Data da Atualização	Responsável	Versão
21.12.2024	Diretor de Compliance e PLD	5

CONTEA CAPITAL

PLANO DE CONTINUIDADE DE NEGÓCIOS

Data da Atualização	Responsável	Versão
21.12.2024	Diretor de Compliance e PLD	5

I. Sumário Executivo

Este Plano de Continuidade de Negócios (PCN) refere-se a um conjunto de estratégias e planos de ação preventivos que garantem o pleno funcionamento dos serviços essenciais da Contea Capital durante quaisquer tipos de falhas, até que a situação seja normalizada, garantindo sua perenidade e sobrevivência diante de circunstâncias inesperadas.

Processos Vitais:		
- Execução de ordens	- Liquidação de operações	
- PLD e KYC	- Gerenciamento de riscos, limites e concentração	
Diretor de Contingência:	Paulo Marins	+55 11 98815-2939
1º Líder de Contingência:	Cristiano Pardi	+55 11 98278-1174
2º Líder de Contingência:	Bruna Veiga	+55 21 99805-2859

II. Premissas e Objetivos do Projeto

O Plano de Continuidade de Negócios (PCN) assegurará à Contea Capital 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 Contea Capital 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), sendo:

• **Plano de Administração de Crises** (PAC): define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência.

É acionado após decretada a Crise e é voltado para todo o processo. Tem seu término quando se volta à normalidade;

• **Plano de Continuidade Operacional** (PCO): seu objetivo é reestabelecer o funcionamento

dos principais processos que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente;

• **Plano de Recuperação de Desastres** (PRD): É acionado junto com o PCO e é focado na recuperação e restauração de componentes que suportam o PCN.

O desenvolvimento do Plano de Continuidade de Negócios tem como base a análise dos processos críticos estabelecidos pela administração compreendendo três pilares essenciais de um PCN:

Análise de riscos de TI: o que de ruim pode vir a acontecer? (principais ameaças)

Análise de impacto nos negócios (Business Impact Analysis-BIA): de que forma eventuais ameaças podem impactar o negócio?

Estratégia de recuperação: perante uma ameaça, quais atitudes e ações se fariam necessárias para a retomada das operações?

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.

II.Site Principal e Site de Redundância

A Contea Capital conta com a "Site Principal" situada na Avenida Brigadeiro Faria Lima, 2369 - 4º Andar, conjuntos 2008-2015, onde a administração de carteiras de valores mobiliários é executada em condições normais e dois sites de redundância.

As unidades de redundância contêm exatamente os mesmos recursos tecnológicos da Unidade Principal, podendo cada estação de trabalho utilizar qualquer uma das unidades.

O servidor de dados da Contea Capital está armazenado no serviço de nuvem da Microsoft, portanto todos os arquivos podem ser acessados na íntegra.

Em situações de contingência, os funcionários designados devem se dirigir para o Site de Redundância de forma que haja o mínimo impacto possível dentro das atividades da Contea

Capital.

III. Plano de Monitoração e Declaração de Desastre

Será considerado desastre quando o tempo total de recuperação dos processos for superior ao tempo máximo apontado no item "V - Processos e Sistemas Críticos".

Qualquer colaborador da Contea Capital, ao constatar alguma anormalidade que paralise quaisquer processos apontados no item "V" deste Plano deverá comunicar o fato ao seu superior imediato, este por sua vez comunicará o fato à equipe contingência.

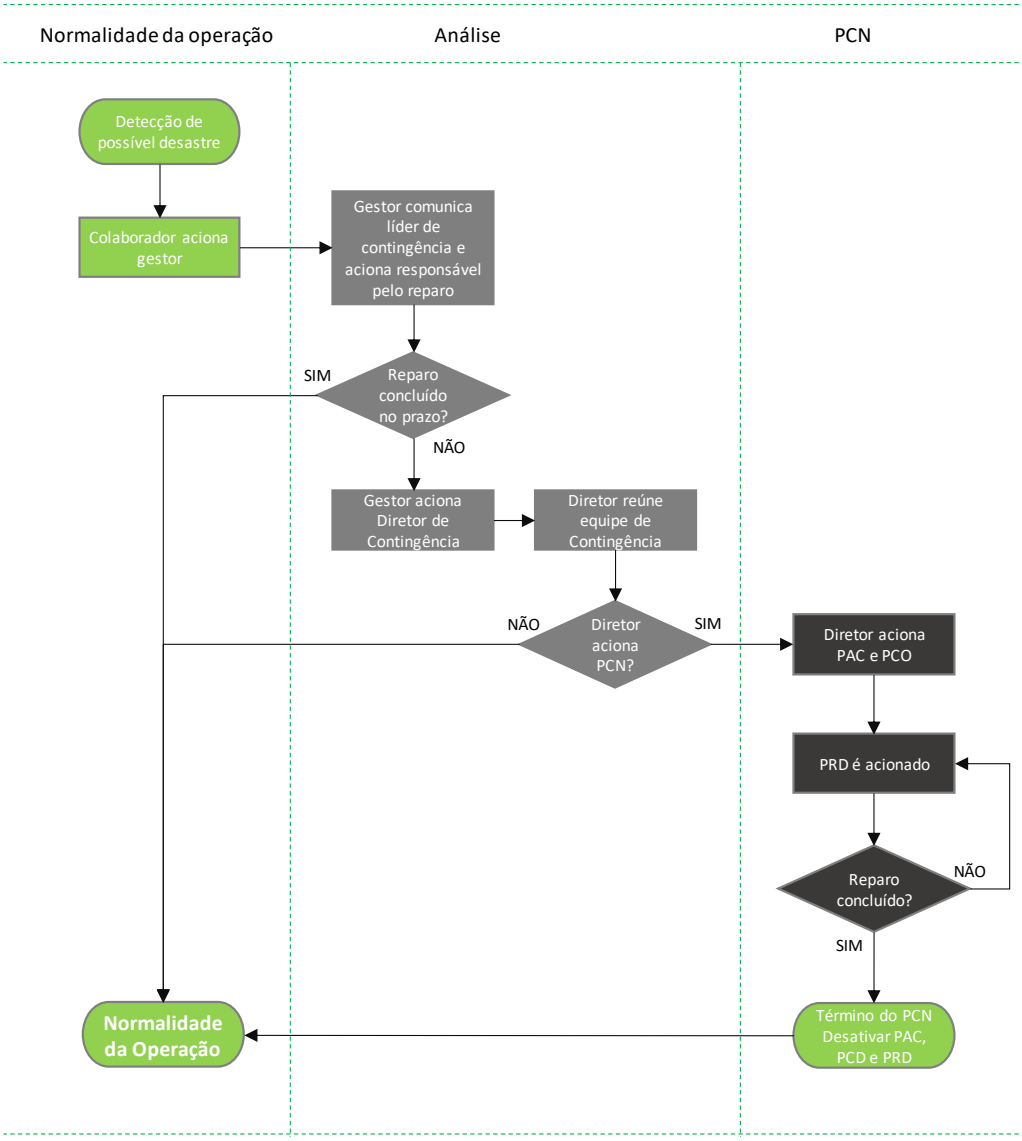
Ao ocorrer quaisquer eventos que paralise algum processo essencial ao negócio, o líder de Contingência avaliará a ocorrência e comunicará ao Diretor responsável pelo PCN.

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.

IV. Fluxograma

Na figura abaixo está descrito o Fluxo de Acionamento do PCN que resultará ou não na declaração da contingência.

Data da Atualização	Responsável	Versão
21.12.2024	Diretor de Compliance e PLD	5



V. Processos e Sistemas Críticos

Processo crítico pode ser 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 pela fórmula (MTD = RTO + WRT).

Definição:

• MTD (Maximum Tolerable Downtime) = Trata-se do tempo máximo que um negócio pode tolerar a ausência ou indisponibilidade de uma função de negócio em particular. Diferentes funções de negócio poderão ter diferentes MTD's.

• RTO (Recovery Time Objective) = Tempo para recuperar hardware, software e configurações de sistemas e recursos após uma ruptura.

• WRT (Work Recovery Time) = Tempo que leva para colocar em produção após o RTO.

Processos e definições de MTD

Área	Processo	MTD
Gestão	Executar ordens	60 Min até às 14h Imediato após às 14:00h
Operações (Back Office)	Liquidar operações Internet banking	60 Min até às 14h Imediato após às 14:00h
Compliance & Risco	PLD KYC Gerenciamento de riscos, limites e concentração	60 Min até às 14h Imediato após às 14:00h

VI. Abrangências

No entendimento dos gestores das áreas avaliadas as ameaças com grau de vulnerabilidade

significante estão divididas em:

(i) Humanas: Greves, Distúrbio Civil, Falha de Prestador de Serviços/Parceiro, Acesso Indevido às Instalações e Erro Humano não intencional.

(ii) Tecnológicas: Falha em Aplicativo (SW), Falha em Hardware (HW), Falha em sistemas Operacionais, Vírus de Computador, Falha em Rede Interna (LAN), Falha na Entrada de Dados, Falha em Rede Externa (WAN), Falha de Telecom – Dados e Falha em Sistema de Acesso.

(iii) Infraestrutura: Falha em Telecom - Voz, Falha em Sistema de Refrigeração, Interrupção de Energia Elétrica, Falha em Instalações Elétricas.

(iv) Naturais: Alagamento Interno do Ambiente, Queda de Raios, Vendaval e Incêndio.

(v) Físicas: Problema Estrutural ou de Instalações e Rompimento de Tubulação Interna (água, esgoto e gás).

Cabe ressaltar que paradas não programadas podem resultar em perdas tangíveis e intangíveis aos negócios da Contea Capital, acarretando perda de confiança de colaboradores e clientes nos processos de negócios. Desta forma, os potenciais impactos apontados pelos gestores numa eventual interrupção no negócio são:

(i) Interrupção de prestação de serviços a clientes;

(ii) Multas e sanções;

(iii) Perda da capacidade de gestão e controle;

(iv) Comprometimento da imagem da organização;

(v) Exposição negativa na mídia e perda de vantagem competitiva.

VII. Ações e Procedimentos

Qualquer colaborador deverá estar apto a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente a equipe do Plano de Continuidade de Negócios.

Dentre as ameaças que impossibilitam o acesso ao prédio destacamos:

(i) Princípio de Incêndio;

(ii) Ameaça de Bomba;

(iii) Bloqueios;

(iv) Manifestações.

Ações de 05 a 10 minutos após a evidência

Responsável: Líder do PCN

Procedimentos: Entrar em contato com a Administração do Imóvel para esclarecimentos e caso necessário, contatar também os órgãos públicos:

Administração do imóvel: Sociedade Administradora Agrícola Comercial São Francisco SAGRISA

Tel.: (11) 3815-9699

email: contato.sjudith@gmail.com

Zelador Edifício Barão de Iguatemi: Sr. José (11) 3032-3170

Bombeiros: 193 (Incêndio e Ameaça de Bomba);

Defesa Civil: 199 (Ameaça de Bomba, Greves, Bloqueios e Inundações);

Polícia Civil: 147 (Ameaça de Bomba, Roubo e Furto de Informações e ativos).

Ações em até 20 minutos após a conclusão da etapa anterior

Responsável: Líder do PCN

Procedimentos: Entrar em contato com o responsável pelo site de contingência, para avisá-lo sobre a ocupação dos integrantes das áreas contingenciadas e disponibilizar local, notebook e impressora, assim como acesso à Internet.

Avisar aos integrantes das áreas contingenciadas para que se dirijam ao endereço do site de contingência, conforme relação indicada abaixo:

Área contingenciada	Nome	Contato
Investimentos	Cristiano Pardi	+551198278-1174

Operações	Rafael Silva	+5511 99209-8681
Compliance e Risco	Paulo Marins	+5511 98815-2939
	Bruna Veiga	+5521 99805-2859
Análise de Crédito	Fabiola Freitas	+5511 98193-1981
TI	Rafael Silva – Internet	+5511 99209-8681
	Rafael Silva – SW e HW	+5511 99209-8681

Disponibilizar alertas no site da Contea Capital indicando o status de contingência, telefones dos colaboradores e telefone fixo do site backup para atendimento.

Para não haver interrupções nas atividades o ambiente de TI foi totalmente estruturado sobre a plataforma de Cloud Solution da Microsoft, permitindo o acesso imediato de todos os dados em qualquer site de contingência.

Os e-mails utilizam a plataforma Microsoft exchange, com redundância de arquivos entre computadores locais e servidor exchange Microsoft.

Na sede e nos dois sites de contingência a conexão com a internet é feita por links redundantes.

O Sistema de Telefonia é 100% Voip o que possibilita o rápido redirecionamento de todas as chamadas de todos os ramais para números externos, sendo fixo no site de contingência ou celulares dos colaboradores responsáveis pelas atividades. Adicionalmente, 100% dessas

ligações são gravadas em servidor externo da empresa IUNGO, maior provedor de PABX em nuvem da América Latina.

Na falta de energia elétrica, além das baterias próprias dos Notebooks, são ativados automaticamente os nobreaks localizados no site principal no CPD com autonomia de 2 horas.

VIII. Acionamento da Contingência externa

Responsável: Líder do PCN

Procedimentos: Manter contato com o gestor do site de contingência primário e secundário, decidir sobre a utilização de qual site e avisar do início do processo de contingência.

As equipes irão para o lugar destinado a cada uma delas.

Manter contato com a empresa IUNGO PABX, tel.: 0800 878-8136 ou (11) 2690-4701 e solicitar o encaminhamento de todas as ligações para os ramais do escritório do Site de Contingência ou celulares dos colaboradores, se for o caso.

VIII. Procedimentos de retorno à normalidade – Site Principal

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

Quando o acesso ao prédio estiver liberado e em condições de normalidade, comunicar a todos os colaboradores da Contea Capital 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 Contea Capital sobre a situação de contingência.

IX. Administração do Plano

A eficiência do PCN na organização é o resultado da elaboração e manutenção de um processo contínuo que envolve planejamento, formalização, monitoração e melhorias.

O PCN é de responsabilidade e gestão da área Riscos e Compliance, 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 Contea Capital.

Para que a área de TI possa verificar o grau de atualização do PCN e decidir quanto ao momento de sua atualização, os processos de planejamento de negócios, gerenciamento de riscos, tratamento de problemas e de incidentes devem prever a participação desta área nas decisões relevantes destes processos.

Um dos fatores primordiais para o funcionamento deste plano é 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 PCN.

Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, a equipe da Contea Capital definiu que serão realizadas anualmente sessões de divulgação a todos os colaboradores e envolvidos no planejamento de continuidade de negócios.

Estas sessões serão organizadas pela área de Riscos e Compliance, em conjunto com a área de TI, 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.

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

O programa de treinamento deverá contemplar os riscos, ameaças, controles, responsabilidades, premissas e as estratégias do PCN, incluindo as alterações recentes.

X.Realização de Testes

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN e deverão ser planejados e executados com periodicidade mínima anual a partir da data da sua implantação.

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da responsabilidade da área de Riscos & Compliance com TI.

Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela alta administração, que deve 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 Contea Capital 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 de ocorrência.