Cingo

PCN

Plano de Continuidade de Negócios

Versão 1.0

Dez/2021

Sobre este documento...

O Plano de Continuidade de Negócios (“PCN”), estabelecido pela norma ABNT NBR 15999 Parte 1, é o desenvolvimento preventivo de um conjunto de estratégias e ações para garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre.

Para a elaboração deste plano foi efetuada a análise dos riscos potenciais, o detalhamento dos procedimentos de ativação, o estabelecimento de prazos para implementação, a designação dos responsáveis pela operacionalização do referido plano, além testes e/ou validações a serem realizados no mínimo a cada doze meses.

A validação e/ou testes mencionados, têm como objetivo avaliar se o PCN desenvolvido é capaz de suportar satisfatoriamente os processos operacionais críticos para a continuidade das atividades da companhia e manter a integridade, a segurança e a consistência dos dados criados pela alternativa adotada, e se tal plano pode ser ativado em qualquer tempo, cumprindo assim sua função e eficácia.

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

OBJETIVO

O PCN tem como objetivo manter o nível de funcionamento adequado das atividades fundamentais da CINGO diante da ocorrência de quaisquer incidentes que possam colocar em risco sua operação normal.

Este plano irá assegurar à CINGO a continuidade de seus negócios em caso de paralisação, decorrente de sinistro, de um ou mais processos considerados críticos, processos estes que 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;
- PCO (Plano de Continuidade Operacional): são acionados os primeiros procedimentos do PAC, e é voltado aos processos de negócio;
- PRD (Plano de Recuperação de desastres): é acionado junto com o PCO, e é focado na recuperação ou restauração de componentes que suportam o PCN.

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

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

- Análise de riscos de TI;
- Análise de Impacto nos Negócios;
- Estratégia de recuperação.

Desta forma será necessário simular situações de 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 para garantir a redução e controle de eventuais perdas com contingências.

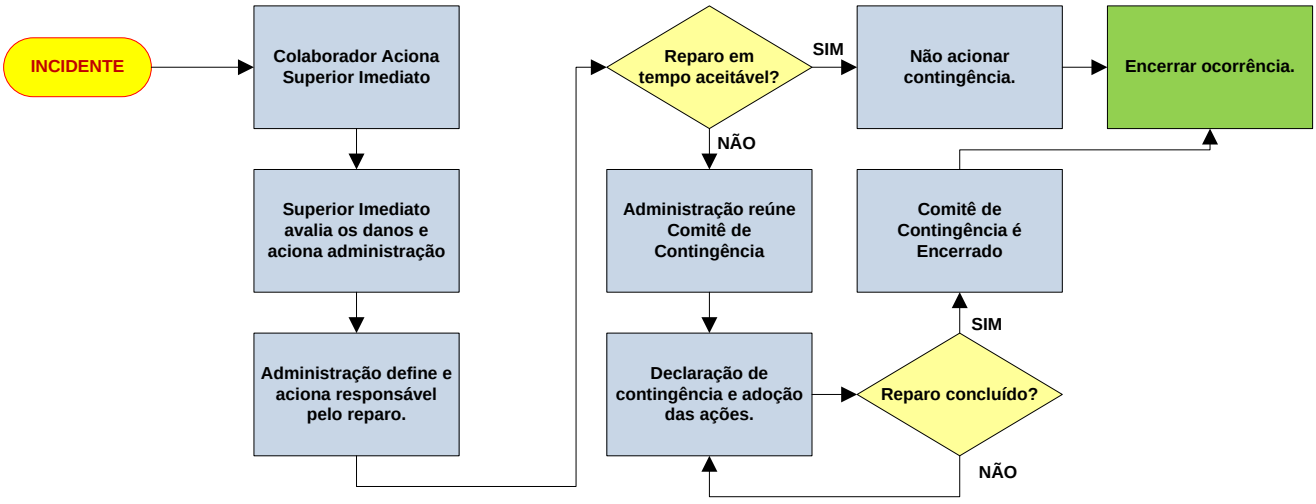
Este PCN será revisado anualmente, porém poderão ocorrer outras revisões sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

ANÁLISE DE RISCOS POTENCIAIS

Os Processos Essenciais são aqueles definidos como um processo de trabalho que uma vez paralisado irá afetar sensivelmente as operações e serviços da organização gerando maior impacto nos clientes internos e externos.

Ao ocorrer quaisquer eventos que paralise algum processo essencial deverá ser aplicado o Processo de Acionamento, conforme imagem apresentada abaixo, que, com base nas informações recebidas e avaliação do grau de impacto irá ou não declarar a contingência.



A CINGO identificou que os principais riscos que possam comprometer sua operação podem ser divididos em 3 grupos:

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

- **Risco de Pessoal**

  O Risco de Pessoal envolve qualquer evento que impossibilite um ou mais colaboradores de exercer sua rotina normal de trabalho. Isso pode ser ocasionado por doenças, acidentes, afastamento por atividades suspeitas, tragédias, entre outros.

- **Risco de Informação**

  O Risco de Informação diz respeito às informações essenciais armazenadas pela empresa. Documentos, ferramentas informatizadas ou sistemas computacionais de uso contínuo estão sujeitos a serem danificadas ou excluídas devido à negligência, imprudência ou má intenção de colaboradores / agentes externos, e danos físicos na infraestrutura de TI.

- **Risco de Infraestrutura**

  O Risco de Infraestrutura envolve qualquer incidente relacionado à estrutura física do escritório. Tais eventos podem ser causados por incêndio, danos elétricos ou hidráulicos, catástrofes naturais e terrorismo. Importante salientar que os sistemas fornecidos pela Cingo a seus clientes se encontram armazenados em nuvem e desvinculados da infraestrutura interna.

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

PLANO DE CONTINGÊNCIA

Adotamos como cenário de contingência as ações necessárias a eliminar ameaças que possam levar a paralisação dos negócios, a interrupção de algum processo essencial ou venha a causar a indisponibilidade total das instalações da empresa.

Deliberado o acionamento do PCN, todos os colaboradores serão notificados de forma verbal (se presentes fisicamente), via e-mail ou por contato telefônico.

Dependendo da gravidade da situação e após deliberação do Comitê de Contingência, a administração deverá informar também os parceiros e órgãos reguladores sobre a situação.

Abaixo as ações e procedimentos que foram elaborados para garantir a mitigação de possíveis prejuízos ou efeitos negativos:

- Comunicação Ativa

  A Área Administrativa entrará em contato com a Administração do Condomínio para relato da ameaça e esclarecimentos, através dos seguintes contatos:

  - Celso Medeiros: (47) 99984-4381
  - Indianara: (47) 99951-3014

Adicionalmente os seguintes serviços públicos também serão acionados caso necessário:

- Bombeiros: 193 (incêndio e ameaça de bomba);
- Defesa Civil: 199 (ameaça de bomba, greves, bloqueios e inundações);
- Polícia: 190 (Militar) e 197 (Civil) (ameaça de bomba, roubo e furto de informações e ativos)
- SAMU: 192 (acidentes e risco à saúde)

De acordo com os serviços que sejam afetados e o tempo previsto de indisponibilidade serão também disponibilizados alertas no website corporativo com indicação da contingência e os telefones alternativos para atendimento.

- NoBreak

A CINGO possui sistema de NoBreak ativo, que garante a utilização de energia elétrica em caso de interrupção no fornecimento pela distribuidora, mantendo os servidores e equipamentos de comunicação funcionando durante um blecaute.

- Acesso Remoto

Em caso de impedimento da presença física do Colaborador no escritório ou caso a estrutura do escritório esteja severamente

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

comprometida, os mesmos poderão realizar acesso remoto à rede, servidores e/ou sistemas através seguintes formas:

- Team Viewer: permite que o Colaborador acesse seu computador corporativo remotamente através de outro computador, bastando que a máquina principal (localizada no escritório) esteja ligada;

- Virtual Private Network (VPN): permite o acesso ao servidor via VPN, onde a comunicação entre ambos os computadores é criptografada, garantindo-se a segurança na troca de informações.

- **Sistema de Detecção e Alarme de Incêndio**

  O prédio onde se situa o escritório possui sistema de detecção e alarme de incêndio, assim em conformidade com as normas NBR 17 240 e NBR 7 240 de segurança.

- **Sistema de Detecção, Alarme e Monitoramento de Invasão**

  O escritório possui sistema de detecção, alarme e monitoramento para casos de invasão, disponibilizando proteção integral 24 x 7 em tempo real, fornecimento de imagens e comunicação autônoma com polícia ou bombeiros, de acordo com a situação de emergência.

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

RETORNO À NORMALIDADE

O retorno à normalidade nos cenários de indisponibilidade ocorre mediante verificação do Comitê de Contingência se o acesso está liberado e em condições confortáveis para o trabalho.

O departamento de TI será responsável por revisar se os principais serviços estão funcionando a nível de desempenho aceitável.

Caso necessário deverão ser realizados processos de planejamento e implementação de procedimentos para reparo, com por exemplo realocação, compra ou aluguel de ativos da instituição; recuperação de servidores eventualmente indisponíveis ou migração para um novo datacenter; e busca por um novo local para as atividades da instituição, caso o escritório principal não possa ser recuperado.

Os prazos para a implementação e conclusão destes procedimentos serão deliberados pelo Comitê de Contingência, conforme as medidas planejadas para o restabelecimento da normalidade.

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

TESTES E VALIDAÇÃO

Os testes de contingência 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 é da Administração em conjunto com a área de Tecnologia da Informação, tendo como objetivo a realização dos seguintes cenários:

- Teste de Acionamento – Call Tree

  O objetivo deste teste é garantir que todos os colaboradores sejam avisados em caso de acionamento do Plano de Contingência. Call Tree é um modelo de comunicação em camadas em que cada pessoa também é responsável por informar outras pessoas, figurando assim uma árvore de chamada.

- Teste de Validação das Ferramentas de Contingência

  O objetivo deste teste é verificar a confiabilidade das ferramentas que possam ser utilizadas em caso de contingência. Os sistemas de NoBreak e Acesso Remoto são periodicamente utilizados para ratificação de sua correta funcionalidade.

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

- **Teste de Escape**

  O teste de escape consiste na simulação de eventuais emergências que possam ocorrer no prédio onde se situa o escritório, tais como incêndio, catástrofes naturais e terrorismo, sendo conduzido pelo próprio condomínio.

Os cenários e seus devidos resultados devem ser analisados para que sejam observadas possíveis fragilidades que possam colocar em risco a continuidade do negócio, onde ao final serão devidamente registrados em documento formal, que deverá ser mantido por um período mínimo de 2 (dois) anos.

Os testes não deverão provocar quaisquer tipos de indisponibilidades ou paradas nos ambientes e/ou operação da companhia 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.

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

Evolução Contínua

Na Cingo buscamos incessantemente conceber e disponibilizar produtos cada vez mais relevantes e atrativos, cenário este onde a necessidade de romper modelos tradicionais, práticas ultrapassadas e procedimentos pouco eficientes, nos fomentam diariamente na constante ampliação do pensamento criativo e busca por mudanças e inovações.

Estar atento às necessidades de nossos clientes sempre foi, e continuará sendo, uma rica fonte de inspiração para nós, ajudando no direcionamento, priorização e evolução de nossos produtos e serviços.

Desta forma reforçamos aos nossos clientes a importância de, sempre que identificar uma oportunidade de melhoria ou sugestão de funcionalidade, fazer o registro da mesma através de nosso sistema eletrônico de atendimento (http://suporte.cingo.com.br). Maiores informações estão disponíveis no Guia de Suporte.

contato@cingo.com.br 47 3034.0101 www.cingo.com.br

Cingo

www.Cingo.com.br

contato@cingo.com.br