



IT Infrastructure and IT Service Management Plan

Subject to regulatory approval

Version Log

Version	Approval Date	Approving Body	Circular Notice*
1.0	04/22/2026	Collegiate Executive Board	Not applicable.

* Circular Notice through which the change was disclosed.

Table of Contents

I.	Introduction	1
II.	Information Technology Governance	1
1.	Overview	1
2.	Roles and Responsibilities	2
3.	Information Technology Service Management	6
4.	Policies and Regulations	7
III.	Systems Architecture	7
1.	Overview	7
2.	Components	8
2.1.1.	Synchronous Integrations via HTTP/HTTPS	8
2.1.2.	Internal Services	9
3.	Application Scalability	9
IV.	Technology Infrastructure Architecture	10
1.	Overview	10
2.	Cloud Computing	10
3.	Data Centers	11
4.	Head Office	11
5.	Connectivity and Interconnections	11
6.	Monitoring, Logs and Observability	13
7.	Backup, Restoration, and Data Protection	13
8.	Testing and Audits	14
V.	General Provisions	14

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

I. Introduction

This IT Infrastructure and IT Service Management Plan (“**Plan**”) of Base Clearing is intended to ensure that Base Clearing’s operational, strategic, and regulatory needs are met effectively, efficiently, and in alignment with internal and external normative instruments, corporate principles, established responsibilities, and formal IT service management guidelines. This alignment is essential to meet the requirements of BCB Resolution 304, which establishes requirements related to operational resilience, technology service management, information security, business continuity, and the governance of critical financial market infrastructures.

The Plan was developed in a manner compatible with the nature, size, complexity, organizational structure, and risk profile of Base Clearing, reflecting modern governance practices and regulatory standards inspired by the Principles for Financial Market Infrastructures (“**PFMI**”) incorporated by BCB Resolution 304. Accordingly, the Plan guides Base Clearing’s technology management based on the following fundamental principles:

- Operational resilience, ensuring that the technology infrastructure adequately supports critical operations and maintains continuity in the face of failures or adverse events;
- Information and cyber security, with policies, controls, and protection mechanisms aligned with regulatory requirements and international best practices;
- Structured risk management, with the identification, assessment, mitigation, and continuous monitoring of risks associated with IT, third-party providers, and essential services;
- Efficiency and quality in IT service management, based on standardized processes and recognized best practices, such as ABNT NBR ISO/IEC 20000-1; and
- Governance, transparency, and regulatory compliance, ensuring full adherence to Central Bank requirements and Base Clearing’s internal policies.

Capitalized terms used in this Plan that are not defined herein have the meaning assigned to them in the Glossary or, alternatively, refer to terms commonly used in the context of information technology.

II. Information Technology Governance

1. Overview

For purposes of corporate governance, including governance of information technology management (“IT Governance”), Base Clearing adopts the 3 (three) lines of defense model, as follows:

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

- (i) 1st Line of Defense: represented by all the legal, finance, operations, technology, and other business and corporate areas of Base Clearing (excluding the RCC, Information and Cyber Security, and Internal Audit Areas), which must ensure effective risk management through the definition, implementation, and improvement of practices and controls, within the scope of their direct organizational responsibilities ("1st Line of Defense"). Members of the 1st Line of Defense must report to the Internal Risk Committee and the RCC Area any Material and/or Recurring Risk Events, or events that are not in line with the risk guidelines and limits established by Base Clearing.
- (ii) 2nd Line of Defense: represented mainly by the RCC and Information and Cyber Security Areas ("2nd Line of Defense"), which are the main structures acting alongside the 1st Line of Defense and are responsible for implementing policies and procedures aimed at risk management, compliance, internal controls, and business continuity, as well as ensuring communication on these matters with the Internal Risk Committee, the Collegiate Executive Board, the Internal Audit, and the General Shareholders' Meeting of Base Clearing, the latter through the Audit Committee (when established).
- (iii) 3rd Line of Defense: represented by the Internal Audit ("3rd Line of Defense"), which reports to the Collegiate Executive Board and the General Shareholders' Meeting of Base Clearing, the latter through the Audit Committee (when established). The Internal Audit's main responsibilities are to provide independent and objective assessments of the corporate governance processes and of risk management and internal controls.

The adoption of the 3 (three) lines of defense model optimizes the decision-making process and responses to risks inherent to information technology, through the definition of roles and responsibilities that act in a coordinated manner to ensure alignment between information technology management and the strategy of Base Clearing.

Additionally, for the definition of the principles, guidelines, and procedures related to information technology management, the requirements and best practices established in normative instruments and *frameworks*, such as: BCB Resolution 304, the Information Technology Infrastructure Library ("ITIL"), and the Control Objectives for Information and Related Technology ("COBIT").

2. Roles and Responsibilities

Base Clearing's IT Governance is structured with clearly defined functions, ensuring segregation of duties, traceability, and adequate oversight of technology processes. The main roles are:

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

2.1. Technology Director

The responsibilities of the Technology Director include the following activities:

- (i) Manage the technology resources and the operational efficiency of the technology systems of Base Clearing;
- (ii) Ensure the preparation and implementation of policies and other internal regulations related to information technology, taking responsibility for defining the strategy, development, and implementation of systems and solutions in line with the business needs of Base Clearing; and
- (iii) Manage and administer the Company's technology department.

2.2. Infrastructure Area

The responsibilities of the Infrastructure Area, which is part of the Information Technology Area, include the following activities:

- (i) Be responsible for managing the hybrid infrastructure of Base Clearing (on-premises and cloud);
- (ii) Oversee the availability, capacity, performance, and continuity of the environments;
- (iii) Coordinate the teams responsible for technology operations and continuous monitoring of the environments; and
- (iv) Support the preparation and review of this Plan.

2.3. Development Area

The responsibilities of the Development Area, which is part of the Information Technology Area, include the following activities:

- (i) Plan, coordinate, and oversee all phases of *software* development; and
- (ii) Ensure that functional and technical definitions are aligned with business needs and regulatory requirements.

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

2.4. Testing Area

The responsibilities of the Testing Area, which is part of the Information Technology Area, include the following activities:

- (i) Define the corporate testing strategy (functional, integration, regression, load, security, and regulatory certification testing);
- (ii) Ensure that the testing scope covers technical, functional, and regulatory requirements; and
- (iii) Conduct structured tests with adequate documentation (plans, *scripts*, and evidence).

2.5. Risk, Compliance, and Internal Controls Area

The following activities related to the management of information technology infrastructure and services shall be the responsibility of the employees of the RCC Area (where necessary, with the assistance of specialized legal counsel):

- (i) Be responsible for the management activities related to: (a) risk, compliance, and internal controls, (b) PLD-FTP, and (c) business continuity, as reinforced in this Plan and in other internal regulations, including: (1) the Business Continuity Policy, (2) the Safeguard Recovery and Restoration Plan, (3) the Policy for the Prevention of Money Laundering, the Financing of Terrorism, and the Financing of the Proliferation of Weapons of Mass Destruction, (4) the Fraud Management Policy, (5) the Policy on Contracting, Risk Management, and Monitoring of the Outsourcing of Services, and (6) the Code of Ethical Conduct;
- (ii) Promote a culture of risk management, compliance, and internal controls, including an organizational culture that encourages ethical conduct and Base Clearing's commitment to compliance with applicable regulations and laws;
- (iii) Establish the principles, guidelines, and practices to be adopted, as well as implement a continuous, integrated, and comprehensive process for the management of risk, compliance, and internal controls at Base Clearing, including proposing the creation or amendment of internal regulations, in line with this Plan and in compliance with applicable internal and external normative instruments, such as: BCB Resolution 304 and BCB Regulatory Instruction No. 374;

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

- (iv) Establish and conduct, together with the other internal areas, procedures for the definition, approval, reporting, and monitoring of treatments for risks identified by Base Clearing, promoting transparency and governance;
- (v) Test and assess the adherence of Base Clearing to the legal framework, infra-legal regulations, the recommendations of supervisory bodies and, where applicable, internal regulations, including the Code of Ethical Conduct; and
- (vi) Prepare, together with the Supervision Director, the reports assessing the functioning and effectiveness of the risk management, internal controls, and compliance system, including the annual risk, internal controls, and compliance report, considering the results of business continuity testing.

2.6. Information and Cyber Security Area

The Information and Cyber Security Area is responsible for acting on and responding to Information and Cyber Security Incidents.

The responsibilities of the Information Security Area include the following activities related to the management of information technology infrastructure and services:

- (i) Prepare and update the Incident Response Plan, with a focus on incidents related to Information and Cyber Security;
- (ii) Propose investments related to information and cyber security, with the main objective of mitigating risks;
- (iii) Control and structure the management of Information Security and cybersecurity controls at Base Clearing, proposing technical guidelines appropriate to business needs and regulatory requirements;
- (iv) Ensure that the engagement of vendors for the provision of information and cyber security risk management services complies with the required technical requirements;
- (v) Issue technical opinions on requests, questions, and needs not addressed in formal procedures;
- (vi) Test the effectiveness of the information and cyber security controls used and inform managers of residual risks. Agree with managers on the level of service to be provided and the procedures for responding to information and cyber security incidents;

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

- (vii) Segregate administrative and operational functions in order to restrict each individual's powers to the minimum necessary and eliminate, or at least reduce, the existence of individuals who could delete the logs and audit trails of their own actions;
- (viii) Work with the technology area, providing direct advice on defining Information Security requirements for the installation of all operating systems used by Base Clearing;
- (ix) Ensure that internal regulations on information and cyber security are implemented and duly disclosed internally;
- (x) Ensure the Information and Cyber Security awareness and training program;
- (xi) Provide support to the second and third lines of defense (the Risk, Compliance, and Internal Controls Area and the Internal Audit, respectively) in their respective review work, ensuring that the recommended corrective actions identified in the reviews are duly implemented; and
- (xii) Ensure that vulnerability testing plans are implemented and testing schedules are programmed in accordance with business criticalities.

3. Information Technology Service Management

Information Technology Service Management is structured based on best practices established in frameworks, such as ITIL and COBIT, ensuring stable, predictable, secure operations aligned with business needs. The model includes formal processes that ensure control, traceability, and quality in the delivery of technology services.

The main processes that make up this structure and their respective objectives are listed below and are reinforced by other internal regulations, such as: the Incident Response Policy, the Information and Cyber Security Policy, and the Business Continuity Policy.

- (i) Incident Management: quickly restores affected services, minimizing operational impact;
- (ii) Problem Management: identifies root causes and implements permanent fixes to prevent recurrences;
- (iii) Change Management: controls and approves changes in a secure, documented, and traceable manner;
- (iv) Release and Deployment Management: controls deployments and versions, ensuring secure and consistent releases;

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

- (v) Configuration Management (CMDB): maintains an inventory of assets and their relationships, ensuring traceability;
- (vi) Service Request Management: handles standard requests with agility and standardization;
- (vii) Service Level Management: defines, monitors, and reports service level indicators to ensure quality and predictability;
- (viii) Capacity and Performance Management: ensures that technology resources support current and future demands;
- (ix) Availability Management: ensures continuous operation through redundancy and monitoring strategies;
- (x) Service Continuity Management: integrates IT with the Business Continuity Policy, defines RTO/RPO, and conducts periodic DR testing;
- (xi) Vendor Management: monitors the quality, risks, and performance of critical third parties; and
- (xii) Observability and Monitoring Management: collects metrics, logs, and traces to identify failures and support operational decisions.

4. Policies and Regulations

The policies, regulations, and other internal regulations are essential for formalizing the principles, guidelines, and practices for managing the technology resources and operational efficiency of the technology systems of **Base Clearing**. These internal regulations, as well as the strategic guidelines for technology management, **are** submitted for approval by the Collegiate Executive Board **and** reviewed periodically, **whenever there are changes in the regulatory framework, significant changes in the technology architecture, relevant changes in the institution's technology risk profile**, among other possible triggers.

III. Systems Architecture

1. Overview

Base Clearing's technology architecture is event-driven and has, as its central element, a message bus that acts as its backbone. Based on this logical structure, both internal services and integrations with the external ecosystem publish and consume events following previously defined communication standards, which significantly reduces coupling between components and favors the continuous evolution of the system.

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

As it is based on asynchronous, event-driven communication, the solution allows for real-time reaction, as well as failure isolation – preventing the unavailability of one service from affecting the others – and independent horizontal scalability of services, with load balancing and capacity increases per component.

Additionally, the persisted event log – maintained in accordance with retention policies – enables end-to-end traceability, control over reprocessing, and auditability, in addition to improving operational observability, allowing real-time visibility of events for proactive diagnosis.

In terms of evolution and versioning, separation by services and event contracts favors independent updates of components and progressive changes, reducing the need for extensive maintenance windows.

2. Components

Base Clearing's technology architecture is systematized based on the functional segregation between two main pillars of the modular structure. At the center of the design are the internal components, modules dedicated to handling business operational rules, such as the registration, settlement, and guarantee management modules. Peripheral to the center are the edge components, responsible for the intermediation and adaptation of interfaces with Participants and Market Infrastructures, including input validations, security controls, and transformation of messages between external API contracts – frequently XML – and the standardized internal communication patterns, allowing data traffic to occur with proper validation before being processed internally.

2.1. Communication Between Components

2.1.1. Synchronous Integrations via HTTP/HTTPS

With respect to the components involved in the API interface – Web API, Registration, and State Manager –, communication is carried out via the HTTPS protocol with application credentials. This guideline ensures end-to-end encryption in transport, preserving the confidentiality of requests and preventing the interception or tampering of data by unauthorized third parties.

With specific respect to the internal Registration and State Manager modules, data both in transit and at rest are protected throughout their entire lifecycle through the Database, with authentication and encryption.

With respect to synchronous integrations between components, communication may occur via HTTP over TLS (HTTPS). Where applicable, service-to-service authentication is used through application credentials

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

(for example, *client credentials*, certificates/mTLS, or service *tokens*), in accordance with the adopted access control policies.

The use of TLS (HTTPS) provides encryption in transport and communication integrity, reducing the risk of interception and alteration of data in transit by unauthorized agents, provided that good configuration practices are observed – such as secure versions and *ciphers*, certificate validation, and key rotation.

2.1.2. Internal Services

Communication among the internal modules occurs through the production/consumption of events on the message bus. Access to the cluster is restricted to a segregated and controlled internal network, with authentication and authorization per component for publishing and consuming.

3. Application Scalability

Base Clearing's systems architecture promotes the effectiveness of the resilience and continuity plan through the classification of components according to the management of their internal state. Accordingly, modules are distinguished between Multi-Instance – components capable of horizontal scalability and load distribution among instances – and Non-Multi-Instance – components that require a single instance handling the entire load.

3.1. Multi-Instance Components

Because they are Multi-Instance, automatic scaling in the number of instances is possible based on processing consumption, with the load distributed across multiple instances. In addition, the strategy based on Active-Active redundancy allows that, in the event of an occurrence causing unavailability in one or more instances, traffic be redistributed to the active instances, ensuring continuity of operation.

3.2. Non-Multi-Instance Components

In view of operational requirements, such as the need for sequential processing, certain components have only one active instance that handles the entire load. In this case, each of these components is periodically subjected to load tests that simulate historical market records, to ensure satisfactory performance even with a single instance. Thus, the redundancy mechanism is Active-Passive for the following components:

- (i) Trading Connector;
- (ii) Reserve Pilot; and
- (iii) Depository Connector.

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

IV. Technology Infrastructure Architecture

1. Overview

Base Clearing's technology infrastructure architecture was designed to allocate workloads according to their specific performance and latency requirements. Accordingly, all services classified as critical and requiring low latency will run in two data centers, ensuring geographic diversity and reducing the correlation of operational risks. The infrastructure of these environments is optimized to support time-response-sensitive operations, contributing significantly to the reduction of operational risks related to performance.

Services that do not depend on low latency, as well as running applications that benefit from elasticity, scalability, and on-demand capacity, will be maintained in the cloud computing environment.

The integration between the *on-premises* environment and the cloud infrastructure will be established through secure, redundant connections, ensuring efficient and resilient communication between the environments. In addition, continuous monitoring and control mechanisms will ensure operational visibility, consistent performance, and full coordination between local and cloud resources.

Lastly, the Rio de Janeiro office will house the teams responsible for the operations center and support of the production environment, ensuring governance, monitoring, and rapid incident response.

2. Cloud Computing

The cloud computing environment was designed to ensure high availability, operational resilience, and business continuity. The infrastructure will be distributed across the three availability zones available in Brazil, ensuring fault tolerance through physical, power, and network isolation between zones. This strategy allows services to continue operating even in the event of localized outages in any of the zones.

In addition, the environment will have synchronous replication between availability zones, ensuring that data is written simultaneously in multiple locations, preserving the consistency and integrity of information in real time. This approach eliminates the risk of data loss and keeps the environment ready for immediate *failover*.

This will result in a robust, scalable cloud architecture aligned with resilience best practices, supporting critical operations with stable performance and advanced protection against outages.

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

3. Data Centers

The on-premises environment will operate in two geographically distributed Data Centers, ensuring operational resilience and continuity of services even in scenarios of localized unavailability. The infrastructure will be composed of dedicated cages, designed to fully meet the institution's technological needs. These cages have exclusive access controls, biometrics, physical keys, and CCTV monitoring, ensuring enhanced physical protection of the environment.

Another essential element of the architecture is distance equity between cabling, achieved through fiber route equalization techniques and balanced distribution of the infrastructure. This approach ensures that all participants operate under equivalent technical conditions, avoiding latency asymmetries arising from physical location within the Data Center.

4. Head Office

Base Clearing's head office will be responsible for the operations center and support of the production environment. The site will have its own Data Processing Center ("CPD"), equipped with UPS units in parallel, ensuring redundancy and greater autonomy capacity, in addition to its own generator to maintain operations during prolonged outages. Connectivity will be redundant, provided by different carriers with independent physical routes, ensuring high availability and continuity of critical services.

5. Connectivity and Interconnections

5.1. Overview

Base Clearing's connectivity and interconnection architecture was designed to ensure high availability, low latency, operational resilience, and secure communication among all components of the technology environment, spanning Data Centers, cloud, and the corporate office.

The interconnection between the on-premises environments and the cloud infrastructure is carried out through dedicated, redundant channels distributed across distinct physical routes, ensuring operational continuity even in the event of carrier, link, or equipment failures. This connectivity model enables efficient, stable communication between critical applications, in addition to supporting synchronous replications, data synchronization, and latency-sensitive traffic flows.

In an integrated manner, the connectivity architecture adopts the following fundamental principles:

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

- (i) Redundancy: multiple links and carriers, with distinct paths;
- (ii) Low Latency: optimized connections between *Data Centers* and the cloud for critical *workloads*;
- (iii) Security: private interconnections, end-to-end encryption, and network segmentation;
- (iv) Resilience: fault tolerance at the network layer, telecommunications carrier circuits, and transport;
- (v) Scalability: capacity for bandwidth expansion and new points of presence as demand requires; and
- (vi) Centralized Management: integrated operation via the Operations Center, with continuous monitoring and traffic observability.

5.2. Modes of Access to the Technology Infrastructure:

Participants may establish connectivity to Base Clearing's systems through different technological solutions, selected in accordance with the guidelines and requirements set forth in the Connectivity Manual. The available access modes are as follows:

- (i) *Cross Connect*;
- (ii) *Fabric*;
- (iii) Dedicated Circuit;
- (iv) Internet VPN (Unicast and Multicast); and
- (v) RTM - Telecommunications Network for the Market.

5.3. Interconnection with the Central Bank

Communication with the Central Bank will be established through a direct connection to the National Financial System Network (RSFN), using the connectivity architecture classified under Routing Profile D. This infrastructure incorporates a high-availability model composed of the *Hot Standby Router Protocol* (HSRP) distributed among four *Customer Premises Equipment* (CPEs), located at two distinct sites – the primary environment and the contingency environment. The primary and secondary *Data Centers* will have redundant links and dedicated CPEs per carrier, ensuring redundancy, operational continuity, and high robustness in Base Clearing's critical communications.

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

5.4. Interconnection with B3

Communication with B3's Central Depository will be established through the B3 Extranet, using the SMP (FIX) protocol. This arrangement ensures dedicated, secure, low-latency connectivity for message traffic and for the necessary operational integrations. The primary and secondary *Data Centers* will have redundant links and dedicated routers per telecommunications carrier, ensuring operational continuity and a high level of robustness in communications.

6. Monitoring, Logs and Observability

Base Clearing maintains a robust structure for monitoring, log collection, and observability to ensure operational continuity, incident detection, and compliance with regulatory requirements, in line with the regulatory guidelines related to operational resilience and information security.

Monitoring operates 24x7 – uninterrupted, 24 hours a day, 7 days a week, covering the availability, performance, and capacity of critical services, with automatic alerts and centralized *dashboards* for rapid failure identification. Observability must integrate metrics, *logs*, and *traces*, enabling in-depth analysis and identification of root causes of incidents.

The management of logs must ensure centralized collection, retention appropriate to criticality, protection against alteration, encryption in transit and at rest, and access controls based on least privilege. Enhanced protection includes the use of immutable *logs* when necessary.

All relevant events must be integrated into the security ecosystem for correlation and threat detection, supporting the cybersecurity practices set forth in BCB Resolution 304.

7. Backup, Restoration, and Data Protection

The backup strategy will be structured to meet business continuity and operational resilience requirements. Critical data and systems will have full and incremental backup routines, stored in isolated, secure environments, ensuring protection against failures, outages, and cyber events.

The adopted backup model will enable rapid recovery and limitation of losses, aligned with the continuity management practices set forth in BCB Resolution 304, which requires mechanisms capable of preserving the integrity of operations even in crisis situations. In addition, the process will include restoration tests, at least annually, ensuring that recovery occurs within the RTO and RPO timeframes defined by the SGCN.

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

The backup solution will be integrated with the Incident Response Plan and with the information security structures, ensuring adherence to the governance, internal controls, and risk management guidelines set forth in external instruments, principally BCB Resolution 304. This approach ensures a resilient environment, capable of quickly restoring its operations and minimizing operational impacts.

Additional security measures, such as encryption, access controls based on the principle of least privilege, integrity validation, and the use of immutability technologies, are applied to ensure the reliability, integrity, and availability of the organization's critical information.

8. Testing and Audits

The testing and audit processes are intended to ensure the effectiveness, integrity, and adherence of the technological, operational, and security controls implemented by the institution. To this end, simulations of operational incidents, validations of continuity and recovery plans, cybersecurity assessments, and reviews of the change management process will be conducted.

Internal and external audits complement these activities, verifying compliance with corporate policies, applicable regulatory requirements, and the effectiveness of control mechanisms. Audit results are formally recorded and submitted to the competent governance bodies, accompanied by action plans aimed at promoting adjustments, corrections, and the continuous improvement of the processes assessed.

Thus, the audits and integrity tests, reflected in reports issued at least annually, ensure the reliability of the environment and support compliance with the regulatory requirements applicable to financial market systems infrastructure.

Restoration and integrity tests are conducted by the Testing Area (which reports to the Technology Director) and are carried out with the support of Base Clearing's business and corporate areas, it being noted that the principles and guidelines for continuity testing are established and monitored by the RCC Area.

V. General Provisions

This Plan was approved by Base Clearing's Collegiate Executive Board and is in effect as of the date of its approval.

The proprietary area responsible for supporting the preparation and review of this Plan is the Information Technology Area. This Plan will be reviewed at least annually and may be amended at any time by resolution of Base Clearing's Collegiate Executive Board. This Plan and any amendments thereto will be disclosed on

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.

INFORMATION TECHNOLOGY AREA			
IT INFRASTRUCTURE AND IT SERVICE MANAGEMENT PLAN			
CLEARING-TI-PLANO-01	VERSION: 1.0	DATE: 04/22/2026	CLASSIFICATION: PUBLIC

the Base Website, through clear, accessible language and at a level of detail compatible with the functions performed and the sensitivity of the information.

Omitted cases and questions of interpretation relating to this Plan will be addressed by the Collegiate Executive Board, in accordance with applicable law and the Base Rules.

Should any provision of this Plan be deemed invalid, illegal, or ineffective, that provision will be limited to the extent possible so that the validity, legality, and effectiveness of the remaining provisions of this Plan are not affected or impaired.

In the event of a conflict between the provisions of this Plan and Base Clearing's other rules, the more specific rule shall prevail, considering the subject matter in conflict. In the event of a conflict between the provisions of this Plan and Base Clearing's Bylaws, the Bylaws shall prevail. In the event of a conflict between the provisions of this Plan and applicable legislation and regulations, the applicable legislation and regulations shall prevail.

This document represents a preliminary version and remains subject to regulatory review and approval.

This document is an English translation of the original document, which was drafted in Portuguese. It is provided for informational and convenience purposes only. In the event of any divergence, inconsistency, discrepancy or conflict between the English version and the Portuguese version, the Portuguese-language original document shall prevail and shall be deemed the sole official and legally binding version.