POLÍTICA DE GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

[PUBLICO | PUBLIC]

SUMÁRIO

CONTROLE DE VERSÃO 3
1. OBJETIVO 4
2. REFERÊNCIAS REGULATÓRIAS E NORMATIVAS 4
3. DEFINIÇÕES 4
4. PRINCÍPIOS 5
5. RESPONSABILIDADES 6
6. DIRETRIZES 7
6.1. DISPONIBILIDADE 7
6.2. CAPACIDADE 7
6.3. DESEMPENHO 7
6.4. SEGURANÇA DA INFORMAÇÃO 8
6.5. GESTÃO DE INCIDENTES DE TI 8
6.6. GESTÃO DE PROBLEMAS 8
6.7. GESTÃO DE MUDANÇAS 8
6.8. GESTÃO DE PRESTADORES DE SERVIÇOS RELEVANTES 8
7. GESTÃO DE RISCOS 9
8. CONTROLE DO DOCUMENTO 9
8.1. VIGÊNCIA E DIVULGAÇÃO 9
8.2. REVISÃO 10
8.3. DIREITOS AUTORAIS E DISTRIBUIÇÃO 10

CONTROLE DE VERSÃO

Data da Versão	Autores	Número da Versão	Descrição
13/02/2026	Departamento de Produção e Segurança da Informação	1.0	Elaboração inicial do documento; Documento aprovado pelo Conselho de Administração em 12/02/2026
20/08/2026	Departamento de Segurança da Informação Diretoria de Operações	2.0	Adequação à nova estrutura organizacional; Documento aprovado pelo Conselho de Administração em 13/08/2026

1. OBJETIVO

O objetivo desta Política de Gestão de Serviços de Tecnologia da Informação ("Política" ou "PGSTI") é estabelecer princípios e diretrizes para que os serviços de tecnologia da informação ("TI") utilizados pela CSD CENTRAL DE SERVIÇOS DE REGISTRO E DEPÓSITO AOS MERCADOS FINANCEIRO E DE CAPITAIS S.A. ("CSD BR", "CSDBr" ou "Companhia"), sejam geridos com qualidade, segurança, disponibilidade e conformidade regulatória, garantindo que a prestação dos serviços pela Companhia seja sustentada por uma base tecnológica robusta e confiável, capaz de suportar as necessidades do negócio, absorver mudanças e responder adequadamente a cenários de estresse operacional.

Os termos e expressões aqui iniciados em maiúsculas, tanto no singular quanto no plural, têm o significado a eles atribuído no Glossário da CSD BR disponível em www.csdbr.com.

2. REFERÊNCIAS REGULATÓRIAS E NORMATIVAS

Esta Política utiliza como referências regulatórias e normativas, incluindo, sem se limitar a(s)/o(s):

- Resolução BCB n° 304, de 20 de março de 2023 ("RBCB 304/2023");
- Resolução CVM nº 135, de 13 de junho de 2022 ("RCVM 135/2022");
- ITIL – *Information Technology Infrastructure Library*;
- ISO/IEC 20000 – Gestão de Serviços de TI.

Qualquer referência a qualquer lei ou normativo aplicável será considerada também como uma referência a todas as suas atualizações e regulamentações promulgadas ao abrigo dele, salvo disposição em contrário.

3. DEFINIÇÕES

Para fins desta Política e dos documentos a ela relacionados, aplicam-se as seguintes definições:

- Capacidade: disciplina que assegura que os recursos de TI (infraestrutura, aplicações e serviços) tenham recursos suficientes para atender à demanda com nível de serviço acordado e custo otimizado;
- Desempenho: qualidade operacional de um serviço de TI relacionada à capacidade de atender à experiência do usuário e aos requisitos do negócio;

- Disponibilidade: princípio de segurança da informação relacionado à garantia de acesso às informações sempre que necessário, por pessoas autorizadas;
- Incidente de TI: interrupção não planejada ou degradação de um serviço de TI que reduz sua qualidade, exigindo restauração rápida ao funcionamento normal;
- Mudança: adição, modificação ou remoção em serviços, componentes ou processos de TI que pode impactar a operação e deve ser avaliada, aprovada, testada e registrada;
- Problema: causa raiz conhecida ou suspeita de um ou mais Incidentes de TI, tratada para eliminar recorrência por meio de análise e ações corretivas/preventivas; e
- Serviço Relevante: serviço considerado relevante para a condução das atividades da Companhia e diretamente relacionado aos processos críticos de negócio.

4. PRINCÍPIOS

- Melhoria contínua: compromisso com a revisão e aprimoramento constante dos processos que suportam a gestão dos serviços de TI, incorporando lições aprendidas, resultados de testes, auditorias e adaptações às mudanças do ambiente de negócios e regulatório;
- Robustez: estruturação dos serviços de TI para garantir alta disponibilidade, tolerância a falhas, resiliência operacional e capacidade de absorver mudanças no modelo de negócio;
- Resiliência: capacidade dos serviços de TI de resistir, adaptar-se e recuperar-se diante de eventos adversos, mantendo a entrega dos serviços críticos da Companhia;
- Conformidade regulatória: observância rigorosa aos requisitos legais, normativos e regulatórios aplicáveis à gestão dos serviços de TI;
- Prevenção: adoção de medidas preventivas para evitar ou reduzir a ocorrência e o impacto de incidentes, falhas ou interrupções nos serviços de TI;
- Resposta rápida: prontidão para identificar, tratar e restaurar os serviços de TI em caso de Incidentes de TI, minimizando impactos ao negócio;
- Integração com Segurança da Informação e Continuidade: alinhamento dos processos de gestão dos serviços de TI com as políticas e planos de Segurança

da Informação, Continuidade de Negócios e demais instrumentos de governança da Companhia.

5. RESPONSABILIDADES

i. Conselho de Administração: responsável por aprovar esta Política, observados os papéis e responsabilidades nela definidos.

ii. Diretoria Estatutária, responsável por:
   a. definir os princípios e diretrizes que norteiam a gestão dos serviços de TI;
   b. garantir a alocação de recursos necessários para a implementação desta Política e dos processos correlatos;

iii. Departamento de Segurança da Informação (“DSI”), responsável por:
   a. avaliar e homologar os requisitos de segurança da informação dos prestadores de serviços de TI;
   b. definir os critérios de segurança aplicáveis aos processos de gestão de mudanças e gestão de incidentes de TI com natureza ou origem cibernética.;

iv. Diretoria de Operações (“DOP”), responsável por:
   a. elaborar, analisar, revisar e implementar esta Política;
   b. executar os processos operacionais de gestão de serviços de TI, *service desk* e infraestrutura em conformidade com esta Política;

v. Diretoria de Governança, Riscos e Controles Internos (“GRC”), responsável por:
   a. submeter esta Política e os demais documentos de gestão de serviços de TI à aprovação dos órgãos de governança aplicáveis;
   b. monitorar a conformidade regulatória e a efetividade dos controles internos;

vi. Departamento Jurídico e Regulatório (JUR&REG): responsável por comunicar aos órgãos reguladores alterações relevantes na gestão de serviços de TI, conforme previsto nas normas internas e externas;

vii. Gestores de departamentos: responsáveis por assegurar o cumprimento das diretrizes estabelecidas nesta Política;

viii. Colaboradores, responsáveis por:
   a. cumprir as diretrizes e procedimentos definidos nesta Política;
   b. reportar ao DOP inconsistências ou irregularidades relativas à gestão dos serviços de TI;

ix. Prestadores de Serviços Relevantes: responsáveis por observar e cumprir as diretrizes aplicáveis aos serviços prestados, conforme instrumento contratual e regulamentações vigentes.

6. DIRETRIZES

A gestão dos serviços de TI da Companhia deve observar as seguintes diretrizes, de modo a garantir a adequada Disponibilidade, Capacidade, Desempenho, segurança, conformidade regulatória e resiliência operacional dos serviços e processos críticos mapeados no *Business Impact Analysis* (“BIA”) da Companhia.

6.1. DISPONIBILIDADE

A Disponibilidade dos serviços de TI da Companhia é garantida por meio de uma arquitetura tecnológica resiliente, com mecanismos de redundância, contingência e monitoramento contínuo.

Os objetivos de confiabilidade operacional devem estar definidos nos documentos de continuidade de negócios da Companhia, de modo a assegurar que os serviços críticos mantenham níveis mínimos de Disponibilidade compatíveis com as necessidades do negócio e com os requisitos regulatórios, sendo submetidos a testes periódicos para validação da resiliência e capacidade de resposta a incidentes que causem indisponibilidade.

6.2. CAPACIDADE

A Companhia deve realizar testes semestrais de Capacidade para validar a *performance* dos serviços de TI sob condições de carga elevada, garantindo que a infraestrutura tecnológica seja capaz de absorver picos de demanda e cenários de estresse operacional.

6.3. DESEMPENHO

O Desempenho dos serviços de TI é acompanhado por meio do monitoramento contínuo de indicadores técnicos, como o número de transações por segundo, utilização de recursos computacionais (CPU, memória, disco, rede) e integridade dos sistemas essenciais para o funcionamento dos serviços de TI. A Companhia deve assegurar que a *performance* da Plataforma atenda às necessidades dos Participantes, bem como

promover ajustes sempre que necessário para garantir a eficiência e a qualidade dos serviços prestados, mesmo em cenários de alta demanda ou estresse operacional.

6.4. SEGURANÇA DA INFORMAÇÃO

A gestão dos serviços de TI deve observar, de forma integral, os princípios e diretrizes da Política de Segurança da Informação e Segurança Cibernética da Companhia, garantindo confidencialidade, integridade e Disponibilidade dos dados e serviços, bem como prevenção, detecção, resposta e recuperação frente a incidentes de segurança da informação e cibernéticos.

6.5. GESTÃO DE INCIDENTES DE TI

Os Incidentes de TI que impactam os serviços de TI devem prever o registro, classificação, tratamento e reporte desses Incidentes de TI. Incidentes Relevantes devem ser reportados ao Conselho de Administração e, quando aplicável, aos órgãos reguladores. Em caso de interrupção da operação, deve-se observar as diretrizes de continuidade de negócio e recuperação de desastres da Companhia, considerando o e *Recovery Point Objective* (“RPO”) e *Recovery Time Objective* (“RTO”) definidos no *Business Impact Analysis* (“BIA”).

6.6. GESTÃO DE PROBLEMAS

A Companhia deve definir mecanismos para identificação e tratamento da causa raiz dos Incidentes de TI que afetam os serviços de TI com o objetivo de diminuir a recorrência desses Incidentes de TI e aprimorar a qualidade dos serviços prestados.

6.7. GESTÃO DE MUDANÇAS

As mudanças nos serviços de TI (adição, modificação ou remoção de componentes/processos) devem ser avaliadas, aprovadas, testadas em ambiente segregado, quando aplicável, e registradas de forma controlada e segura.

6.8. GESTÃO DE PRESTADORES DE SERVIÇOS RELEVANTES

A Companhia deve garantir que terceiros que prestem serviços de TI estejam alinhados aos requisitos de segurança e conformidade da Companhia. Os prestadores de serviços devem possuir procedimentos e controles de segurança equivalentes aos controles da CSD BR, proporcionais à natureza do serviço prestado, conforme previsto na Política de Segurança da Informação e Segurança Cibernética.

Os instrumentos contratuais firmados entre o prestador de serviços e a CSD BR devem contemplar cláusulas mínimas, contando com acordo de nível de serviço (conforme aplicável), requisitos técnicos e organizacionais, obrigações de reporte e mecanismos de monitoramento contínuo, assegurando que a prestação se mantenha aderente aos padrões exigidos pela Companhia ao longo de todo o ciclo de vida contratual.

Para Serviços Relevantes, além das diretrizes acima, devem ser observados requisitos mínimos adicionais em alinhamento integral à Política de Gestão de Terceirização de Serviços.

7. GESTÃO DE RISCOS

A gestão de riscos no âmbito da gestão de serviços de TI da CSD BR tem como objetivo identificar, avaliar, tratar e monitorar os riscos associados à prestação, operação e suporte dos serviços de TI, de forma proativa e contínua, visando mantê-los em níveis compatíveis com a continuidade da operação, a qualidade dos serviços, as melhores práticas de mercado e a regulamentação vigente, em conformidade com a Política de Riscos e Controles Internos da Companhia.

A CSD BR está em constante ação, fazendo que seus processos sejam sustentáveis e que estejam de acordo com o estabelecido em suas políticas, manuais e procedimentos, visando: (i) a coleta de informações necessárias para a verificação de possíveis riscos; (ii) a identificação e a quantificação do risco; (iii) o desenvolvimento da estratégia para mitigar o possível risco; (iv) a comunicação e o engajamento dos *stakeholders* na busca da melhor solução em caso de materialização de um risco; (v) envolvimento da alta liderança para a tomada de decisões e construção de planos de ação; e (vi) a garantia de que os prestadores de serviços contratados possuam procedimentos e controles de segurança para prevenção e tratamento de incidentes equivalentes aos controles da Companhia, de acordo com o serviço a ser prestado.

8. CONTROLE DO DOCUMENTO

8.1. VIGÊNCIA E DIVULGAÇÃO

Este documento deverá ser divulgado no site da Companhia após a sua aprovação pelo Conselho de Administração, entrando em vigor na data mais recente do quadro no item “CONTROLE DE VERSÃO”, acima, cancelando e substituindo o documento vigente desde a data imediatamente anterior.

8.2. REVISÃO

Este documento deverá ser revisado, no mínimo, anualmente, considerando a data de publicação mais recente (quadro no item “CONTROLE DE VERSÃO”, acima), podendo ser atualizado a qualquer tempo para incorporar melhorias, corrigir erros ou atender normativos.

8.3. DIREITOS AUTORAIS E DISTRIBUIÇÃO

A Companhia possui sobre esse documento todos os direitos de elaboração, alteração, reprodução e distribuição. Este documento substitui todas as versões anteriores. A Companhia não se responsabiliza por versões desatualizadas, modificadas, ou por quaisquer versões provenientes de outras fontes que não a fonte oficial designada para fornecer este material.