21. PCN – Plano de Continuidade de Negócios

1. Objetivo

O Plano de Continuidade de Negócios (PCN) tem como diretriz promover estratégias e medidas de proteção eficazes e rápidas para os processos críticos de TI, a fim de garantir sua preservação após a ocorrência de um desastre, até a retomada em tempo hábil.

O Plano de Continuidade de Negócios (PCN) atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos, provendo quais as ações serão realizadas em cada etapa do plano.

2. Aplicabilidade

Todos os colaboradores da Cogem.

3. Etapas

Este plano divide-se em outras 3 (três) etapas:

- Plano de Administração de Crises (PAC) - Define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes, durante e após a ocorrência;
- Plano de Continuidade Operacional (PCO) - Seu objetivo é restabelecer o funcionamento dos principais ativos que suportam as operações da instituição, reduzindo o tempo de queda e os impactos provocados por um eventual incidente;
- Plano de Recuperação de Desastres (PRD) - Determina o planejamento para que, uma vez controlada a contingência e passada a crise, sejam retomados os níveis originais de operação.

4. Modelo do Plano (PDCA)

Os planos aqui definidos seguirão o Modelo “PLAN-DO-CHECK-ACT” (PDCA) para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente a eficácia do Sistema.

O modelo PDCA ajudará na melhoria contínua do Plano de Continuidade de Negócios.

- PLAN (estabelecer) - Seguir uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimento pertinentes para a melhoria da continuidade de negócios, de forma a ter resultados alinhados com os objetivos.
- Do (Implementar e operar) - Implementar e operar a política de continuidade de negócios, controles, processos e procedimentos.
- CHECK (Monitorar e analisar criticamente) - Monitorar e analisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a Direção para análise crítica, definir e autorizar ações de melhorias e correções.
- ACT (Manter e Melhorar) - Manter e melhorar o PCN, tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica da direção e reavaliando o escopo, as políticas e objetivos de continuidade de negócios.

5. Início do PCN

Ao ocorrer quaisquer eventos que paralise algum processo essencial ao negócio, o líder de Contingência da unidade em questão avaliará a ocorrência e comunicará ao 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 1º líder da equipe de Contingência.

Qualquer colaborador da Cooperativa, ao constatar alguma anormalidade que paralise quaisquer dos processos deverá comunicar o fato ao seu superior imediato que comunicará ao Líder de Contingência da unidade de negócio a que pertence.

Unidades		**Líder de Contingencia**	**Telefones**	**E-mail**
SEDE - São Bernardo do Campo/SP	1º Lider	Priscila Oliveira	(11) 3080-3939 / (11) 91130-2954	PCN@cogem.com.br
P.A. - Todas as Localidades	2º Lider	Devanir Pereira	(11) 3080-3954 / (11) 91130 3362	
Suplente SEDE e P.A.	3º Lider	Josimara Lima	(11) 3080-3941 / (11) 91159-4516	

Em caso da ausência 1º líder de Contingência, o segundo assumirá interinamente e assim sucessivamente.

6. Principais Riscos

O PCN foi elaborado para ser acionado quando houver alguma ocorrência de desastre que apresente riscos à continuidade do negócio ou serviços essenciais. Abaixo segue o quadro que define estes riscos, bem como aponta quais os parâmetros para reportar as possíveis causas das ocorrências.

EVENTO DE DESASTRE	**POSSÍVEIS CAUSAS**
Humana	Greves internas, manipulação indevida de dados e sistemas, distúrbio civil, falha de prestador de serviços/parceiro, roubo e/ou furto de recursos e informações, acesso indevido às instalações e erro humano não intencional.
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 Telecom – dados e falha em sistema de acesso e ataques cibernéticos.
Infraestrutura	Falha em Telecom - voz, falha em sistema de refrigeração, interrupção de energia elétrica, falha em instalações elétricas.
Naturais	Alagamento interno do ambiente, queda de raios, vendaval e incêndio.
Físicas	Problema estrutural ou de instalações e rompimento de tubulação interna (água, esgoto e gás).

7. Papéis e Responsabilidades

7.1 Comitê de Segurança da Informação

Integrantes

- Wanderson Oliveira
- Emerson Pereira

Atribuições

Avaliar o plano periodicamente, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.

7.2 Diretor Responsável por PCN

Integrantes

- Diretor de riscos - Ronaldo Teixeira da Silva

Atribuições

Compete ao diretor declarar ou não a contingência, com base nas informações recebidas e avaliando o grau de impacto versus horário crítico.

7.3 Líderes de Contingência

Integrantes

- Priscila Oliveira
- Devanir Pereira
- Josimara Lima

Atribuições

Orientar os colaboradores que possam trabalhar remotamente com as ferramentas específicas à sua atuação.

7.4 Compliance

Integrantes

- Carla Ilinski

Atribuições

É responsável por contribuir com a identificação de riscos às atividades críticas que porventura tenham sido identificados através do processo de gerenciamento de riscos integrados da cooperativa.

8. Processos e Sistema Críticos

Processos e sistemas críticos podem ser definidos como um processo de trabalho que, uma vez paralisado por um tempo superior ao definido pelos gestores de negócio, irá afetar sensivelmente as operações, gerando impacto aos clientes.

Esse impacto é definido pela seguinte formula: MTD = RTO + WRT, conforme definição:

- MTD (Maximum Tolerable Downtime) = Define a quantidade total de tempo que um processo de negócios pode ser interrompido sem causar quaisquer consequências inaceitáveis. Diferentes funções de negócio terão diferentes MTD's.

- RTO (Recovery Time Objective) = Determina a quantidade máxima tolerável de tempo necessário para colocar todos os sistemas críticos novamente on-line (por exemplo, restaurar dados de backup ou consertar uma falha).

- WRT (Work Recovery Time) = Determina a quantidade de tempo tolerável necessário para verificar o sistema e/ou a integridade dos dados (verificar os bancos de dados e logs, por exemplo). Quando todos os sistemas afetados pelo desastre são verificados e/ou recuperados, o ambiente está pronto para retomar a produção novamente.

Processos Críticos	**Área**	**Recursos**	**MTD**	**Procedimento**
Contas a Pagar	Financeiro	Acesso aos Bancos (Banking) Notebook Internet Microsoft	2hrs	· Entrar em contato com T.I, para suporte à retomada das operações. · Entrar em contato com os gerentes e suporte dos bancos para acesso ao Banking.
Pagamento de Empréstimo aos Associados	Financeiro	Acesso aos Bancos (Banking) Notebook Internet Microsoft Syscoop Prodaf	2hrs	· Entrar em contato com T.I, para suporte à retomada das operações. · Entrar em contato com os gerentes e suporte dos bancos para acesso ao Banking. · Entrar em contato o suporte da Prodaf Informática para suporte à retomada as operações.
Atendimento aos associados e empresas	Atendimento	Notebook Internet Microsoft Telefonia Syscoop Prodaf	2hrs	· Entrar em contato com T.I. para suporte à retomada das operações. · Entrar em contato com os gerentes e suporte dos bancos para acesso ao Banking.

9. Plano de Administração de Crises (PAC)

Este plano especifica as ações ante os cenários de desastres. As ações incluem administrar, gerir, eliminar ou neutralizar os impactos inerentes ao relacionamento entre os envolvidos e/ou afetados, até a superação da crise.

9.1 Objetivo

O objetivo do PAC é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de um desastre.

São objetivos específicos do PAC:

- Garantir a segurança à vida das pessoas;
- Orientar os funcionários e demais colaboradores sobre as condutas que serão tomadas;
- Informar aos associados e empresas conveniadas com esclarecimentos condizentes com o ocorrido em tempo hábil;
- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para a superação da crise.

9.2 Execução do Plano

Na ocorrência de um desastre será necessário entrar em contato com as áreas afetadas para informá-las de seu efeito na continuidade dos serviços e tempo para recuperação. O plano deve incluir ações para redirecionar as chamadas telefônicas recebidas para um segundo número.

A comunicação ocorrerá da seguinte forma:

9.2.1 Desastre com risco as pessoas:

Deve-se comunicar as autoridades competentes em caso dedesastre que envolva risco às pessoas, fornecendo informações de localização, natureza, magnitude e impacto do desastre.

- Polícia Militar - 190
- SAMU – 192
- Corpo de Bombeiros – 193
- Defesa Civil – 199

9.2.2 Demais Desastres:

- Comunicar Fornecedores e Prestadores de serviços;
- Comunicar Colaboradores Externos;
- Comunicar as áreas envolvidas das ações de contingência em andamento.

10. Plano de Continuidade Operacional (PCO)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços e restabelecer o funcionamento dos principais ativos que suportam as operações de T.I., reduzindo o tempo de queda e os impactos provocados por um eventual desastre.

10.1 Objetivo

Garantir ações de continuidade durante e depois da ocorrência de uma crise ou desastre, tratando-se apenas de ações de contingência, destinados a manter a continuidade dos processos de negócios e serviços vitais. É através deste, que as equipes de processos saberão como agir na falta ou na falha de algum componente que o suporte, garantindo assim a continuidade do processo, reduzindo os seus impactos;

Prover meios para manter o funcionamento dos principais serviços de T.I. e a continuidade das operações e sistemas essenciais;

Estabelecer controles, regras e procedimentos alternativos que possibilitem a continuidade das operações de T.I. durante uma crise ou cenário de desastre.

10.2 Execução do Plano

Identificada a ocorrência de um incidente, crise ou desastre, deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido. Após a avaliação de impacto de desastre e o acionamento do plano pelos responsáveis, será convocada uma reunião de emergência com os líderes com o intuito de:

- Coordenar prazos e orquestrar as ações de contingência;
- Informar as equipes de ações de contingência com a priorização dos serviços essenciais.

10.3 Procedimentos de Retomada

Para que se tenha a retomada do negócio, será necessário a verificação das seguintes etapas:

- Estimar o impacto de perda de dados;
- Identificar ativos afetados;
- Mapear ativos a serem recuperados;
- Estimar volume dos dados a serem recuperados;
- Tempo de recuperação e possíveis perdas operacionais;
- Implantar procedimento de recuperação;
- Testar procedimentos realizados; e
- Repassar os procedimentos aos servidores e verificar melhorias.

11. Plano de Recuperação de Desastres (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos, para que, uma vez definindo as atividades prioritárias para restabelecer o nível de operação dos serviços, controlada a contingência e passada a crise, a organização retorne aos seus níveis normais de operação.

Para garantir o retorno das operações depois da ocorrência de uma crise ou desastre, são objetivos do plano de recuperação:

- Avaliar danos aos ativos, conexões de internet e plataformas, e prover meios para sua recuperação;
- Evitar desdobramento de outros incidentes.

12. Substituição dos Ativos e Equipamentos

Em caso de perda de ativos, deverá ser imediatamente informado a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar cada serviço, comunicando se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição. As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes de PCO e PAC.

13. Ativos e Equipamentos

A equipe responsável deverá verificar se as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estejam, prover o cronograma estimado para configurar estes ativos.

14. Teste de Ambiente

O ambiente principal deverá ser testado antes da recuperação dos dados, a fim de garantir que o processo de recuperação ocorra conforme o planejado.

Os testes e recuperações deverão:

- Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre;
- Garantir a integridade dos dados, que podem estar corrompidos ou defasados;
- Validar todas as configurações anteriores;
- Suportar o retorno dos sistemas de acordo com a demanda;
- Verificar a integridade dos dados e restaurar os backups, caso necessário.

15. Execução do Plano de Recuperação

Para que o plano transcorra como planejado, deve-se executar os seguintes passos:

- Identificar e listar todos os ativos danificados da ocorrência do desastre;
- A equipe de rede deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, WAN ou com o provedor de serviços;
- Os responsáveis pelo PRD deverão mapear quais os serviços foram descontinuados contendo as informações de perda de ativo e de conexão;

O comitê responsável pelo PRD, após o mapeamento das perdas e impactos, elaborará um cronograma de recuperação das aplicações, levando em consideração as seguintes aplicações para recuperação:

- Substituição dos ativos e equipamentos;
- Reconfiguração de ativos e equipamentos;
- Teste de ambiente.

16. Encerramento dos Planos

O plano será encerrado assim que os procedimentos de recuperação forem realizados por todas as equipes. Ao término de todos os procedimentos, as informações de recuperação de serviços serão consolidadas em parecer específico, informando o horário de restabelecimento de cada serviço, equipamentos adquiridos e/ou realocados, se for o caso, fornecedores que tiveram de ser acionados, procedimentos de recuperação realizados, entre outras informações relevantes.

17. Relação de Fornecedores de Sistemas e Infraestrutura Encerramento do Plano

Serviço	Fornecedor	Nome do Contato	Telefone	E-mail
Syscoop	Prodaf	Suporte	(27) 4062 - 8002	suporte@prodaf.com.br
Telecom	TESA	Suporte	0800 038 3838	atendimento@tesatelecom.com
Suporte Técnico T.I.	ALTCOM	Suporte	(11) 2381 - 6455	suporte@altcom.com.br

18. Revisão

A revisão do Plano será realizada nas seguintes situações:

- Em no máximo 2 (dois) anos;
- Nos momentos em que o Comitê de Segurança da Informação julgar necessário;
- Em função dos resultados dos testes realizados; e
- Após ocorrência de algum evento ou mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

Registro de Alteração			
Data	**Versão**	**Páginas alteradas**	**Informações Relevantes**
jun/23	2ª	Todas	Revisão do PCN
out/23	3º	2, 3 e 4.	Capítulo 5 – Atualizado lista de líderes de Contingência. Capítulo 7.1 – Atualizado lista de integrantes de Segurança da Informação. Capítulo 7.3 – Atualizado lista de integrantes de Líderes de Contingência. Capítulo 7.4 – Atualizado lista de integrantes de Compliance.