Plano de Continuidade de Negócio (PCN)

HOOBOX

FOLHA DE CONTROLE

Informações Gerais

Título	Plano de Continuidade de Negócio
Número de Referência	PLN_CONT_NGC
Número da Versão	V2
Status	Nova
Aprovador	Comitê de Privacidade
Data da Próxima Revisão	1 ano após a data da aprovação

Aprovado pelo Comitê de privacidade em 15 de agosto de 2021

Sumário

Objetivo deste documento

O Plano de Continuidade de Negócios (PCN) da HOOBOX é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorreria de um acidente e/ou desastre, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio da qual ela faz parte. Além disso, sob o ponto de vista do PCN da HOOBOX, o funcionamento da empresa deve-se a duas variáveis: os componentes e os processos. Os componentes são as variáveis utilizadas para a realização dos processos: energia, telecomunicações, informática, infraestrutura e pessoas. Todos os componentes podem ser substituídos ou restaurados, de acordo com características específicas. Os processos são as atividades realizadas para operar os negócios da empresa.
O Plano de Continuidade de Negócios HOOBOX é constituído pelos seguintes planos:

- Plano de Administração de Crises (PAC),
- Plano de Recuperação de Desastres (PRD) e
- Plano de Continuidade Operacional (PCO).

Todos estes planos têm como objetivo principal a formalização de ações a serem tomadas para que, em momentos de crise, a recuperação, a continuidade e a retomada dos negócios possam ser efetivas, evitando que processos críticos de negócio da organização sejam afetados, o que pode, no extremo negativo, acarretar perdas financeiras generalizadas para clientes, colaboradores e sócios.

Quanto às atualizações, o Plano de Continuidade de Negócios da HOOBOX deve ser revisado de anualmente, pois mudanças significativas em componentes, atividades ou processos críticos de negócio podem fazer com que novas estratégias e planos de ação sejam previstos, evitando assim com que eventuais desastres desestabilizem profundamente o andamento regular do negócio da empresa.

1 Plano de Administração de Crises (PAC)

o PAC da HOOBOX relaciona o funcionamento das equipes, antes, durante e depois da ocorrência de um evento negativo a continuidade dos negócios. O PAC exibe uma cadeia de comando e comunicação durante uma crise de qualquer natureza. Também define procedimentos a serem executados, pela mesma equipe responsável à administração de crises, até o período de retorno à normalidade. O PAC da HOOBOX, no seu envolvimento pessoal, para que possa compor de forma adequada e satisfatória, tem nomeado o responsável pelas decisões gerenciais, que serão afetados por uma emergência, e substitutos em caso de ocorrer o evento de crise e o responsável, por algum motivo de força maior, não estiver presente.

Assim, o PAC tem o **Dr. Paulo Gurgel Pinheiro** como responsável, como substituto o **Sr. Cláudio Gurgel Pinheiro**. O PAC será acionado em caso de:

- Roubos, furtos, sabotagem, sequestros, vandalismo e crimes de qualquer natureza
- Queda de energia elétrica
- Perda, roubo ou vazamento de informações computacionais
- Incêndios, explosões, queda de edifícios ou sinistros de qualquer natureza
- Boicotes, greves
- Ausências de capital humano
- Boatos, intrigas ou acusações desonestas e/ou antiéticos de concorrentes
- Crises de mídia eletrônica e/ou impressas
- Extravio de documentos
- Paralisações de setores públicos
- Desastres naturais
- Doenças do tipo contágio/contaminação ou química
- Emergências civis
- Fraudes
- Ações judiciais contra a empresa
- Denúncias da corrupção
- Vazamento de documentos internos
- Sucessão de comando da organização
- Demissão de colaboradores
- Rompimento de contratos com fornecedores
- Falha de equipamentos eletrônicos de qualquer natureza

- Colapso em rede de computadores
- Acidentes de trabalho
- Outros imprevistos que afetem a continuidade dos negócios

Alguns dos fatores citados acima podem afetar a reputação da HOOBOX no mercado em que atua. Para isso, exige-se planejamento de comunicação, mobilização de pessoas chaves, bons mecanismos de relações públicas, como marketing e imprensa, e investigação caso a caso. A gestão da(s) crise(s) do PAC será executada, de acordo com a espécie da crise, com procedimentos listados a seguir:

a) Repassar uma lista a todos os sócios e colaboradores da HOOBOX de quem e onde informar em caso de crise.
b) Coletar o máximo de informações e provas possíveis;
c) Montar um centro de gerenciamento de crise em local próprio e adequado designado pelo responsável;
d) Estratégia para a mídia (com rapidez e planejamento da abordagem);
e) Estratégia para informar os sócios, colaboradores, investidores e fornecedores pelos diversos canais de comunicação existentes (telefones, e-mail, redes de relacionamentos, correspondência, imprensa escrita, mídia visual ou eletrônica);

2 Plano de Continuidade Operacional (PCO)

O PCO da HOOBOX define procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, consequentemente, os impactos potenciais do negócio. Através do PCO, os gestores dos processos de negócios saberão como agir na falha e/ou falta de algum componente que garante a continuidade dos negócios. O Plano de Continuidade Operacional (PCO) consiste em quatro etapas:

I. Planejar: definição de estratégias, políticas internas, controles e procedimentos de rotina para garantir segurança das informações;
II. Executar: os processos definidos são implementados. Coleta de informações são de extrema relevância;
III. Checar: são feitas avaliações de processos implementados para verificar se o planejado foi realmente executado de forma adequada para alcançar as metas. São identificados desvios de execução e apresentados resultados para análise crítica da direção da empresa. Aqui existe um monitoramento contínuo dos processos no intuito de evitar qualquer tipo de falha ou erros;
IV. Agir: são realizadas ações corretivas e preventivas baseadas na identificação de desvios de execução e nas considerações apresentadas nas etapas (I), (II) e (III). A figura abaixo mostra o fluxo do Plano de Continuidade Operacional

Na fase de comunicação do risco, as partes envolvidas e as partes interessadas, pessoa ou grupo que tem interesse no desempenho ou no sucesso da organização, devem ser identificadas e os seus papéis e responsabilidade devem ser definidos. O pano de comunicação entre as partes envolvidas é acionado (telefone, e-mail, correspondência, mensagens instantâneas). Quanto ao contexto, existem inúmeros motivos para preocupações (nomeadas e identificadas no PAC). O papel da identificação dos riscos é identificar junto ao Comitê de Gerenciamento de Crise (PAC) os eventos de cada processo de negócio existente que possam afetar o funcionamento das atividades essenciais e causar perdas potenciais.

Respondem-se perguntas como:
a) O que pode acontecer se isso acontecer?
b) Quando, onde e como pode acontecer?
c) Por que pode acontecer? Identifica-se ameaças operacionais, controles existentes, vulnerabilidades e as consequências operacionais.

O objetivo principal é preservar a confidencialidade, a integridade e a disponibilidade. Quanto ao risco, utilizam-se escalas com atributos (baixa, média, alta). O PCO da HOOBOX se preocupa com todas as escalas. A transferência do risco é compartilhada entre pessoas envolvidas, analisada e avaliada. Na análise, é importante notar se haverá transferência de risco (efeito contágio) ou se não vai gerar novos riscos operacionais (encadeamento). Tendo em vista diversos riscos operacionais existentes, temos o material humano, a segurança da informação e a tecnologia da informação como fatores de extrema relevância para a continuidade das operações. De fato, nomeamos abaixo possíveis fatores de risco operacional:
- Hardware
- Software
- Rede
- Recursos humanos
- Estrutura da Organização

O impacto operacional imediato de um problema numa das estruturas nomeadas acima pode ser direto (baixo, médio, alto) ou indireto (baixo, médio, alto).

Para minimizar riscos operacionais, nomeamos abaixo as principais ameaças e medidas preventivas tomadas para contê-las, assim como os procedimentos que a empresa adota para cada um dos itens citados:

Ameaças em hardware	Impacto	Valor	Ordem de Importância	Procedimento
Quebra estrutural	Direto	Alto	1	Conserto ou aquisição de novo hardware
Obsolescência	Indireto	Médio	2	Aquisição e manutenção

Ameaças em software	Impacto	Valor	Ordem de Importância	Procedimento
Ataques físicos - vírus	Direto	Alto	3	Atualização de antivírus atualizado
Softwares desatualizados	Indireto	Médio	4	Atualização
Senhas vulneráveis	Direto	Alto	2	Trocar senhas padrão, senhas com no mínimo 8 caracteres, incluindo sempre n úmero, letras e especiais
Falta de compatibilidade	Indireto	Médio	5	Aquisição de programas que funcionem em diversas plataformas
Perda de dados	Direto	Alto	1	Back-up semanal de dados sensíveis
Spam	Direto	Médio	5	Utilização de filtros AntiSpam
Internet	Direto	Alto	1	Conexões redundantes
Pessoas não autorizadas	Direto	alto	4	Criar níveis de segurança da rede

Ameaças em Recursos Humanos	Impacto	Valor	Ordem de Importância	Procedimento
Pessoas	Direto	Alto	1	Treinamento e reciclagem
Assuntos confidenciais	Direto	Alto	2	Adoção do Código de Ética e padrões de conduta profissional
Falecimento, invalidez ou afastamento por problemas de saúde	Direto	Alto	3	Redundância
Contratação eventual	Direto	Alto	4	Verificação da veracidade das informações
Boatos, intrigas e acusações desonestas e/ou antiéticas	Direto	Alto	5	Adoção do Código de Ética e padrões de conduta profissional
Roubo, furto, sabotagem,	Direto	Alto	1	Sistema de segurança, controle

sequestros, vandalismo e crimes de qualquer natureza				de entrada e saída, educação e treinamento
Falta de energia e interrupções	Direto	Alto	5	Utilização de nobreaks
Segurança física e do ambiente	Direto	Alto	4	Segregação física de atividades e controle de acesso de pessoas não autorizadas
Documentações	Direto	Alto	2	Controle de acesso a documentos restritos
Extravio de documentos e fraudes	Direto	Alto	3	Boletim de Ocorrência policial, trabalho preventivo com treinamento e processo jurídico

3 Plano de Recuperação de Desastres (PRD)

O PRD da HOOBOX define um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais da operação. O PRD é composto por procedimentos para recuperação de ativos, quando ocorrer uma falha devido a alguma inconsistência ocorrida em virtude de ameaças como incêndio, enchente, vandalismo, sabotagem ou falhas de tecnologia.

Desastres	**Impacto**	**Valor**	**Ordem de Importância**	**Procedimento**
Incêndio	Direto	Alto	2	Acionar corpo de Bombeiros
Explosões	Direto	Alto	3	Acionar corpo de Bombeiros
Queda de edifício	Direto	Alto	1	Acionar corpo de Bombeiros
Desastres naturais	Direto	Alto	4	Defesa Civil

Nos itens listados acima, a preocupação será primeiramente com as pessoas e, em seguida, com o salvamento de bens materiais. Dado que grande parte dos procedimentos da empresa são feitos eletronicamente e com sistemas de informação, um desastre de grande magnitude no local físico, que realmente destruiria 100% de materiais, documentos e bens de qualquer natureza, certamente não impactaria no processo de continuidade dos negócios porque

existem condições técnicas, principalmente, de segurança em TI que permite-nos dar continuidade aos negócios em outra localização.

4 Procedimento do Plano de Continuidade para COVID-19

Na perspectiva de viabilizar a observância dos padrões de segurança, em caso de pandemia como a COVID-19, a HOOBOX implementa protocolos relativos à continuidade dos trabalhos:

4.1. Avaliação para ampliação do regime home-office mais amplamente

Atualmente, a empresa aplica mesmo sem pandemia o regime de home-office com todos os seus colaboradores, em níveis de carga diferentes. Dependendo do grau de pandemia e estágio, o regime pode variar para 100% da equipe e 100% da carga de trabalho.

Ampliação do regime home-office exige reserva de fundo da empresa para custear equipamentos necessários para os colaboradores realizarem as suas atividades com empenho, a ser avaliado no ato da crise. Para referência, durante a COVID-19, foram alocados 10% do salário mensal do colaborador, pago uma única vez para a compra desses equipamentos. O uso da verba deve ser solicitado pelo colaborador com justificativa.

- Priorizar as ferramentas de comunicação aberta
- Certificar que todos recebam a informação
- Avaliar a ampliação das reuniões de sprints
- Implementação do “buddy virtual” para acompanhamento das novas contratações com bônus de 1 dia de folga para cada contratado e taxa de sucesso para cada um que complete 6 meses de casa.
- Implementação do programa de bônus para contratação por indicação para manutenção do plano de expansão da empresa.

4.2. Protocolos para regime presencial

Na perspectiva de viabilizar a observância dos padrões de segurança, em caso de pandemia, são estipulados protocolos gerais para estações de trabalho, alimentação.

- Manter distanciamento recomentado nas estações de trabalho de 2m entre eles.
- Manter a circulação de ar no ambiente, sem fechamento simultâneo de portas e janelas ou de aparelhos de ar-condicionado.
- Manter a limpeza do ambiente, disponibilizando álcool em gel, adequando a rotina de limpeza ao grau da pandemia e as sugestões dos órgãos competentes.
- Máscaras
    - Utilizar máscara
    - Trocar a cada 2 horas ou quando úmida

- As máscaras devem ser descartadas de maneira adequada
- Não retirar a máscara para falar

4.3. Procedimento caso o colaborador esteja com algum sintoma da doença

- Não vá a HOOBOX, pelo menos 14 dias, independentemente do tipo de vínculo que você tenha e avise sua diretoria imediata.
- Em casos de sintomas respiratórios mais graves, procure uma unidade de saúde mais próxima à sua residência.

5 Procedimento do Plano de Continuidade para ataques cibernéticos

5.1. Ataque de Navegação de Serviço Contra a Infraestrutura do Provedor

Probabilidade: Média
Impacto: Médio
Risco: Médio

Procedimento:

- Ativar o Plano de Recuperação de Desastre (DR), alteração de DNS externo, alterações em Servidores WEB, Servidores RDS, APP, Alterações no Servidor de Arquivos, Validação do sistema.

5.2. Ataque de Negação de Serviço Contra um Ativo Específico

Probabilidade: Alta
Impacto: Médio
Risco: Alto

Procedimento:

- Ativar o Plano de Recuperação de Desastre (DR), alteração de DNS externo, alterações em Servidores WEB, Servidores RDS, APP, Alterações no Servidor de Arquivos, Validação do sistema.

5.3. Destruição de Ativos em Nuvem

Probabilidade: Médio
Impacto: Alto
Risco: Alto

Procedimento:

- Realizar restauração do backup do ativo destruído na AWS

- Ativar o Plano de Recuperação de Desastre (DR), alteração de DNS externo, alterações em Servidores WEB, Servidores RDS, APP, Alterações no Servidor de Arquivos, Validação do sistema.

5.4. Paralização Parcial da Infraestrutura do Provedor de Nuvem

Probabilidade: Baixa
Impacto: Baixo
Risco: Muito Baixo

Procedimento:

- Ativar servidores e serviços de contingência.
- Ativar o Plano de Recuperação de Desastre (DR), alteração de DNS externo, alterações em Servidores WEB, Servidores RDS, APP, Alterações no Servidor de Arquivos, Validação do sistema.

5.5. Interrupção de Suprimento de Energia

Probabilidade: Alta
Impacto: Baixo
Risco: Médio

Procedimento:
Ativar gerador de energia.

5.6. Saturação de Sistema

Probabilidade: Baixa
Impacto: Baixo
Risco: Muito Baixa

Procedimento:

- Ativar o Plano de Recuperação de Desastre (DR), alteração de DNS externo, alterações em Servidores WEB, Servidores RDS, APP, Alterações no Servidor de Arquivos, Validação do sistema.

5.7. Ataques de Ransonware

Probabilidade: Alto
Impacto: Alto
Risco: Crítico

Procedimento:

- Realizar restauração do backup do ativo destruído na AWS
- Ativar o Plano de Recuperação de Desastre (DR), alteração de DNS externo, alterações em Servidores WEB, Servidores RDS, APP, Alterações no Servidor de Arquivos, Validação do sistema.

5.8. Perda da Sede Principal da Instituição

Probabilidade: Baixa
Impacto: Médio
Risco: Baixo

Procedimento:

- Preparação da sede alternativa
- Utilizar backup dos arquivos do servidor de arquivo em nuvem
- Realizar conexão de VPN direta ao provedor de nuvem para acesso aos ativos.