Plano de Contingência e Continuidade de Negócios

Plano de Contingência e Continuidade de Negócios

Código: SG-MN-26

Versão 00

São José dos Campos, maio de 2022.

Diretor Geral

Jorge Almeida

Qualidade

Lina Padilha Ramos

Segurança da Informação

Filipe Soares

Suporte Técnico

Guilherme Almeida

www.fenoxtec.com.br

Controle de Revisões

Rev.	Data	Modificações	Elaboração	Aprovação
00	02/06/2022	Publicação Inicial.	Lina Padilha	Guilherme Almeida Jorge Almeida

Índice

1. PLANO DE CONTINUIDADE DE NEGÓCIOS

1.1. **Objetivos do Plano:**

Definir as regras aplicáveis com base na estrutura da Fenox.

Evitar a disrupção dos negócios e a interrupção em tempo maior que o aceitável.

Assegurar que todos conheçam o Plano de Continuidade de Negócios (PCN).

1.2. **Processos Vitais:**

Emissão de Laudos de Vistoria

Análise das Vistorias

Suporte Técnico aos Clientes

Gerenciamento de riscos

Comercial

Financeiro

1.3. Definições de Continuidade de Negócios

Nível de Contingência: Por exemplo em situações de backup, os dados são salvos em cópias de segurança, por meio de procedimentos formais de backup, testes e restauração, porém não há um acordo temporal para o retorno destes dados em caso de incidente (crise ou desastre). As informações se tornam acessíveis no momento que for possível.

Nível de Continuidade: Nas situações de backup, os dados são salvos em cópias de segurança, através de procedimentos formais de backup, testes e restauração. Além disso, existe um acordo temporal para o retorno destes dados em caso de incidente (crise ou desastre) por meio de um acordo de nível de serviço. Este acordo estabelece o tempo máximo para que os dados estejam disponíveis novamente.

Nível de Disponibilidade: Os dados possuem um nível de preservação muito elevado, onde as soluções de contingência e continuidade juntas estão oferecendo alta disponibilidade. Durante um incidente, os usuários nem chegam a perceber que estão trabalhando em uma plataforma do tipo site backup.

Contingência: As atividades que contemplam a contingência são as mais realizadas pelas organizações. Por mais que ainda existem exceções, a grande maioria realiza procedimentos

de contingência, que no ambiente de Tecnologia da Informação dentro de alguns critérios, pode-se entender como Backup. Para que este backup ofereça contingência, é necessário:

- ✓ **Infraestrutura de backup:** para que seja possível tratar apropriadamente as informações e ter um mínimo de garantia delas, é importante possuir os dispositivos adequados para realizar backup.
- ✓ **Políticas de Backup:** as políticas de backup estão diretamente relacionadas com o que será copiado, com qual periodicidade, qual o tempo de retenção dos dados, qual a expectativa de tempo de backup e de restauração.
- ✓ **Plano de Execução e Testes do Backup:** Este plano tem o perfil totalmente operacional, e apresenta os procedimentos que devem ser realizados durante a execução do backup.

A Contingência é uma situação de risco com potencial de ocorrer, inerente às atividades, serviços e equipamentos, e que ocorrendo transformará em uma emergência. Diz respeito a uma eventualidade, possibilidade de ocorrer.

Data Center: Centro de processamento de dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores e outros.

Incidente: É o evento inesperado ou situação que altera a ordem normal das coisas, capaz de causar danos leves ou graves aos sistemas e aos equipamentos.

Intervenção: É a atividade de atuar durante a emergência, seguindo planos de ações para corrigir ou minimizar os possíveis danos aos equipamentos e sistemas.

Firewall: É uma solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

Emergência: Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos ou ao desempenho dos serviços dos clientes e da Fenox.

TI: Tecnologia da Informação.

VM: Máquina virtual, virtualizada no servidor.

Hard Drive: Um disco rígido (HDD) ou disco fixo, é um dispositivo de armazenamento de dados eletromecânicos que usa armazenamento magnético para armazenar e recuperar informações digitais usando um ou mais discos rígidos de rotação rápida (discos) revestidos com material magnético.

1.4. SITE DE CONTINGÊNCIA

Localização: Rua Patrício Santana, 85 – Sala 03 – Térreo – Jardim Satélite – São José dos Campos – SP.
Contato: Jorge Almeida – Diretor de Operações
Telefones: 55 (12) 3028-7644 55 (12) 98134-2294
e-mail: jorge.almeida@fenoxtec.com.br

1.5. RESPONSÁVEIS PELA CONTINGÊNCIA

Responsável	Nome	Telefone / E-mail
Diretor de Contingência	Jorge Almeida	Celular: 55 (12) 98134-2294
1º Líder de Contingência	Victor Corrêa	Celular: 55 (12) 99186-0404
2º Líder de Contingência	Filipe Soares	Celular 55 (12) 98209-3323

O Diretor de Contingência é responsável por apoiar e disponibilizar recursos aos Líderes de Contingência.

Os Líderes de Contingência são responsáveis por mitigar os impactos que porventura venham a ocorrer decorrentes de emergências ou emergências que afetem os sistemas, equipamentos, infraestrutura ou pessoas.

Os colaboradores da empresa são responsáveis por informar ao Comitê do Plano de continuidade de negócios e Contingência, caso detectem algum tipo de emergência ou hipótese acidental que ocorram em alguma das áreas da organização.

1.6. PREMISSAS E OBJETIVOS DO PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

O Plano de Continuidade de Negócios (PCN) assegurará à Fenox a continuidade 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 processos.

Os processos críticos ao negócio da Fenox foram mapeados por meio de levantamento de informações com os Gestores das principais áreas de negócio.

Para tanto, o PCN é definido como (PCN = PAC + PCO + PRD), a saber:

• PAC = Programa de Administração da Crise – é acionado após decretada a Crise, e é voltado para todo o processo. Tem seu término quando se volta à normalidade. Traz as

responsabilidades das equipes envolvidas com as ações de contingência. Com eles, os profissionais sabem o que fazer, antes, durante e após o incidente.

• PCO = Plano de Continuidade Operacional – são acionados os primeiros procedimentos do PAC, e é voltado aos processos de negócio. Tem como principal função o restabelecimento do funcionamento dos principais ativos necessários para a operação da empresa. É o que reduz os impactos provocados por um eventual incidente e o tempo de queda.

• PRD = Plano de Recuperação de Desastres – é acionado junto com o PCO, e é focado na recuperação/restauração de componentes que suportam o PCN. Traz as ações necessárias para que a empresa retome os níveis originais de operação após controle da contingência e arrefecimento da crise, a empresa retome seus níveis originais de operação.

O Plano de Contingência (Emergência) só deve ser acionado em último caso e diante das falhas de todas as demais prevenções. Ele define necessidades e ações mais imediatas.

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

• Análise de riscos de TI

• Análise de Impacto nos Negócios (BIA)

• Estratégia de recuperação

Desta 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.

1.6.1 NÍVEIS DE INCIDENTES

Nível I – Hipótese acidental que pode ser controlada pelo responsável de Infraestrutura da empresa e que não afeta o andamento das atividades.

Nível II – Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo servidor. Ex: Problema com o funcionamento do computador (não liga, travado etc.) ou ainda sistemas offline impedindo o uso dele.

Nível III – Hipótese acidental que impede o uso de sistemas ou equipamentos de toda a empresa e do sistema utilizado pelos clientes, impedindo assim a realização dos atendimentos aos clientes e das atividades dos clientes. Ex: falha na conexão com a internet ou queda de energia elétrica ou ainda problema técnico em algum servidor de rede.

1.6.2 PRINCIPAIS RISCOS

O quadro abaixo define os principais riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

Riscos	Parâmetros
1 – Interrupção de energia elétrica	Causada por fator externo à rede elétrica da empresa com duração da interrupção superior a 60 minutos. Causada por fator interno que comprometa a rede elétrica da empresa com curto-circuito, incêndio e infiltrações.
2 – Falha na climatização do DataCenter	Superaquecimento dos ativos devido a falha no sistema de refrigeração.
3 – Indisponibilidade de rede	Rompimento de cabos decorrente de execuções de serviços na empresa, desastres ou acidentes.
4 – Falha humana	Acidente ao manusear equipamentos e sistemas.
5 – Ataques internos	Ataque aos ativos do Data Center e equipamentos de TI.
6 – Falha de hardware	Falha que necessite de reposição de peça.
7 – Ataque externo	Ataque virtual que comprometa o desempenho, acesso aos dados ou configuração dos serviços essenciais.

1.6.3 POLÍTICA E PROCEDIMENTOS PARA BACKUP

1.6.3.1. BACKUP

Os servidores foram configurados para que diariamente, entre meia-noite e 06h00, sejam realizadas as atividades de backup de arquivos transferidos e localizados no Data Center para um Hard Drive interno e para um servidor externo ao Data Center. Após esse horário para os arquivos enviados pelos clientes durante o dia são armazenados e realizados backups em tempo real.

Além do backup local, a empresa conta com um outro servidor para receber os arquivos de backup, como um Plano de Contingência, armazenando os backups.

1.6.3.2. RESTAURAÇÃO E TESTE

A restauração de dados deve ser solicitada ao responsável pela Infraestrutura e será realizada de acordo com os procedimentos específicos dele. A verificação e o teste de recuperação, serão realizados sempre que possível por meio de um software de backup, configurado para verificar automaticamente as condições do backup.

1.6.3.3. PRINCIPAIS INCIDENTES E AÇÕES DE CONTINGÊNCIA

Incidente	Ações de contingência	Responsável pela ação
Problemas com computadores (internos – colaboradores)	O usuário entra em contato com o responsável pela Infraestrutura e informa o tipo de problema e número do ativo. Após a verificação o solicitante é informado da conclusão/resolução do problema.	Responsável pela Infraestrutura
Problemas de conexão com a rede interna	O setor de Infraestrutura identificará os problemas por meio de um sistema de monitoramento PRTG, que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual área está ocorrendo o problema. Identificar e corrigir a causa do problema. Caso o problema de conexão seja em toda a empresa, verificar se os servidores de endereços e de autenticação estão funcionando adequadamente. Informar a previsão de correção ou solução do problema às partes interessadas.	Responsável pela Infraestrutura
Problemas de conexão com a Internet	O setor de Infraestrutura identificará por meio de um sistema de monitoramento do Firewall que irá comutar para o Link Backup, que irá emitir alerta com a descrição do incidente, os dispositivos envolvidos e em qual setor está ocorrendo o problema. Verificar se o Firewall comutou automaticamente para o Link de Backup.	Responsável pela Infraestrutura

	Identificar a causa do problema. Detectado o problema externo de internet, abrir um chamado de Suporte com a Operadora, visando o reestabelecimento do serviço. Informar a previsão do conserto ou solução às partes interessadas.	
Problemas com acesso ao sistema interno Podio	O setor de Infraestrutura identificará por meio de um sistema de monitoramento, que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual setor está ocorrendo o problema. Verificar se a VM onde ele está instalado está em execução. Caso esteja em execução, verificar as conexões de rede da VM. Caso não esteja em execução, iniciá-la no servidor VMWare e testar seu acesso novamente. Caso seja necessário acionar o sistema de backup para a recuperação da máquina ou arquivos. Informar a previsão do conserto ou solução aos colaboradores.	Responsável pela Infraestrutura
Problemas com equipamentos de rede	O setor de Infraestrutura identificará por meio de um sistema de monitoramento, que emitirá um alerta com a descrição do incidente, os dispositivos e setores envolvidos. Caso tenha garantia, acionar. Caso possível, realizar a manutenção dele. Caso não sejam viáveis as possibilidades acima, realizar a troca do equipamento.	Responsável pela Infraestrutura
Problemas físicos com cabeamento da rede interna	O setor de Infraestrutura por meio de um sistema de monitoramento, que emitirá um alerta com a descrição do incidente, o setor e os dispositivos envolvidos. Detectar a causa do problema por meio de testes no cabeamento. Detectado problema de cabeamento de rede, refazer as	Responsável pela Infraestrutura

	conexões. Verificar as demais ligações caso seja em um rack com switch e testá-lo. Caso haja necessidade, agendar ou efetuar a troca do (s) cabo (s) que estão apresentando falhas. Detectado problema de cabeamento, contingenciar com cabeamento de rede UTP.	
Problemas com falta de energia elétrica	Manter os colaboradores do Suporte Técnico em suas estações de trabalho, enquanto as ações do PCN são executadas. Comunicar aos clientes, caso a interrupção de energia elétrica seja perceptível para eles, ou seja, o tempo de interrupção seja maior que 1 min, tempo esse que o Gerador leva para entrar em funcionamento quando este reconhece a falha no fornecimento de energia elétrica. Sinalizar aos colaboradores do Suporte Técnico àqueles que conseguirão manter o trabalho presencial nas estações onde há fornecimento de energia elétrica pelo Gerador e sinalizar àqueles que irão trabalhar em regime de home office, caso não tenham Notebook com bateria de autonomia de até 2 horas, ou ocorra falha no acionamento automático do Gerador. Realizar verificação do funcionamento do Data Center, No Break e do Gerador, se há necessidade de projeção dos dados do Data Center para a nuvem contratada como redundância em emergências. Sinalizar à Direção, caso encontre divergências no acionamento do Gerador e/ou do NoBreak e entrar em contato com o fornecedor/prestador de serviço para realização de manutenção corretiva e/ou preventiva, caso necessário. Declarar fim do Plano de Contingência, caso o fornecimento de energia elétrica retornar à normalidade e se manter por 30 min sequentes em contínuo fornecimento.	Responsável pela Infraestrutura

	Ordem para o desligamento dos servidores: - Acessar o ambiente virtual e desligar primeiramente os servidores atuais de serviços/web; - Desligar os servidores virtuais de Autenticação; - Desligar o servidor virtual do Firewall; - Desligar os servidores físicos. Ordem para religar os servidores: - Ligar os servidores físicos; - Acessar o ambiente virtual e ligar os servidores de Autenticação; - Ligar o servidor virtual do Firewall; - Ligar os demais servidores virtuais; - Realizar testes de acesso à Internet, autenticação e demais sistemas web.	
Problemas ocasionados por Desastres naturais (Enchente, incêndio e outros)	Executar o SG-MN-27 - Plano de Emergência contra incêndio, no qual contém instruções para evacuação da empresa e definição dos responsáveis, também detalhada em SG-DC-05 – Mapa de fuga e em FT0008 – Rota de fuga. Comunicar aos clientes quanto à interrupção temporária de serviços por 20 min, conforme procedimento SG-PR-02 – Procedimento de Comunicação. Sinalizar aos colaboradores do Suporte Técnico que irão trabalhar em regime de home office, caso não tenham Notebook em casa, a empresa fornecerá um dispositivo similar ou Desktop para ser utilizado durante o novo regime de trabalho, conforme sistemática para entrega de ativos, descrita em SG-MN-14 – Gestão de ativos. Realizar verificação do funcionamento do Data Center, No Break e do Gerador, se há necessidade de projeção dos dados do Data Center para a nuvem contratada como redundância em emergências.	1º e 2º Líder de Contingência

	Sinalizar à Direção, caso encontre divergências no acionamento do Gerador e/ou do NoBreak e entrar em contato com o fornecedor/prestador de serviço para realização de manutenção corretiva e/ou preventiva, caso necessário. Declarar fim do Plano de Contingência, caso o cenário volte à normalidade.	

Área	**Processo**	**Sistemas**
Direção	Análise de capacidade	Podio e Backoffice
Suporte Técnico	Atendimento ao cliente	Backoffice e Sistema de Atendimento
Mesa de Análise	Análise das vistorias	Backoffice e Sistema de Atendimento
Recursos Humanos	Contratação	Podio
Infraestrutura	Gerenciamento de Ativos	Podio
Infraestrutura	Gerenciamento de configuração	Podio e PRTG
Financeiro	Pagamento dos boletos	Bancários e Backoffice

1.7. SITE DA UNIDADE DE NEGÓCIO E REDUNDÂNCIA

A Fenox conta com uma unidade, que é a principal e responsável pelo procedimento de redundância.

A unidade principal (Site Principal ou Site de Contingência) situa-se à Rua Patrício Santana, 85, Térreo, Jardim Satélite, São José dos Campos – SP, onde as atividades da Fenox são executadas em condições normais.

A mesma unidade principal é a responsável pela redundância, que possui um servidor espelho em tempo real para nuvem contratada para emergências.

Em função do site principal ser o de redundância e atender os processos críticos em caso de contingência, segue abaixo a designação do local que os colaboradores das áreas devem se dirigir nas emergências.

Área	**Local de Contingência**
Supor te Técnico, Mesa de Análise, Infraestrutura e Gestão	Site redundância Fenox – servidor espelho em tempo real para nuvem contratada
Comercial, Administrativo, Financeiro e Qualidade	Home-Office
Recursos Humanos	Depende da situação

2. PLANO DE MONITORAÇÃO E DECLARAÇÃO DE DESASTRE

2.1 DEFINIÇÃO DE DESASTRE

Será considerado desastre quando o tempo total de recuperação dos processos for superior ao tempo máximo apontado para Processos **e Sistemas Críticos** provenientes da Análise de Impacto em Negócios (BIA), realizado pelo Comitê de continuidade de negócios no sistema Podio.

2.2 MONITORAÇÃO DE COMUNICAÇÃO DE EVENTOS

Qualquer colaborador da Fenox, ao constatar alguma anormalidade que paralise quaisquer processos apontados no **item Processos e Sistemas Críticos** deverá comunicar o fato ao seu superior imediato, este por sua vez comunicará o fato a um dos Líderes de Contingência:

Responsável do PCN	Nome	Telefones
Diretor de Contingência	Jorge Almeida	Celular: 55 (12) 98134-2294
1º Líder de Contingência	Victor Corrêa	Celular: 55 (12) 99186-0404
2º Líderes de Contingência	Filipe Soares	Celular: 55 (12) 98209-3323
	Mateus Souza	Celular: 55 (12) 94559-8000
	Gilson Rocha	Celular: 55 (12) 99119-1790
	Guilherme Almeida	Celular: 55 (12) 99281-8198
Equipe Contingência	Mateus Souza Filipe Soares Guilherme Almeida Victor Corrêa Lina Ramos	Celular: 55 (12) 94559-8000 Celular: 55 (12) 98209-3323 Celular: 55 (12) 99281-8198 Celular: 55 (12) 99186-0404 Celular: 55 (12) 99147-3093

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

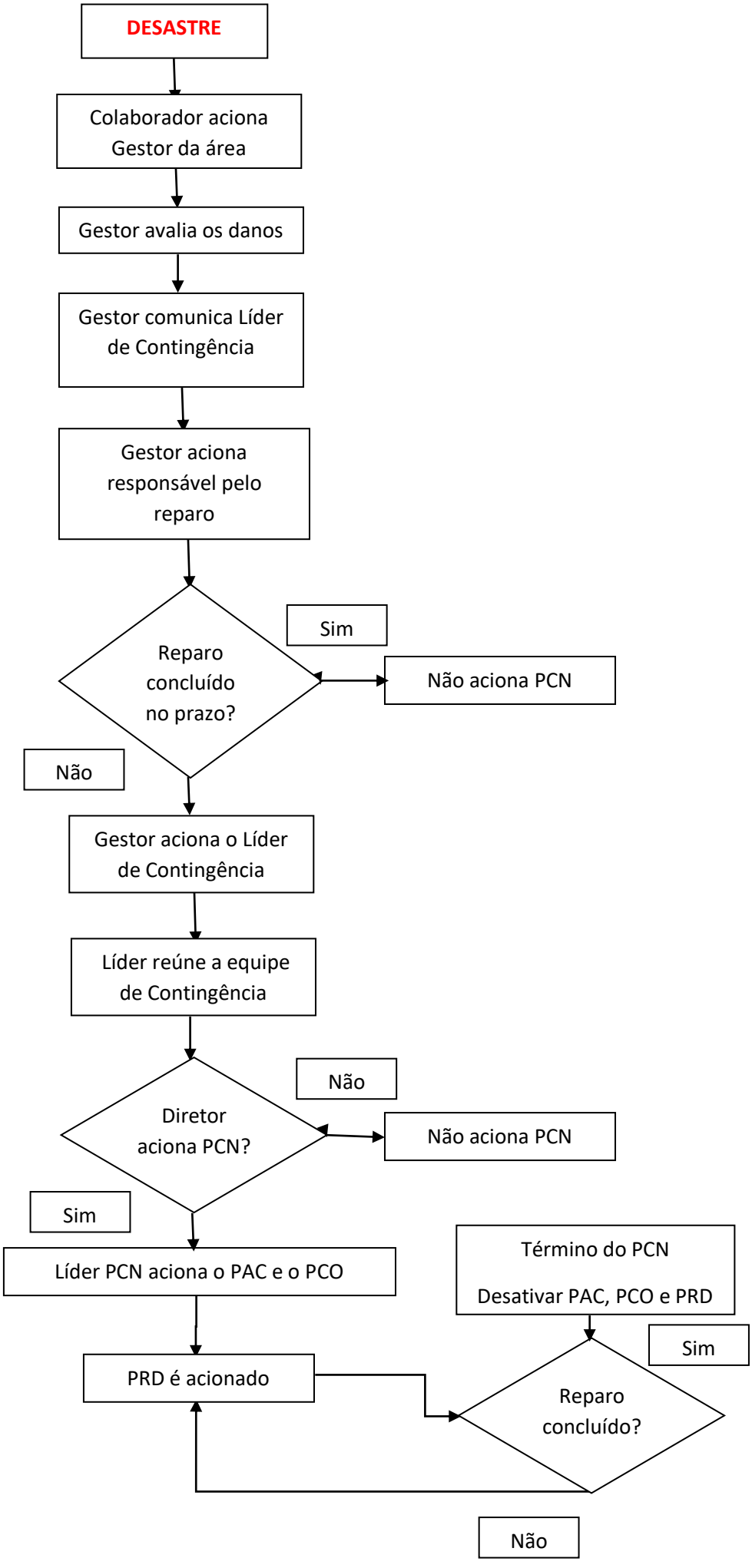
3. DECLARAÇÃO DE DESASTRE/CONTINGÊNCIA (PROGRAMA DE ADMINISTRAÇÃO DA CRISE – PAC)

Ao ocorrer quaisquer eventos que paralise algum **Processo e Sistema Crítico**, o Líder de Contingência avaliará a ocorrência e comunicará ao Diretor responsável pelo PCN.

Com base nas informações recebidas e avaliação do 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 de Contingência.

Na figura abaixo está descrito Fluxo de acionamento do PCN que resultará ou não na Declaração da Contingência.


DESASTRE
Colaborador aciona Gestor da área
Gestor avalia os danos
Gestor comunica Líder de Contingência
Gestor aciona responsável pelo reparo
Reparo concluído no prazo?
Sim
Não aciona PCN
Não
Gestor aciona o Líder de Contingência
Líder reúne a equipe de Contingência
Diretor aciona PCN?
Não
Não aciona PCN
Sim
Líder PCN aciona o PAC e o PCO
PRD é acionado
Término do PCN
Desativar PAC, PCO e PRD
Reparo concluído?
Sim
Não

4. PROCESSOS E SISTEMAS CRÍTICOS

Processo crítico foi definido como um processo de trabalho que uma vez paralisado por tempo superior ao definido pela unidade gestora do negócio irá afetar sensivelmente as operações e serviços da organização gerando maior impacto nos clientes internos e externos, definido na análise de impacto em negócios, conforme parâmetros estabelecidos:

• MTPD (Maximum Tolerable Period of Disruption – Período Máximo Tolerável de Disrupção) - Tempo necessário para que os impactos adversos se tornem inaceitáveis, que pode surgir como resultado de não fornecer um produto/serviço ou realizar uma atividade.
• RTO (Recovery Time Objective – Tempo objetivo de recuperação) – Período após um incidente em que:

- O produto ou serviço deve ser retomado

- A atividade deve ser retomada, ou

- Os recursos devem ser recuperados.

• RPO (Recovery Point Objective – Objetivo de Ponto de Recuperação) – Ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade na retomada.

Foram definidos como **Processos e Sistemas Críticos**:

Área	**Processo**	**Sistemas**
Direção	Análise de capacidade	Podio e Backoffice
Suporte Técnico	Atendimento ao cliente	Backoffice e Sistema de Atendimento
Mesa de Análise	Análise das vistorias	Backoffice e Sistema de Atendimento
Recursos Humanos	Contratação	Podio
Infraestrutura	Gerenciamento de Ativos	Podio
Infraestrutura	Gerenciamento de configuração	Podio e PRTG
Financeiro	Pagamento dos boletos	Bancários e Backoffice

4.1 AÇÕES E PROCEDIMENTOS (PLANO DE CONTINUIDADE OPERACIONAL – PCO)

Qualquer colaborador está apto a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente ao líder do Plano de Continuidade de Negócios.

4.1.1 Impossibilidade de Acesso ao Prédio (inclusive Incêndio)

Dentre as ameaças que impossibilitam o acesso ao prédio destacamos:

• Princípio de Incêndio;

• Ameaça de Bomba;

• Bloqueios;

• Manifestações.

Tempo de duração	Ação	Responsável
Ações Imediatas 5 a 10 minutos	Comunicação às partes interessadas	Direção e Coordenador Técnico do Suporte
Ações até 1minuto	Acionamento da Redundância	Analista de Infraestrutura
Ações	Acionamento do Plano de Emergência – Rota de fuga	Direção e Coordenador Técnico do Suporte
Ações de 1 dia a 5 dias	Acionamento da força de trabalho em Home Office	Coordenador do Suporte Técnico Líder do Suporte Técnico Coordenador da Mesa de Análise Responsável Recursos Humanos
Fim da Contingência	Declarar fim da Contingência	Analista de Infraestrutura

O Plano de Emergência (PAE) é a apresentação de procedimentos estruturados, contemplando as ações de resposta às situações emergenciais, compatíveis com os cenários acidentais identificados, além disso o plano apresenta importantes itens como:

- ✓ Pontos de encontro;
- ✓ Rotas de fuga;
- ✓ Procedimentos de emergência.

Falha na Infraestrutura e Tecnologia

A seguir destacamos a infraestrutura de TI da unidade de negócio.

- Servidor
- NoBreak
- Gerador à diesel

- Conexão Internet
- Energia Elétrica

Na falta de energia elétrica é ativado automaticamente o Gerador localizado na área externa do prédio, para prover energia ao DataCenter, e se houver necessidade, ou seja, se o tempo de interrupção for longo, o Gerador é desligado e o NoBreak entra em funcionamento.

As áreas abastecidas pelo Nobreak e /ou Gerador são as mesmas mapeadas com processos críticos pelo BIA.

- Tecnologia da Informação
- BackOffice
- Sistema de Atendimento

Tempo de duração	Ação	Responsável
Ações Imediatas 5 a 10 minutos	Comunicação às partes interessadas	Coordenador do Suporte Técnico
Ações até 1 minuto	Acionamento da Redundância	Analista de Infraestrutura
Fim da Contingência	Declarar fim da Contingência	Analista de Infraestrutura

4.2 PROCEDIMENTOS DE RETORNO À NORMALIDADE (PROGRAMA DE RECUPERAÇÃO DE DESASTRES – PRD)

Cabe ao Líder da Contingência encerrar o PCN e comunicar ao Diretor e aos Gestores envolvidos no processo.

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

Solicitar à área de TI que retire o comunicado publicado no site da Fenox sobre a situação de contingência.

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.

O processo de Continuidade de Negócios é de responsabilidade e gestão da área T.I., 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 Fenox.

Para que a área de TI possa verificar o grau de atualização do PCN e decidir quanto ao momento em que o processo de continuidade de negócios será atualizado devem ser considerados na Análise Crítica pela Alta Direção:

- Os processos de planejamento de negócios e tecnológico

- O gerenciamento de mudanças

- O gerenciamento de riscos

- O tratamento de problemas e de incidentes

4.3 PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

Falhas nos serviços de TI (Tecnologia da Informação) impactam diretamente todos os setores da Fenox e as operações dos clientes. Neste plano serão definidos os procedimentos, ações e medidas rápidas para os processos críticos. Este plano deve ser seguido para garantir os serviços essenciais em caso de emergências que possam ocorrer durante as atividades, visando aplicar as ações necessárias para correção e/ou eliminação do problema.

4.4 PLANO DE CONTINUIDADE DE NEGÓCIO

Para que este conhecimento seja preservado, os colaboradores admitidos e os transferidos para funções de negócios críticas, principalmente aqueles que pertencem à Equipe de Contingência, são instruídos das suas respectivas responsabilidades no plano.

O programa de treinamento deverá contemplar:

- Riscos, ameaças, controles;

- Responsabilidades PCN;

- Premissas e as estratégias do PCN.

4.4.1 Plano de Continuidade de Negócios – Falha no fornecimento de energia elétrica

Risco	Ameaça	Controle
Interrupção do fornecimento de energia elétrica	Falha no acionamento automático do Gerador – Interrupção no processo do Suporte Técnico e Mesa de Análise	Acionamento automático do NoBreak para alimentar o Data Center Trabalho em regime de home office
Falha na distribuição da energia elétrica para o prédio/empresa	Falha no acionamento do NoBreak para alimentar o Data Center	Acionamento automático/manual do Gerador
Oscilação no fornecimento da energia elétrica para o prédio/empresa	Acionamento automático repetitivo do Gerador	Controle visual do Display de monitoramento do sistema de funcionamento do Gerador

Sequência das ações	Participantes do Plano PCN	Ações/Responsabilidades
1º	Coordenador do Suporte Técnico	Mantém os colaboradores do Suporte Técnico em suas estações de trabalho, enquanto as ações do PCN são executadas. Comunica aos clientes, caso a interrupção de energia elétrica seja perceptível para eles, ou seja, o tempo de interrupção seja maior que 1 min, tempo esse que o Gerador leva para entrar em funcionamento quando este reconhece a falha na rede elétrica.
2º	Líder do Suporte Técnico	Sinaliza aos colaboradores do Suporte Técnico àqueles que conseguirão manter o trabalho presencial nas estações onde há fornecimento de energia elétrica pelo Gerador e sinaliza àqueles que irão trabalhar em regime de home office, caso não tenham Notebook com bateria de autonomia de até 2 horas, ou ocorra falha no acionamento automático do Gerador.

3º	Coordenador da Mesa de Análise	Mantém os colaboradores da Mesa de Análise em suas estações de trabalho, enquanto as ações do PCN são executadas. Sinaliza aos colaboradores da Mesa de Análise àqueles que conseguirão manter o trabalho presencial nas estações onde há fornecimento de energia elétrica pelo Gerador e sinaliza àqueles que irão trabalhar em regime de home office, caso não tenham Notebook com bateria de autonomia de até 2 horas, ou ocorra falha no acionamento automático do Gerador.
4º	Analista de Infraestrutura	Realiza verificação do funcionamento do Data Center, No Break e do Gerador, se há necessidade de projeção dos dados do Data Center para a nuvem contratada como redundância em emergências. Sinaliza à Direção, caso encontre divergências no acionamento do Gerador e/ou do NoBreak e entra em contato com o fornecedor/prestador de serviço para realização de manutenção corretiva e/ou preventiva, caso necessário.
5º	Recursos Humanos	Verifica se há Notebook com bateria de autonomia de até 2 horas para o setor Administrativo, se não houver, caso a interrupção esteja identificada em 30 min sem diferenças no cenário, e caso ocorra falha no acionamento automático do Gerador, sinalizar ao setor Comercial, Administrativo e de Qualidade para continuidade do trabalho em regime home office.
6º	Analista de Infraestrutura	Declara fim do Plano de Continuidade, caso o fornecimento de energia elétrica retornar à normalidade e se manter por 30 min sequentes em contínuo fornecimento, sem grandes oscilações. Este plano deverá ser testado mensalmente.

4.4.2 Plano de Continuidade de Negócios – Disponibilidade do Sistema (Redundância)

Risco	Ameaça	Controle
Interrupção dos serviços prestados pela Fenox e das atividades dos clientes	Falha no funcionamento do Data Center	Monitoramento PRTG Acionamento do link para nuvem contratada

Sequência das ações	Participantes do Plano PCN	Ações/Responsabilidades
1º	Analista de Infraestrutura	Caso nosso Data Center principal esteja inacessível, todo nosso tráfego é enviado para o cloud privado da Azure (Datacenter backup). Neste caso, será realizada uma modificação de DNS da Cloudflare, alterando os hosts do domínio *.fenoxapp.com.br para o IP da Azure.
2º	Analista de Infraestrutura	Declara fim do Plano de Continuidade, caso o Data Center esteja acessível. Este plano deverá ser testado semestralmente.

4.4.3 Plano de Continuidade de Negócios – Data Center Backup

Risco	Ameaça	Controle
Perda das informações, vídeo e fotos dos clientes	Falha no funcionamento do Data Center	Monitoramento PRTG Acionamento do link para nuvem contratada Backup em mais de uma unidade

Sequência das ações	Participantes do Plano PCN	Ações/Responsabilidades
1º	Analista de Infraestrutura	Caso nosso Data Center principal esteja inacessível, todo o tráfego é enviado para o cloud privado da Equinix (Datacenter backup). Neste caso, será realizada uma modificação de DNS da Cloudflare, alterando os hosts do domínio *.fenoxapp.com.br para o IP da Equinix.
2º	Analista de Infraestrutura	Declara fim do Plano de Continuidade, caso o Data Center esteja acessível. Este plano deverá ser testado semestralmente.

4.4.4 Plano de Continuidade de Negócios – Exercício de trabalho remoto (Simulação)

Risco	Ameaça	Controle
Interrupção da prestação dos serviços de Suporte Técnico da Fenox	Falhas em ICs, rede elétrica, eventos naturais adversos	Monitoramento por log de acesso Backup em nuvem contratada

Sequência das ações	Participantes do Plano PCN	Ações/Responsabilidades
1º	Coordenador do Suporte Técnico Líder do Suporte Técnico Coordenador da Mesa de Análise	Sinaliza àqueles que conseguirão realizar o trabalho em regime de home office, que possuem notebook e internet em casa, para darem continuidade nos atendimentos neste formato. Verifica e sinaliza àqueles que irão trabalhar em regime de home office, caso não tenham Notebook e/ou Internet em casa, para levarem Notebook e Celular da empresa, para realizar o roteamento da Internet.
2º	Responsável pelo setor de Recursos Humanos	Sinaliza aos colaboradores dos setores Comercial, Administrativo, Recursos Humanos e Qualidade, que conseguirão realizar o trabalho em regime de home office, que possuem notebook e internet em casa, para darem continuidade nos atendimentos neste formato. Verifica e sinaliza àqueles que irão trabalhar em regime de home office, caso não tenham Notebook e/ou Internet em casa, para levarem Notebook e Celular da empresa, para realizar o roteamento da Internet.
3º	Analista de Infraestrutura	Declara fim do Plano de Continuidade, caso ICs, rede elétrica e outros itens essenciais para prestação de serviços retornem à normalidade. Este plano deverá ser testado semestralmente.

4.4.5 Plano de Continuidade de Negócios – Backup da última versão do sistema de Desenvolvimento

Risco	Ameaça	Controle
Erros em sistema recém alterados para nova versão	Falhas nas funcionalidades do sistema Interrupção das atividades dos clientes	Testes em ambiente de Desenvolvimento Acompanhamento da implementação nos clientes

Sequência das ações	Participantes do Plano PCN	Ações/Responsabilidades
1º	Desenvolvimento	Realizar download do arquivo salvo no módulo de "Desenvolvimento", do sistema Podio, do aplicativo "Version Control", da versão anterior do sistema, no computador Desktop e realizar upload no (s) computador (es) do (s) cliente (s).
2º	Desenvolvimento	Realizar correções da versão atual, no sistema do arquivo salvo em "Version Control", conforme erros observados no (s) cliente (s) e salvar em "Version Control".
3º	Desenvolvimento	Testar a versão corrigida em ambiente de Desenvolvimento quanto às funcionalidades com erros descritos pelo (s) cliente (s).
4º	Desenvolvimento	Realizar download do arquivo salvo no módulo de "Desenvolvimento", do sistema Podio, do aplicativo "Version Control", da versão corrigida do sistema, no computador Desktop e realizar upload no (s) computador (es) do (s) cliente (s).
5º	Desenvolvimento	Acompanhar a utilização da versão corrigida pelo (s) cliente (s) com a confirmação de que as funcionalidades estão em funcionamento contínuo, sem oscilações para transição entre funções e sem oscilações nos resultados obtidos pelo (s) cliente (s). Este plano deverá ser testado semestralmente.

4.4.6 Plano de Continuidade de Negócios – Testes de Recuperação de desastres (enchente, incêndio e outros eventos)

Risco	Ameaça	Controle
Interrupção do fornecimento dos serviços críticos	Disrupção das atividades Perda de clientes	Execução do Plano de Contingência conforme testes de recuperação de desastres

Sequência das ações	Participantes do Plano PCN	Ações/Responsabilidades
1º	Coordenador do Suporte Técnico Líder do Suporte Técnico Coordenador da Mesa de Análise	Comunica aos clientes a interrupção temporária dos serviços, por tempo limitado, até o início da prestação de serviços em regime de trabalho home office. Sinaliza àqueles que conseguirão realizar o trabalho em regime de home office, que possuem notebook e internet em casa, para darem continuidade nos atendimentos neste formato. Verifica e sinaliza àqueles que irão trabalhar em regime de home office, caso não tenham Notebook e/ou Internet em casa, para levarem Notebook e Celular da empresa, para realizar o roteamento da Internet.
2º	Responsável pelo setor de Recursos Humanos Analista de Infraestrutura	Sinaliza aos colaboradores dos setores Comercial, Administrativo, Recursos Humanos e Qualidade, que conseguirão realizar o trabalho em regime de home office, que possuem notebook e internet em casa, para darem continuidade nos atendimentos neste formato. Verifica e sinaliza àqueles que irão trabalhar em regime de home office, caso não tenham Notebook e/ou Internet em casa, para levarem Notebook e Celular da empresa, para realizar o roteamento da Internet.
3º	Analista de Infraestrutura	Caso nosso Data Center principal esteja inacessível, todo o tráfego é enviado para o cloud privado da Equinix (Datacenter backup). Neste caso, será realizada uma modificação de DNS da Cloudflare, alterando os hosts do domínio *.fenoxapp.com.br para o IP da Equinix.
4º	Direção Analista de Infraestrutura Coordenador do Suporte Técnico Líder do Suporte Técnico Coordenador da Mesa de Análise	Declara fim do Plano de Continuidade, caso ICs, rede elétrica e outros itens essenciais para prestação de serviços retornem à normalidade. Comunica o fim do Plano de Continuidade aos clientes. Comunica aos colaboradores o fim do regime de trabalho em home office. Este plano deverá ser testado semestralmente.

4.5 DIVULGAÇÃO E TREINAMENTO

Um dos fatores primordiais para o funcionamento deste plano são o conhecimento e a familiaridade das pessoas 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, a equipe da Fenox definiu que serão realizadas semestralmente sessões de divulgação a todos os colaboradores e envolvidos no planejamento de continuidade de negócios.

Estas sessões serão organizadas pela área de TI em conjunto com a área de Administrativa com o objetivo de 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.

4.6 REALIZAÇÃO DE TESTES

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN e são planejados e executados com periodicidade mínima anual a partir da data da sua implantação. Os testes PCN estão definidos no SG-MN-04 - Painel de Indicadores e no presente documento, onde constam as descrições, métodos, metas, responsável e periodicidade.

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da área de Tecnologia da Informação. Os cenários de continuidade definidos na Fenox estão definidos em:

Cenário 1 – Impossibilidade de Acesso ao Prédio (inclusive Incêndio, inundação, incidência de raios e falhas na infraestrutura da construção)

Cenário 2 – Falha na Infraestrutura e Tecnologia (NoBreak, Gerador, Data Center, Software de monitoramento dos processos e computadores)

Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela alta administração, que dever ser arquivado por um período mínimo de 5 (cinco) anos.

Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes de negócios da Fenox e deverão ser conduzidos pela equipe de contingência em total conformidade com o definido.

As simulações deverão ser realizadas sobre cenários e ameaças contemplados no plano, devendo cobrir os riscos e ameaças com maior probabilidade e impacto de ocorrência.

Os exercícios simulados são registrados por meio de resultados, prints dos sistemas e fotos e arquivados no sistema Podio.

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

• Análise de riscos de TI

• Análise de Impacto nos Negócios (BIA)

• Estratégia de recuperação

Desta forma é necessário simular as 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 críticos de sucesso.