Título do Documento:

PLANO DE CONTINUIDADE DE NEGÓCIOS

Informações Importantes

FENOX TECNOLOGIA LTDA
Avenida Salmão, 325 - Salas 91 a 96 e 101
São José dos Campos - SP
CEP: 12246-260 - Brasil
(12) 3028-7644

www.fenoxtec.com.br
fenox@fenoxtec.com.br

INFORMAÇÕES DO DOCUMENTO

DADOS DO DOCUMENTO			
Título do Documento: PLANO DE CONTINUIDADE DE NEGÓCIOS **Título do Resumido:** P.C.N			
CONSIDERANDO a necessidade de estabelecer, manter e controlar os processos relacionados à continuidade dos negócios, este documento vem para descrever o Plano de Continuidade de Negócios (PCN), em conformidade com os requisitos da ISO 22301:2020, definindo os critérios, procedimentos e responsabilidades para a declaração, ativação, gerenciamento e encerramento do plano, bem como para a gestão das contingências aplicáveis.			
Tipo: Documento Confidencial / Cópia Controlada	**Numeração**: 23081039-M-SP		**Páginas**: 266
Área Emitente: Qualidade / Operações	**Distribuição**: ☒ Interno	☐ Externo	
Distribuído por: Qualidade	**Autor:** Jorge Luis Almeida	**Cliente:** FENOX	**Data:** 25/11/2025
Palavras Chaves: P.C.N	**Categoria:** Documento Confidencial / Cópia Controlada		

REFERÊNCIA
Documentos de Referência: Manual de Sistema de Gestão Integrado SG-MN-01 e antigo SG-MN-26 – Plano de Contingência e Continuidade de Negócios.

DADOS DO PROJETO	
Cliente: FENOX TECNOLOGIA	**Projeto:** Unificação de codificação e armazenamento de documentação FENOX.

ELABORAÇÃO / REVISÃO

Rev.	Data	Ordem	Departamento	Quem	Justificativa	Status
00	28/11/23	Elaboração	Operações	JLA	Elaboração do Documento	P/ Aprovação
00	28/11/23	Revisão	Qualidade	ALS	Revisão de Texto	P/ Aprovação
00	28/11/23	Revisão	Operações	GA	Revisão de Texto	P/ Aprovação
01	26/04/24	Revisão	Direção	JLA	Revisão de Texto	Aprovado
02	25/11/25	Revisão	Qualidade	LM	Revisão de texto	Aprovado
02	08/01/26	Revisão	Direção	JLA	Aprovação das Revisões	Aprovado

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

a. Emissão de Laudos de Vistoria
b. Análise das Vistorias
c. Suporte Técnico aos Clientes
d. Gerenciamento de riscos
e. Comercial
f. Financeiro

1.3 DEFINIÇÕES DE CONTINUIDADE DE NEGÓCIOS

a. **Nível de Contingência:** Nível no qual os dados e sistemas são protegidos por meio de procedimentos formais de backup, incluindo cópias de segurança, testes e restauração. Neste nível, não há acordo temporal definido para a recuperação dos dados ou serviços em caso de incidente, crise ou desastre. As informações tornam-se acessíveis quando a restauração for tecnicamente possível.

b. **Nível de Continuidade:** Nível no qual, além da existência de procedimentos formais de backup, testes e restauração, há um acordo temporal previamente definido para a recuperação dos dados e serviços em caso de incidente. Este acordo é formalizado por meio de Acordos de Nível de Serviço (SLA), que estabelecem o tempo máximo aceitável para o restabelecimento das operações.

c. **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, a transição para ambientes alternativos ocorre de forma transparente, de modo que os usuários não percebam a indisponibilidade ou a utilização de ambientes de contingência.

d. **Contingência:** As atividades que contemplam a contingência são as mais realizadas pelas organizações. Por mais que ainda existem exceções, no contexto de Tecnologia da Informação TI a contingência é frequentemente associada a procedimentos de backup e restauração, desde que atendam aos critérios técnicos, operacionais e organizacionais definidos neste plano. Para que este backup ofereça contingência, é necessário:

e. **Infraestrutura de backup:** Conjunto de equipamentos, sistemas, softwares e meios de armazenamento utilizados para a realização, manutenção e recuperação de cópias de segurança, garantindo a integridade, confidencialidade e disponibilidade das informações.

f. **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.

g. **Plano de Execução e Testes do Backup:** Este plano tem o perfil totalmente operacional, que estabelece 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, que, ao se concretizar, pode resultar em uma emergência ou incidente com impacto nos processos de negócios.

h. **Data Center:** Centro de processamento de Dados (CPD), é um ambiente projetado para abrigar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores e outros.

i. **Incidente:** É o evento inesperado ou situação anormal que interrompe ou altera a operação normal dos sistemas, serviços ou equipamentos, podendo causar impactos leves, moderados ou graves aos processos de negócio

j. **Intervenção:** Atividade executada durante uma emergência ou incidente, com o objetivo de corrigir, conter ou minimizar os impactos aos sistemas, equipamentos e serviços, conforme os planos de ação, procedimentos operacionais e diretrizes estabelecidos no PCN.

k. **Firewall:** Solução de segurança implementada por meio de 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.

l. **Emergência:** Situação decorrente de um evento ou incidente 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.

m. **TI: Tecnologia da Informação.**

n. **VM: Máquina virtual, virtualizada no servidor.**

o. **Hard Drive:** 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

- Fenox Tecnologia
- CNPJ: 26.507.563/0001-64
- Endereço: Av. Salmão, nº 325, salas 91 a 96 e 101, Parque Residencial Aquarius – São José dos Campos – SP
- Contato: Jorge Luis Almeida – Diretor de Operações
- Telefone: (12) 98134-2294
- E-mail: jorge.almeida@fenoxtec.com.br

1.5 RESPONSÁVEL PELA CONTIGÊNCIA

Responsável	Nome	Telefone / E-mail
Diretor de Contingência	Jorge Luis Almeida	Celular: (12) 98134-2294
1º Líder de Contingência	Victor Corrêa	Celular: (12) 98859-4239
2º Líder de Contingência	Gabriel Souza	Celular: (12) 99106-9556

A continuidade de negócios é responsabilidade da Alta Direção da Fenox, cabendo à área de TI a execução técnica das estratégias, planos e procedimentos definidos neste PCN.

O Diretor de Contingência é responsável por assegurar o apoio institucional, bem como por disponibilizar os recursos necessários aos Líderes de Contingência.

Os Líderes de Contingência são responsáveis por coordenar e mitigar os impactos decorrentes de emergências, incidentes ou situações de crise que afetem sistemas, equipamentos, infraestrutura ou pessoas, conforme os procedimentos definidos neste plano.

Os colaboradores da empresa são responsáveis por comunicar imediatamente aos Líderes de Contingência a identificação de qualquer incidente, emergência, condição anormal ou situação de risco potencial.

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

O PCN tem como premissa assegurar à Fenox a continuidade de seus negócios em caso de paralisação total ou parcial, decorrente de incidente, crise ou desastre (sinistro) que afete um ou mais processos considerados críticos.

Considera-se que um sinistro se concretiza quando ameaças internas ou externas exploram vulnerabilidades existentes nos processos, sistemas, infraestrutura ou pessoas, resultando em impacto relevante para a organização.

Os processos críticos ao negócio da Fenox foram mapeados por meio de levantamento estruturado de informações junto aos Gestores das principais áreas de negócio, servindo de base para a definição das estratégias de continuidade e recuperação.

Para tanto, o PCN é estruturado conforme a seguinte composição: (PCN = PAC + PCO + PRD), a saber:

a) PAC - Programa de Administração da Crise – É acionado após declaração formal da crise e possui abrangência sobre todo o processo de gerenciamento do evento. Permanece ativo até o retorno à normalidade operacional e define as responsabilidades das equipes envolvidas nas ações de contingência, orientando os profissionais quanto às atividades a serem executadas antes, durante e após o incidente.
b) PCO = Plano de Continuidade Operacional – É acionado de forma integrada aos primeiros procedimentos do PAC, e é voltado aos processos de negócio. Tem como principal função o restabelecimento do funcionamento dos principais ativos críticos necessários à operação da empresa, reduzindo os impactos provocados por eventuais incidentes e minimizando o tempo de indisponibilidade das atividades essenciais.

c) PRD = Plano de Recuperação de Desastres – é acionado em conjunto com o PCO, e é focado na recuperação/restauração de componentes que suportam o PCN. Define as ações necessárias para que, após o controle da contingência e o arrefecimento da crise, a empresa retome seus níveis originais de operação.
d) 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.
e) O desenvolvimento do PCN é baseado na avaliação dos processos críticos conforme diretrizes estabelecidas pela Administração da Fenox compreendendo às suas principais etapas:
    i. Análise de riscos de TI
    ii. Análise de Impacto nos Negócios (BIA)
    iii. 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 – Incidente pontual, de baixa criticidade, que pode ser controlado e solucionado pelo responsável pela Infraestrutura de TI, sem impacto significativo no andamento das atividades da empresa ou na prestação dos serviços.

Nível II – Incidente que impede a utilização de equipamento ou sistema específico, ocasionando a interrupção temporária das atividades de um colaborador ou de uma área, sem comprometer integralmente a operação da empresa**.** Exemplos**:**

- Falha no funcionamento de estação de trabalho (não liga, travamento, falha de hardware);
- Indisponibilidade temporária de sistemas que impeça o uso local.

Nível III – Incidente que impede a utilização de sistemas ou equipamentos essenciais, afetando todas a empresa e/ou os sistemas utilizados pelos clientes, impossibilitando a realização de atendimentos e execução das atividades essenciais do negócio. Exemplos:

- Falha generalizada na conexão com a internet;
- Queda de energia elétrica;
- Falha técnica em servidores, infraestrutura de rede ou ambiente de hospedagem.

1.6.2 PLANO DE CONTINUIDADE DE NEGÓCIOS

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.

	Causada por fator interno que comprometa a rede elétrica da empresa com curto-circuito, incêndio e infiltrações. superior a 60 minutos
2 – Falha na climatização do Data Center	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 PROCEDIMENTO PARA BACKUP

1.6.3.1 BACKUP

São realizadas rotinas de backup periódico para garantir a integridade e disponibilidade das informações críticas de negócio.

- Fotos e Laudos: sincronismo a cada 5 minutos para *storage* local, com backup incremental enviado a um segundo *storage*.
- Vídeos: sincronismo a cada 5 minutos para *storage* local, com backup incremental a cada 15 minutos armazenado em nuvem.
- Banco de Dados: backup completo diário às 22h, armazenado em *storage* dedicado.
- Máquinas Virtuais: backup incremental diário via *CrashPlan*, com cópia adicional em HD externo.

1.6.3.2 VALIDAÇÃO DE CONTEÚDOS

Uma restauração mensal deve ser realizada, escolhendo-se aleatoriamente uma base para teste.
Anomalias identificadas devem ser registradas e corrigidas pela Infraestrutura.

1.6.3.3 ARMAZENAMENTO

Os *storages* principais estão localizados em sala técnica de acesso controlado.

1.6.3.4 RESTAURAÇÃO

A restauração de dados deve ser solicitada ao responsável pela Infraestrutura e que 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.

1.6.4 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 (coordenador) que aciona Infraestrutura ou Suporte Técnico N2 – dependendo do caso - 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 / Suporte Técnico N2
Problemas de conexão com a rede interna	O setor de Infraestrutura identificará os problemas e corrigirá a causa. 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 os problemas por meio de um sistema de monitoramento (site24x7) que irá emitir alerta com a descrição do incidente e em qual link. Deverá ser verificado se o link principal – caso seja o link impactado - comutou automaticamente para o Link de Backup. Identificar e corrigir a causa do problema se possível internamente. Detectado problema externo de internet, abrir um chamado de suporte com a Operadora, visando o reestabelecimento do serviço. Informar a previsão do conserto ou solução das partes.	Responsável pela Infraestrutura

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 Plano de Emergência contra incêndio, no qual contém instruções para evacuação da empresa e definição dos responsáveis, também detalhada em – Mapa de fuga e Rota de fuga. Sinalizar aos colaboradores do Suporte Técnico – se possível na circunstância - 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 - Gestão de Ativos. Após a fuga, comunicar aos clientes quanto à interrupção temporária de serviços Manual de Sistema de Gestão Integrado. Realizar verificação do funcionamento do Data Center, Nobreak e do Gerador – após ciência das contenções cabíveis - 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 e conforme o cenário aplicável. Declarar fim do Plano de Contingência, caso o cenário volte à normalidade.	1º e 2º Líder de Contingência

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
Suporte Técnico / Qualidade	Gerenciamento de Ativos	Podio
Infraestrutura	Gerenciamento de configuração	Podio e NAGIOS
Financeiro	Pagamento dos boletos	Bancários e Backoffice

1.7 SITE DA UNIDADE DE NEGÓCIO E REDUNDÂNCIA

A Fenox possui duas unidades operacionais, sendo:

- Unidade Principal (Matriz): localizada em São José dos Campos – SP, onde se concentram os principais processos operacionais, tecnológicos e de armazenamento de dados;
- Unidade Filial: localizada no Estado de Goiás, que atua apenas como domicílio fiscal, para emissão de NF, conforme exigido pelo DETRAN/GO.

A Unidade Principal (Matriz), situada na Av. Salmão, nº 325, salas 91 a 96 e 101, Parque Residencial Aquarius, São José dos Campos – SP, é o Site Principal da organização, no qual as atividades da Fenox são executadas em condições normais e onde estão hospedados os ativos críticos de informação e infraestrutura de TI.

A estratégia de continuidade e redundância da Fenox está centralizada na Unidade Principal, a qual conta com servidor espelhado em tempo real em ambiente de nuvem contratado, destinado a suportar a operação em situações de emergência, contingência ou desastre, conforme definido neste PCN.

Em situações de emergência que impactem os processos críticos, a diretriz de deslocamento, permanência ou trabalho remoto dos colaboradores será definida conforme a natureza do incidente, o nível de impacto e as orientações do PCN.

Área	Local de Contingência
Operação, Desenvolvimento e Gestão	Site redundância Fenox – servidor espelho em tempo real para nuvem contratada

Comercial, Administrativo, Financeiro e Qualidade	Home-Office
Recursos Humanos	Home-Office

1.8 DEFINIÇÕES - PCN

1.8.1 DEFINIÇÃO DE DESASTRE

Será caracterizado como desastre todo evento ou incidente cujo tempo total de recuperação dos processos ultrapasse o tempo máximo aceitável definido para os Processos e Sistemas Críticos, conforme estabelecido na BIA.

A BIA é realizada e mantida pelo Comitê de Continuidade de Negócios e registrada no sistema Podio, sendo este o repositório oficial das informações relacionadas aos limites de tolerância, tempos máximos de recuperação e critérios de criticidade.

1.9 MONITORAMENTO DE COMUINICAÇÃO 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: (12) 98134-2294
1º Líder de Contingência	Victor Corrêa	Celular: (12) 98859-4239
Equipe Contingência	Gabriel Souza Janaina Sousa Victor Corrêa Leonardo Machado	Celular: (12) 99106-9556 Celular: (11) 99281-8198 Celular: (12) 98859-4239 Celular: (12) 99131-5329

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.

2 DECLARAÇÃO DE DESASTRE / CONTINGÊNCIA – PROGRAMA DE ADMINISTRAÇÃO DE 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.

3 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:
  i. O produto ou serviço deve ser retomado
  ii. A atividade deve ser retomada, ou
  iii. 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
Qualidade	Gerenciamento de Ativos	Podio
Infraestrutura	Gerenciamento de configuração	Podio e NAGIOS
Financeiro	Pagamento dos boletos	Bancários e Backoffice

3.1 AÇÕES E PROCEDIMENTOS - PLANO DE CONTINUIDADE OPERACIONAL (PCO)

3.1.1 IMPOSSIBILIDADE DE ACESSO AO PRÉDIO – INCUSIVE 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 de 1 min a 1h	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 Coordenador da Mesa de Análise Responsável Recursos Humanos
Fim da Contingência	Declarar fim da Contingência	Analista de Infraestrutura

3.2 PROCEDIMENTO DE RETORNO A NORMALIDADE - PRD

Cabe ao Líder de Contingência coordenar o retorno à normalidade e formalizar o encerramento do Plano de Continuidade de Negócios (PCN), comunicando a Alta Direção e os gestores envolvidos.

O retorno à normalidade ocorre após a estabilização da contingência, com o restabelecimento dos processos e sistemas críticos, conforme definido na BIA, respeitando os RTO e RPO estabelecidos.

Quando aplicável, após a liberação do acesso ao prédio e a validação das condições de segurança, os colaboradores deverão ser comunicados por meio de seus gestores para retorno às atividades presenciais. Eventuais comunicados temporários publicados nos canais institucionais da Fenox deverão ser retirados pela área de Tecnologia da Informação.

O PCN será considerado encerrado quando os processos e sistemas críticos estiverem operando de forma estável, sem reincidência do incidente, e após validação do Líder de Contingência, com ciência da Alta Direção.

Após o encerramento do PCN, o Comitê de Continuidade de Negócios deverá avaliar a execução das ações realizadas, registrar evidências, identificar lições aprendidas e, quando necessário, propor ações de melhoria e atualização do PCN e do PRD, garantindo a melhoria contínua do Sistema de Gestão de Continuidade de Negócios.

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

As falhas nos serviços de TI impactam diretamente todos os setores da Fenox bem como as operações dos clientes. Este PCN define os procedimentos, ações e medidas de resposta aplicáveis aos processos críticos, com o objetivo de assegurar a continuidade dos serviços essenciais em situações de emergência que possam ocorrer durante a execução das atividades. O plano deve ser seguido sempre que necessário, visando à correção, mitigação e/ou eliminação das causas do problema, bem como à redução dos impactos operacionais.

3.4 PLANO DE CONTINUIDADE DE NEGÓCIO

Para assegurar a preservação do conhecimento relacionado à continuidade dos negócios, os colaboradores recém-admitidos e aqueles transferidos para funções de negócios críticas, principalmente aqueles que pertencem à Equipe de Contingência, são instruídos das suas respectivas responsabilidades, atribuições e procedimentos previstos no Plano de Continuidade de Negócios.

O programa de treinamento deverá contemplar:

- Riscos, ameaças, controles;
- Responsabilidades PCN;
- Premissas e as estratégias do PCN.

3.4.1 FALHA NO FORNECIMENTO DE ENERGIA

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 PCN	Ações/Responsabilidades
1º Ação	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 Ação	Coordenador 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 bem como 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 Ação	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 bem como 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 Ação	Analista de Infraestrutura	Realiza verificação do funcionamento do Data Center, nobreak e do gerador, se há necessidade de projeção dos dados do Data Center para a nuvem contratada como redundância em emergências.
5º Ação	Analista de Infraestrutura	Sinaliza 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.
6º Ação	Recursos Humanos	Verifica se há notebook com autonomia de bateria 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.
7º Ação	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 anualmente

3.4.2 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 NAGIOS Acionamento do link para nuvem contratada

Sequência das ações	Participantes do PCN	Ações/Responsabilidades
1º Ação	Analista de Infraestrutura	Caso nosso Data Center principal esteja inacessível, todo nosso tráfego é enviado para o cloud privado da Azure (Data Center 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 Ação	Analista de Infraestrutura	Declara fim do Plano de Continuidade, caso o Data Center esteja acessível. Este plano deverá ser testado anualmente

3.4.3 ESTRUTURA DATA CENTER BACKUP

Risco	Ameaça	Controle
Perda das informações, vídeo e fotos dos clientes	Falha no funcionamento do Data Center Acidentes naturais (princípio de incêndio)	Monitoramento NAGIOS Acionamento do link para Data Center Backup Backup em mais de uma unidade
Sequência das ações	**Participantes do PCN**	**Ações/Responsabilidades**

1º Ação	Analista de Infraestrutura	PLANTA SP – SÃO JOSÉ DOS CAMPOS Acionamento Sistema Autônomo de Incêndio Caso nosso Data Center principal esteja inacessível, todo o tráfego é enviado para Data Center - backup. Neste caso, será realizada uma modificação de DNS, alterando os hosts do domínio *.fenoxapp.com. br. (Backup diário em mídia removível de 10T, guardada em cofre e sala com controle de acesso)
2º Ação	Analista de Infraestrutura	Declara fim do Plano de Continuidade, caso o Data Center esteja acessível. Este plano deverá ser testado anualmente.

3.4.4 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 PCN**	**Ações/Responsabilidades**

1º Ação	Coordenador 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 Ação	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.

3.4.5 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 PCN	Ações/Responsabilidades
1º Ação	Desenvolvimento	Realizar o download do arquivo referente à versão anterior do sistema, armazenado no módulo “Desenvolvimento” do sistema Wiki, por meio do aplicativo “Controle de versão”, salvando-o em computador desktop autorizado. Em seguida, proceder com o upload do referido arquivo no(s) computador(es) do(s) cliente(s), conforme os procedimentos técnicos estabelecidos.
2º Ação	Desenvolvimento	Realizar as correções necessárias na versão atual do sistema, conforme erros identificados no ambiente do cliente, e salvar a versão atualizada no aplicativo “Controle de versão”.
3º Ação	Desenvolvimento	Testar a versão corrigida em ambiente de Desenvolvimento quanto às funcionalidades com erros descritos pelo(s) cliente(s).
4º Ação	Desenvolvimento	Realizar download do arquivo salvo no módulo de “Desenvolvimento”, do sistema Wiki, do aplicativo “Controle de versão”, da versão corrigida do sistema, no computador Desktop e realizar upload no(s) computador(es) do(s) cliente(s).

5º Ação	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 anualmente.

3.4.6 TESTE DE RECUPERAÇÃO DE DESASTRES (ENCHENTE, INCÊNDIO E OUTROS)

Risco	**Ameaça**	**Descrever**
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 PCN**	**Ações/Responsabilidades**
1º Ação	Coordenador 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
2 ºAção	Responsável pelo setor de Recursos Humanos Analista de Infraestrutura	Sinaliza aos colaboradores dos setores Comercial, Administrativo 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.

3 º Ação	Analista de infraestrutura	Caso nosso Data Center principal esteja inacessível, todo o tráfego é enviado para o *cloud* privado da Azure (Data Center *backup*). Neste caso, será realizada uma modificação de DNS da *Cloudflare*, alterando os hosts do domínio *fenoxapp.com.br para o IP da Azure.
4 º Ação	Direção Analista de Infraestrutura	Declara fim do Plano de Continuidade, caso o Data Center esteja acessível.

3.5 DIVULGAÇÃO E TREINAMENTO

Um dos fatores primordiais para a efetividade deste Plano de Continuidade de Negócios é o conhecimento e a familiaridade dos colaboradores e demais envolvidos com as estratégias, recursos e procedimentos definidos para a continuidade dos negócios e a recuperação de desastres.

Para assegurar esse conhecimento e conferir a credibilidade e eficácia ao plano, a Fenox estabelece a realização de sessões semestrais de divulgação e conscientização, direcionada a todos os colaboradores e às partes envolvidas no planejamento de continuidade de negócios.

As sessões serão organizadas conjuntamente pelas áreas de TI e Administrativa, com o objetivo de manter os colaboradores atualizados quanto aos conceitos de continuidade adotados, aos objetivos do planejamento e ao funcionamento das estratégias de continuidade e recuperação de desastres.

3.6 REALIZAÇÃO DE TESTES

Os testes do PCN têm como objetivo assegurar sua eficiência e a efetividade, sendo planejados e executados com periodicidade mínima anual, a partir da data implantação do plano. Os testes PCN estão nos Indicadores e no presente documento, onde constam as descrições, métodos, metas, responsável e periodicidade aplicáveis.

A responsabilidade pelo planejamento, organização e definição dos cenários de teste é da área de TI.

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 devem ser registrados por meio de resultados, prints dos sistemas e fotos e arquivados no sistema PODIO.

O desenvolvimento do 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

Dessa forma, torna-se necessário simular emergências, definir claramente responsabilidades e escopo de atuação de cada colaborador envolvido na execução do PCN.
A manutenção do PCN atualizado e o treinamento contínuo dos colaboradores são considerados fatores críticos de sucesso para a efetividade da continuidade dos negócios.

3.7 MANUTENÇÃO, GOVERNANÇA E ANÁLISE CRÍTICA DO PCN

A continuidade de negócios e a recuperação de desastres resultam da execução e manutenção de um processo contínuo, que envolve planejamento, formalização, monitoramento e melhoria contínua.

O PCN é de responsabilidade da Alta Direção da Fenox, cabendo à área de TI a gestão operacional, manutenção e execução técnica do plano, incluindo a definição do ciclo de revisão e das etapas necessárias para atualização dos cenários de risco, impacto nos negócios e das estruturas e estratégias que o fundamentam.

Para fins de Análise Crítica pela Alta Direção, devem ser considerados, no mínimo:

- Os processos de planejamento de negócios e tecnológico;
- O gerenciamento de mudanças;
- O gerenciamento de riscos;
- O tratamento de problemas e incidentes.

3.8 APROVAÇÃO DA ALTA DIREÇÃO

Este PCN foi analisado, aprovado pela Alta Direção da Fenox Tecnologia, que assegura os recursos necessários para sua implementação, manutenção e melhoria contínua.