

base CLEARING

Plano de Infraestrutura Tecnológica e Gestão de Serviços de Tecnologia da Informação

Sujeito à aprovação regulatória

Registro de Versões

Versão	Data de Aprovação	Órgão Aprovador	Ofício Circular*
1.0	22/04/2026	Diretoria Colegiada	Não aplicável.

* Ofício Circular por meio do qual a alteração foi divulgada.

Sumário

I.	Introdução.....	1
II.	Governança da Tecnologia da Informação.....	2
1.	Visão Geral.....	2
2.	Papéis e Responsabilidades.....	3
3.	Gestão de Serviços de Tecnologia da Informação.....	6
4.	Políticas e Normas.....	8
III.	Arquitetura de Sistemas.....	8
1.	Visão Geral.....	8
2.	Componentes.....	8
2.1.1.	Integrações síncronas via HTTP/HTTPS.....	9
2.1.2.	Serviços internos.....	9
3.	Escalabilidade das Aplicações.....	10
IV.	Arquitetura de Infraestrutura Tecnológica.....	10
1.	Visão Geral.....	10
2.	Computação em Nuvem.....	11
3.	<i>Data Centers</i>	11
4.	Sede Principal.....	12
5.	Conectividade e Interconexões.....	12
6.	Monitoramento, <i>Logs</i> e Observabilidade.....	14
7.	<i>Backup</i> , Restauração e Proteção dos Dados.....	14
8.	Testes e Auditorias.....	15
V.	Disposições Gerais.....	15

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

I. Introdução

O presente Plano de Infraestrutura Tecnológica e Gestão de Serviços de Tecnologia da Informação (“**Plano**”) da Base Clearing tem como finalidade assegurar que as necessidades operacionais, estratégicas e regulatórias da Base Clearing sejam atendidas de forma eficaz, eficiente e alinhada aos instrumentos normativos internos e externos, princípios corporativos, responsabilidades estabelecidas e diretrizes formais de gestão de serviços de TI. Esse alinhamento é essencial para atender às exigências da Resolução BCB 304 que estabelece requisitos relacionados à resiliência operacional, à gestão de serviços de tecnologia, à segurança da informação, à continuidade de negócios e à governança das infraestruturas críticas de mercado financeiro.

O Plano foi desenvolvido de maneira compatível com a natureza, o porte, a complexidade, a estrutura organizacional e o perfil de risco da Base Clearing, refletindo práticas modernas de governança e padrões regulatórios inspirados nos Princípios para Infraestruturas do Mercado Financeiro (“**PFMI**”) incorporados pela Resolução BCB 304. Assim, o Plano orienta a gestão tecnológica da Base Clearing com base nos seguintes princípios fundamentais:

- Resiliência operacional, assegurando que a infraestrutura tecnológica suporte adequadamente as operações críticas e mantenha continuidade diante de falhas ou eventos adversos;
- Segurança da informação e cibernética, com políticas, controles e mecanismos de proteção alinhados às exigências regulatórias e às melhores práticas internacionais;
- Gestão estruturada de riscos, com identificação, avaliação, mitigação e monitoramento contínuo dos riscos associados à TI, aos provedores terceirizados e aos serviços essenciais;
- Eficiência e qualidade na gestão de serviços de TI, fundamentada em processos padronizados e melhores práticas reconhecidas, como a ABNT NBR ISO/IEC 20000-1; e
- Governança, transparência e conformidade regulatória, assegurando aderência integral às exigências do Banco Central e às políticas internas da Base Clearing.

Os termos iniciados em letra maiúscula e utilizados neste Plano que não estejam aqui definidos, têm o significado a eles atribuído no Glossário ou, alternativamente, se referem a termos usualmente utilizados no contexto da tecnologia da informação.

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

II. Governança da Tecnologia da Informação

1. Visão Geral

Para fins de governança corporativa, incluindo para governança da gestão de tecnologia da informação ("Governança de TI"), a Base Clearing adota o modelo de 3 (três) linhas de defesa, sendo:

- (i) 1ª Linha de Defesa: é representada por todas as áreas jurídica, financeira, operações, tecnologia e demais áreas de negócio e corporativas da Base Clearing (excluídas as Áreas de RCC, Segurança de Informação e Cibernética e Auditoria Interna), as quais devem assegurar a efetiva gestão de riscos, por meio da definição, operacionalização e aprimoramento de práticas e controles, dentro do escopo das suas responsabilidades organizacionais diretas ("1ª Linha de Defesa"). Cabe aos integrantes da 1ª Linha de Defesa reportar ao Comitê Interno de Riscos e à Área de RCC os Eventos de Riscos Materiais e/ou Recorrentes, ou que não estejam em consonância com as diretrizes e limite de riscos estabelecidos pela Base Clearing.
- (ii) 2ª Linha de Defesa: é representada principalmente pelas Áreas de RCC e Segurança da Informação e Cibernética ("2ª Linha de Defesa"), que são as principais estruturas que atuam junto à 1ª Linha de Defesa e às quais compete a implementação das políticas e procedimentos voltados ao gerenciamento de riscos, conformidade, controles internos e continuidade de negócios, além de assegurar a comunicação acerca do tema junto ao Comitê Interno de Riscos, à Diretoria Colegiada, à Auditoria Interna e à Assembleia Geral da Base Clearing, esta última por meio do Comitê de Auditoria (quanto instalado).
- (iii) 3ª Linha de Defesa: é representada pela Auditoria Interna ("3ª Linha de Defesa"), a qual se reporta à Diretoria Colegiada e à Assembleia Geral da Base Clearing, esta última por meio do Comitê de Auditoria (quando instalado). A Auditoria Interna tem como principais responsabilidades prover avaliações independentes e objetivas sobre os processos de governança corporativa e gerenciamento de riscos e controles internos.

A adoção do modelo de 3 (três) linhas de defesa otimiza o processo de tomada de decisão e as respostas aos riscos inerentes à tecnologia da informação, por meio da definição de papéis e responsabilidades que atuam de forma coordenada para assegurar o alinhamento entre a gestão da tecnologia da informação e a estratégia da Base Clearing.

Adicionalmente, para definição dos princípios, diretrizes e procedimentos relacionados à gestão de tecnologia da informação são consideradas as exigências e boas práticas estabelecidas em instrumentos

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

normativos e *frameworks*, tais como: Resolução BCB 304, *Information Technology Infrastructure Library* ("ITIL") e *Control Objectives for Information and Related Technology* ("COBIT").

2. Papéis e Responsabilidades

A Governança de TI da Base Clearing é estruturada com funções claramente definidas, assegurando segregação de funções, rastreabilidade e supervisão adequada dos processos tecnológicos. Os principais papéis são:

2.1. Diretor de Tecnologia

São responsabilidades do Diretor de Tecnologia as seguintes atividades:

- (i) Gerir os recursos de tecnologia e a eficiência operacional dos sistemas de tecnologia da Base Clearing;
- (ii) Zelar pela elaboração e implementação de políticas e demais normativos internos relacionados à tecnologia da informação, responsabilizando-se pela definição de estratégia, desenvolvimento e implementação de sistemas e soluções em consonância com as necessidades do negócio da Base Clearing; e
- (iii) Gerir e administrar o departamento de tecnologia da Companhia.

2.2. Área de Infraestrutura

São responsabilidades da Área de Infraestrutura, que integra a Área de Tecnologia da Informação, as seguintes atividades:

- (i) Ser responsável pela gestão da infraestrutura híbrida da Base Clearing (*on-premises* e nuvem);
- (ii) Supervisionar a disponibilidade, capacidade, performance e continuidade dos ambientes;
- (iii) Coordenar os times responsáveis pela operação de tecnologia e monitoramento contínuo dos ambientes; e
- (iv) Apoiar na elaboração e revisão deste Plano.

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

2.3. Área de Desenvolvimento

São responsabilidades da Área de Desenvolvimento, que integra a Área de Tecnologia da Informação, as seguintes atividades:

- (i) Planejar, coordenar e supervisionar todas as fases de desenvolvimento de *software*; e
- (ii) Garantir que as definições funcionais e técnicas estejam alinhadas às necessidades de negócio e aos requisitos regulatórios.

2.4. Área de Testes

São responsabilidades da Área de Testes, que integra a Área de Tecnologia da Informação, as seguintes atividades:

- (i) Definir a estratégia corporativa de testes (funcionais, integrados, regressão, carga, segurança e homologação regulatória);
- (ii) Garantir que o escopo de testes cubra os requisitos técnicos, funcionais e regulatórios; e
- (iii) Conduzir testes estruturados com documentação adequada (planos, *scripts* e evidências).

2.5. Área de Riscos, Conformidade e Controles Internos

Será de responsabilidade dos colaboradores da Área de RCC as seguintes atividades atreladas à gestão de infraestrutura e serviço de tecnologia da informação (eventualmente com auxílio de assessoria jurídica especializada, conforme necessário):

- (i) Ser responsável pelas atividades de gestão de: (a) riscos, conformidade e controles internos, (b) PLD-FTP, e (c) continuidade de negócios, reforçadas neste Plano e em demais normativos internos, dentre eles: (1) Política de Continuidade de Negócios, (2) Plano de Recuperação e Recomposição de Salvaguardas, (3) Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa, (4) Política de Gestão de Fraudes, (5) Política de Contratação, Gestão de Risco e Monitoramento de Terceirização de Serviços e (6) Código de Conduta Ética;
- (ii) Promover a cultura de gestão de riscos, conformidade e controles internos, incluindo uma cultura organizacional que incentive condutas éticas e o compromisso da Base Clearing com o cumprimento das regulamentações e leis vigentes;

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

- (iii) Estabelecer princípios, diretrizes e práticas a serem adotadas, bem como implementar processo contínuo, integrado e abrangente para a gestão de riscos, conformidade e controles internos da Base Clearing, incluindo a proposta de criação ou alteração de normativos internos, em linha com este Plano e em conformidade com instrumentos normativos internos e externos aplicáveis, tais como: Resolução BCB 304 e a Instrução Normativa BCB nº 374;
- (iv) Estabelecer e conduzir, em conjunto com as demais áreas internas, procedimentos para definição, aprovação, reporte e monitoramento dos tratamentos aos riscos identificados pela Base Clearing, promovendo transparência e governança;
- (v) Testar e avaliar a aderência da Base Clearing ao arcabouço legal, à regulamentação infralegal, às recomendações dos órgãos de supervisão e, quando aplicável, aos normativos internos, inclusive ao Código de Conduta Ética; e
- (vi) Elaborar, em conjunto com o Diretor de Supervisão, os relatórios de avaliação do funcionamento e eficácia do sistema de gerenciamento de riscos, controles internos e conformidade, incluindo o relatório anual de riscos, controles internos e conformidade, e considerando os resultados dos testes de continuidade de negócios.

2.6. Área de Segurança da Informação e Cibernética

A Área de Segurança da Informação e Cibernética é a responsável pela ação e resposta aos Incidentes de Segurança da Informação e Cibernética.

São responsabilidades da Área de Segurança da Informação as seguintes atividades atreladas à gestão de infraestrutura e serviço de tecnologia da informação:

- (i) Elaborar e atualizar o Plano de Resposta a Incidentes, com enfoque em incidentes relacionados à Segurança da Informação e Cibernética;
- (ii) Propor investimentos relacionados à segurança da informação e cibernética, com o objetivo principal de mitigar riscos;
- (iii) Controlar e estruturar a gestão em Segurança da Informação e controles de cibersegurança da Base Clearing, propondo as diretrizes técnicas adequadas às necessidades do negócio e requerimentos regulatórios;

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

- (iv) Assegurar que a contratação de fornecedores para prestação de serviços para gestão de riscos da segurança da informação e cibernética cumpram os requisitos técnicos exigidos;
- (v) Emitir pareceres técnicos relativos a solicitações, dúvidas e necessidades não previstas em procedimentos formais;
- (vi) Testar a eficácia dos controles de segurança da informação e cibernética utilizados e informar aos gestores os riscos residuais. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes de segurança da informação e cibernética;
- (vii) Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;
- (viii) Trabalhar com a área de tecnologia provendo consultoria direta na definição dos requerimentos de Segurança da Informação para instalação de todos os sistemas operacionais utilizados pela Base Clearing;
- (ix) Assegurar que os normativos internos sobre segurança da informação e cibernética estejam implementados e devidamente divulgados internamente;
- (x) Garantir o programa de conscientização e treinamentos de Segurança da Informação e Cibernética;
- (xi) Prover suporte segunda e à terceira linhas de defesa (Área de Riscos, Conformidade e Controles Internos e Auditoria Interna, respectivamente) nos respectivos trabalhos de revisões dessas áreas, assegurando que as recomendações de ações de correções identificadas nas revisões sejam devidamente implementadas; e
- (xii) Assegurar que os planos de testes de vulnerabilidades estejam implementados e as agendas de testes programadas de acordo com as criticidades dos negócios.

3. Gestão de Serviços de Tecnologia da Informação

A Gestão de Serviços de Tecnologia da Informação é estruturada com base em boas práticas estabelecidas em *frameworks*, tais como ITIL e COBIT, assegurando uma operação estável, previsível, segura e alinhada às necessidades do negócio. O modelo contempla processos formais que garantem controle, rastreabilidade e qualidade na entrega dos serviços tecnológicos.

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

Os principais processos que compõem essa estrutura e respectivos objetivos estão listados abaixo e são reforçados por demais normativos internos, tais como: Política de Resposta a Incidentes, Política de Segurança da Informação e Cibernética e Política de Continuidade de Negócios.

- (i) Gestão de Incidentes: restaura rapidamente serviços afetados, minimizando impacto operacional;
- (ii) Gestão de Problemas: identifica causas raízes e implementa correções definitivas para evitar recorrências;
- (iii) Gestão de Mudanças: controla e aprova alterações de forma segura, documentada e rastreável;
- (iv) Gestão de Liberações e Deploy: controla implantações e versões, garantindo entregas seguras e consistentes;
- (v) Gestão de Configuração (CMDB): mantém inventário dos ativos e suas relações, garantindo rastreabilidade;
- (vi) Gestão de Requisições de Serviço: trata solicitações padrão com agilidade e padronização;
- (vii) Gestão de Nível de Serviço: define, monitora e reporta os indicadores de nível de serviço para garantir qualidade e previsibilidade;
- (viii) Gestão de Capacidade e Desempenho: assegura que os recursos tecnológicos suportem as demandas atuais e futuras;
- (ix) Gestão de Disponibilidade: garante operação contínua por meio de estratégias de redundância e monitoramento;
- (x) Gestão de Continuidade de Serviços: integra TI à Política de Continuidade de Negócios, define RTO/RPO e conduz testes periódicos de DR;
- (xi) Gestão de Fornecedores: monitora qualidade, riscos e desempenho de terceiros críticos; e
- (xii) Gestão de Observabilidade e Monitoramento: coleta métricas, *logs* e *traces* para identificar falhas e apoiar decisões operacionais.

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

4. Políticas e Normas

As políticas, regulamentos e demais normativos internos são fundamentais para a formalização dos princípios, diretrizes e práticas para gestão dos recursos de tecnologia e da eficiência operacional dos sistemas de tecnologia da **Base Clearing**. Esses normativos internos, bem como as diretrizes estratégicas para gestão de tecnologia, **são** submetidos à aprovação da Diretoria Colegiada e revisados periodicamente, **sempre que ocorrerem alterações no arcabouço regulatório, modificações significativas na arquitetura tecnológica, mudanças relevantes no perfil de risco tecnológico da instituição**, dentre outros possíveis motivadores.

III. Arquitetura de Sistemas

1. Visão Geral

A arquitetura tecnológica da Base Clearing é orientada a eventos e tem como elemento central um barramento de mensagens que atua como sua espinha dorsal. A partir dessa estrutura lógica, tanto os serviços internos quanto as integrações com o ecossistema externo passam a publicar e consumir eventos seguindo padrões de comunicação previamente definidos, o que reduz significativamente o acoplamento entre componentes e favorece a evolução contínua do sistema.

Em se tratando de comunicação assíncrona por eventos, a solução permite a reação em tempo real, bem como o isolamento de falhas – impedindo que a indisponibilidade de um serviço afete os demais – e a escalabilidade horizontal independente dos serviços, com balanceamento e incremento de capacidade por componente.

Adicionalmente, o *log* persistido de eventos – mantido conforme políticas de retenção – viabiliza a rastreabilidade ponta a ponta, o controle de reprocessamentos e a auditabilidade, além de aprimorar a observabilidade operacional, permitindo a visibilidade de eventos em tempo real para diagnóstico proativo.

Em termos de evolução e versionamento, a separação por serviços e contratos de eventos favorece as atualizações independentes dos componentes e mudanças progressivas, mitigando a necessidade de janelas de manutenção amplas.

2. Componentes

A arquitetura tecnológica da Base Clearing é sistematizada com base na segregação funcional entre dois pilares principais da estrutura modular. No centro do desenho, residem os componentes internos, módulos dedicados ao tratamento das regras operacionais de negócio, como os módulos de cadastro, liquidação e

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

gestão de garantias. Periférico ao centro, encontram-se os componentes de borda, responsáveis pela intermediação e adaptação de interfaces com Participantes e Infraestruturas de Mercado, incluindo validações de entrada, controles de segurança e transformação de mensagens entre contratos de API externos – frequentemente XML – e os padrões de comunicação internos padronizados, permitindo que o tráfego de dados ocorra com a devida validação antes de serem processados internamente.

2.1. Comunicação entre Componentes

2.1.1. Integrações síncronas via HTTP/HTTPS

No âmbito dos componentes envolvidos na interface de API – Web API, Cadastro e Gerenciador de Estado –, a comunicação é realizada via protocolo HTTPS com credenciais de aplicação. Esta diretriz assegura a criptografia ponta-a-ponta no transporte, preservando a confidencialidade das requisições e impedindo a interceptação ou adulteração de dados por terceiros não autorizados.

No que se refere especificamente aos módulos internos de Cadastro e Gerenciador de Estado, tanto os dados em trânsito como aqueles em repouso são protegidos em seu ciclo completo de vida através do Banco de Dados com autenticação e criptografia.

No âmbito das integrações síncronas entre componentes, a comunicação pode ocorrer via HTTP sobre TLS (HTTPS). Quando aplicável, utiliza-se autenticação entre serviços por credenciais de aplicação (por exemplo, *client credentials*, certificados/mTLS ou *tokens* de serviço), em conformidade com as políticas de controle de acesso adotadas.

O uso de TLS (HTTPS) provê criptografia no transporte e integridade da comunicação, reduzindo o risco de interceptação e alteração de dados em trânsito por agentes não autorizados, desde que observadas boas práticas de configuração – como versões e *ciphers* seguros, validação de certificado e rotação de chaves.

2.1.2. Serviços internos

A comunicação dos módulos internos ocorre via produção/consumo de eventos no barramento de mensagens. O acesso ao cluster é restrito a uma rede interna segregada e controlada, com autenticação e autorização por componente para publicação e consumo.

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

3. Escalabilidade das Aplicações

A arquitetura de sistemas da Base Clearing promove a eficácia do plano de resiliência e continuidade por meio da tipificação dos componentes quanto à gestão do seu estado interno. Assim, os módulos são distinguidos entre Multi-instanciáveis – componentes aptos à escalabilidade horizontal e à distribuição de carga entre as instâncias – e Não Multi-instanciáveis – componentes que exigem a execução singular que lida com toda a carga.

3.1. Componentes Multi-instanciáveis

Por serem Multi-instanciáveis, é possível a escalabilidade automática em número de instâncias mediante consumo de processamento, sendo a carga distribuída em múltiplas instâncias. Além disso, a estratégia fundamentada em redundância Ativo-Ativo permite que, mediante evento que cause indisponibilidade em uma ou mais instâncias, o tráfego seja redistribuído para as instâncias ativas, garantindo continuidade de operação.

3.2. Componentes Não Multi-instanciáveis

Tendo em vista exigências operacionais, como necessidade de processamento sequencial, determinados componentes possuem apenas uma instância ativa que lida com toda a carga. Nesse caso, cada um desses componentes é submetido periodicamente a testes de carga que simulam recordes históricos de mercado, para garantir a performance satisfatória mesmo com uma instância. Assim, o mecanismo de redundância é Ativo-Passivo para os seguintes componentes:

- (i) Conector negociação;
- (ii) Piloto de Reserva; e
- (iii) Conector Depositária.

IV. Arquitetura de Infraestrutura Tecnológica

1. Visão Geral

A arquitetura de infraestrutura tecnológica da Base Clearing foi planejada para alocar as cargas de trabalho conforme suas necessidades específicas de desempenho e latência. Dessa forma, todos os serviços classificados como críticos e que exigem baixa latência serão executados em dois *data centers*, garantindo diversidade geográfica e reduzindo a correlação de riscos operacionais. A infraestrutura desses ambientes é

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

otimizada para suportar operações sensíveis a tempo de resposta, contribuindo significativamente para a redução de riscos operacionais relacionados à performance.

Os serviços que não dependem de baixa latência, bem como aplicações em execução que se beneficiam de elasticidade, escalabilidade e capacidade sob demanda, serão mantidos no ambiente de computação em nuvem.

A integração entre o ambiente *on-premises* e a infraestrutura em nuvem será estabelecida por meio de conexões seguras e redundantes, garantindo comunicação eficiente e resiliente entre os ambientes. Além disso, mecanismos contínuos de monitoramento e controle assegurarão visibilidade operacional, desempenho consistente e coordenação plena entre os recursos locais e em nuvem.

Por fim, o escritório do Rio de Janeiro abrigará as equipes responsáveis pelo centro de operações e sustentação do ambiente produtivo, assegurando governança, monitoramento e resposta rápida a incidentes.

2. Computação em Nuvem

O ambiente de computação em nuvem foi projetado para garantir alta disponibilidade, resiliência operacional e continuidade do negócio. A infraestrutura será distribuída nas três zonas de disponibilidade disponíveis no Brasil, assegurando tolerância a falhas por meio de isolamento físico, energético e de rede entre as zonas. Essa estratégia permite que os serviços continuem operando mesmo diante de interrupções localizadas em qualquer uma das zonas.

Além disso, o ambiente contará com replicação síncrona entre as zonas de disponibilidade, garantindo que os dados sejam gravados simultaneamente em múltiplos locais, preservando consistência e integridade das informações em tempo real. Essa abordagem elimina riscos de perda de dados e mantém o ambiente pronto para *failover* imediato.

Com isso, teremos uma arquitetura em nuvem robusta, escalável e alinhada às melhores práticas de resiliência, suportando operações críticas com desempenho estável e proteção avançada contra indisponibilidades.

3. Data Centers

O ambiente *on-premises* operará em dois Data Centers geograficamente distribuídos, assegurando resiliência operacional e continuidade dos serviços mesmo em cenários de indisponibilidade localizada. A

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

infraestrutura será composta por cages dedicados, projetados para atender plenamente às necessidades tecnológicas da instituição. Esses cages contam com controles de acesso exclusivos, biometria, chave física, e monitoramento por CFTV, garantindo proteção física reforçada do ambiente.

Outro elemento essencial da arquitetura é a equidade de distância entre cabeamentos, obtida por meio de técnicas de equalização de rotas de fibra e distribuição balanceada da infraestrutura. Essa abordagem assegura que todos os participantes operem sob condições técnicas equivalentes, evitando assimetrias de latência decorrentes da localização física dentro do *Data Center*.

4. Sede Principal

A sede principal da Base Clearing será responsável pelo centro de operações e sustentação do ambiente produtivo. O local contará com um Centro de Processamento de Dados (“CPD”) próprio, equipado com nobreaks em paralelismo, garantindo redundância e maior capacidade de autonomia, além de um gerador próprio para manter a operação durante interrupções prolongadas. A conectividade será redundante, fornecida por operadoras distintas e com rotas físicas independentes, assegurando alta disponibilidade e continuidade dos serviços críticos.

5. Conectividade e Interconexões

5.1. Visão Geral

A arquitetura de conectividade e interconexões da Base Clearing foi concebida para garantir alta disponibilidade, baixa latência, resiliência operacional e comunicação segura entre todos os componentes do ambiente tecnológico, abrangendo *Data Centers*, nuvem e escritório corporativo.

A interconexão entre os ambientes *on-premises* e a infraestrutura em nuvem é realizada por meio de canais dedicados, redundantes e distribuídos em rotas físicas distintas, assegurando continuidade operacional mesmo em casos de falhas de operadoras, enlaces ou equipamentos. Esse modelo de conectividade permite uma comunicação eficiente e estável entre aplicações críticas, além de oferecer suporte a replicações síncronas, sincronizações de dados e fluxos de tráfego sensíveis à latência.

De forma integrada, a arquitetura de conectividade adota os seguintes princípios fundamentais:

- (i) Redundância: múltiplos enlaces e operadores, com caminhos distintos;
- (ii) Baixa Latência: conexões otimizadas entre *Data Centers* e nuvem para *workloads* críticos;

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

- (iii) Segurança: interconexões privadas, criptografia ponta a ponta e segmentação de redes;
- (iv) Resiliência: tolerância a falhas em camada de rede, circuitos de operadoras de telecomunicações e transporte;
- (v) Escalabilidade: capacidade de expansão de banda e novos pontos de presença conforme demanda; e
- (vi) Gerenciamento Centralizado: operação integrada via Centro de Operações, com monitoramento contínuo e observabilidade de tráfego.

5.2. Modalidades de Acesso à Infraestrutura Tecnológica:

Os Participantes poderão estabelecer conexão com os sistemas da Base Clearing por meio de diferentes soluções tecnológicas, selecionadas conforme as diretrizes e requisitos definidos no Manual de Conectividade. As modalidades de acesso disponibilizadas são as seguintes:

- (i) *Cross Connect*;
- (ii) *Fabric*;
- (iii) Circuito Dedicado;
- (iv) VPN Internet (Unicast e Multicast); e
- (v) RTM - Rede de Telecomunicações para o Mercado.

5.3. Interconexão com o Banco Central

A comunicação com o Banco Central será estabelecida por meio de conexão direta à Rede do Sistema Financeiro Nacional (RSFN), utilizando a arquitetura de conectividade classificada sob o Perfil de Roteamento D. Essa infraestrutura incorpora um modelo de alta disponibilidade composto por *Hot Standby Router Protocol* (HSRP) distribuído entre quatro *Customer Premises Equipments* (CPEs), alocados em dois sites distintos – ambiente principal e ambiente de contingência. Os *Data Centers* primário e secundário contarão com links redundantes e CPEs dedicados por operadora, assegurando redundância, continuidade operacional e elevada robustez nas comunicações críticas da Base Clearing.

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

5.4. Interconexão com a B3

A comunicação com a Central Depositária da B3 será estabelecida por meio da Extranet B3, utilizando o protocolo SMP (FIX). Esse arranjo assegura uma conectividade dedicada, segura e de baixa latência para o tráfego de mensagens e para as integrações operacionais necessárias. Os *Data Centers* primário e secundário contarão com links redundantes e roteadores dedicados por operadora de telecomunicações, assegurando a continuidade operacional e elevado nível de robustez nas comunicações.

6. Monitoramento, Logs e Observabilidade

A Base Clearing mantém uma estrutura robusta de monitoramento, coleta de *logs* e observabilidade para garantir a continuidade operacional, a detecção de incidentes e a conformidade com requisitos regulatórios, em linha com as diretrizes regulatórias relacionadas à resiliência operacional e segurança da informação.

O monitoramento opera 24x7 – ininterruptamente durante 24 horas por dia, 7 dias na semana, cobrindo disponibilidade, desempenho e capacidade dos serviços críticos, com alertas automáticos e *dashboards* centralizados para rápida identificação de falhas. A observabilidade deve integrar métricas, *logs* e *traces*, permitindo análises profundas e identificação de causas raízes de incidentes.

A gestão de *logs* deve assegurar coleta centralizada, retenção adequada conforme criticidade, proteção contra alterações, criptografia em trânsito e em repouso e controles de acesso baseados no menor privilégio. A proteção reforçada inclui o uso de *logs* imutáveis quando necessário.

Todos os eventos relevantes devem ser integrados ao ecossistema de segurança para correlação e detecção de ameaças, apoiando as práticas de segurança cibernética previstas na Resolução BCB 304.

7. Backup, Restauração e Proteção dos Dados

A estratégia de *backup* será estruturada para atender aos requisitos de continuidade e resiliência operacional. Os dados e sistemas críticos terão rotinas de *backup* completas e incrementais, armazenadas em ambientes isolados e seguros, garantindo proteção contra falhas, indisponibilidades e eventos cibernéticos.

O modelo de *backup* adotado permitirá recuperação rápida e limitação de perdas, alinhado às práticas de gestão de continuidade previstas na Resolução BCB 304 que exige mecanismos capazes de preservar a integridade das operações mesmo em situações de crise. Além disso, o processo incluirá testes, no mínimo anuais, de restauração, assegurando que a recuperação ocorra dentro dos prazos de RTO e RPO definidos pelo SGCN.

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

A solução de *backup* será integrada ao Plano de Resposta a Incidentes e às estruturas de segurança da informação, garantindo aderência às diretrizes de governança, controles internos e gerenciamento de riscos previstas nos instrumentos externos, principalmente a Resolução BCB 304. Essa abordagem assegura um ambiente resiliente, capaz de restaurar rapidamente suas operações e minimizar impactos operacionais.

Medidas adicionais de segurança, como criptografia, controles de acesso baseados no princípio do menor privilégio, validação de integridade e uso de tecnologias de imutabilidade, são aplicadas para garantir a confiabilidade, a integridade e a disponibilidade das informações críticas da organização.

8. Testes e Auditorias

Os processos de testes e auditoria têm como finalidade assegurar a eficácia, a integridade e a aderência dos controles tecnológicos, operacionais e de segurança implementados pela instituição. Para esse fim, serão contempladas simulações de incidentes operacionais, validações de planos de continuidade e recuperação, avaliações de segurança cibernética e revisões do processo de gestão de mudanças.

As auditorias internas e externas complementam essas atividades, verificando o cumprimento das políticas corporativas, dos requisitos regulatórios aplicáveis e da efetividade dos mecanismos de controle. Os resultados das auditorias são formalmente registrados e submetidos às instâncias de governança competentes, acompanhados de planos de ação destinados a promover ajustes, correções e a melhoria contínua dos processos avaliados.

Assim, as auditorias e testes de integridade, refletidos em relatórios, no mínimo, anuais, garantem a confiabilidade do ambiente e suportam o cumprimento das exigências regulatórias aplicáveis às infraestruturas dos sistemas do mercado financeiro.

Os testes de restauração e de integridade são conduzidos pela Área de Testes (subordinada ao Diretor de Tecnologia) e realizados com apoio das áreas de negócios e corporativas da Base Clearing, observado que os princípios e diretrizes dos testes de continuidade são estabelecidos e acompanhados pela Área de RCC.

V. Disposições Gerais

Este Plano foi aprovado pela Diretoria Colegiada da Base Clearing e se encontra em vigor a partir da data de sua aprovação.

A área proprietária responsável pelo apoio na elaboração e revisão deste Plano é a Área de Tecnologia da Informação. Este Plano será revisado, no mínimo, anualmente e pode ser modificado a qualquer tempo por

ÁREA DE TECNOLOGIA DA INFORMAÇÃO			
PLANO DE INFRAESTRUTURA TECNOLÓGICA E GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO			
CLEARING-TI-PLANO-01	VERSÃO: 1.0	DATA: 22/04/2026	CLASSIFICAÇÃO: PÚBLICA

deliberação da Diretoria Colegiada da Base Clearing. Este Plano e quaisquer alterações serão divulgadas no Site da Base, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

Os casos omissos e dúvidas de interpretação relativos a este Plano serão tratados pela Diretoria Colegiada, de acordo com a legislação vigente e o Ordenamento Base.

Caso qualquer disposição deste Plano venha a ser considerada inválida, ilegal ou ineficaz, essa disposição será limitada na medida do possível para que a validade, legalidade e eficácia das disposições remanescentes deste Plano não sejam afetadas ou prejudicadas.

No caso de conflito entre as disposições deste Plano e nos demais normativos da Base Clearing, deve prevalecer o normativo mais específico, considerando a matéria objeto de conflito. No caso de conflito entre as disposições deste Plano e o Estatuto Social da Base Clearing, prevalecerá o Estatuto Social. No caso de conflito entre as disposições deste Plano e da legislação e regulamentação vigente, prevalecerá o disposto na legislação e regulamentação vigente.