Política de Continuidade de Negócios

Versão 3.0

SUMÁRIO

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:

- **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.
- **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.
- **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.
- **Responsabilização (*Accountability*)**: garantir que todas as partes interessadas sejam responsáveis por suas ações e decisões relacionadas à preparação, resposta e recuperação de crises.
- **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)

Para uma adequada gestão de continuidade negócios na CERC, deverá ser realizada periodicamente uma Análise de Impacto nos Negócios (também conhecido como BIA, do inglês, "*Business Impact Analysis"*), que serve de apoio para a elaboração de estratégias que assegurem a continuidade das atividades e limitem as perdas decorrentes da interrupção dos processos críticos de negócio.

A Análise de Impacto nos Negócios deve ser utilizada com a finalidade identificar, analisar os processos e/ou as atividades de negócios, classificando o nível de impacto do tempo de inatividade desses processos nas atividades "*core business*" da organização, estabelecendo metas de recuperação e

priorização de ações preventivas. As metas de retomada da operação (RTO) deverão observar os tempos mínimos previstos na regulamentação aplicável.

4.2 Análise de Riscos

A Gestão de Riscos adotada pela CERC deverá identificar, avaliar e atuar acerca dos riscos ao negócio, de forma que a assunção de riscos (*risk apettite statement*) da Companhia esteja dentro de parâmetros adequados à continuidade da operação.

Além disso, os processos e procedimentos relacionados à gestão de riscos da CERC devem atender aos requerimentos regulatórios vigentes, bem como as melhores práticas.

4.3 Plano de Continuidade de Negócios (PNC)

O Plano de Continuidade de Negócios (BCP, do inglês "*Business Continuity Plan*") é o conjunto de documentos estratégicos que são elaborados para garantir a resiliência e a continuidade das operações diante de eventos disruptivos.

Os planos devem abranger uma variedade de situações, como desastres naturais, falhas tecnológicas e pandemias, que são capazes de interromper as atividades normais da CERC.

Os Planos de Continuidade de Negócios devem estabelecer procedimentos e prazos estimados para o reinício e a recuperação das atividades, em caso de interrupção dos processos críticos de negócio. Além disso, devem prever ações e procedimentos claros para a comunicação interna e externa, definir responsabilidades específicas e estabelecer métricas para a avaliação e o aprimoramento contínuo.

O objetivo principal é assegurar que a organização consiga enfrentar as adversidades de maneira organizada, minimizando os impactos negativos e garantindo a continuidade de suas operações essenciais.

Desse modo, devem ser adotados os seguintes planos como suporte:

4.3.1 Plano de Recuperação de Desastres – PRD

O Plano de Recuperação de Desastres (PRD) deve consolidar todas as informações necessárias para viabilizar, de forma tempestiva e organizada, a ativação da infraestrutura de contingência estabelecida.

O PRD deve estabelecer papéis e responsabilidades, documentar os pontos focais técnicos estratégicos, assim como os procedimentos técnicos que deverão ser executados em situações de desastres para assegurar, sempre que necessário, a ativação da infraestrutura de contingência e consequentemente, a continuidade dos negócios críticos referente a infraestrutura tecnológica da CERC.

4.3.2 Plano de Comunicação - PCOM

O Plano de Comunicação (PCOM) deve direcionar a correta gestão da comunicação em situações de crise que envolvem a CERC, seus executivos, seus ativos e suas operações, indicando ações de forma a mitigar ou reduzir os prejuízos para a Companhia.

Em momentos de crise, a condução da comunicação deve ser organizada, estruturada e imediata, visando preservar a credibilidade e a reputação da organização, tanto no sentido de minimizar possíveis impactos causados pela repercussão do evento como também para auxiliar a rápida reestruturação da empresa do cenário de crise.

Quanto mais preparada a empresa estiver para enfrentar esses momentos, mais ágil, consistente e confiável será a sua resposta e consequentemente, a percepção e a manutenção de sua imagem.

4.3.3 Plano de Emergência de Segurança da Informação – PESI

O Plano de Emergência de Segurança da Informação (PESI) deve consolidar todas as informações necessárias para identificar, tratar e mensurar incidentes relacionados à área de Segurança da Informação.

Deverá fazer parte do PESI a documentação de papéis, responsabilidades, procedimentos e recursos que são necessários para a ativação e a execução do Plano nos momentos necessários.

O objetivo do documento é assegurar a identificação, tratativa, comunicação e recuperação dos negócios sempre que um dos cenários descritos no Plano (*ransomware* e vazamento de informações) se materializar.

4.3.4 Plano de Emergência: Pandemia - PEP

O Plano de Emergência: Pandemia (PEP) deverá ser empregado para minimizar o risco de disseminação doenças infecciosas, em um cenário pandêmico, entre os colaboradores, com o intuito de preservação da vida e a continuidade das operações por meio do trabalho remoto.

O seu objetivo é identificar as atividades, papéis e responsabilidades durante a execução do Plano, em cada uma das etapas.

4.3.5 Plano de Emergência: Integridade Física - PEIF

O Plano de Emergência: Integridade Física (PEIF) deverá ser usado em situações que comprometam a integridade física dos colaboradores ou da sociedade em geral.

O seu acionamento deverá ocorrer no caso de emergências que coloquem em risco as vidas e/ou a integridade física dos funcionários e prestadores de serviços, especificando suas atividades, papéis e responsabilidades durante a execução do Plano.

4.3.6 Plano de Prestadores de Serviços Críticos - PSC

O Plano de Prestadores de Serviços Críticos (PSC) deve conter os procedimentos a serem seguidos em caso de interrupção dos serviços relevantes contratados, especialmente os de processamento e armazenamento de dados e de computação em nuvem, abrangendo cenários que consideram a substituição da empresa contratada e o reestabelecimento da operação normal da CERC.

4.3.7 Plano de Gestão de Crise - PGC

O Plano de Gestão de Crises (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;
- Aprender com os erros e efetuar mudanças para evitar sua recorrência.

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.

4.3.10 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.

4.3.11 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

5.1 Guarda e disponibilização da documentação

» Toda a documentação que suporta a Gestão de Continuidade de Negócios deve estar disponível a todos os colaboradores da CERC em um diretório específico.

» As informações relativas ao PCN deverão ser arquivadas por, no mínimo, dez (10) anos.

5.2 Medidas coordenadas

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

» Deverão ser observados conforme atribuição de cada membro abaixo listado, as diretrizes contidas nos seguintes documentos: Estatuto Social, Regimentos Internos e demais Normativos Internos da CERC.

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; e

» 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; e

» Acompanhar os relatórios finais de exercícios e testes.

6.4 Diretoria Executiva

» Garantir que a Gestão de Continuidade de Negócios esteja adequada às necessidades da CERC e em linha com os objetivos estratégicos;

» Garantir a existência dos recursos necessários para manutenção da continuidade do negócio; e

» Deliberar sobre questões estratégicas no que tange ao tema.

6.5 Área de Gestão de Continuidade do Negócio (GCN)

» Estabelecer e gerir continuamente o sistema de gestão de continuidade de negócios, desenhado de acordo com as necessidades e objetivos da CERC;

» Elaborar e manter atualizados os documentos relacionados a Continuidade de Negócios, incluindo a análise de impacto ao negócio (BIA);

» Prover treinamentos e conscientização relacionadas à Gestão de Continuidade aos colaboradores e terceiros;

» Determinar as abordagens necessárias para a realização das avaliações de risco e impacto ao negócio;

» Mapear novos planos de continuidade, conforme alterações estruturais e *input* das áreas;

» Garantir que os requisitos regulatórios são atendidos pelo sistema de gestão de continuidade de negócio; e

» Elaborar relatório final de exercícios e testes, bem como acompanhar as ações corretivas e compartilhá-los junto aos *stakeholders*, incluindo o Comitê de Auditoria (COAUD).

6.6 Área de Governança, Riscos e *Compliance* (GRC)

» Avaliar os cenários e identificar os eventuais impactos;

» Orientar/contextualizar os executivos sobre os principais riscos de negócio e *compliance*;

» Acompanhar e monitorar as crises; e

» Garantir que os requisitos regulatórios são atendidos pelo sistema de gestão de continuidade de negócio.

6.7 Área de Comunicação

» Entender os cenários de crise e receber as demandas pertinentes à comunicação;

» Acionar a empresa responsável pela assessoria de imprensa;

» Atuar de forma a preservar a credibilidade e a reputação da organização, tentando minimizar os possíveis impactos causados pela repercussão do evento;

» Providenciar as comunicações internas aplicáveis (conforme orientação jurídica e de *compliance*); e

» Validar e disparar comunicados.

6.8 Área do Jurídico

» Entender o cenário e avaliar os impactos jurídicos;

» Orientar/contextualizar os executivos sobre os principais riscos legais;

» Acionar os grupos de apoio, como escritórios jurídicos especializados; e

6.9 Área de Tecnologia da Informação

» Gerenciar e atualizar os planos de recuperação de desastres sempre que necessário;

» Realizar e documentar testes periódicos de continuidade e recuperação; e

» Atuar com foco na garantia de alta disponibilidade da CERC.

6.10 Gestores da Companhia

» Atuar em conjunto com os responsáveis de Continuidade de Negócios em atividades que sejam escopo de seus mandatos;

» Fornecer informações sobre os seus processos para que seja realizada uma adequada análise de risco e de impacto ao negócio;

» Participar dos treinamentos e testes dos planos de continuidade de negócio;

» Gerenciar e atualizar os procedimentos e os planos relativos à continuidade/contingência de suas áreas; e

» Informar a área de GRC sobre mudanças relevantes em suas estruturas.

6.11 Colaboradores, fornecedores e usuários dos sistemas CERC

» Cumprir as diretrizes desta Política, bem como os procedimentos de continuidade estabelecidos nos respectivos Planos; e

» Participar dos treinamentos obrigatórios sempre que convocados.

6.12 Auditoria Interna

» Acompanhar testes de continuidade e recuperação; e

» Emitir parecer sobre a situação 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**
1.7	**1.8**	**22/03/2024**	**Conselho de Administração**
Diretoria Responsável		**Área Responsável**	
Operações		**Command Center – Gestão de Continuidade do Negócio**	
PRINCIPAIS MODIFICAÇÕES			
Esta Política foi integralmente reformulada para atender as melhores práticas de Gestão de Continuidade de Negócios e assegurar a aderência à Resolução 304/2023 BCB.			

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 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 report 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.