POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS

SUMÁRIO

CONTROLE DE VERSÃO 3
1. OBJETIVO 4
2. DEFINIÇÕES 4
3. ABRANGÊNCIA 4
4. PRINCÍPIOS 5
5. GESTÃO DE CONTINUIDADE DE NEGÓCIOS 5
5.1 Alocação de Recursos para o Risco de Continuidade 6
6. RESPONSABILIDADES 6
7. PLANO DE CONTINUIDADE DE NEGÓCIO E RECUPERAÇÃO DE DESASTRES . 7
7.1 Testes 8
8. TREINAMENTO 8
9. DISPOSIÇÕES FINAIS 8
10. CONTROLE DO DOCUMENTO 9
10.1 Vigência 9
10.2 Revisão 9
10.3 Direitos Autorais e Distribuição 9

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

1. OBJETIVO

Essa Política de Gestão de Continuidade de Negócios ("Política") tem por objetivo estabelecer princípios e diretrizes norteadores da Gestão de Continuidade dos Negócios na CSD CENTRAL DE REGISTRO E DEPÓSITO AOS MERCADOS FINANCEIRO E DE CAPITAIS S.A. ("CSD BR" ou "Companhia"), visando assegurar a continuidade de suas atividades críticas na ocorrência de eventos que impossibilitem a utilização, total ou parcial, de sua infraestrutura operacional, de recursos de Tecnologia da Informação e de Resiliência Cibernética, no intuito de evitar que os prejuízos financeiros, reputacionais e os impactos negativos à imagem institucional da Companhia atinjam níveis inaceitáveis.

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. 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, causam prejuízo 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: situação que implique ameaça para a Companhia;

(v) Desastre: evento que causa dano e/ou interrompe a execução de atividade crítica, por período superior a 2 (duas) horas;

(vi) Incidente: situação que pode representar ou levar à interrupção de negócios, perdas, emergências ou crises;

(vii) Plano de Continuidade de Negócios e Recuperação de Desastres ("PCN-RD"): documento que registra as ações a serem tomadas nos casos de crise e desastre, com o objetivo de manter um nível adequado e seguro de serviços aos Participantes, reguladores e ao mercado;

(viii) Plataforma: conforme definido no Glossário da Companhia.

3. ABRANGÊNCIA

Esta Política aplica-se a todos os colaboradores diretores e administradores da Companhia.

4. PRINCÍPIOS

(i) Prevenção: capacidade de evitar ou reduzir a possibilidade de ocorrência e os impactos de um incidente ou desastre;

(ii) 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;

(iii) Recuperação: processo de reparação do ambiente normal de trabalho e de seus recursos para o restabelecimento das atividades críticas após a ocorrência de incidentes ou desastres.

5. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

O objetivo da gestão de continuidade de negócios é: identificar ameaças em potencial à Companhia, os impactos nas operações de negócios que as ameaças podem vir a causar, e oferecer uma estrutura para desenvolver resiliência organizacional com a capacidade de resposta eficaz.

A Companhia definiu as situações, a saber:

(i) 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: comunicações/reportes de áreas e pessoas para as quais deverão ser efetuadas as comunicações em caso de incidentes e/ou interrupção dos processos críticos;

(iv) Aplicação de testes: serão realizados testes preventivos e de monitoramento, com objetivo de validar todos os processos da Companhia e evitar eventual incidente e/ou interrupção na prestação dos serviços;

(v) Continuidade operacional: procedimentos de resposta 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 as atividades essenciais da Companhia.

5.1 Alocação de Recursos para o Risco de Continuidade

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 de eventuais incidentes ou desastres, a Diretoria Executiva 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 reconstrução de toda a estrutura de um datacenter (servidores, *switches*, *firewalls* e outros).

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) Departamento de Produção e Segurança da Informação ("DPSI"): responsável pela análise e revisões desta Política, por submetê-la à aprovação do Conselho de Administração da Companhia, e pela aprovação do PCN-RD;

(iii) 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.

7. PLANO DE CONTINUIDADE DE NEGÓCIO E RECUPERAÇÃO DE DESASTRES

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, no qual 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;

(iii) identificação das localidades e sistemas considerados importantes para a continuidade do negócio:

  (a) Sistemas críticos são todos aqueles que impactam as atividades vinculadas ao processo de registro na Plataforma.

  (b) Sistemas não-críticos são todos aqueles que não impactam os sistemas descritos nos itens (a) e (b) acima, na Plataforma, como cobrança, apreçamento de Ativos e cadastro de novos Participantes.

  (c) Sistemas acessórios são todos aqueles que não impactam os sistemas descritos nos itens (a), (b) e (c) acima.

(iv) Prazo para retomada do serviço, prevalecendo, quando aplicável, aqueles constantes e normativos e na legislação:

  (a) Sistemas críticos: até 2 (duas) horas.

  (b) Sistemas não-críticos: até 4 (quatro) horas.

  (c) Sistemas acessórios: até 24 (vinte e quatro) horas.

(v) Cenários para Recuperação de Desastres;

(vi) Política 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.

(vii) 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:

i) Sistemas críticos e não-críticos: 1 (um) ano.

ii) Sistemas acessórios: 1 (um) ano.

iii) Em não havendo definição específica, deve ser considerada a periodicidade dos sistemas críticos e não-críticos.

(viii) O plano 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, conforme item 7 (vii) desta Política, considerando os seguintes pontos:

(i) acompanhamento da Diretoria de Governança, Riscos e Controles Internos ("GRC");

(ii) elaboração de um relatório com os resultados obtidos nos testes, em até 15 (quinze) dias da data de execução;

(iii) o relatório deverá ser encaminhado ao Conselho de Administração da Companhia, com análise e recomendações prévias por parte do Comitê de Fiscalização e Supervisão da Companhia.

8. TREINAMENTO

O treinamento visa alinhar o conhecimento relativo ao desenvolvimento e implantação do PCN-RD, avaliação de riscos, execução e análise de impacto nos negócios, execução dos testes previstos no PCN-RD, comunicação interna e externa, e o que mais for necessário para a melhor aplicação desta Política. Deve acontecer pelo menos uma vez ao ano.

O material de treinamento deverá ser desenvolvido pelos gestores das áreas e o treinamento deverá ser aplicado e, conjunto com a área de Recursos Humanos.

9. DISPOSIÇÕES FINAIS

Na existência de um PCN-RD que venha sofrer alterações em virtude da publicação desta Política, a Companhia terá prazo de 60 (sessenta) dias para revisá-lo 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

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", 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.