



CSD_{BR}
registradora

POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS



SUMÁRIO

CONTROLE DE VERSÃO	3
1. OBJETIVO	4
2. REFERÊNCIAS REGULATÓRIAS E NORMATIVAS.....	4
3. DEFINIÇÕES.....	5
4. PRINCÍPIOS.....	5
5. GESTÃO DE CONTINUIDADE DE NEGÓCIOS.....	6
5.1. Alocação de Recursos para a Gestão e Continuidade dos Negócios.....	7
6. RESPONSABILIDADES	7
7. PCN-RD DA CSD BR.....	8
7.1. Testes.....	9
8. TREINAMENTO E ACULTURAMENTO.....	9
9. DISPOSIÇÕES FINAIS	10
10. CONTROLE DO DOCUMENTO	10
10.1. Vigência e Divulgação.....	10
10.2. Revisão.....	10
10.3. Direitos Autorais e Distribuição	10



CONTROLE DE VERSÃO

Data da Versão	Autores	Número da Versão	Descrição
19/02/2020	Presidente, GRC, Departamento de Operações e Tecnologia	1.0	Elaboração inicial do documento
30/03/2021	Departamento de Produção e Segurança da Informação	2.0	Revalidação do documento
16/07/2021	Departamento de Produção e Segurança da Informação Diretoria de Governança, Riscos e Controles Internos	3.0	Adequação relativa à alteração da infraestrutura da Plataforma para computação em nuvem (<i>cloud computing</i>)
05/08/2022	Departamento de Produção e Segurança da Informação	4.0	Revalidação do documento
10/10/2023	Departamento de Produção e Segurança da Informação	5.0	Revisão do documento
12/11/2024	Departamento de Produção e Segurança da Informação	6.0	Inclusão do capítulo de Referências Regulatórias e Normativas; Atualização documento; Documento aprovado pelo Conselho de Administração em 12/11/2024
19/12/2024	Departamento de Produção e Segurança da Informação	7.0	Atualizações considerando a inclusão das atividades de Depósito Centralizado e de Compensação e Liquidação de Ativos; Reorganização textual e complementação dos demais capítulos; Revisão geral; Documento aprovado pelo Conselho de Administração em 19/12/2024



1. OBJETIVO

O objetivo desta Política de Gestão de Continuidade de Negócios (“Política”) é definir os princípios e diretrizes que orientam a gestão da continuidade das operações da CSD CENTRAL DE REGISTRO E DEPÓSITO AOS MERCADOS FINANCEIRO E DE CAPITAIS S.A. (“CSD BR” ou “Companhia”). Esta Política serve como base para a implementação e execução do Plano de Continuidade de Negócios e Recuperação de Desastres (“PCN-RD”), garantindo a resiliência e a pronta recuperação das atividades essenciais da Companhia em situações de interrupção ou crise.

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.csdb.com.

2. REFERÊNCIAS REGULATÓRIAS E NORMATIVAS

Essa Política adota como referências:

- *Principle 3 - Framework for the comprehensive management of risks e Principle 17 – Operational Risk do PFMI - Principles for Financial Market Infrastructures*, de 15 de abril de 2012;
- *Recovery of financial market infrastructures – Revised report*, de 05 de julho de 2017 (“*Recovery Report*”);
- Resolução BCB nº 304 de 20 de março de 2023 (“RBCB nº 304/2023”);
- Resolução CVM nº 135, de 10 de junho de 2022 (“RCVM 135/2022”);
- Documento da Companhia de Autoavaliação da Observância aos Princípios para Infraestruturas do Mercado Financeiro (“Autoavaliação PFMI”).

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

- (i) Atividade: processo ou conjunto de processos executados pela Companhia (ou em seu nome) que produzem ou suportem um ou mais serviços;
- (ii) Processos críticos: atividades que, se interrompidas, tenham potencial de causar prejuízos à Companhia;
- (iii) Continuidade dos Negócios: capacidade de a Companhia continuar a prestar os serviços em um nível aceitável previamente definido após incidentes de interrupção;
- (iv) Crise: evento inesperado que tenha potencial de causar danos significativos na Companhia.
- (v) Desastre: evento que causa danos e/ou interrompe a execução de atividade crítica, por período superior ao *Recovery Time Objective* (“RTO”) definido;
- (vi) Incidente: situação que pode representar ou levar à interrupção de negócios, perdas, emergências ou crises;
- (vii) Interrupção: Evento que causa a suspensão temporária de uma ou mais atividades críticas da Companhia;
- (viii) Ruptura Operacional: é a indisponibilidade da Plataforma ocasionada em decorrência da indisponibilidade simultânea de 2 (duas) zonas de disponibilidade da AWS;
- (ix) Plano de Continuidade de Negócios e Recuperação de Desastres (“PCN-RD”): documento que registra as ações a serem tomadas nos casos de crise e/ou desastre, com o objetivo de manter um nível adequado e seguro de serviços aos Participantes, reguladores e ao mercado;
- (x) Plataforma: conforme definido no Glossário da Companhia.

4. PRINCÍPIOS

- (i) Melhoria contínua: compromisso com a revisão e aprimoramento contínuo da gestão de continuidade de negócios e recuperação de desastres da Companhia. Isso inclui a incorporação de lições aprendidas de incidentes passados, análise de testes, treinamentos periódicos, e a adaptação a mudanças no ambiente de negócios;
- (ii) Prevenção: capacidade de evitar ou reduzir a possibilidade de ocorrência e os impactos de um incidente ou desastre, com a adoção de medidas preventivas e mecanismos de recuperação, considerando a implementação de testes regulares;



- (iii) Recuperação: processo de reparação do ambiente normal de trabalho e de seus recursos para o restabelecimento das atividades críticas após a ocorrência de incidente(s) e/ou desastre(s); e
- (iv) Resposta e/ou resiliência: capacidade de a Companhia se manter em operação diante de atividades críticas, protegendo as pessoas e o patrimônio da Companhia, após a ocorrência de incidentes ou desastres, de acordo com a estratégia previamente definida, neste caso, no Plano de Continuidade de Negócios e de Recuperação de Desastres (“PCN-RD”).

5. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

- (i) O objetivo da gestão de continuidade de negócios é identificar potenciais ameaças à Companhia, avaliar seus possíveis impactos nas operações e estabelecer uma estrutura que promova a resiliência organizacional e uma resposta eficaz a incidentes. A Companhia adota as seguintes práticas para assegurar a continuidade de suas operações: Análise de impacto, identificação, classificação e documentação de processos críticos, bem como avaliação dos potenciais efeitos de eventual incidente e/ou interrupção desses processos;
- (ii) Estratégias de continuidade: capacidade de continuidade das atividades pela Companhia, limitando perdas decorrentes de eventual incidente e/ou interrupção dos processos críticos;
- (iii) Administração de crise: providências e mobilização de pessoas que devam estar preparadas e/ou tomar as ações necessárias para tratamento de uma situação de crise até o retorno à normalidade, considerando a comunicação interna e externa da Companhia sobre os incidentes e/ou interrupção dos processos críticos;
- (iv) Aplicação de testes: serão realizados testes preventivos e de monitoramento, cujo objetivo é validar se a estratégia definida no PCN-RD da Companhia contém as informações necessárias, e se produz o resultado esperado caso seja colocado em prática em uma situação real;
- (v) Continuidade operacional: ações e procedimentos de resposta à crise, com objetivo de estabilizar uma situação decorrente de um incidente; e
- (vi) Recuperação de desastre: instauração, no menor tempo possível, de procedimentos de operações de tecnologia da informação em caso de interrupção dos serviços, bem como análise dos impactos da interrupção e o tempo máximo necessário para a recuperação das atividades essenciais da Companhia.



5.1. Alocação de Recursos para a Gestão e Continuidade dos Negócios

Com o objetivo de fazer frente a potenciais perdas que a Companhia venha a enfrentar, no intuito de manter a continuidade de suas operações e a recuperação em caso de eventuais incidentes ou desastres, a Diretoria Estatutária da Companhia deverá manter a aplicação de recursos em investimentos de disponibilidade imediata (“Recursos Líquidos”).

Os Recursos Líquidos deverão ser de, no mínimo, o valor necessário para o restabelecimento operacional de uma zona de disponibilidade, conforme disposto no PCN-RD.

Em situações de anormalidade do mercado, o Conselho de Administração da Companhia, poderá determinar que a reserva de Recursos Líquidos seja maior que o mínimo definido acima.

6. RESPONSABILIDADES

- (i) Conselho de Administração: responsável pela aprovação desta Política, observados os papéis e responsabilidades nela definidos;
- (ii) Diretoria Estatutária: responsável por definir os princípios e as diretrizes que norteiam a gestão de continuidade dos negócios, bem como a estrutura de comando que deverá conduzir providências de tratamento da crise até o retorno à normalidade;
- (iii) Departamento de Produção e Segurança da Informação (“DPSI”): responsável pela elaboração, análise e revisões desta Política e do PCN-RD, em conjunto com a Diretoria de Governança, Riscos e Controles Internos.
- (iv) GRC: responsável por:
 - (a) Submeter esta Política e o PCN-RD à aprovação do Conselho de Administração; e da Diretoria Estatutária da Companhia, respectivamente;
 - (b) Comunicar aos órgãos reguladores, conforme aplicável, as alterações planejadas que venham afetar de maneira relevante a gestão da continuidade dos negócios.
- (v) Gestores de Áreas, conforme aplicável: responsáveis por:
 - (a) Solicitação de adequação desta Política;



- (b) Garantir a participação e contribuição das equipes sob sua gestão no processo de elaboração e testes do PCN-RD;
 - (c) Realizar análise de impacto nos negócios dos processos sob sua responsabilidade;
 - (d) Elaborar e manter o PCN-RD com base na análise de impacto nos negócios.
- (vi) Demais colaboradores: responsáveis por participar dos treinamentos e testes, conforme solicitado pela Companhia, e de cumprir com seus papéis e responsabilidades nos testes e/ou em casos reais de necessidades de acionamento do PCN-RD.

7. PCN-RD DA CSD BR

A implementação desta Política e de itens relativos à continuidade dos negócios presentes nas demais políticas da Companhia será feita por meio do PCN-RD, documento interno da Companhia, em que estão descritos um conjunto de ações que identificam contingências, planos de ação, e estabelece estratégias e prazos para reinício e recuperação das atividades, a serem executados em situações de crise e/ou desastre.

No PCN-RD constam as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta Política. Adicionalmente, deve-se considerar:

- (i) Estrutura de comando;
- (ii) Avaliação e comunicação de incidente, em caso de indisponibilidade de atividade crítica, considerando os cenários previstos:
 - Indisponibilidade da Plataforma;
 - Indisponibilidade da Comunicação com a Rede do Sistema Financeiro Nacional (“RSFN”);
 - Indisponibilidade dos escritórios;
 - Regime de Contingência – CSD BR x STR
- (iii) Acionamento do Plano de Gestão de Crise;
- (iv) *Recovery Time Objective* (“RTO”) de no máximo:
 - (a) 2 (duas) horas para as atividades de registro e de depósito centralizado; e
 - (b) 30 (trinta) minutos para as atividades de compensação e liquidação.
- (v) *Recovery Point Objective* (“RPO”) de 0 (zero);



- (vi) Prazo para retomada dos serviços prestados, dos processos e das atividades executadas, de acordo com o *Business Impact Analysis* ("BIA") da Companhia;
- (vii) Regras de backup, considerando o período mínimo de retenção dos dados, conforme abaixo:
 - (a) Sistemas críticos e não-críticos: 10 (dez) anos.
 - (b) Sistemas acessórios: 1 (um) ano.
- (viii) Testes a serem realizados para validação de todos os elementos do plano, incluindo, mas não se limitando a:
 - (a) Descrição do teste e controles aplicáveis.
 - (b) Periodicidade de execução dos testes de continuidade: semestral.
- (ix) O PCN-RD deverá ser revisado, no mínimo, anualmente.

7.1. Testes

Para garantir a eficácia e a efetividade dos negócios da Companhia, serão realizados testes periódicos ou extraordinários do PCN-RD, considerando os seguintes pontos:

- (i) Inclusão de Participante(s) e prestador(es) de serviço(s) crítico(s) na execução dos testes;
- (ii) Acompanhamento da área de Gestão de Riscos e Controles Internos ("GRCI");
- (iii) Avaliação pela Auditoria Interna na figura de equipe independente;
- (iv) Elaboração de um relatório com os resultados obtidos nos testes;
- (v) Encaminhamento do relatório dos testes realizados ao Conselho de Administração da Companhia.

8. TREINAMENTO E ACULTURAMENTO

Para promover a conscientização e o entendimento das diretrizes estabelecidas nesta Política e no PCN-RD, a Companhia realiza treinamentos teóricos para todos os colaboradores com o objetivo de alinhar o conhecimento sobre o desenvolvimento e a implementação do PCN-RD. Este treinamento é obrigatório e deverá ser aplicado no mínimo anualmente.

Além disso, são realizados treinamentos práticos voltados para as equipes técnicas diretamente envolvidas na gestão da continuidade de negócios, por meio da execução dos testes previstos no PCN-RD.



9. DISPOSIÇÕES FINAIS

Na existência de um PCN-RD que venha sofrer alterações em virtude da publicação desta Política, a Companhia deverá revisá-lo no prazo de 30 (trinta) dias e, caso necessário, adequá-lo às diretrizes desta Política.

Em havendo conflito entre o disposto nesta Política e no PCN-RD, prevalecerá o disposto nesta Política.

10. CONTROLE DO DOCUMENTO

10.1. 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.

10.2. 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.

10.3. 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.