PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

Sumário

O Plano de Continuidade de Negócios (PCN) da Inva Capital 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 Inva Capital, 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, infra-estrutura 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 da Inva Capital 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 em perdas financeiras generalizadas para clientes, colaboradores e sócios.

Quanto às atualizações, o Plano de Continuidade de Negócios da Inva Capital 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.

Propósito do Plano de Continuidade de Negócios (PCN) Inva Capital

O propósito do Plano de Continuidade de Negócios da Inva Capital é permitir que a organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios.

Os propósitos do PCN da Inva Capital são ativados para dar suporte às atividades críticas necessárias para cumprir os objetivos da organização. Inclusive, o PCN da Inva Capital pode ser executado integralmente no caso de um desastre extremo ou parcialmente no caso de um desastre menos agudo e também em qualquer etapa da resposta a um incidente de qualquer magnitude.

O PCN da Inva Capital é um processo contínuo com melhorias rotineiras no qual a instituição identifica e analisa impactos nos negócios e perdas potenciais; garante a continuidade dos negócios, serviços e operações; contém detalhadamente as atividades, procedimentos, responsabilidade e necessidades de recursos no momento de eventual interrupção transitória; garante que informações sobre o PCN da Inva Capital estejam sempre atualizadas e acessíveis, física e eletronicamente; atenta para alterações na legislação vigente que garanta a comunicação às pessoas da Inva Capital responsáveis pela sua manutenção; permite que pessoas da Inva Capital estejam preparadas para comunicações externas em caso de desastres de qualquer natureza; informa as pessoas da Inva Capital sobre a política do PCN e incentiva a participação em treinamentos do PCN da Inva Capital. Define responsabilidade de atuação de cada funcionário, na execução do PCN da Inva Capital; analisa periodicamente a documentação existente para suportar períodos de restaurações em situação de desastre; mantém uma lista de contatos atualizada (de fornecedores, clientes, utilidade pública), simula situações emergenciais, prepara ações necessárias à recuperação e proteção de documentos digitais referentes à área de tecnologia da informação.

O conteúdo e os componentes do PCN da Inva Capital possuem diferentes níveis de detalhamentos, sendo composto pelos seguintes elementos (descritos nas próximas subseções): Plano de Administração de Crises (PAC), Plano de Recuperação de Desastres (PRD) e Plano de Continuidade Operacional (PCO). Todos os planos são testados periodicamente e envolvem basicamente quatro infra-estruturas:

I. pessoas e suas responsabilidades
II. física (local e recursos)
III. tecnológica (software e hardware)
IV. serviços externos (essenciais ao processo)

Plano de Administração de Crises (PAC)

O PAC da Inva Capital relaciona o funcionamento das equipes, antes, durante e depois da ocorrência de um evento negativo a continuidade dos negócios da Inva Capital. 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 Inva Capital, 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 a Sra. Roberta Análio como responsável, como substituto o Sr. Raphael Alves Rodrigues Cordeiro e como segundo substituto o Sr. Luiz Augusto Baasch Pacheco.

O PAC Inva Capital 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 anti-éticos 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 Inva Capital 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 à todos os sócios e colaboradores da Inva Capital de quem e onde informar em caso de crise (ver Lista de Contatos e Telefones Úteis);

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);

f) O porta voz oficial da Inva Capital para comunicar qualquer tipo de crise é o Sr. Raphael Alves Rodrigues Cordeiro. Na sua ausência, o substituto é o Sr. Luiz Augusto Baasch Pacheco. Na sua ausência, a substituta é a Sra. Roberta Análio. Este procedimento é adotado porque acreditamos que todas as informações sobre um determinado problema devam ser transmitidas à imprensa, colaboradores, investidores e a quem interessar possa apenas por uma única pessoa. No caso de detalhamento técnico, o porta-voz é assessorado por uma das pessoas que fazem parte do comitê de gerenciamento de crise. Desta maneira, a organização evita que informações incorretas ou desencontradas sejam repassadas para a mídia. Falhas na comunicação durante o processo de crise podem gerar novas crises.

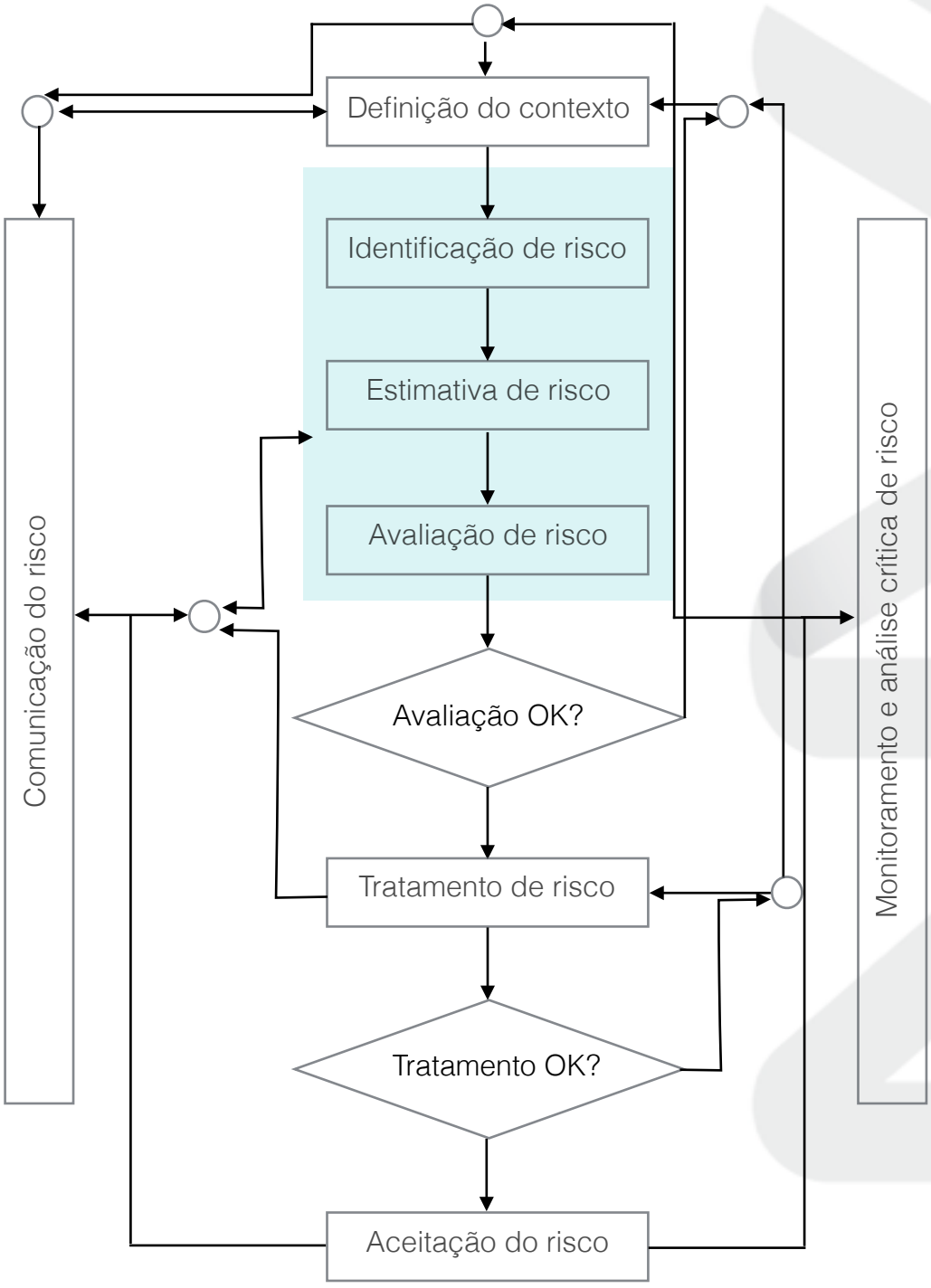
Plano de Continuidade Operacional (PCO)

O PCO da Inva Capital define procedimentos para contingenciamento dos ativos que suportam cada processo de negocio, 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.


Definição do contexto
Identificação de risco
Estimativa de risco
Avaliação de risco
Avaliação OK?
Tratamento de risco
Tratamento OK?
Aceitação do risco
Comunicação do risco
Monitoramento e análise crítica de risco

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 Inva Capital 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 transferencia 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 e reserva de lucro para tal finalidade
Obsolecência	Indireto	Médio	2	Aquisição e manutenção de reserva de lucro para tal finalidade

Ameaças em software	Impacto	Valor	Ordem de importância	Procedimento
Ataques físicos - vírus	Direto	Alto	3	Utilização de anti-vírus atualizado
Softwares desatualizados	Indireto	Médio	4	Atualização
Senhas vulneráveis	Direto	Alto	2	Trocar senhas padrão, senhas com no mínimo 8 caracteres, incluindo sempre números, letras e caracteres especiais
Falta de compatibilidade	Indireto	Médio	5	Aquisição de programas que funcionam em diversas plataformas (Windows e MacOS)
Perda de dados	Direto	Alto	1	Back-up semanal de dados sensíveis
Spam	Direto	Médio	5	Utilização de filtros anti-spam
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, conscientização 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 anti-éticos	Direto	Alto	5	Adoção do Código de Ética, padrões de conduta profissional e, em último caso, processo jurídico
Roubo, furto, sabotagem, sequestros, vandalismo e crimes de qualquer natureza	Direto	Alto	1	Sistema de segurança, controle de entrada e saída, educação e treinamento
Falta de energia e interrupções	Direto	Alto	5	Utilização de no-breaks
Segurança física e do ambiente	Direto	Alto	4	Segregação física de atividades e controle de acesso a 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 treinamentos e processo jurídico

Plano de Recuperação de Desastres (PRD)

O PRD da Inva Capital 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
Incêndios	Direto	Alto	2	Acionar corpo de Bombeiros
Explosões	Direto	Alto	3	Acionar Síndico e corpo de Bombeiros
Queda de edifício	Direto	Alto	1	Acionar corpo de Bombeiros
Desastres naturais	Direto	Alto	4	Defesa Civil

Nos items 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.