cooperunicamp
Cooperativa de Economia e Crédito Mutuo dos Servidores da UNICAMP

POLÍTICA DE GESTAO DE CONTINUIDADE DE NEGÓCIOS E CONTINGÊNCIAS

SUMÁRIO

1. HISTÓRICO DE REVISÃO

Versão:	Data da Aprovação:	Histórico:
01	11/09/2024	Elaboração da Política

1. OBJETIVO

Este documento tem por objetivo estabelecer rotinas e procedimentos para assegurar a não interrupção das atividades do negócio, proteger os processos críticos contra efeitos de falhas ou desastres significativos, considerando sua retomada em tempo hábil e em conformidade com diretrizes de segurança da informação da COOPERUNICAMP.

2. ABRANGÊNCIA

Este é um documento interno, com aplicabilidade imediata e indistinta, a partir de sua publicação, aos cooperados, colaboradores, parceiros e fornecedores de serviços da COOPERUNICAMP.

3. DEFINIÇÕES

Continuidade de Negócios: compreende a capacidade da organização para manter a entrega de produtos e serviços a níveis aceitáveis e predefinidos, em seguida a um evento de interrupção.

Gestão de Continuidade de Negócios: processo de gestão holística com o objetivo de identificar ameaças potenciais para uma organização e antecipar ações corretivas e reativas para minimizar os impactos, caso estes se concretizem.

Incidente de Segurança da Informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou Normas Complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

Objetivo de Ponto de Recuperação: tolerância para a perda de dados de sistemas.

Tempo de Recuperação Emergencial: tempo máximo que um processo crítico pode ficar indisponível, medido a partir da detecção da falha e/ou interrupção até o restabelecimento do processo.

Tentativa de Burla: tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

Testes de Mesa: avaliação das ações descritas em Plano de Continuidade de Negócios PCN, com objetivo de atualizar e ou validar conteúdo do PCN, tendo como base um exercício de simulação, a partir da apresentação de um cenário de falhas.

4. PREVENÇÕES A VIOLAÇÕES DE DADOS

O processo de continuidade de negócios na COOPERUNICAMP deve ser definido formalmente pela Diretoria Executiva, apoiada pela Gerência, funcionários ou empresa de

TI (Tecnologia da Informação), Auditoria Interna, Jurídico e, entre outras que, conforme característica da ocorrências, se façam necessária a participação.

O Plano de Continuidade de Negócios (PCN), bem como esta política, devem ser aprovados pela Diretoria executiva da COOPERUNICAMP.

O escopo dos processos de continuidade de negócio deve garantir um nível aceitável de risco e proteger os interesses das principais partes interessadas, além de ser baseado nos processos críticos do negócio que suportam:

a) o cumprimento das obrigações contratuais e legais;

b) operações e atividades críticas do negócio;

c) operações financeiras relevantes.

5. EQUIPES DE CONTINUIDADE DE NEGÓCIO

Para a gestão da continuidade do negócio da COOPERUNICAMP, deve ser:

a) estabelecida uma estrutura de planejamento e equipes de continuidade de negócios responsáveis pela manutenção da documentação dos processos, ativação dos planos, tomada de decisão em cenário de crise (gestão de crise);

b) definido um grupo de colaboradores para compor o time de gestão de crise (grupo de tomada de decisão) e aprovar o acionamento do plano.

6. ANÁLISE DE RISCOS

O desenvolvimento do Plano de Continuidade de Negócios – PCN deve ser iniciado pela execução de Análise de Riscos para identificação das ameaças que podem interromper os processos de negócio.

Os PCNs devem ser elaborados para assegurar que as operações essenciais sejam recuperadas dentro de uma escala de tempo aceitável, limitando as consequências aos danos verificados, e garantindo que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

As áreas responsáveis pela realização de identificação de riscos devem detectar os processos críticos de negócio das áreas da COOPERUNICAMP, por meio de entrevistas com as áreas/departamentos da COOPERUNICAMP, e avaliá-los quanto a ocorrência e consequências de desastres, falhas de segurança, perda de serviços e disponibilidade de serviços e quais os impactos nos negócios decorrentes. Nas entrevistas também devem ser identificados:

a) Tempo de Recuperação Emergencial;

b) Objetivo de Ponto de Recuperação;

c) Pessoas chave responsáveis pela execução do processo;

d) Recursos necessários para execução do processo (registros vitais, formulários, manuais, equipamentos, dispositivos móveis, dentre outros).

Sempre que for identificado um risco relacionado à Segurança da Informação e de Segurança Cibernética, devem ser seguidos os procedimentos de Gestão de Riscos de Segurança da Informação e Riscos Cibernéticos.

7. INTERRUPÇÕES DE PROCESOS POR INCIDENTES

Alguns processos críticos podem ser interrompidos devido à indisponibilidade e/ou falhas de seus processos diante de ataques externos, dentre outros. Nestes casos, a contingência necessária para interromper o fato gerador da falha ou interrupção deve acontecer conforme descrito no PCN correspondente, incluindo a comunicação com partes externas se necessário.

8. DESENVOLVIMENTO DE PLANOS

Após a identificação dos processos considerados críticos deve-se planejar as ações necessárias de recuperação para caso de falha ou interrupções e as documentar nos PCNs.

O Plano de Continuidade de Negócios (PCN) deve conter, no mínimo:

a) Escopo e Objetivos: Escopo do plano e objetivos;

b) Premissas: Cenários cobertos pelo plano;

c) Responsabilidades: descreve quem é responsável por cada uma das atividades, incluindo possíveis substitutos quando necessário;

d) Como e quando deve ser utilizado o plano;

e) Ciclo de Gestão de Continuidade de Negócios: Começo, meio e fim do processo de gestão de continuidade de negócio;

f) Estrutura de Continuidade de Negócios (Equipes): Indicação das Equipes responsáveis pelas atividades descritas no plano;

g) Processo de Resposta Inicial de Incidente: descreve quais as ações devem ser executadas após a ocorrência de um incidente;

h) Descrever o responsável pelo PCN e seus substitutos;

i) Processo de Gestão de Crises: Processos e respectivas regras para tomada de decisão em cenário de crise;

j) Plano de Avaliação de Danos: descreve ações para avaliar danos decorrentes do incidente;

k) Condições de ativação do PCN: descreve os processos obrigatórios antes da ativação do plano;

l) Procedimentos de retorno a operação normal: ações necessárias durante a restauração e recuperação do processo;

m) Procedimentos de finalização: descreve as ações a serem tomadas após o restabelecimento das operações;

n) Procedimentos Alternativos: Procedimentos alternativos são ações manuais que podem ser empregadas para executar as atividades críticas do processo se os sistemas que apoiam estes processos de negócio não estiverem disponíveis;

o) Identificação dos prazos aceitáveis: Descreve o Tempo de Recuperação Emergencial, isto é, qual o tempo máximo que um processo crítico pode ficar indisponível, que mede desde o momento aproximado que o processo ficou indisponível até o momento em que este seja restabelecido;

p) Serviços e recursos em geral: descreve os recursos em geral, além dos de Tecnologia da informação;

q) Testes e Manutenção: Neste caso, para cada tipo de ocorrência, os testes e manutenção serão ajustados de modo que reflitam com a máxima fidedignidade a situação;

r) Programa de Conscientização: Processo de conscientização das partes interessadas sobre o plano;

s) Aprovações e Revisão: Histórico de revisões e aprovações.

O PCN deve ser desenvolvido e mantido de modo a atender também as normas de Segurança da Informação e de Riscos Cibernéticos da COOPERUNICAMP.

O PCN deve conter as instruções para acionamento e recuperação do ambiente operacional produtivo, assim como as equipes responsáveis por essas atividades;

O PCN deve prever a redundância de processamento da informação e recursos de tecnologia que suportam os processos críticos.

9. DETECÇÃO E COMUNICAÇÃO PARA ACIONAMENTO DO PLANO

A COOPERUNICAMP deve implementar controles para detecção de interrupção ou falha de um processo crítico, tais como:

a) monitoramento dos sistemas (através da verificação dos logs);

b) informação de usuários;

c) sistemas automáticos de detecção (sensor de calor, sensor de fumaça, discadora automática, dentre outros);

d) monitoramento de terceiros (por exemplo, links de transmissão de dados).

10. ACIONAMENTO DO PCN

Após a detecção de falhas ou interrupção de um processo crítico, o processo de acionamento do PCN pode ser iniciado, conforme descrito a seguir:

a) O PCN só deve ser ativado mediante declaração de situação de crise pela Gerência. Antes da ativação, caberá a Gerência justificar e propor a Diretoria Executiva o acionamento do PCN;

b) O gerenciamento de crise, que envolve o atendimento de emergências como incêndio e outros desastres naturais, devem ser tratados observando também os normativos próprios elaborados por áreas relacionadas;

c) Devem ser observadas também instruções da COOPERUNICAMP e da Mantenedora para a fuga e abandono quando ocorrer emergências desta natureza. Estes planos devem conter os responsáveis por verificações necessárias antes da evacuação da área.

11. REGISTRO DO INCIDENTE NO MONITORAMENTO DE RISCO OPERACIONAL

Após acionamento do PCN, deve ser registrada a ocorrência, conforme cada natureza, no controle de monitoramento de Risco Operacional.

O registro da ocorrência exige o estabelecimento de Plano de Ação com objetivo de mitigação de novas ocorrências e melhoria contínuo nos processos internos da Cooperativa.

Semestralmente, o monitoramento do Risco Operacional é apresentado à Diretoria Executiva para acompanhamento e direcionamentos, quando for o caso.

12. RETORNO À NORMALIDADE

Após o retorno à normalidade, deve-se então avaliar quais foram os impactos causados no negócio pela interrupção/crise, avaliando impactos em cada processo crítico, ativos e equipes.

Caso seja necessário, a Diretoria Executiva deve ser convocada novamente para aprovações quanto à disponibilização de recursos financeiros ou estratégias alternativas para mitigar os danos e consequências causadas a COOPERUNICAMP durante a crise.

Todas as atividades executadas, desde o acionamento do PCN, até o retorno à normalidade, devem ser registradas em um formulário interno de registro de informações elaborado pela Gerência.

13. SIMULAÇÕES, TESTES, MANUTENÇÃO E TREINAMENTO DO PCN

O PCN deve ser testado no mínimo anualmente pelas áreas responsáveis pela realização de Auditorias Interna e Identificação de Riscos, de forma a assegurar permanente efetividade e atualização, além de garantir que todos os envolvidos no PCN estejam aptos a atuar em caso de necessidades, conhecendo e sabendo executar as ações a eles atribuídas.

Os ativos e recursos críticos devem também ser testados de modo a verificar se estão aptos a desempenhar os procedimentos de emergências de recuperação e reativação.

Após a sua realização, a simulação deve ser avaliada e registrada na "Avaliação da Simulação/Ativação de PCN". O responsável pela execução do teste, conforme descrito no programa, é também o responsável pelo preenchimento do formulário e envio a Gerência.

Todos os colaboradores envolvidos no Sistema de Gestão de Continuidade de Negócios devem participar do processo de conscientização de continuidade de negócios.

A realização das simulações deve contemplar:

a) Testes de mesa simulando diferentes cenários;

b) Simulações de recuperação técnicas, assegurando que os sistemas possam ser efetivamente recuperados;

c) Testes de recuperação em local alternativo, executando os processos de negócio em paralelo com a recuperação das operações distantes do local principal;

d) Testes de recursos, serviços e instalações de fornecedores, assegurando que os serviços e produtos fornecidos por terceiros atendem aos requisitos contratados;

e) Simulação do PCN, onde aplicável, testando se a organização, o pessoal, os equipamentos, os recursos e os processos estão aptos para enfrentar interrupções.

14. AVALIAÇÃO E ATUALIZAÇÃO DO PCN

O PCN deve ser atualizado pela Gerência, com apoio de unidades técnicas da Cooperativa, quando for o caso, nas situações ocorridas abaixo:

Ocorrência de um incidente, com ativação do PCN;

a) Realização de testes do PCN;

b) Mudanças significativas nas atividades do negócio;

c) Mudança de pessoal ou funções, ou informações sobre estes;

d) Mudança de localização, instalação e recursos;

e) Mudança de legislação;

f) Mudança de prestadores de serviços que envolva risco de segurança;

g) Mudanças nos processos.

h) Adicionalmente, os riscos devem ser tratados e revisados anualmente.

15. APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLÍTICA

A Política de Gestao de Continuidade de Negócios e Contingências foi aprovada pela Diretoria Executiva da COOPERUNICAMP e está disponível no site da Cooperativa para conhecimento de todos os cooperados e foi amplamente divulgada para todos os colaboradores e prestadores de serviços para o seu efetivo cumprimento.

16. BASE REGULATÓRIA

Resolução CNN nº 4.557 de 23 de fevereiro de 2017

Diretor responsável pelo Gerenciamento Contínuo de Riscos

Presidente

Diretor Tesoureiro