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 gerente responsável pelo PCN. Com base nas informações recebidas e avaliando o grau de impacto versus horário crítico, compete ao gerente declarar ou não a contingência. Em caso da ausência do gerente 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 Contingência**	**Telefones**	**E-mail**
SEDE - São Bernardo do Campo/SP	1º Lider	Priscila Oliveira	(11) 3080-3940 / (11) 91130-3301	PCN@cogem.com.br
P.A. - Todas as Localidades	2º Lider	Priscila Oliveira	(11) 3080-3940 / (11) 91130 3301	
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 Gerente Responsável por PCN

Integrantes

- Gerente de Riscos – Wanderson Oliveira

Atribuições

Compete ao Gerente 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
- 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

Os Processos Críticos são aqueles que impactam com maior intensidade no Negócio, independente da ameaça.

Processos com RTO de 01 hora

- Email e Rede Microsoft indisponível

Processos com RTO de 02 horas

- Sede Indisponível
- Posto de Atendimento indisponível
- Home Office usuários Sede
- Links de internet indisponíveis
- Mau funcionamento de computadores

Processos com RTO de 04 horas

- Mau funcionamento de computadores

Processos com prazos limitados

- Contas a pagar
- Contas a pagar - associados
- Conciliação diária - Banco
- Conciliação da Folha
- Reposta - Desligamentos enviados pelos RHs das empresas
- Portabilidade

9. Cenários

Os Cenários avaliados neste Plano de Continuidade do Negócio foram definidos juntamente com os responsáveis pelas áreas de negócio, decorrentes de análise de risco.

Foram relacionadas ameaças para cada um dos Cenários, que são consequências diretas de eventos não programados.

Considerando a classificação das ameaças de acordo com o nível de Gravidade, são relacionadas às ações necessárias e o tempo previsto para suas execuções, garantindo a continuidade operacional

Cenários e Ameaças Relacionadas

Impossibilidade de Acessos a Sede

- **Ameaças:**
  - Epidemias
  - Interrupção de energia elétrica
  - Risco a segurança física
  - Proibição do condomínio
  - Incêndio
  - Inundação
  - Greves e Bloqueios
  - Ameaças de Bomba
  - Roubo/Furto de Informações e/ou Ativos

Impossibilidade de Acessos ao Posto de atendimento

- **Ameaças:**
  - Epidemias
  - Interrupção de energia elétrica
  - Risco a segurança física
  - Proibição da Empresa
  - Incêndio
  - Inundação
  - Greves e Bloqueios
  - Ameaças de Bomba
  - Roubo/Furto de Informações e/ou Ativos

Impossibilidade de uso *Home Office*

  - Interrupção de energia
  - Problemas no provedor de serviço de Internet
  - Falha no pacote office
  - Falha de equipamentos

Falta de Infraestrutura Tecnológica

- **Ameaças:**
  - Problemas no provedor de serviço de Internet
  - Falha no Sistema operacional
  - Falha de Aplicação/Banco de Dados
  - Falha no pacote office
  - Falha de Equipamentos

Estabelecendo Ações e Procedimentos por cenários

<u>Impossibilidade de Acessos a Sede</u>

De acordo com a Análise de risco, as ameaças são: Incêndio, Inundação, Queda de Energia, Greves e Bloqueios, Ameaça de Bomba, Roubo/Furto de Informações e/ou Ativos.

- Incêndio (Impacto ao negócio – Severidade: Vital)
  - **Evidência:** Alarme de incêndio e/ou aviso de um dos membros da equipe de brigadistas do Prédio/Andar.

- Inundação (Impacto ao negócio – Severidade: Crítica)
  - **Evidência:** Informe na mídia, período antecedido por forte tempestade ou eventos similares que causem inundação.
    - A inundação não necessariamente precisa acontecer no prédio da Cogem, mas em suas proximidades, impossibilitando o acesso à região e consequentemente à Instituição.

- Queda de energia (Impacto ao negócio – Severidade: Crítica)
  - **Evidência:** Constância da falta de energia e confirmação de retomada sem previsão ou superior a 02 (duas) horas.
    - Caso a falta de energia tenha previsão de término até 02 (duas) horas, deve-se continuar a operação da unidade principal, que é suportada por *nobreak* durante este período. Se for verificado que a retomada da energia será após 02 (duas) horas, o *Home Office* deverá ser acionado.

- Ameaça de bomba (Impacto ao negócio – Severidade: Crítica)
  - **Evidência:** Confirmação formal da administração predial, após diagnóstico efetivo por peritos.
    - O procedimento de confirmação desta ameaça é seguir o plano de emergência do condomínio para ameaças de bomba.
    - Dirija todos os colaboradores para pontos de encontro seguros e longe do prédio.

- Roubo e furto de informação e ativos (Impacto ao negócio – Severidade: Crítica)
  - **Evidência:** Confirmação de falta de ativos ou evidência de furto de informação.
    - Esta ameaça apenas impactará em indisponibilidade total (infraestrutura física e tecnológica), caso seja uma ocorrência de grande porte, impedindo o acesso dos colaboradores, para que não se perca as eventuais provas que levem ao autor do roubo ou furto.

- Greves e bloqueios (Impacto ao negócio – Severidade: Significativa)
  - **Evidência:** Informe na mídia ou percepção local sobre paralisação sejam greves ou manifestações na região que dificultem o acesso ao Prédio.
    - O procedimento de ativação do *Home Office,* somente será devidamente aplicado caso a ocorrência for percebida antes do horário comercial, havendo tempo hábil para deslocamento dos colaboradores a sede, ou se o evento causar transtorno por mais dias após seu início. Do contrário, estando já os colaboradores na sede, já em operação, não haverá necessidade efetiva.

- Risco a segurança física
  - **Evidência:** Deve-se comunicar as autoridades competentes em caso de desastre que envolva risco às pessoas, fornecendo informações de localização, natureza, magnitude e impacto do desastre.

- Proibição de acesso ao condomínio (Impacto ao negócio – Severidade: Significativa
  - **Evidência**: Falhas no fornecimento de água, gás, podem afetar o funcionamento normal do condomínio, assim como vandalismo e ataques deliberados podem causar danos físicos e afetar a segurança dos colaboradores.
    O procedimento de avaliar o impacto potencial da ameaça, tanto em termos de interrupção das operações quanto de segurança dos colaboradores.

Tempo para tomada de decisão: em até 5 minutos após evidência da ameaça.

Tempo Máximo para retomada da Operação: 02 Horas, a partir da tomada de decisão.

<u>Ações em tempo: de 05 até 10 minutos</u>

Responsável: Todos os colaboradores envolvidos no Plano de Continuidade de Negócios.

Procedimento:

- Evidência 1: Atender e respeitar os procedimentos de evacuação do prédio assim como seguir as orientações dos brigadistas de acordo com os procedimentos do CIPA.
- De acordo com o cenário, relatar o acontecido aos serviços de suporte:
  - Bombeiros: 193 (Incêndio e Ameaça de bomba);

- Defesa Civil: 199 (Ameaça de bomba, Greves e bloqueios e Inundação);
- Polícia Civil: 197 (Ameaça de bomba, Roubo e Furto de informações e ativos);
- Polícia Militar – 190;
- SAMU – 192.

Responsável: Facilities

Procedimento:

Evidência 2: notificar colaboradores envolvidos no plano para alterar rota para *Home Office.*

Tempo Restante para a execução das demais ações: 01h50 minutos restantes.

Impossibilidade de Acessos ao Posto de Atendimento

De acordo com a Análise de risco, as ameaças são: Incêndio, Inundação, Queda de Energia, Greves e Bloqueios, Ameaça de Bomba, Roubo/Furto de Informações e/ou Ativos.

- Incêndio (Impacto ao negócio – Severidade: Vital)
  - **Evidência:** Alarme de incêndio e/ou aviso de um dos membros da equipe de brigadistas do Prédio/Andar.

- Inundação (Impacto ao negócio – Severidade: Crítica)
  - **Evidência:** Informe na mídia, período antecedido por forte tempestade ou eventos similares que causem inundação.
    - A inundação não necessariamente precisa acontecer no prédio da Cogem, mas em suas proximidades, impossibilitando o acesso à região e consequentemente à Instituição.

- Queda de energia (Impacto ao negócio – Severidade: Crítica)
  - **Evidência:** Constância da falta de energia e confirmação de retomada sem previsão ou superior a 02 (duas) horas.
    - Caso a falta de energia tenha previsão de término até 02 (duas) horas, deve-se continuar a operação da unidade principal, que é suportada por *nobreak* durante este período. Se for verificado que a retomada da energia será após 02 (duas) horas o *Home Office* deverá ser acionado.

- Ameaça de bomba (Impacto ao negócio – Severidade: Crítica)
  - **Evidência:** Confirmação formal da administração predial, após diagnóstico efetivo por peritos.
    - O procedimento de confirmação desta ameaça não é imediato à sua identificação, mas a ação após a evidência deverá ser imediata.

- Roubo e furto de informação e ativos (Impacto ao negócio – Severidade: Crítica)
  - **Evidência:** Confirmação de falta de ativos ou evidência de furto de informação.
    - Esta ameaça apenas impactará em indisponibilidade total (infraestrutura física e tecnológica), caso seja uma ocorrência de grande porte, impedindo o acesso dos colaboradores, para que não se perca as eventuais provas que levem ao autor do roubo ou furto.

- Greves e bloqueios (Impacto ao negócio – Severidade: Significativa)
  - **Evidência:** Informe na mídia ou percepção local sobre paralisação sejam greves ou manifestações na região que dificultem o acesso ao Prédio.
    - O procedimento de ativação do *Home Office,* somente será devidamente aplicado caso a ocorrência for percebida antes do horário comercial, havendo tempo hábil para deslocamento dos colaboradores ao posto e, ou se o evento causar transtorno por mais dias após seu início. Do contrário, estando os colaboradores no posto, já em operação, não haverá necessidade efetiva.

- Risco a segurança física
  - **Evidência:** Deve-se comunicar aos responsáveis competentes em caso de desastre que envolva risco às pessoas, fornecendo informações de localização, natureza, magnitude e impacto do desastre.

- Proibição da Empresa
  - **Evidência**: Falhas no fornecimento de água, gás, podem afetar o funcionamento normal da empresa, assim como vandalismo e ataques deliberados podem causar danos físicos e afetar a segurança dos colaboradores.
    O procedimento de avaliar o impacto potencial da ameaça, tanto em termos de interrupção das operações quanto de segurança dos colaboradores.

Tempo para tomada de decisão: em até 5 minutos após evidência da ameaça.

Tempo Máximo para retomada da Operação: 02 Horas, a partir da tomada de decisão.

<u>Ações em tempo: de 05 até 10 minutos</u>

Responsável: Todos os colaboradores envolvidos no Plano de Continuidade de Negócios.

Procedimento:

- Evidência 1: Atender e respeitar os procedimentos de evacuação da empresa assim como seguir as orientações dos brigadistas de acordo com os procedimentos do CIPA.

Responsável: Analista de atendimento

Procedimento:

Evidência 2: notificar colaboradores envolvidos no plano para alterar rota para *Home Office.*

Tempo Restante para a execução das demais ações: 01h50 minutos restantes.

Falta de Infraestrutura Tecnológica

De acordo com a análise de risco, as ameaças são: Incêndio, Queda de Energia, Falha em Equipamentos de Informática, Falha de Softwares, Falha em Equipamentos de Telecom ou Componentes de Rede, Ações de Funcionários Insatisfeitos, Consequência de Erros Humanos, Consequência de Concentração da Informação, Roubo/Furto de Informações e/ou Ativos.

Cenário Impactado:

- Indisponibilidade de Infraestrutura Tecnológica e Física

Ameaças pertinentes

- Incêndio (Impacto ao negócio – Severidade: Vital)
  - **Evidência:** Alarme de incêndio e/ou aviso de um dos membros da equipe de brigadistas do prédio ou empresa.

- Roubo e furto de informação e ativos (Impacto ao negócio – Severidade: Crítica)
  - **Evidência:** Confirmação de falta de ativos ou evidência de furto de informação.
    - Esta ameaça apenas impactará em indisponibilidade total (infraestrutura física e tecnológica), caso seja uma ocorrência de grande porte, impedindo o acesso dos colaboradores, para que não se perca as eventuais provas que levem ao autor do roubo ou furto.

- Ocorrência de falhas em equipamentos de informática (Impacto ao negócio – Severidade: Crítica), Ocorrência de falhas de software (Impacto ao negócio – Severidade: Crítica), Ocorrência de falha em equipamento de Telecom ou componente de rede (Impacto ao negócio – Severidade: Crítica), e Consequência de erros humanos (Impacto ao negócio – Severidade: Significativa).
  - **Evidência:** Solicitação de reparo em equipamentos ou servidores, ou restauração de arquivos por alguma área da Cooperativa, quando há dependência da Área de TI.
    - Estes tipos de ameaças somente causam inoperância, para qual seja necessário o acionamento do *Home Office* quanto tratar-se de uma ocorrência de grande porte, que impacte a utilização dos recursos por áreas críticas ou que estejam em período crítico. Do contrário, apenas o suporte técnico interno, *help desk* dos *softwares* utilizados serão suficientes para resolução da falha. Deve-se observar que o *Home Office* deve ser acionado sempre que a inoperância for igual ou superior a 1 (uma) hora.

Tempo para tomada de decisão: em até 5 minutos após evidência da ameaça.

Tempo Máximo para retomada da Operação: 02 Horas, a partir da tomada de decisão.

Falta de Infraestrutura da Rede e Telecom

Ações em tempo: de 05 até 10 minutos

Responsável: Tecnologia da informação

Procedimento:

- Acionar provedores de acesso à internet;
- Informar a gestores que estão em contingência;
- Acompanhar estabelecimento da conexão.

Ações em tempo: até 50 minutos após a conclusão da etapa anterior

Responsável: Tecnologia da informação

Procedimento:

- Testar conexões provedores de acesso à internet;
- Avisar Diretoria sobre resultado do procedimento.

Concluído em: 01 hora.

Tempo Restante – margem de segurança: 01 hora.

Falha na Conexão com Servidores de Aplicação e/ou Banco de Dados

Ações em tempo: de 05 a 10 minutos após a tomada de decisão

Responsável: Tecnologia da Informação.

Procedimento:

- Verificar qual é a origem da falha e se a recuperação será inferior a 2 (duas) horas.
  - Se a previsão de recuperação for inferior a 2(duas) horas:
    - E a solução for interna, efetuar o procedimento;
    - E a solução for externa, contatar prestador de serviço/fornecedor.
  - Se a previsão de recuperação for superior a 2 (duas) horas acionar gerencia.

Ações em tempo: até 50 minutos após a conclusão da etapa anterior

Responsável: Tecnologia da Informação.

Procedimento:

- Testar conexão com Prestadora de Serviço
- Informar a posição a Diretoria

Responsável: Tecnologia da Informação.

Concluído em: 01 hora

Tempo Restante – margem de segurança: 01 hora

Atividades prioritárias

Contas a pagar – associados: Não pagar as obrigações operacionais (empréstimos / RDC / capital de ex-associados).

Responsável: Financeiro

- **Ameaças**:
  - Banking fora do ar;
  - Ausência do responsável pelo processo;
  - Problema com computadores;
  - Internet;
  - Sistema Prodaf;
  - Problemas com a equipe dos postos.

Contingência: Banco principal Santander, utilização do banco backup (Itaú) - atenderá no caso de problemas com Santander. Há também backup do responsável pelo processo, dentro da equipe. Para Internet temos como backup - a internet do celular corporativo.

Contas a pagar: Não pagar contas, fornecedores do dia (Tributos / serviços) e Folha da Pagamento.

Responsável: Financeiro

- **Ameaças:**
  - Banking fora do ar;
  - Ausência do responsável pelo processo;
  - Problema com computadores;
  - Internet;
  - Sistema Prodaf.

Conciliação diária Banco: Não conseguir conciliar a data/ lançamentos dos créditos que podem impactar os pagamentos do dia.

Responsável: Financeiro

- **Ameaças:**
  - Banking fora do ar;
  - Ausência do responsável pelo processo;
  - Problema computadores;
  - Internet;
  - Sistema Prodaf;
  - Problemas com a equipe dos postos.

Conciliação da Folha: Não conseguir realizar o cálculo da folha para envio aos RHs das empresas conveniadas dos valores a serem descontados na folha do mês vigente.

Responsável: Financeiro

- **Ameaças:**
  - E-mail (forma de envio);
  - Ausência do responsável pelo processo;
  - Problema com computadores;
  - Internet;
  - Sistema Prodaf.

Reposta - Desligamentos enviados pelos RHs das empresas: Não conseguir enviar o encontro de contas dos desligados para desconto em rescisão do saldo devedor.

Responsável: Financeiro

- **Ameaças:**
  - E-mail (a comunicação chega via e-mail);
  - Ausência do responsável pelo processo;
  - Problema com computadores;
  - Internet.

Portabilidade: Não conseguir responder no prazo as portabilidades.

Responsável: Financeiro

- **Ameaças:**
  - Uniprime (banco liquidante);
  - Sistema Prodaf;

- Ausência do responsável pelo processo;
- Problema com computadores;
- Internet;
- Problemas com a equipe dos postos.

10. 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.

10.1 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.

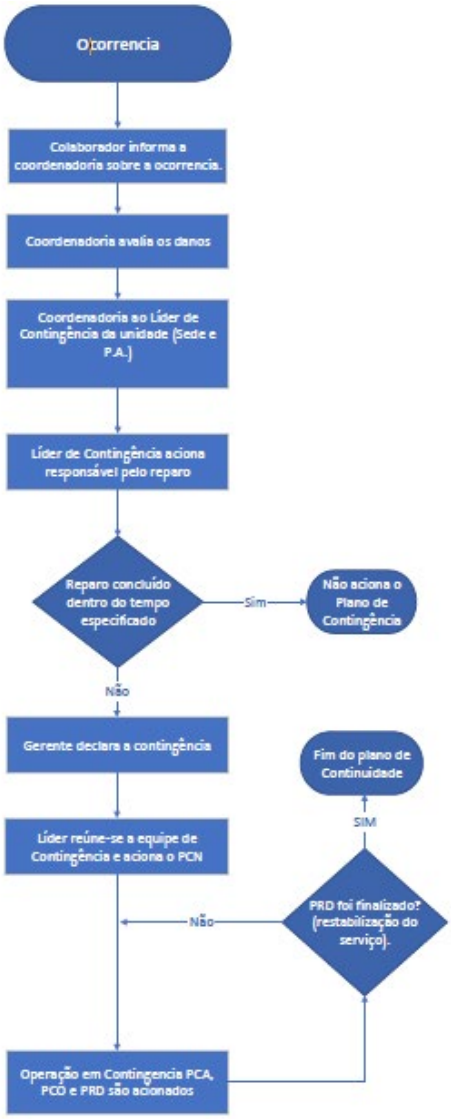
São objetivos específicos do PAC:

- 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.

10.2 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:



10.2.1 Demais Desastres:

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

11. 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.

11.1 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 dasoperações de T.I. durante uma crise ou cenário de desastre.

11.2 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 deemergência 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.

11.3 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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
Internet	WCS	Suporte	(11)4800-4800	
Internet	VIVO	Suporte	10315	
Internet	Hostfiber	Suporte	(11)3777-3480	
Internet	Ligga	Suporte	08004141810	
Internet	ITS	Suporte	(071)3402-0800	

19. 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.
jul/24	4º	Todas	Revisão do PCN