IDGR | INVESTIMENTOS ALTERNATIVOS ID | ADMINISTRAÇÃO FIDUCIÁRIA

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

JUNHO 2019

PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS - INTRODUÇÃO

Este Plano de Contingência e Continuidade de Negócios (**PCCN**) objetiva prover a IDGR de um conjunto de planos de ações que suportem o gerenciamento de situações de contingência provocada por incidentes causadores de interrupção no andamento normal de suas atividades, garantindo as condições mínimas necessárias para a continuidade e normalização das mesmas.

As etapas abrangidas pelo **PCCN** são representadas abaixo:
O **PCCN** está dividido em partes, a saber:
• Conceituação;
• Recomendações de Ações Preventivas;
• Planos de Contingência para Incidentes de Impacto Global na Empresa; e
• Monitoramento do **PCCN** e Melhorias.

Em "Conceituação", o principal objetivo é familiarizar os colaboradores da **IDGR** com os termos utilizados em projetos de contingência e continuidade de negócios, nivelando o conhecimento e facilitando o entendimento do conteúdo deste **PCCN**.

A "Relação do **PCCN** com o Planejamento Estratégico da IDGR" evidencia a importância do **PCCN** no alcance dos objetivos estratégicos da empresa.

As **Recomendações de Medidas Preventivas** estão diretamente relacionadas às providências para mitigação de risco na ocorrência de algum incidente.

Os **Planos de Contingência para Incidentes de Impacto Global na Empresa** são aquelas ações que, uma vez ocorrido o incidente que cause impacto na organização como um todo, permitirão à empresa a continuidade das atividades vitais ao atendimento de sua missão, nas condições mínimas necessárias de funcionamento, até o retorno à normalidade. Exemplos de incidentes causadores de contingência de âmbito geral: incêndio ou alagamento em grandes proporções, pane generalizada nos recursos de informática e telecomunicações, interdição do prédio onde funciona a IDGR por motivos externos, etc.

O respaldo metodológico para o desenvolvimento deste **PCCN** é a **ISSO 22.301:2013**, que trata de Segurança da Sociedade – Sistema de Gestão de Continuidade de Negócios – Requisitos.

Para garantia de sua eficácia e efetividade, este **PCCN** deve ser de conhecimento de todos os colaboradores da IDGR e daqueles que, na estrutura da IDGR, têm interface com os seus processos de negócio. Sua revisão periódica é requisito básico para o atingimento de seus objetivos.

Como observação final desta introdução, é importante lembrar que as pessoas são os principais ativos da IDGR e que, em caso de incidente provocado por desastres como incêndios ou desabamentos, a prioridade será sempre a preservação de vidas.

1. CONCEITUAÇÃO

Os conceitos abaixo relacionados objetivam o nivelamento de conhecimento de todos os colaboradores da IDGR, quanto ao objeto deste **PCCN**, e perfeito entendimento do contexto no qual ele se insere. Estes conceitos devem ser interpretados sob o ponto de vista da continuidade de negócios.

1.1. Sistema de Gestão de Continuidade de Negócios (**SGCN**)

É o conjunto de ferramentas de gestão concorrendo para a garantia do atendimento às demandas dos clientes da IDGR em situações de contingência. O **PCCN** é parte integrante deste sistema.

Importante:

• A liderança do **SGCN** tem que ser da Diretoria da **IDGR**.

• As pessoas envolvidas num processo de continuidade de negócios têm que ser capacitadas para tal.

• Deve haver a garantia de que os recursos necessários para a continuidade dos negócios estejam sempre disponíveis.

• O **SGCN** deve estar alinhado com o Planejamento Estratégico.

• Qualquer alteração em processos que tenha interferência no **SGCN** deve acarretar a revisão do mesmo.

• A Gestão de Riscos e a Gestão de Continuidade de Negócios devem estar alinhadas, uma vez que a análise de riscos fornece subsídios para a análise de impacto nos negócios em casos de descontinuidades.

• A Comunicação é atividade fundamental para a eficácia do **SGCN.**

• Todos os colaboradores devem conhecer o **SGCN**.

• O **SGCN** deve ser periodicamente avaliado e melhorado.

1.2. Contingência

É uma eventualidade, um acontecimento que tem como fundamento a incerteza do que pode ou não acontecer.

1.3. Incidente

No contexto do **PCCN**, é o evento imprevisto e indesejável que pode resultar em algum tipo de dano a pessoas, ao patrimônio ou ao meio ambiente, provocando a paralisação de atividades vitais ao negócio.

1.4. Continuidade de Negócio

Capacidade estratégica e tática que a empresa tem para planejar e responder a incidentes, com a finalidade de continuar a execução das atividades críticas, dentro de um nível aceitável e assumido pela organização.

1.5. Atividade

Conjunto de processos que suportam um ou mais serviços/produtos (Ex.: TI, Investimentos, Benefícios, Empréstimos, Financeiro, etc).

1.6. Infraestrutura

Sistema de instalações, equipamentos e serviços necessários para o funcionamento da empresa em caso de incidência OffSite, utilizando uma instalação de escritório compartilhado até o reestabelecimento do Site principal.

1.7. Parte Interessada
Pessoa ou organização que pode afetar ou ser afetado ou que entende ser afetado por uma situação de contingência. Ex.: **IDGR** Participantes, Beneficiários, Colaboradores da **IDGR**, etc.

1.8. Período Máximo de Interrupção Tolerável
Tempo necessário para que os impactos adversos de uma situação de contingência tornem-se inaceitáveis.

1.9. Tempo Objetivado de Recuperação
Período de tempo após um incidente/acidente em que o serviço deve ser retomado ou os recursos recuperados (retorno à normalidade).

1.10. Objetivo Mínimo de Continuidade de Negócios
Níveis mínimos aceitáveis de serviços para a empresa realizar suas atividades vitais durante uma interrupção provocada por uma contingência.

1.11. Acordo de Ajuda Mútua
Pré-disposição de entendimento entre duas ou mais áreas para prestação de assistência mútua, visando a manutenção de algum processo vital em funcionamento.

1.12. Registro
Formalização dos resultados atingidos durante e após a execução de um **PCCN**.

1.13. Risco
Possibilidade de ocorrência de eventos que interfiram no alcance dos objetivos da empresa. O gerenciamento de riscos está relacionado com os objetivos da organização, que incluem, mas não se limitam aos objetivos de continuidade de negócios.

1.14. Impacto
Consequência da indisponibilidade de recursos, tecnológicos e humanos, decorrente da efetiva ocorrência de falhas.

2. RECOMENDAÇÃO DE MEDIDAS PREVENTIVAS

Com o objetivo de reduzir os riscos de ocorrência de incidentes e de prover recursos para a garantia da vida, a adoção das seguintes medidas deve ser avaliada e decidida pela Diretoria da IDGR:

2.1. Rota de Fuga e Sinalização de Emergência
Instalação de Rota de Fuga e Sinalização de Emergência em pontos estratégicos do escritório, instruindo aos colaboradores e visitantes um padrão de conduta adequado em caso de sinistros com o fogo.

2.2. Revisão Periódica de Equipamentos de Combate a Incêndios
Estabelecer cronograma de revisão periódica em extintores, mangueiras e *sprinklers.* Se no caso das mangueiras a responsabilidade for do condomínio, cobrar laudo sobre as condições das mesmas.

2.3. Formar Grupo de Brigadistas

Garantir que, pelo menos, dois colaboradores de cada andar sejam certificados em cursos especializados para atuação em caso de incêndio ou outros casos de incidentes que gerem a necessidade de evacuação do escritório.

2.4. Simulações

Caso não seja prática do condomínio a realização de simulações periódicas de evacuação do prédio, estabelecer um procedimento interno para este fim, pré-determinando: tempo ideal para a evacuação, ponto de encontro, coordenação do procedimento, etc. Acordos para participação de empresas instaladas em andares vizinhos aumentam a eficácia do procedimento.

2.5. Disponibilização de Telefones da Polícia, do Corpo de Bombeiros, da Defesa Civil e do SAMU.

Afixar os telefones de emergência em locais estratégicos. Em situações de pânico, esta medida pode facilitar a comunicação com essas instituições.

2.6. Identificação de Visitantes

Estabelecer procedimento para a identificação de visitantes no âmbito da **IDGR** (crachá ou etiqueta), como medida para aumento do nível de segurança.

2.7. Circulação de Terceiros

Estabelecer procedimento para circulação de terceiros na IDGR, tanto de visitantes como de prestadores de serviço.

2.8. Monitoramento do Ambiente Corporativo

Implantação de sistema de monitoramento com câmeras em locais estratégicos.

2.9. Melhoria Operacional na Central de Controle de Documentos

Em função da natureza da atividade (manuseio e guarda de documentos), recomendasse a adoção de recursos específicos para controle de umidade e pragas.

2.10. Avaliação Periódica dos Circuitos Elétricos

Verificação periódica para mitigar o risco de curto-circuito.

2.11. Avaliação Periódica das Instalações Hidráulicas

Verificação periódica de registros, válvulas e pontos de infiltração.

2.12. Telefones de Colaboradores

Disponibilização de lista de telefones celulares e residenciais dos colaboradores, para utilização em caso de necessidade de comunicação de situações de contingência, se necessário.

3. Planos de Contingência para incidentes de Impacto Global na Empresa

Os planos aqui estabelecidos baseiam-se na análise das Matrizes de Impacto x Risco por Processo, onde foram verificadas as falhas em ativos que impactam a organização como um todo.

Algumas ações recomendadas exigirão da Diretoria Executiva da IDGR decisão de investimento, visando atingir com as soluções propostas níveis acima do objetivo mínimo aceitável de continuidade de negócios, o que se traduz em melhoria significativa de eficácia de recuperação (exemplo: montagem de *site* de contingência).

Relativamente à decisão de entrada em situação de contingência, recomendam-se os seguintes níveis de alçada:

Incidente	Tomadores de Decisões
Falha em Ativos de TI	Coordenador de TI + 1 Diretor
Incidente nas instalações Prediais	Coordenador de Administração + 1 Diretor
Incidente nas Instalações Elétricas	Coordenador de Administração + 1 Diretor
Incidente em Envolvimento de Colaboradores	Coordenador de Administração + Coordenador de Área + 1 Diretor

Ativo: Rede de Dados Interna (LAN)

AMEAÇAS	VULNERABILIDADE	RISCOS	
Falha no equipamento (switch)	Fornecimento de acesso à rede de forma interrompida, por inexistência de redundância.	Parada da rede corporativa - LAN	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO – INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer de forma emergencial a funcionalidade da rede de dados interna (LAN)	Coordenador de TI	Interrupção não tolerável	Implantar ação imediatamente
Viabilizar a disponibilização da rede em modo redundante.	Coordenador de TI e Diretoria		Implantar ação a médio prazo

Ativo: Link de dados (WAN) – Internet

AMEAÇAS	VULNERABILIDADE	RISCOS	
Interrupção do serviço de fornecimento de acesso internet (WAN) pelo prestador do serviço e falha no equipamento (modem/roteador).	Fornecimento de acesso a internet de forma interrompida por inexistência de redundância.	Perda de acesso a internet com indisponibilidade dos serviços de e-mail, WEB e com possibilidade de perdas de transações eletrônicas.	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO – INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer de forma emergencial a funcionalidade da rede de dados WAN.	Coordenador de TI	Interrupção não tolerável	Implantar ações imediatamente
Viabilizar o fornecimento de acesso em modo redundante para disponibilizar o acesso a internet e seus serviços de forma ininterrupta.	Coordenador de TI e Diretoria		

Ativo: Link de Voz (telefonia)

AMEAÇAS	VULNERABILIDADE	RISCOS	
Interrupção do serviço de voz.	Fornecimento de link de voz interrompido por falha adversa, sem aviso prévio e por inexistência de redundância.	Perder a comunicação via telefone com as entidades externas à empresa.	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO – INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Utilizar de forma emergencial os telefones celulares corporativos.	Colaboradores portadores desse recurso	Interrupção não tolerável	Implantar ações imediatamente
Viabilizar o fornecimento de link de voz em modo redundante, para disponibilizar este serviço de forma ininterrupta.	Coordenador de Administração, Diretoria Executiva e Conselho Deliberativo		
Informar a interrupção e a previsão de retorno à Guiar Investimentos	Assessoria de Comunicação		

Ativo: Servidor de Banco de Dados

AMEAÇAS	VULNERABILIDADE	RISCOS	
Falha no equipamento (servidor).	Interrupção do acesso às informações *core* da empresa.	Parada do servidor	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO – INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer a funcionalidade física do servidor (componentes eletrônicos)	Coordenador de TI	Interrupção não tolerável	Implantar ações imediatamente
Reestabelecer a funcionalidade do banco de dados do servidor (base de dados)	Coordenador de TI		
Viabilizar provisionamento para substituição do equipamento em caso de falha e/ou criação de ambiente redundante com sincronização dos dados.	Coordenador de TI e Diretoria		Implantar ação a médio prazo

Ativo: Instalações Prediais

AMEAÇAS	VULNERABILIDADE	RISCOS	
Desastres (Incêndio, inundação, sabotagem, assalto, atentado terrorista).	Indisponibilização do acesso às instalações prediais.	Impossibilidade de operação da empresa.	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO – INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Salvaguardar a vida dos colaboradores providenciando a evacuação do escritório.	Brigadistas	Não definido. Quanto mais ágil for a empresa em prover os recursos necessários para atuação em modo de contingência, menor será o prejuízo.	Implantar ações imediatamente
Acionar os orgãos competentes (SAMU, Bombeiros, Defesa Civil, Polícia, etc), conforme a natureza do incidente/desastre	Coordenador de Administração		
Nas situações extremas (por exemplo: existência de vítimas) , informar aos familiares			
Informar a interrupção e a previsão de retorno à Guiar Investimentos e aos clientes.	Assessoria de Comunicação		
Se necessário, informar à mídia (jornal, tv, rádio, etc), com o suporte da Assessoria Jurídica.			
Reestabelecer de forma emergencial as cópias de segurança em ambiente de nuvem para que os colaboradores possam ter acesso via internet aos documentos de uso diário (planilhas, textos, etc).	Coordenador de TI		
Providenciar junto aos órgãos competentes os documentos necessários para as medidas de reestabelecimento da empresa junto às seguradoras (financeiro e operacional)	Coordenador de Administração		
Viabilizar montagem de site de contigência, visando disponibilizar em local seguro que não seja afetado pelo mesmo incidente os recursos mínimos necessários para manter a operação da empresa em modo de contingência (**vide Anexo - Recursos Mínimos para a Manutenção de Operação em Modo de Contingência**)	Coordenador de TI e Diretoria		Implantar ação a médio prazo.

Ativo: Energia Elétrica

AMEAÇAS	VULNERABILIDADE	RISCOS	
Falha na prestação do serviço; Desastre (acidente, sabotagem, curto-circuito).	Fornecimento de energia interrompida por falta de redundância.	Interromper a operação da empresa.	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO – INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer a energia elétrica de forma emergencial e, se houver necessidade, contratar energia elétrica de outro fornecedor (gerador) até o retorno através da prestadora de serviço (Ligth, Ampla, etc)	Coordenador de Administração	4 horas	Implantar ações imediatamente
Executar medidas para preservação dos equipamentos de TI.	Coordenador de TI		
Viabilizar o fornecimento de energia elétrica de forma ininterrupta e estável, por um período maior e abrangendo os equipamentos essenciais/mínimos para o funcionamento da empresa.	Coordenador de Administração e Diretoria		

Ativo: Colaboradores

AMEAÇAS	VULNERABILIDADE	RISCOS	
Desligamento em massa por motivo adverso; Movimentos sociais (greves, passeatas, etc).	Quadro de pessoal enxuto.	Operação da empresa interrompida parcial ou totalmente.	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO – INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
No caso de impossibilidade de comparecimento à Guiar Investimentos, disponibilizar recursos para acesso remoto para que os colaboradores possam acessar as informações necessárias para o desenvolvimento do trabalho (home office)	Coordenador de TI	Interrupção não tolerável	Implantar ações imediatamente
Para os casos de desligamento em massa, utilizar os recursos de setores remanescentes com atividades afins estabelecendo um acordo de ajuda mútua.	Coordenadores das Áreas Impactadas		
Prover transporte alternativo para os elementos chave dos principais processos.	Coordenador de Administração		

4. Plano de Contingência para Incidentes de Impacto Específico em Processos

Os planos aqui estabelecidos baseiam-se na análise das Matrizes de Impacto x Risco por Processo .

Algumas ações recomendadas exigirão da Diretoria Executiva da IDGR decisão de investimento, visando atingir com as soluções propostas níveis acima do objetivo mínimo aceitável de continuidade de negócios, o que se traduz em melhoria significativa de eficácia de recuperação (exemplo: redimensionamento do quadro de pessoal).

Relativamente à decisão de entrada em situação de contingência, a responsabilidade é exclusiva dos Coordenadores de Área, com a devida formalização junto ao respectivo Diretor.

Na sequência são apresentados os planos de ação, divididos por ativo da empresa com risco de falhas de impacto específico em processos:

INVESTIMENTOS

AMEAÇAS	VULNERABILIDADE	RISCOS
Entidades externas inacessíveis; Falha na interface com outros setores; Interrupção do serviço de fornecimento de acesso internet para bancos e corretoras; e Ausência de recursos humanos para execução e aprovação.	Quadro de pessoal enxuto; Não atingimento dos objetivos da área; e Fornecimento de acesso à internet de forma interrompida, por inexistência de redundância.	Processos não serem executados parcial ou totalmente; e Descumprimento de prazos legais e de negócio; Afetar a imagem da empresa e impactar na receita.

AÇÕES	RESPONSÁVEIS	PRIORIDADE
Utilizar recursos alternativos para comunicação com as entidades externas.	Coordenador de Investimentos Coordenador de Liquidação e Custódia Analista de Investimento – Compliance	Implantar ações imediatas
Relatar a falha na interface com outros setores, buscando consenso com os mesmos e, se necessário, escalar problema ao nível superior.		
Utilizar os recursos de setores com atividades afins, e estabelecendo um acordo de ajuda mútua.		
Elaborar plano de revisão do quadro de colaboradores, visando identificar os que necessitam de espelhamento para que a execução do processo não sofra interrupção.		Implantar ação a médio prazo
Reestabelecer o acesso às entidades externas de forma emergencial	Coordenador de TI	Implantar ações imediatas
Em relação ao acesso internet interrompido, vide planos globais para o ativo: "Link de dados (WAN) - Internet".		Ver plano para Link de Dados (WAN) - Internet

5. Monitoramento do PCNN e Melhorias

5.1. Revisões:

O **PCCN** deve ser revisado **anualmente** ou, eventualmente, na ocorrência das seguintes situações:

EVENTO	AÇÃO	RESPONSÁVEL
Alteração em processos (otimização ou adaptação a alterações na legislação).	Analisar impacto no **PCCN** e, se necessário, atualizá-lo.	Coordenador de Área
Introdução de nova tecnologia.	Analisar risco de falha, impacto nos processos, definir contingência e atualizar **PCCN**.	Coordenador de TI (em trabalho conjunto com os Coordenadores das áreas afetadas).

A revisão anual ocorrerá em data definida pela Diretoria Executiva e será composta das seguintes etapas:

ETAPA	AÇÃO	RESPONSÁVEL
Análise crítica do **PCCN**	Leitura prévia e análise do conteúdo do **PCCN**.	Coordenadores de Área (recomendável participação dos colaboradores).
Validação da revisão	Reunião da Diretoria Executiva com os Coordenadores, para apresentação de sugestões.	Presidência

Ao final do processo de revisão, os seguintes produtos serão gerados:
• **PCCN** atualizado e/ou corrigido (se for o caso);
• Registro da validação da revisão (ata contendo sumário de atualizações/correções realizadas, assinada por todos os participantes; caso não existam atualizações/correções, observar na ata que o **PCCN** foi revisado e que seu conteúdo atende aos requisitos de negócio para o próximo período).
• Caso ocorra atualização/correção no **PCCN**, a área de Comunicação procederá à devida atualização na Intranet (e outros veículos de divulgação do plano, se existirem).

5.2. Testes

A realização de testes do **PCCN** é **obrigatória** e deverá seguir o seguinte critério de execução:

EVENTO	PERIODICIDADE	RESPONSÁVEL
Simulação de evacuação do escritório em caso de desastre (incêndio, alagamento, suspeita de atentado terrorista, etc.).	Semestral	Coordenador de Administração
Rodízio de colaboradores, para execução de atividades (exemplo: alocar, por um dia, um colaborador de "Empréstimos" na área de "Seguridade").	Eventual (fora de períodos críticos)	Coordenador de Área
Home Office: liberar, por um dia, colaboradores cuja atividade principal possa ser executada de casa, estabelecendo controles de atuação remota.	Eventual	Coordenador de Área
Simulação de situações para validar se os planos possuem informações suficientes para a atuação em caso de contingência.	Semestralmente (selecionar plano e executá-lo)	Coordenador de Área
Testar recursos alternativos de TI.	Anualmente	Coordenador de TI

Todo teste de **PCCN** deve ser formalmente planejado e acordado entre as áreas envolvidas. Simulações de evacuação do escritório devem ser aprovadas pela Diretoria Executiva. Os testes com recursos de TI e utilização de Home Office devem ter a aprovação de, pelo menos, um Diretor. A execução dos demais testes será decidida pelos próprios Coordenadores.