POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS

SUMÁRIO

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 (*cloud computing*)
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
01/08/2025	Departamento de Produção e Segurança da Informação	8.0	Atualização para novo leiaute de documentos; Normalização do RTO para as atividades de registro, depósito centralizado, compensação e liquidação de Ativos; Atualizações considerando revisões normativas; Documento aprovado pelo Conselho de Administração em 01/08/2025

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", "CSDBr" ou "Companhia"). Esta Política estabelece diretrizes para a implementação e execução do Plano de Continuidade de Negócios e Recuperação de Desastres ("PCN-RD") e demais documentos voltados para a gestão de continuidade de negócios, garantindo a resiliência e a pronta recuperação das atividades essenciais da Companhia em situações de Impedimento Operacional 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.csdbr.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 infraestructures – Revised report*, de 05 de julho de 2017 ("*Recovery Report*");
- Resolução BCB n° 304 de 20 de março de 2023 ("RBCB n° 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

As definições a seguir servem como base para a interpretação deste documento e de todos os documentos da Companhia aqui mencionados, no que couber:

(i) Atividade: ações específicas realizadas para a composição de um processo ou conjunto de processos executados pela Companhia (ou em seu nome) que produzam ou suportam um ou mais serviços;

(ii) Atividade crítica: atividade essencial de um processo cuja interrupção pode causar impacto significativo na Companhia;

(iii) Ativo: qualquer recurso essencial utilizado pela Companhia para a execução de atividades, processos ou serviços;

(iv) Confiabilidade Operacional: capacidade da Companhia de manter a continuidade e a integridade de seus serviços críticos, mesmo diante de eventos adversos;

(v) Continuidade dos Negócios: capacidade da Companhia continuar a prestar os serviços em um nível aceitável, conforme RTO previamente definido, durante um incidente de interrupção;

(vi) Crise: evento inesperado que tenha potencial de causar danos significativos na Companhia e que necessita de tomada de estratégica;

(vii) Desastre: um ou mais eventos que causem danos e/ou interrompam a execução de uma atividade, processo ou serviço crítico, exigindo resposta imediata;

(viii) Evento: ocorrência detectável que pode impactar as atividades, processos ou serviços da Companhia;

(ix) Impedimento ou Impedimento Operacional: condição que compromete a capacidade da Companhia em manter suas operações essenciais;

(x) Incidente: evento não planejado que causa, ou tem o potencial de causar, uma interrupção, degradação ou falha em um sistema, processo e/ou atividade;

(xi) Processo: conjunto estruturado de atividades interligadas que, quando executadas em sequência, garantem a entrega de um produto ou serviço;

(xii) Processo crítico: processo cuja interrupção causa impacto significativo na Companhia;

(xiii) *Recovery Point Objective* (“RPO”) ou Ponto de Recuperação de Dados: tempo máximo permitido de perda de dados em caso de uma interrupção. Ele define o ponto até o qual as informações devem ser recuperadas, determinando a frequência necessária de backups para minimizar perdas;

(xiv) *Recovery Time Objective* (“RTO”) ou Tempo de Recuperação: é o tempo máximo aceitável para que uma atividade, processo ou serviço interrompido seja retomado após um incidente. Ele serve como um parâmetro essencial para planejar os esforços de recuperação;

(xv) Resiliência operacional: é a capacidade da Companhia de resistir, adaptar-se e se recuperar de eventos adversos sem comprometer a entrega de seus serviços;

(xvi) Ruptura Operacional: é a indisponibilidade da Plataforma ocasionada em decorrência da indisponibilidade simultânea de 2 (duas) zonas de disponibilidade da AWS;

(xvii) Serviço: é o conjunto de processos estruturados e organizados, destinados a cumprir uma função específica e gerar valor para os Participantes e usuários finais, como, por exemplo, o registro, o depósito centralizado, a compensação e liquidação de Ativos;

(xviii) Serviço crítico: serviço cuja interrupção ou degradação pode causar impacto significativo na Companhia. Esses serviços são essenciais para o cumprimento da missão institucional e para a entrega de valor aos Participantes; e

(xix) Serviço relevante: serviço considerado relevante para a condução das atividades da Companhia e diretamente relacionado aos processos críticos de negócio.

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 da Companhia manter em operação as atividades críticas, protegendo as pessoas e seu o patrimônio 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

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, compostas por:

(i) Práticas para assegurar a continuidade de suas operações, consolidadas no *Business Impact Analysis* ("BIA") da Companhia, como:
   (a) identificação dos ativos, atividades, processos e serviços da Companhia;
   (b) realização da análise de impacto nos negócios;
   (c) classificação da criticidade; e
   (d) documentação dos processos considerando os potenciais efeitos de eventual incidente e/ou interrupção desses processos;

(ii) Metodologia de Governança, Riscos e Controles Internos, abrange a identificação, avaliação, tratamento e monitoramento de riscos, com foco na prevenção, conformidade regulatória e eficiência operacional. A metodologia considera fatores internos e externos ao negócio, utilizando critérios qualitativos de impacto e probabilidade para a análise de riscos. São aplicadas ferramentas como o *Risk and Control Self Assessment* ("RCSA") e testes de controle, com o objetivo de assegurar a efetividade dos controles internos e fortalecer a governança corporativa.

(iii) Relatório anual de GRC, Instrumento estratégico que apresenta os resultados consolidados das práticas de Governança, Gestão de Riscos e Controles Internos e Compliance, com os seguintes objetivos:
   (a) Consolidação de resultados sistematizando as atividades realizadas ao longo do ano.
   (b) Identificação de inconsistências, detectação falhas, fragilidades ou desvios nos processos e controles internos, com base em evidências coletadas durante as avaliações.
   (c) Recomendações de mitigação propondo ações corretivas e preventivas para os riscos identificados, visando o fortalecimento dos controles e a melhoria contínua dos processos.

(d) Compromisso com a conformidade, reforça o alinhamento das áreas de negócio às exigências regulatórias e normativas aplicáveis, promovendo uma cultura de integridade e responsabilidade corporativa.

(e) Comunicação institucional como canal formal de prestação de contas aos órgãos reguladores e demais partes interessadas, demonstrando transparência e governança.

(f) Suporte à tomada de decisão, fornece insumos estratégicos para o planejamento de ações corretivas e preventivas, contribuindo diretamente para a resiliência operacional e a sustentabilidade dos negócios.

(g) Fortalecimento da cultura de GRC, promovendo a disseminação da cultura de controle e gestão de riscos em todos os níveis da organização, incentivando o engajamento das áreas e a adoção de boas práticas de governança.

(ii) Estratégias de recuperação e continuidade: capacidade de continuidade dos serviços críticos da Companhia, limitando perdas decorrentes de eventual incidente e/ou interrupção dos processos críticos;

(iii) Administração de crise: providências e mobilização, conforme Plano de Gestão de Crise ("Plano GCR"), 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 serviços e/ou 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 este 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 Impedimento Operacional, 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 FINANCEIROS 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”), em conformidade com a Política de Investimentos.

Os Recursos Líquidos deverão ser de, no mínimo, o valor necessário para a reconstrução completa da infraestrutura da Plataforma, em caso de eventos extremos que comprometam simultaneamente todas as zonas de disponibilidade. As diretrizes para essa alocação de recursos, incluindo estimativas de custo, estão detalhadas no Plano de Recuperação ou Saída Ordenada (“PRSO”).

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.

Caso os Recursos Líquidos disponíveis não sejam suficientes para o restabelecimento operacional, a Companhia poderá adotar estratégias complementares, como o reforço de capital, venda de ativos, acesso a linhas de crédito ou reestruturação de despesas. Essas estratégias estão detalhadas no PRSO, seguindo as diretrizes desta Política.

5.2. ESTRUTURA INTEGRADA DE DOCUMENTOS DE CONTINUIDADE

A Gestão de Continuidade de Negócios da Companhia é sustentada por um conjunto de documentos interdependentes, que se complementam em diferentes níveis de atuação.

A Política de Gestão de Continuidade de Negócios estabelece as diretrizes e responsabilidades gerais, sendo o documento de maior hierarquia. A partir dela, são desdobrados os seguintes instrumentos:

- O *Business Impact Analysis* identifica os ativos, atividades, processos e serviços, bem como, os impactos de sua interrupção, que orientam a priorização dos serviços e recursos no PCN-RD, Plano GCR e PRSO.
- O Plano de Continuidade de Negócios e Recuperação de Desastres define as ações para manter ou restabelecer os serviços críticos da Companhia diante de

eventos de indisponibilidade, com base nas diretrizes desta Política e nos RTOs identificados no BIA;

- O Plano de Gestão de Crise estrutura a resposta organizacional em situações de crise. Ele é acionado quando a indisponibilidade tratada pelo PCN-RD evolui para um cenário de crise institucional, com impactos significativos à Companhia; e
- O Plano de Recuperação ou Saída Ordenada estabelece estratégias para restaurar a operação da Companhia em crises que não puderam ser tratadas pelo Plano de Gestão de Crise e, se necessário, orientar sua saída estruturada do mercado. Este plano é ativado quando a crise ultrapassa a capacidade de resposta e não consegue ser contida seguindo as diretrizes do Plano GCR, comprometendo a continuidade institucional no mercado.

A figura a seguir ilustra, de forma exemplificativa, a relação entre esses documentos, evidenciando suas relações para questões de gestão de continuidade de negócios.

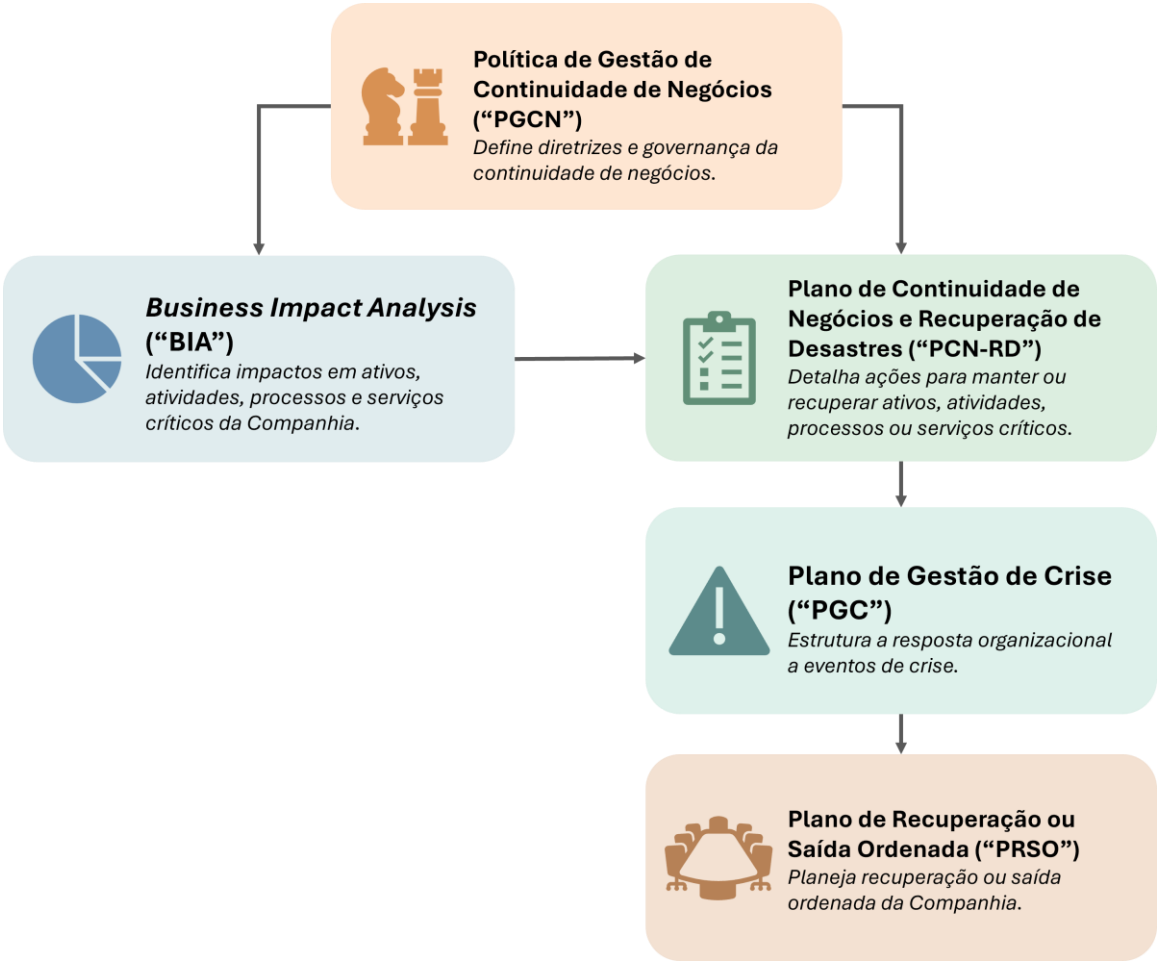

Figura 1 - Hierarquia de Documentos de Gestão de Continuidade de Negócios

6. RESPONSABILIDADES

(i) Conselho de Administração: responsável pela aprovação desta Política, observados os papéis e responsabilidades nela definidos;

(ii) Diretoria Estatutária: responsável por:

(a) 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;

(b) elaboração, análise e revisões do PRSO, em conjunto com a Diretoria de Governança, Riscos e Controles Internos;

(c) elaboração, análise e revisões do Plano GCR, em conjunto com a Diretoria de Governança, Riscos e Controles Internos.

(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) Diretoria de Governança, Riscos e Controles Internos ("GRC"): responsável por:

(a) submeter esta Política e os demais documentos de Gestão de Continuidade de Negócio para os órgãos de governança aplicáveis;

(b) comunicar aos órgãos reguladores, conforme aplicável, as alterações planejadas que venham afetar de maneira relevante;

(c) 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 atualizado 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 das Interconexões;
- 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 30 (trinta) minutos para os serviços de registro, depósito centralizado, compensação e liquidação;

(v) *Recovery Point Objective* (“RPO") de 0 (zero) para os serviços de registro, depósito centralizado, compensação e liquidação;

(vi) Prazo para retomada dos demais serviços prestados, dos processos e das atividades executadas, de acordo com o BIA da Companhia;

(vii) Regras de backup, considerando o período mínimo de retenção dos dados conforme estabelecido nas referências regulatórias e normativas.

(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.

(x) Testes 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

No caso de mudanças desta Política que acarretem na necessidade de alterações e adequações do PCN-RD, a Companhia deverá revisar este em até 30 (trinta) dias contados da publicação da 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.