



Política de Continuidade de Negócios

Versão 4.0



SUMÁRIO

1	INTRODUÇÃO	4
2	ABRANGÊNCIA	4
3	PRINCÍPIOS GERAIS	4
4	DIRETRIZES.....	4
4.1	Análise de Impacto ao Negócio (BIA).....	4
4.2	Análise de Riscos.....	5
4.3	Plano de Continuidade de Negócios (PCN)	5
4.3.1	Plano de Recuperação de Desastres (PRD)	6
4.3.2	Plano de Comunicação em Crise (PCOM).....	6
4.3.3	Plano de Emergência de Segurança da Informação (PESI)	6
4.3.4	Plano de Emergência Integridade Física e Saúde Pública (PEIFSP) 6	
4.3.5	Plano de Prestadores de Serviços Críticos (PSC).....	7
4.3.6	Plano de Gestão de Crise (PGC).....	7
4.3.7	Plano de Saída Ordenada (PSO).....	7
4.3.8	Contingência física	7
4.3.9	Contingência lógica	7
4.4	Treinamento	8
4.5	Testes e Melhorias Contínuas	8
5	DISPOSIÇÕES FINAIS.....	8
6	ATRIBUIÇÕES E RESPONSABILIDADES	8
6.1	Conselho de Administração.....	8
6.2	Comitê de Riscos	8
6.3	Comitê de Auditoria	9
6.4	Diretoria Estatutária	9
6.5	Área de GCN – Diretoria de Tecnologia e Operações	9
6.6	Área de Riscos, Controles e Compliance – Diretoria de Integridade e Conformidade	9
6.7	Área de Comunicação e Marketing – Diretoria de Produtos	9
6.8	Área do Jurídico Corporativo – Diretoria Jurídica.....	10

6.9	Área de Tecnologia da Informação	10
6.10	Gestores da Companhia	10
6.11	Colaboradores, Fornecedores e Usuários dos Sistemas CERC.....	10
6.12	Auditoria Interna – Diretoria de Integridade e Conformidade	10
6.13	Grupos de Crise (Operacional, Tático e Estratégico).....	10
7	CONTROLE DOCUMENTAL	10
8	ANEXOS.....	11
8.1	Anexo 1 - Definições.....	11

1 INTRODUÇÃO

O documento tem o objetivo de documentar as diretrizes de Gestão de Continuidade de Negócios que serão adotadas para minimizar os impactos negativos causados por interrupções abruptas que possam impactar a integridade física dos funcionários e prestadores de serviços, as operações críticas de negócios, a imagem e o patrimônio da CERC. Assim, trazendo diretrizes para respostas adequadas quando ocorrer situações adversas que ocasionem a interrupção ou a ruptura operacional das atividades, mantendo o funcionamento da empresa em níveis aceitáveis, garantindo maior agilidade e velocidade nas tomadas de decisões e por fim, minimizando as perdas.

Esta Política descreve a abordagem adotada para a Gestão de Continuidade de Negócios da CERC, estabelecendo princípios, definições, diretrizes e responsabilidades que assegurem que todas as medidas preventivas e mecanismos de recuperação de desastres sejam implantados e submetidos a testes regulares, garantindo a sustentabilidade dos negócios da CERC, mesmo em situações adversas.

2 ABRANGÊNCIA

São usuários do normativo os funcionários e prestadores de serviços da CERC, incluindo todos os envolvidos na operação da CERC, contemplando administradores e colaboradores que definem, executam ou participam dos processos de negócios, de controle e administrativos da CERC.

3 PRINCÍPIOS GERAIS

A Política de Continuidade de Negócios possui como direcionadores os seguintes princípios:

- » **Princípio da Integridade:** agir de maneira ética e honesta na construção e manutenção de sistemas, dados e processos, garantindo a excelência operacional e, por consequência, no momento de resposta aos incidentes, garantindo a continuidade das operações mesmo diante de adversidades.
- » **Princípio da Transparência:** criar procedimentos de continuidade acessíveis e claros, acarretando a confiança, o engajamento e a colaboração de todas as partes interessadas, aumentando, assim, a eficácia da resposta a crises e a resiliência operacional em face de interrupções.
- » **Princípio da Equidade:** fazer com que todos os profissionais e partes interessadas tenham acesso igualitário a recursos e suporte durante uma crise, promovendo, assim, uma cultura organizacional mais robusta e resiliente.
- » **Princípio da Responsabilização (Accountability):** garantir que todas as partes interessadas sejam responsáveis por suas ações e decisões relacionadas à preparação, resposta e recuperação de crises.
- » **Princípio da Sustentabilidade:** adotar procedimentos sólidos e bem estruturados para garantir que as operações sejam ecologicamente responsáveis, socialmente justas e economicamente viáveis a longo prazo, mesmo em face de crises ou interrupções.

4 DIRETRIZES

4.1 Análise de Impacto ao Negócio (BIA)

A Análise de Impacto nos Negócios (BIA – *Business Impact Analysis*) deve ser realizada periodicamente para identificar os processos essenciais da CERC e entender as consequências de sua interrupção.

A BIA deve analisar os seguintes impactos:

- » Financeiro;
- » Reputacional;

- » Conformidade / Regulatório;
- » Cliente;
- » Tecnológico e Segurança da Informação; e
- » Operacional.

Com base nesses impactos, a BIA deve:

- » Classificar a criticidade dos processos;
- » Identificar dependências e recursos necessários para sua operação e recuperação;
- » Definir os tempos máximos de interrupção aceitáveis (RTO/RPO); e
- » Orientar a priorização dos processos e as ações preventivas.

Os tempos de retomada devem observar, no mínimo, o estabelecido na regulamentação aplicável.

4.2 Análise de Riscos

A Gestão de Riscos da CERC deve identificar, avaliar e tratar riscos que possam comprometer a continuidade das operações, garantindo que a Companhia opere dentro dos limites definidos em seu apetite de risco (*risk appetite statement*).

Com base nesses impactos, a BIA deve estabelecer:

- » Os requisitos regulatórios aplicáveis;
- » As melhores práticas de mercado; e
- » Metodologias formais de avaliação, monitoramento e tratamento de riscos.

A Análise de Riscos deve alimentar as estratégias do PCN e apoiar a definição de controles, redundâncias e mitigadores.

4.3 Plano de Continuidade de Negócios (PCN)

Plano de Continuidade de Negócios (PCN) reúne os documentos, procedimentos e orientações necessários para manter ou restabelecer as operações da CERC em situações de interrupção.

O PCN deve considerar diferentes tipos de eventos, como:

- » Desastres naturais;
- » Falhas tecnológicas;
- » Indisponibilidade de prestadores críticos;
- » Incidentes de segurança da informação;
- » Pandemias ou emergências de saúde pública; e
- » Eventos que afetem infraestrutura física ou lógica.

O PCN deve definir:

- » Procedimentos para resposta e recuperação;
- » Responsabilidades e fluxos decisórios;
- » Prazos estimados de retomada;
- » Modos de operação alternativa;
- » Mecanismos de comunicação interna e externa; e
- » Critérios de teste, atualização e melhoria contínua.

Para sua efetividade, o PCN é composto pelos seguintes planos:

4.3.1 Plano de Recuperação de Desastres (PRD)

O PRD consolida as informações e os procedimentos técnicos necessários para ativar a infraestrutura de contingência tecnológica.

O Plano deve:

- » Definir papéis e responsabilidades;
- » Registrar os pontos focais técnicos;
- » Documentar os procedimentos de recuperação; e
- » Garantir a ativação tempestiva da infraestrutura alternativa sempre que necessário.

Seu objetivo é assegurar a continuidade dos serviços críticos suportados pela infraestrutura tecnológica da CERC.

4.3.2 Plano de Comunicação em Crise (PCOM)

O PCOM orienta a gestão da comunicação em situações de crise envolvendo a CERC, seus executivos, ativos ou operações.

O plano deve:

- » Estruturar mensagens e fluxos de comunicação;
- » Definir responsáveis e canais oficiais;
- » Garantir comunicação ágil, alinhada e tempestiva; e
- » Preservar a reputação, credibilidade e transparência da Companhia.

Uma comunicação bem coordenada reduz impactos e contribui para a retomada organizada das atividades.

4.3.3 Plano de Emergência de Segurança da Informação (PESI)

O PESI reúne os procedimentos para identificar, tratar, comunicar e recuperar incidentes de Segurança da Informação.

O plano deve incluir:

- » Papéis e responsabilidades;
- » Processos de detecção, avaliação e resposta a incidentes;
- » Mecanismos de comunicação e escalonamento; e
- » Cenários mínimos, como *ransomware* e vazamento de informações.

O objetivo é garantir que incidentes de segurança sejam rapidamente identificados, tratados e controlados, minimizando seus impactos ao negócio.

4.3.4 Plano de Emergência Integridade Física e Saúde Pública (PEIFSP)

O PEIFSP deve ser acionado quando houver risco à vida ou à integridade física de colaboradores, prestadores ou da sociedade em geral.

O plano deve:

- » Definir responsabilidades e pontos de contato;
- » Orientar ações imediatas de proteção;
- » Estabelecer fluxos de comunicação; e
- » Garantir a segurança das pessoas envolvidas.

4.3.5 Plano de Prestadores de Serviços Críticos (PSC)

O PSC orienta como agir em caso de indisponibilidade de prestadores essenciais, especialmente serviços de:

- » Processamento e armazenamento de dados;
- » Computação em nuvem; e
- » Serviços tecnológicos críticos.

O plano deve prever:

- » Cenários de interrupção;
- » Medidas emergenciais;
- » Possíveis substituições; e
- » Estratégias para restabelecimento da operação normal.

4.3.6 Plano de Gestão de Crise (PGC)

O PGC deve viabilizar os procedimentos a serem adotados antes, durante e após uma situação de crise, bem como definir a estrutura organizacional da equipe de gerenciamento de crises e os seus papéis e responsabilidades.

O documento deve estabelecer padrões estruturados que objetivam auxiliar nas respostas a possíveis situações que caracterizam uma crise, conforme a descrito a seguir:

- » Obter o controle da situação o mais breve possível;
- » Comunicar as partes interessadas internas e externas;
- » Descrever a estrutura, os papéis e as responsabilidades de forma objetiva;
- » Contar com uma liderança efetiva em todos os níveis da organização;
- » Garantir pessoas com competência em papéis específicos de gestão de crises por meio de treinamentos, exercícios e avaliações de conhecimentos, habilidades e experiência;
- » Manter um log compreensivo de registros e políticas de todas as decisões tomadas; e
- » Aprender com os erros e efetuar mudanças para evitar sua recorrência.

4.3.7 Plano de Saída Ordenada (PSO)

O PSO define as ações necessárias para garantir a descontinuação organizada das atividades da CERC caso as estratégias de recuperação adotadas não sejam suficientes para manter sua viabilidade.

4.3.8 Contingência física

A indisponibilidade de instalações físicas é compreendida por situações de catástrofes naturais ou não, como inundações, incêndios, desabamentos, interdições, manifestações etc., que impeçam o acesso e/ou a utilização das instalações físicas de uso regular da CERC para condução de suas operações.

Nestes casos, os funcionários e terceiros da CERC devem se direcionar para as suas residências ou permanecerem em casa, atuando remotamente utilizando as ferramentas disponibilizadas pelo time de Tecnologia, até que o ambiente físico seja liberado para o retorno à normalidade.

4.3.9 Contingência lógica

A indisponibilidade lógica é compreendida por situações que envolvem, principalmente, as tecnologias hospedadas em nuvem. Para diferentes cenários possíveis, devem ser elaborados planos que permitam a atuação das equipes de forma coordenada a fim de diminuir os impactos.

4.4 Treinamento

O treinamento e a conscientização de todos os colaboradores objetivam preparar as pessoas para os momentos de contingência, de forma a garantir a continuidade do negócio.

A realização deve ser periódica, de modo a ratificar a importância da contribuição individual para a eficácia do sistema de gestão, dos papéis durante incidentes que causem interrupção, bem como das implicações da não conformidade com os requisitos estabelecidos nesta Política e nos demais documentos relacionados.

4.5 Testes e Melhorias Contínuas

Para garantir que as atividades compreendidas nesta Política cumpram com os seus objetivos, a CERC deve realizar, anualmente, testes, de forma a garantir que o PCN contenha as informações necessárias e produza o resultado desejado, quando colocado em prática.

Os resultados dos testes devem ser consolidados em relatórios específicos, em que são apresentadas as deficiências, os planos de ação, bem como os prazos para implementação. Os pontos de atenção e melhoria identificados nos testes servem de insumo para atualização da estratégia e dos planos, em um processo constante de evolução.

Os relatórios devem ser armazenados em diretório de rede e, sempre que solicitado, devem ser disponibilizados para as partes interessadas. Após realização do calendário de testes, os resultados devem ser enviados, via e-mail, ao Conselho de Administração e aos órgãos reguladores (Comissão de Valores Mobiliários e Banco Central do Brasil).

Devem ser elaboradas melhorias nos planos após os resultados dos testes que contemplam cenários de incidentes de continuidade de negócios e de operações de riscos significativos de ruptura, incluindo eventos que podem causar uma interrupção em larga escala.

As alterações planejadas pela CERC, que venham a afetar de maneira relevante a gestão da continuidade de negócios, deve ser comunicada ao Banco Central do Brasil com 30 (trinta) dias de antecedência.

5 DISPOSIÇÕES FINAIS

- » Deverão ser observadas as diretrizes contidas nos seguintes documentos: Estatuto Social, Regimentos Internos e demais Normativos Internos da CERC.
- » Esta Política ficará armazenada na estrutura de documentos da área de Gestão de Continuidade do Negócio em Plataforma de Normativos e será disponibilizado a todos os envolvidos.
- » As informações relativas ao PCN deverão ser arquivadas por, no mínimo, dez (10) anos.
- » A Gestão de Continuidade de Negócios envolve a conscientização e o treinamento de funcionários, a revisão contínua de políticas e procedimentos, bem como a colaboração de partes interessadas externas, como fornecedores e parceiros, para garantir uma resposta coordenada em emergências.

6 ATRIBUIÇÕES E RESPONSABILIDADES

6.1 Conselho de Administração

- » Aprovar esta Política, após recomendação dos comitês de assessoramento responsáveis.

6.2 Comitê de Riscos

- » Validar o monitoramento de riscos da Companhia.

- » Monitorar se os controles e Planos para continuidade de negócio estão alinhados com os riscos identificados e as melhores práticas do setor.
- » Desempenhar um papel crítico na gestão dos riscos de continuidade de negócios e na garantia de que a empresa esteja preparada para enfrentar eventos adversos e manter suas operações de forma resiliente.

6.3 Comitê de Auditoria

- » Supervisionar a implementação da Política de Continuidade de Negócios, assegurando que os mecanismos de prevenção, detecção e resposta aos incidentes estejam em funcionamento e sejam efetivos.
- » Acompanhar os relatórios finais de exercícios e testes.

6.4 Diretoria Estatutária

- » Garantir que a Gestão de Continuidade de Negócios esteja adequada às necessidades da CERC e em linha com os objetivos estratégicos.
- » Garantir a disponibilidade de recursos necessários para a continuidade das operações.
- » Deliberar sobre temas estratégicos relacionados à continuidade de negócios.

6.5 Área de GCN – Diretoria de Tecnologia e Operações

- » Elaborar, revisar e atualizar a Política de Continuidade de Negócios, bem como normativos relacionados.
- » Definir metodologia, critérios, premissas e orientações para elaboração dos planos de contingência e BIAs pelas áreas responsáveis.
- » Coordenar, apoiar e supervisionar a construção dos planos e BIAs, assegurando padronização e aderência regulatória.
- » Promover treinamentos e ações de conscientização sobre continuidade de negócios.
- » Consolidar e elaborar relatórios de testes e exercícios, acompanhando a implementação dos planos de ação.

6.6 Área de Riscos, Controles e Compliance – Diretoria de Integridade e Conformidade

- » Avaliar se os cenários para teste contemplam todos os principais itens dos planos listados no PCN e identificar os eventuais impactos.
- » Orientar/contextualizar os executivos sobre os principais riscos de negócio e compliance.
- » Acompanhar e monitorar as crises.
- » Garantir que os requisitos regulatórios são atendidos pelo sistema de gestão de continuidade de negócio.

6.7 Área de Comunicação e Marketing – Diretoria de Produtos

- » Gerenciar e atualizar o Plano de Comunicação em Crise (PCOM).
- » Compreender os cenários de crise e receber as demandas relacionadas à comunicação.
- » Acionar a assessoria de imprensa, quando necessário.
- » Atuar para preservar a credibilidade e reputação da Companhia, minimizando impactos de repercussão pública.
- » Emitir comunicações internas, em conformidade com orientações jurídica e de compliance.

- » Validar e enviar comunicados oficiais.

6.8 Área do Jurídico Corporativo – Diretoria Jurídica

- » Avaliar o cenário e identificar impactos jurídicos potenciais.
- » Orientar os executivos sobre riscos legais associados ao evento.
- » Acionar escritórios jurídicos especializados quando necessário.

6.9 Área de Tecnologia da Informação

- » Gerenciar e atualizar o Plano de Recuperação de Desastres (PRD).
- » Executar e documentar testes periódicos de continuidade e recuperação tecnológica.
- » Assegurar a alta disponibilidade, resiliência e integridade dos ambientes tecnológicos da Companhia.

6.10 Gestores da Companhia

- » Colaborar com a área de Continuidade de Negócios em atividades relacionadas aos seus processos.
- » Fornecer informações completas e atualizadas sobre seus processos para análises de risco e impacto.
- » Participar de treinamentos, testes e exercícios de continuidade.
- » Gerenciar e atualizar os procedimentos e os planos relativos à continuidade/contingência de suas áreas.
- » Informar a área de GRC e GCN sobre mudanças relevantes que possam impactar a continuidade operacional.

6.11 Colaboradores, Fornecedores e Usuários dos Sistemas CERC

- » Cumprir as diretrizes desta Política, bem como os procedimentos de continuidade estabelecidos nos respectivos Planos.
- » Participar dos treinamentos obrigatórios sempre que convocados.

6.12 Auditoria Interna – Diretoria de Integridade e Conformidade

- » Acompanhar testes de continuidade e recuperação.
- » Emitir parecer independente sobre a efetividade do Sistema de Gestão de Continuidade de Negócios.

6.13 Grupos de Crise (Operacional, Tático e Estratégico)

- » Gerenciar situações de crises em diversas frentes, conforme estabelecido em normativos internos.

7 CONTROLE DOCUMENTAL

CRIAÇÃO REVISÃO REVOGAÇÃO			
Versão Anterior	Versão Atual	Data da Aprovação	Ref. De ATA/Aprovação

3.1	4.0	02/06/2026	Conselho de Administração
Diretoria Responsável		Área Responsável	
Tecnologia e Operações		Gestão de Continuidade do Negócio	
PRINCIPAIS MODIFICAÇÕES			
Alterações: » Unificação dos “Planos de Emergência”: “Pandemia – PEP” e “Emergência: Integridade Física – PEIF” para “Plano de Emergência Integridade Física e Saúde Pública (PEIFSP)”; » Reescrita dos Capítulos, visando maior clareza das diretrizes e descrições.			
Inclusões: » Inclusão do Plano de Saída Ordenada.			
Revogações: » N/A			

LEGISLAÇÕES OU DOCUMENTOS RELACIONADOS
» Resolução 304/2023 BCB; » ABNT NBR ISO22301 DE 06/2020 - Segurança e resiliência — Sistema de gestão de continuidade de negócios — Requisitos; e » Disaster Recovery Institute International (DRI).

8 ANEXOS

8.1 Anexo 1 - Definições

- » **Ativação:** Significa trocar o modo de normalidade para o modo de contingência, o que deverá ser realizado em conformidade com a alçada definida.
- » **Cenários:** Situações hipotéticas que podem afetar os recursos utilizados para sustentar a operação, causando impactos relevantes para o negócio.
- » **Continuidade de Negócios:** A capacidade da organização continuar a entrega de seus produtos e serviços, em níveis aceitáveis previamente definidos, após incidentes de interrupções abruptas.
- » **Grupos de Crise:** Grupos (operacional, tático e estratégico) constituídos para gerir situações de crise em diversas frentes, como as seguintes:
 - Grupo Operacional: atua em cenários previstos, com ações de contorno e reestabelecimento conhecidos e testados com tempo de solução conhecido;
 - Grupo Tático: atua em cenários previstos, não controlados, sem solução/contorno definido e com tempo de solução não conhecido ou que excede aos tempos aceitáveis;

- Grupo Estratégico: atua em cenários não previstos, não controlados, com tempo de solução não conhecido e que exigem reporte externo.
- » **Níveis de Ativação:** Categorias definidas para a ativação dos processos e recursos de contingência, conforme nível de impacto, e que representam uma resposta adequada à relevância e criticidade de cada situação.
- » **Plano de Continuidade de Negócios (PCN):** Conjunto de processos, planos, regras e parâmetros a serem seguidos e/ou considerados para a CERC lidar com ameaças em potencial e impactos nas operações de negócio, que constitui um guia para nortear as ações de continuidade de negócios.
- » **RTO (ponto de recuperação):** Tempo máximo que o processo tolera de indisponibilidade. Representa o momento exato após o incidente que o processo começa a causar impactos relevantes para o negócio e precisa ser recuperado em níveis aceitáveis.
- » **Business Impact Analysis (BIA):** Avaliação realizada por processo ou produto objetivando aferir os possíveis impactos durante situações de interrupções abruptas e os seus respectivos RTOs.