MANUAL DE CONTROLES INTERNOS

8.5 Plano de Continuidade de Negócio (PCN)

SUMÁRIO

8. Lei Geral de Proteção de Dados

8.5. Plano de Continuidade de Negócio (PCN)

8.5.1. Objetivo

O plano de continuidade de negócios (PCN) visa a assegurar à **COOPERFAC** a continuação de seus negócios, em caso de paralisação decorrente de sinistro, de um ou mais processos considerados críticos. O sinistro torna-se realidade quando ameaças internas ou externas exploram as vulnerabilidades dos procedimentos.

8.5.2. Aplicabilidade

Este Plano de Continuidade de Negócios (PCN) é aplicável a todos os envolvidos no processo e fluxo de contingências.

8.5.3. Diretrizes

Em situações de contingência, os funcionários designados devem trabalhar em *Home Office* de forma que haja o mínimo impacto possível dentro das atividades da **COOPERFAC.**

O desenvolvimento do Plano de Continuidade de Negócios é baseado na avaliação dos processos críticos estabelecidos pela Administração compreendendo às suas principais etapas:

- Análise de riscos do negócio;
- Análise de Impacto nos Negócios;
- Estratégia de recuperação.

Dessa forma, será necessário simular emergências, definir responsabilidades e escopo de atuação para cada colaborador na execução do PCN. A manutenção do PCN atualizado e o treinamento dos colaboradores são fatores crítico de sucesso.

A implantação de um Plano de Continuidade de Negócios pelas instituições objetiva também atender às determinações que constam na Resolução 4557/17.

8.5.4. Responsabilidades

A Cooperfac atua neste Plano de Continuidade de Negócios (PCN) com a estrutura descritas a seguir:

8.5.5. Diretoria

São responsabilidades da Diretoria:

a) Aprovar e revisar a Plano de Continuidade Negócios (PCN);
b) Garantir que o PCN esteja alinhado aos objetivos estratégicos da Cooperativa;
c) Deliberar pela comunicação das diretrizes desse PCN a todos os níveis da Cooperativa e garantir que todos os empregados sejam treinados para efetiva implementação das medidas previstas;
d) Aprovar a realização de testes e simulações periódicas para avaliar a eficácia dos planos de continuidade operacional e identificar melhorias;
e) Assegurar a compatibilidade e a integração do PCN às demais políticas estabelecidas pela Cooperativa, principalmente a de gerenciamento de riscos.

Ao desempenhar essas funções de forma adequada, a Diretoria contribui para garantir que a organização esteja preparada para enfrentar e se recuperar de eventos disruptivos e proteger seus interesses, funcionários e partes interessadas.

8.5.6. Diretor Responsável pelo Plano de Continuidade de Negócio

São responsabilidades do Diretor responsável pelo PCN:

a) Responder pelo cumprimento deste PCN;
b) Responsabilizar para que a área e/ou processos sob sua supervisão tenham participação e comprometimento com as responsabilidades conforme direcionamentos deste PCN;
c) Adotar procedimentos de controles de atualização deste PCN, bem como documentar suas estratégias, rotinas e procedimentos para cumprimento de suas diretrizes;
d) Auxiliar as áreas internas da Cooperativa conforme necessidade e relevância dos acontecimentos;

Repassar as informações para os demais membros da Diretoria e apoiar os colaboradores.

8.5.7. Colaboradores

Tomar conhecimento das diretrizes deste Plano de Continuidade de Negócios (PCN).

8.5.8. Unidade Principal Cooperfac e Backup

A COOPERFAC fica localizada no endereço: Via de Acesso Professor Paulo Donato Castellani s/n, Rural, Jaboticabal/SP situada dentro do campus da Unesp de Jaboticabal na Alameda Periquitos.

As informações da COOPERFAC são armazenadas em DataCenter utilizando a estrutura da empresa Amazon, responsável por gerenciar o cloud da empresa Fácil Informática e as planilhas eletrônicas e documentos internos da cooperativa pelo Google Workspace que compreende servidor em nuvem, o acesso à informação é restrito as pessoas que devem acessar e este controle é feito através de ferramentas específicas que permitem que o responsável pela informação acesse ou não a aplicação.

Além do controle de acesso, a COOPERFAC possui diversas ferramentas para proteção de dados, tais como: monitoração do ambiente, antivírus e *firewalls.*

Além destas ferramentas, a área Gestora da segurança da informação também possui políticas e processos específicos que fornecem informações importantes sobre o que usuário pode ou não fazer quando está utilizando um computador da COOPERFAC, sendo que para que todos os usuários tenham conhecimento destas políticas, treinamentos são feitos quando colaborador começa a trabalhar na empresa e anualmente treinamentos de reciclagem devem ser feitas.

No sistema FacCred da empresa Facil Informática é utilizado um método de salva periódica dos sistemas e informações. O *Backup* é realizado diariamente em espaço na nuvem, de forma criptografada. É executado os testes semanalmente (restauração em ambiente de homologação) para garantir sua integridade.

As informações armazenadas nos discos rígidos locais das estações não possuem *backup*. Assim todos os colaboradores da Cooperfac são orientados a armazenar os arquivos em geral, como documentos de texto, planilhas eletrônicas e apresentações no Google Workspace.

8.5.9. Analise de Riscos

A análise de riscos do negócio tem por objetivo identificar, tanto no setor da Tecnologia da Informação, quanto nas demais áreas do **COOPERFAC**, os serviços vitais para o funcionamento e o seu impacto nas operações, caso estejam inoperantes.

Deste modo, voltando-se ao tratamento de dados perante a LGPD, apontamos a criticidade dos sistemas no tocante a operacionalidade perante as atividades.

Os serviços/sistemas de criticidade alta para a continuidade das operações são denominados de camada VERMELHA, sendo eles:

- Sistema *FacCred* (gestão);
- Sistel Fibra (fornecedor do link de Dados Dedicado)

Os serviço/sistema de criticidade média para continuidade das operações, denominado de camada LARANJA, é:

- Google Workspace.

Por sua vez, os sistemas/serviço de criticidade baixa para continuidade das operações, denominados camada VERDE, são:

- *E-mail;*
- Telefone.

Os sistemas a seguir apresentados trazem a **COOPERFAC** risco aceitável na sua utilização, pois não possuem gerência quanto a sua funcionalidade

- E-Social e
- INSS.

8.5.10. Análise de Impacto nos Negócios

Para pleno funcionamento da cooperfac, apenas os *softwares* da camada VERMELHA são essenciais para continuação imediata das operações, sendo que os itens mínimos para prosseguimento são:

- Computador *desktop* ou *notebook*;
- Acesso à *internet* para utilização dos sistemas da camada VERMELHA;
- Restauração dos dados no *backup.*

Desta forma, será necessário simular situações de emergências, definir responsabilidades e escopo de atuação para cada colaborador na execução do PCN atualizado e o treinamento dos colaboradores são fatores críticos de sucesso.

8.5.11. Plano de Monitoração de Declaração de Desastre

8.5.11.1. Definição de Desastre

Será considerado desastre quando o tempo total de recuperação dos dados ultrapasse 1 (um) dia útil, impossibilitando, assim, a efetivação das atividades na **COOPERFAC**.

8.5.11.2. Monitoramento de Comunicação de Eventos

Qualquer colaborador da **COOPERFAC**, ao constatar alguma anormalidade que paralise quaisquer processos deverá comunicar o fato ao seu Diretor responsável pela área gestora.

Responsáveis	Gestor/Líder	Telefones	E-mail
Diretor responsável pela área Gestora	Antonio Carlos Sanches	16-99777-5393	carlos.sanches@unesp.br

Este é o meio de comunicação a ser utilizado pelos colaboradores da Cooperfac como ponto central de contato para solicitar ajuda ou relatar alguma situação que demande o acionamento do PCN.

Em casos de vazamento de dados, considerado como incidente relevante e/ou que configurem uma situação de crise pela Cooperfac, as notificações devem ser feitas também ao Banco Central do Brasil, para as devidas providências, de acordo com o Art. 20 da Resolução 4.893/2021.

8.5.11.3. Fluxo do Plano de Continuidade de Negócio PCN

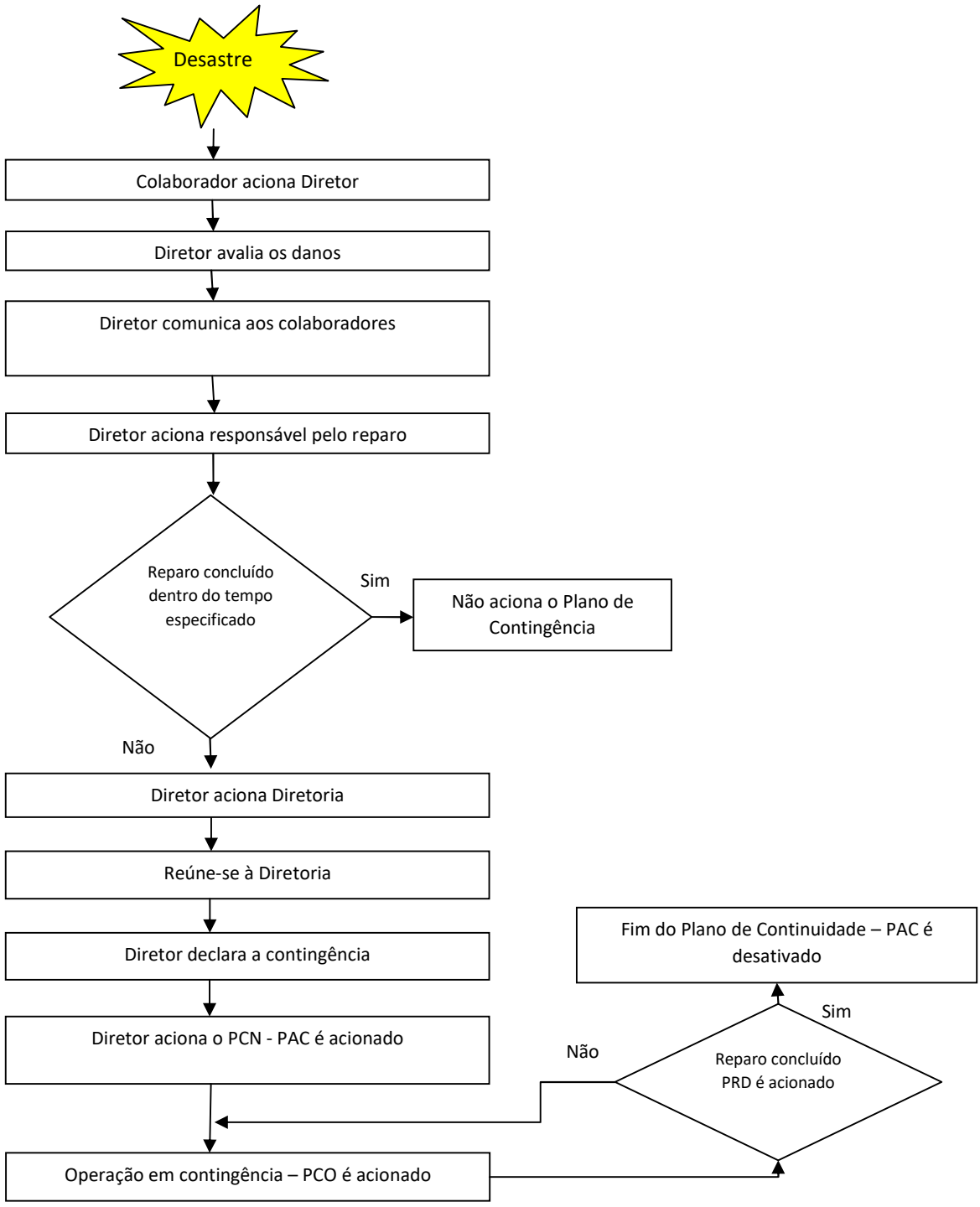
Ao acionar o PCN existem duas possibilidades de execução:

- PCN I (Interno) - A continuidade do negócio no site principal, no caso de o impacto não atingir o local físico da operação;
- PCN E (Externo) – Reunir a equipe e definir local para continuidade da prestação de serviços, caso o impacto atinja as instalações físicas do lugar de operação.

Ao ocorrer quaisquer eventos que paralise algum processo essencial ao negócio, o colaborador em questão avaliará e comunicará o Diretor responsável pelo PCN.

Com base nas informações recebidas e avaliando o grau de impacto versus horário crítico, compete ao Diretor declarar ou não a contingência. Em caso da ausência do Diretor responsável pelo PCN assumirá interinamente o Diretor Presidente.

Na figura abaixo está descrito Fluxo de Acionamento do PCN que resultará ou não na declaração da contingência.


Desastre
Colaborador aciona Diretor
Diretor avalia os danos
Diretor comunica aos colaboradores
Diretor aciona responsável pelo reparo
Reparo concluído dentro do tempo especificado
Sim
Não aciona o Plano de Contingência
Não
Diretor aciona Diretoria
Reúne-se à Diretoria
Diretor declara a contingência
Diretor aciona o PCN - PAC é acionado
Operação em contingência – PCO é acionado
Reparo concluído PRD é acionado
Não
Sim
Fim do Plano de Continuidade – PAC é desativado

8.5.12. Processos e Sistemas Críticos

Processo crítico pode ser definido como um processo de trabalho que, uma vez paralisado por tempo superior ao definido pela área gestora do negócio, irá afetar sensivelmente as operações e serviços da organização gerando maior impacto nos clientes, definido pela fórmula (MTD = RTO + WRT).

Definição:

- MTD (Maximum Tolerable Downtime) = Trata-se do tempo máximo que um negócio pode tolerar a ausência ou indisponibilidade de uma função de negócio em particular. Diferentes funções de negócio terão diferentes MTD's.
- RTO (Recovery Time Objective) = Tempo disponível para recuperar sistemas e recursos de uma ruptura.
- WRT (Work Recovery Time) = Tempo que leva para copiar e rodar uma vez os sistemas (hardware, software e configuração) a serem restaurados para as funções de negócios críticas.

8.5.13. Abrangências

Das ameaças relacionadas, no entendimento da diretoria as áreas avaliadas com grau de vulnerabilidade significante estão divididas em:

a) Humanas: Greves, Distúrbio Civil, Falha de Prestador de Serviços/Parceiro, Acesso Indevido às Instalações e Erro Humano não intencional;

b) Tecnológicas: Falha em Aplicativo (SW), Falha em *Hardware* (HW), Falha em sistemas Operacionais, Vírus de Computador, Falha em Rede Interna (LAN), Falha na Entrada de Dados, Falha em Rede Externa (WAN), Falha de Dados e Falha em Sistema de Acesso;

c) Infraestrutura: Falha em Telecom - Voz, Falha em Sistema de Refrigeração, Interrupção de Energia Elétrica, Falha em Instalações Elétricas;

d) Naturais: Alagamento Interno do Ambiente, Queda de Raios, Vendaval, Incêndio e pandemia;

e) Físicas: Problema Estrutural ou de Instalações e Rompimento de Tubulação Interna (água, esgoto e gás).

Cabe ressaltar que paradas não programadas podem resultar em perdas tangíveis e intangíveis aos negócios da **COOPERFAC**, acarretando perda de confiança de colaboradores e cooperados nos processos de negócios. Desta forma, os potenciais impactos apontados pela diretoria numa eventual interrupção no negócio são:

- Interrupção de prestação de serviços aos cooperados;
- Multas e sanções;
- Perda da capacidade de gestão e controle;
- Comprometimento da imagem da organização;
- Exposição negativa na mídia e perda de vantagem competitiva.

8.5.14. Ações e Procedimentos

Todos os colaboradores deverão estar aptos a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente ao líder do plano de continuidade de negócios.

a. Impossibilidade de Acesso ao Prédio

Dentre as ameaças que impossibilitam o acesso ao prédio destacam-se:

- Princípio de Incêndio;
- Ameaça de Bomba;
- Bloqueios;
- Manifestações.

b. Ações de 05 a 10 minutos após a evidência

Responsável: Líder do PCN na Cooperfac.

Procedimentos:

Entrar em contato com a Administração do local onde o prédio fica situado para esclarecimentos e caso necessário, também fazer contato com os seguintes órgãos públicos:

- Bombeiros: 193 (Incêndio e Ameaça de Bomba);
- Defesa Civil: 199 (Ameaça de Bomba, Greves, Bloqueios e Inundações);
- Polícia Civil: 147 (Ameaça de Bomba, Roubo e Furto de Informações e ativos).

c. Ações em até 20 minutos após a conclusão da etapa anterior

Entrar em contato com o responsável pelo site *backup*, para avisá-lo sobre a ocupação dos integrantes das áreas contingenciadas e disponibilizar local, *notebook* e impressora, assim como acesso à *Internet*, bem como avisar os componentes que atuarão em regime *Home Office*.

Avisar aos integrantes das áreas contingenciadas para que se dirijam ao endereço determinado, ou às residências para atuação no regime *Home Office*.

Disponibilizar alertas no *site* e nas Mídias sociais da **COOPERFAC** indicando o *status* de contingência, telefones dos colaboradores e telefone fixo para atendimento.

d. Falha na Infraestrutura e Tecnologia

Para não haver interrupções nas atividades o ambiente de TI deve ter infraestrutura mínima para continuidade do negócio:

- Servidores;
- Dados armazenados nos sistemas;
- Energia Elétrica.

Na falta de energia elétrica, além das baterias próprias dos *Notebooks*, deverão ser ativados automaticamente os *nobreaks* de 600VA para computadores, não gerenciáveis, com autonomia de 30 minutos em média.

e. Acionamento da Contingência externa

As equipes irão para o lugar destinado a cada uma delas.

Manter contato com a Unesp responsável pelas telecomunicações através do e-mail dti.fcav@unesp.br e telefone (16) 3209-7182 e solicitar o encaminhamento de todas as ligações para os ramais do local de contingência, se for o caso.

8.5.15. Procedimentos de Retorno à Normalidade

Cabe ao setor responsável encerrar o PCN e comunicar a Diretoria.

Quando o acesso ao prédio estiver liberado e em condições de normalidade, comunicar a todos os colaboradores da **COOPERFAC**, por meio Diretor Responsável, para que retornem aos seus postos de trabalho no dia seguinte.

Retirar o comunicado publicado no site da empresa sobre a situação de contingência.

8.5.16. Administração do Plano

A continuidade de negócios de uma organização, assim como a recuperação de desastres é o resultado da execução e da manutenção de um processo contínuo que envolve planejamento, formalização, monitoração e melhorias, definido para este plano como o Processo de Continuidade de Negócios.

O processo de Continuidade de Negócios é de responsabilidade e gestão da área administrativa, que determina o ciclo e as etapas que deverão ser executadas para que tanto os cenários de risco e impacto sobre os negócios como as estruturas e estratégias que embasam o PCN possam ser atualizadas refletindo o ambiente de negócios da COOPERFAC.

Para que a área de administrativa possa verificar o grau de atualização do PCN e decidir quanto ao momento em que o processo de continuidade de negócios será atualizado, os processos de planejamento de negócios e tecnológico, gerenciamento de mudanças,

gerenciamento de riscos, tratamento de problemas e de incidentes devem prever a participação desta área nas decisões relevantes destes processos.

a. Divulgação e Treinamento

Um dos fatores primordiais para o funcionamento deste plano são o conhecimento e a familiaridade dos colaboradores e demais envolvidos na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planejamento.

Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, devem ser realizadas, anualmente, sessões de divulgação a todos os colaboradores e envolvidos no planejamento de continuidade de negócios.

Estas sessões serão organizadas pela área Administrativa em conjunto com a Diretoria, visando a manter os colaboradores atualizados sobre os conceitos de continuidade adotados, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação de desastres e continuidade de negócios.

Para que este conhecimento seja preservado, os colaboradores admitidos e os transferidos para outras funções de negócios deverão ser instruídos das suas respectivas responsabilidades no plano.

O programa de treinamento deverá contemplar os riscos, ameaças, controles, responsabilidades, premissas e as estratégias do PCN, incluindo as alterações recentes.

b. Realização de Testes

Os testes de Continuidade de negócio serão realizados através de teste de mesa, geralmente realizado em uma mesa de reunião, é um teste simples, no qual é efetuada uma análise dos procedimentos e informações descritas no Plano de Continuidade de Negócio. Irá ser através de uma entrevista com os envolvidos nos processos, com objetivo de atualizar e/ou validá-lo.

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN e deverão ser realizados em reunião com a diretoria com periodicidade mínima anual a partir da data da sua implantação.

A responsabilidade pelo testes de mesa, será do Diretor Responsável pela área gestora irá criar medidas para verificar se valida as operações de contingência.

A reunião deverá ser registrada em um documento formal que deverá ser aprovado pela diretoria, com arquivamento por um período mínimo de 5 (cinco) anos.

O teste de mesa será fundamental para verificar se o processo está correto e se os colaboradores não possuem duvida quanto seu papel dentro do Plano de Continuidade de Negócio.

8.5.17. Relação de Fornecedores de Sistema

Sistema	Fornecedor	Nome do Contato	Telefone	E-mail
Fácil	Fácil Informática	Suporte Técnico	(31) 3319-1900	fácil@facilinformatica.com.br
Link de Dados Dedicado Principal	Sistel Fibra	Suporte Técnico	(16) 3212-8558 ou 0800 602 1801	contato@sistelfibra.com.br
Link de Dados Secundário	Unesp	Polo Computacional	(16) 3209-7182	dti.fcav@unesp.br

8.5.18. Eventos

A Cooperativa está sujeita a enfrentar uma série de eventos que representam ameaças à continuidade de suas atividades e que podem resultar em paralisações.

A seguir, elencamos os acontecimentos que, caso ocorram, poderão acarretar consequências significativas para a continuidade das operações da Cooperativa:

8.5.18.1. Riscos Ambientais

INCÊNDIO	
Risco	**Incêndio**
Causa	Ações humanas; Curtos-circuitos; Queimada.
Consequência	Indisponibilidadede recursos e serviços informatizados; Dano físico no equipamento.
Probabilidade	Baixa
Impacto	Alto
Controle	Presença de extintores de incêndio

INTERRUPÇÃO DE ENERGIA ELETRICA	
Risco	**Interrupção de Energia Elétrica**
Causa	Falha no sistema de distribuição de energia por parte do provedor do serviço; Curtos-circuitos; Defeito em algum componente do sistema elétrico (disjuntores, fusíveis etc.; Falha humana.
Consequência	Indisponibilidade de recursos e serviços informatizados; Dano físico no equipamento.
Probabilidade	Média
Impacto	Média
Controle	Instalação de nobreaks; Manutenção preventiva / corretiva da rede elétrica;

PRESENÇA DE ÁGUA E/OU UMIDADE NAS SALAS DE EQUIPAMENTOS	
Risco	Presença de água e/ou unidade nas salas de equipamentos
Causa	Entupimento ou vazamento no sistema hidráulico do ambiente próximos às salas de equipamento ocasionado infiltrações; Entupimento no sistema de drenagem dos aparelhos de ar-condicionado; Alagamento causado por fortes chuvas.
Consequência	Indisponibilidade de recursos e serviços informatizados; Dano físico nos equipamentos.
Probabilidade	Baixa.
Impacto	Médio.
Controle	Contratação de serviço de manutenção predial; Contratação de serviço de manutenção preventiva / corretiva dos sistemas de refrigeração.

DESASTRES NATURAIS	
Risco	**Desastres naturais**
Causa	Chuvas; Vendavais; Tempestades atmosféricas; Alagamentos; Raios.
Consequência	Indisponibilidade de recursos e serviços informatizados; Danos físicos nos equipamentos.
Probabilidade	Média.
Impacto	Médio.
Controle	Adoção de infraestrutura remota própria ou contratada.

CLIMATIZAÇÃO INADEQUADA DA SALA DE EQUIPAMENTOS	
Risco	**Climatização inadequada da sala de equipamentos**
Causa	Sistema de refrigeração defeituoso ou mal dimensionado.
Consequência	Indisponibilidade de recursos e serviços informatizados; Dano físico nos equipamentos causados por superaquecimento.
Probabilidade	Baixo.
Impacto	Baixo.
Controle	Instalação de sistema redundante de refrigeração; Contratação de serviço de manutenção preventiva / corretiva dos sistemas de refrigeração.

8.5.18.2. Riscos Tecnológicos

RISCOS DO SERVIÇO INTERNET DEVIDO A FALHAS INTERNAS	
Risco	**Indisponibilidade do serviço de internet devido falhas internas**
Causa	Falha nos equipamentos de rede (roteadores, *switches, firewalls*); Configuração incorreta dos equipamentos de rede; Rompimento no cabeamento existente.
Consequência	Indisponibilidade de recursos e serviços informatizados.
Probabilidade	Baixa.
Impacto	Médio.
Controle	Manutenção preventiva nos equipamentos de rede; Aquisição de reserva técnica de equipamentos e componentes de redes. Manutenção na rede da Unesp como forma alternativa.

INDISPONIBILIDADE DOS RECURSOS DE SEGURANAÇA ANTIVÍRUS E FIREWALL	
Risco	
Causa	Falta de recursos financeiros para aquisição de equipamentos; Falha no planejamento para a contratação de recursos de segurança.
Consequência	Roubo ou perda de informação; Indisponibilidade de recursos e serviços informatizados.
Probabilidade	Baixa
Impacto	Alto
Controle	Capacitação na gestão de contratos e planejamentos de contratações, tomando o processo mais eficiente.

INDISPONIBILIDADE DOS SISTEMAS DO CONTROLE DE ACESSO	
Risco	**Indisponibilidade dos sistemas do controle de acesso**
Causa	Falha ou defeito nos dispositivos que compõe a solução; Término do contrato de ***Outsourcing*** Fácil.
Consequência	Não atendimento aos cooperados e aos procedimentos operacionais; Comprometimento de imagem.
Probabilidade	Baixa.
Impacto	Alto.
Controle	Contratação / renovação de sistema operacional, incluindo os serviços de manutenção e reposição; Capacitação na gestão de contratos e planejamentos de contratações, tornando o processo mais eficiente.

ATAQUES CIBERNÉTICOS	
Risco	**Ataques cibernéticos**
Causa	Falha humana relacionada a configuração de regras de segurança dos firewalls e antivírus; Falta de atualização do antivírus instalados devido à problema de conexão com o servidor; Manutenção de sistemas operacionais desatualizados ligados a rede de dados; Vulnerabilidade ou erros de configuração em equipamentos, serviços e sistemas operacionais; Falta de sistema de monitoramento de vulnerabilidades; Falta de treinamentos dos empregados e conscientização sobre segurança cibernética; Ausência de sistema de monitoramentos de vulnerabilidades; Falha na disponibilidade de sistemas e recursos decorrentes de incompatibilidade tecnológica.
Consequência	Roubo ou perda de informação; Vazamento de informações críticas; Indisponibilidade de recursos e serviços informatizados; Comprometimento da imagem da Cooperativa.
Probabilidade	Baixa.
Impacto	Alto.
Controle	Manutenção dos recursos de atualização automática dos softwares de proteção contra invasão; Revisões periódicas nas regras de filtragem de firewall e e-mail; Plano de capacitação periódica relacionadas ao tema.

8.5.18.3. Ausência de Liquidez

AUSÊNCIA DE LIQUIDEZ	
Risco	**Ausência de liquidez**
Causa	Crédito de inadimplente; Má gestão de ativos e passivos; Flutuação econômica; Políticas regulatórias; Concentração de riscos.
Consequência	Restrição de operações de crédito; Aumento dos custos com captação de recursos; Riscos de insolvência; Risco de imagem.
Probabilidade	Baixa.
Impacto	Alto.
Controle	Monitoramento do fluxo de caixa; Políticas de empréstimos com informações claras dos limites e prazos; Diversificação de ativos – aplicação do excedente em bancos; Análise de riscos; Planejamento de contingência.

8.5.19. Periodicidade de Revisão

Este Plano de Continuidade de Negócios deve ser revisado e/ou atualizado sempre que houver mudanças, de forma a evidenciar a sua apreciação, discussão e reformulação através de ata de reunião da Diretoria.

Quaisquer indícios de irregularidades no cumprimento das determinações deste serão alvo de investigação interna e devem ser comunicados imediatamente a Diretoria.

8.5.20. Atendimento a Lei Nº 13.709/2018

Todos os procedimentos e diretrizes dessa Política são realizados em conformidade com a Política Interna de Privacidade de Dados da Cooperfac, a qual dispõe sobre o tratamento de dados em observância a Lei nº 13.709/2018 (LGPD).

8.5.21. Considerações Finais

Este Plano de Continuidade deverá ser compartilhado com todos os componentes da estrutura organizacional da Cooperativa.

8.5.22. Controle de Atualizações

Edição	Data	Instrumento de atualização	Atualizações
1ª	10/12/2019	Criação	Revogado
2ª	28/09/2022	Revogou 7.11	Reforma Completa
3ª	13/09/2024	Atualização	Responsabilidades Redação Detalhamento dos Riscos

Este documento é parte integrante da estrutura de controles internos e gerenciamento de riscos. Conheça a estrutura completa no **ANEXO I - ESTRUTURA DE CONTROLES INTERNOS E GERENCIAMENTO DE RISCOS** destacada no grupo 1.Estrutura, item: **1.1 – ESTRUTURA DE CONTROLES INTERNOS**.

Wagner Aparecido Mendes
Diretor Presidente

Marcos Donizeti Antonio
Diretor Operacional

Antonio Carlos Sanches
Diretor Administrativo