, of BCB Resolution No. 520/2025.

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

6.3. Minimum acceptable level of operation

For each critical process, the BIA defines the minimum acceptable level of operation during contingency. For the processes of custody and movement of virtual assets, the minimum level includes, in any scenario, the ability to block movements, to confirm balances and to comply with orders from authorities, even if normal operations are suspended.

7. Interruption Scenarios

Strategies, plans and tests consider, at a minimum, the scenarios below, which include the incident scenarios required by article 3, V, "a", and article 19, III, of BCB Resolution No. 85/2021:

- compromise, suspected compromise or unavailability of a virtual asset control instrument, including due to failure or unavailability of the wallet infrastructure provider;
- unavailability of a relevant provider of data processing, data storage or cloud computing services, including the unavailability of an entire region of the infrastructure provider, with the provider replacement scenario required by the Cloud Chapter of the Cybersecurity Policy;
- loss, corruption or malicious encryption of production data, requiring restoration from a backup copy;
- cyber incident requiring the isolation of environments or the preventive suspension of services, including denial-of-service attacks and compromise of privileged credentials;
- unavailability of key personnel, in particular holders of control instruments and platform administrators, including simultaneous unavailability;
- unavailability of the physical facilities or of the usual means of communication, with fully remote operation;
- unavailability of an edge, identity or observability service that prevents client access or the operation of security controls.

Each scenario has a strategy defined in the BCP and, where it involves technological recovery, a procedure in the DRP. A scenario without a strategy is recorded as a risk accepted by the competent authority, with a deadline for treatment.

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

8. Crisis Management

A crisis situation is an interruption that meets the criteria of Section 19.3 of the Cybersecurity Policy: unavailability of a critical process for a period longer than the MTPD defined in the BIA; compromise of a virtual asset control instrument of a client or user; or inability to restore by the ordinary procedures of the Incident Action and Response Plan.

The crisis situation is declared by the responsible Officer, who activates the Crisis Desk composed, at a minimum, of the Officer, the Business Continuity Manager, Compliance and the owners of the affected processes. The Crisis Desk decides the recovery order according to the categories of Section 6.1, authorizes the use of contingency strategies and approves communications. Decisions, times and grounds are recorded in real time and consolidated after closure.

The activation and deactivation of plans, the stabilization criteria and the return to normal operations follow the Business Continuity Management Standard. The return to normal operations depends on a security check by Information Security, which is recorded.

9. Communication

The Organization promptly informs the Central Bank of Brazil of the crisis situation and of the measures taken to resume activities, in the form and through the channels set out in regulation, with a reasoned decision by the responsible Officer recorded in accordance with the Incident Action and Response Plan. The internal and external communication needed to guide the restoration of activities forms part of the resumption timeframe, in accordance with article 43, paragraph 4, of BCB Resolution No. 520/2025.

Clients and users are informed of any service interruption that affects them, of the status of their assets and of the expected restoration, through a channel defined in the BCP and with language that distinguishes confirmed facts from estimates. Where the interruption involves personal data, the Personal Data Protection Policy applies. External communications are approved by the responsible Officer jointly with Compliance.

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

10. Service Providers and Cloud

For each relevant service provider, a continuity alternative is maintained that covers the replacement of the provider and the restoration of operations, with an estimated resumption timeframe consistent with the BIA timeframes, in accordance with the Cloud Chapter of the Cybersecurity Policy. The continuity capacity of providers is assessed in prior due diligence and in ongoing monitoring, with documentary evidence, and contracts contain the continuity, data access and return clauses required therein.

Concentration in a single infrastructure provider, in a single region or in a single wallet infrastructure provider is recorded as a concentration risk under the Risk Management Policy and reassessed annually, with the treatment or acceptance decision recorded by the Compliance Committee.

11. Testing Program

The annual testing program, approved with the acknowledgment of the Compliance Committee, includes at a minimum: one integrated tabletop exercise per year, with a cyber scenario and the participation of the Crisis Desk; one technical recovery test per year for each system supporting a Critical process, including a scenario of unavailability of a relevant provider; and backup restoration tests at the frequency set by the Backup Restoration Testing Process.

Each test has an objective, scenario, success criteria and responsible persons defined in advance and is recorded in a report, with the timeframes actually measured, deviations and corrective actions, monitored until completion. An approved timeframe that is not achieved in a test is reported to the Compliance Committee and addressed before the plan is considered effective for that process.

The results of the continuity tests form part of the annual report on the implementation of the Incident Action and Response Plan, in accordance with the Cybersecurity Policy and article 8 of BCB Resolution No. 85/2021.

12. Review

This Policy is reviewed annually and on an extraordinary basis upon a regulatory change, the approval or revision of the BIA that changes the category or timeframe of a critical process, the activation of the plans, a test result that shows an inability to meet an approved timeframe, a material change in the technology architecture or in relevant providers, or an audit or supervisory finding.

	Business Continuity Policy	SEG-POL-010-FIN
Publication Date: 10/15/2026	Information Security	Public

13. Reference Standards

- BCB Resolution No. 520 of November 10, 2025, in particular article 43, IV and paragraph 4, and articles 32 to 42.
- BCB Resolution No. 85 of April 8, 2021, in particular article 3, V, articles 8, 19 and 20 and Chapter III, as currently in force, applicable to virtual asset service provider companies under BCB Resolution No. 552 of March 3, 2026, as amended by BCB Resolution No. 538/2025.
- Law No. 14,478 of December 21, 2022.
- ISO 22301:2019: Security and resilience, Business continuity management systems, Requirements.
- ISO/IEC 27001:2022 and ISO/IEC 27002:2022, in particular controls 5.29 (information security during disruption) and 5.30 (ICT readiness for business continuity).

14. Effectiveness

This Policy enters into force on the date of its publication, after approval by the Organization's Board of Executive Officers, formalized in minutes, following prior deliberation by the Compliance Committee, and remains in force until its review or express revocation.

15. Version Control and History

Version	Date	Change/Addition History	Approved by
1.0	10/15/2026	Initial issue.	Board of Executive Officers, following deliberation by the Compliance Committee