POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS

SUMÁRIO

CONTROLE DE VERSÃO

Data da Versão	Autores	Número da Versão	Descrição
19/02/2020	Presidente, GRC, Diretoria de Operações	1	Elaboração inicial 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 e os impactos negativos à imagem institucional da Companhia atinjam níveis inaceitáveis.

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 02 (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 financeiro.

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

3. ABRANGÊNCIA

Esta Política aplica-se a todos os colaboradores, incluindo 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 da Companhia de 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 da 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 responder de forma 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/Reporte 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.

(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

A fim de fazer frente a potenciais perdas que a Companhia venha a enfrentar, para 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 etc.).

O Conselho de Administração da Companhia, em situações de anormalidade do mercado, 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 Executiva: 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: Responsáveis por:

(a) elaboração 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 Plano de Continuidade de Negócio e Recuperação de Desastres (PCN-RD), onde serão descritos um conjunto de ações que identificam contingências, planos de ação, e estabelecerão estratégias e prazos para reinício e recuperação das atividades, a serem executados em situações de crise e/ou desastre.

No Plano, devem constar 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 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 impactam as atividades não-críticas ao processo de registro na Plataforma, como Cobrança, Apreçamento de Ativos e Cadastro de Novos Participantes.
    (c) Sistemas acessórios são todos aqueles que impactam as atividades não diretamente relacionadas ao processo de registro na Plataforma.
(iv) Prazo para retomada do serviço, prevalecendo, quando aplicável, aqueles constantes 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 Desastre;
(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: 6 (seis) meses.

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 (vii) do tópico 7, considerando os seguintes pontos:

(i) acompanhados pelo Departamento de Governança, Risco e Controles (“GRC”);

(ii) deverá ser elaborado um relatório com os resultados obtidos, em até 15 (quinze) dias da data de execução dos testes;

(iii) o relatório deverá ser encaminhado para o Conselho de Administração da Companhia, com análise e recomendações 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 externa, e o que mais for necessário para a melhor aplicação desta Política.

O material de treinamento deverá ser desenvolvido pelos gestores das áreas e o treinamento deverá ser aplicado pela área de Recursos Humanos em parceria com o GRC.

9. DISPOSIÇÕES FINAIS

Na existência de um PCN-RD na data de 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 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.

10.2 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.