



PLANO DE CONTINGÊNCIA E GESTÃO DE RISCOS

Companhia Amazonense de
**Desenvolvimento
e Mobilização de Ativos**



AMAZONAS
GOVERNO DO ESTADO

1. INTRODUÇÃO

Este Plano de Contingência e Gestão de Riscos (PCGR) objetiva prover a Companhia Amazonense de Desenvolvimento e Mobilização de Ativos - CADA de um conjunto de planos de ação que suportem o gerenciamento de situações de qualquer contingência provocada por incidentes causadores de interrupção ao andamento normal de atividades, garantindo as condições mínimas necessárias para a continuidade e normalização dessas.

O PCGR está dividido em partes, a saber:

- Conceituação;
- Principais Riscos e Planos de Contingência;
- Monitoramento do PCGR e Melhorias; e
- Recomendações de Ações Preventivas.

Em “conceituação”, o principal objetivo é familiarizar os colaboradores da CADA com os termos utilizados em projetos de contingência, nivelando o conhecimento entre a equipe e facilitando o entendimento do conteúdo deste PCGR.

A relação do PCGR com o Planejamento Estratégico da CADA evidencia a importância do PCGR no alcance dos objetivos estratégicos da empresa.

As Recomendações de Medidas Preventivas estão diretamente relacionadas às providências para mitigação de quaisquer riscos na ocorrência de algum incidente que provoque problemas na continuidade do negócio.

Os **Planos de Contingência e Gestão de Riscos para Incidentes de Impacto Global na Empresa** são 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 **CADA** (por motivos externos), dentre outros.

2. CONCEITUAÇÃO

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

2.1 CONTINGÊNCIA

É uma situação ou acontecimento que tem como fundamento a incerteza do que pode ou não acontecer.

2.2 INCIDENTE

No contexto do **Plano Contingência e Gestão de Riscos - PCGR**, 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 total ou parcial de atividades vitais ao negócio.

2.3 CONTINUIDADE DE NEGÓCIO

Capacidade de a empresa planejar e responder a incidentes, com a finalidade de continuar a execução das atividades críticas, dentro de um nível aceitável pela organização.

2.4 ATIVIDADE

Conjunto de processos que suportam um ou mais serviços/produtos (Ex.: Atividades das equipes Operacional e Administrativa).

2.5 INFRAESTRUTURA

Sistema de instalações, equipamentos e serviços necessários para o funcionamento da empresa.

2.6 PARTE INTERESSADA

Pessoa ou organização que pode afetar ou ser afetado por uma situação de contingência. Ex.: Colaboradores, Acionistas, Sociedade, entre outros.

2.7 PERÍODO MÁXIMO DE INTERRUPÇÃO TOLERÁVEL

Tempo necessário para que os impactos adversos de uma situação de contingência tornem-se inaceitáveis.

2.8 TEMPO OBJETIVADO DE RECUPERAÇÃO

Período após um incidente/acidente em que o serviço deve ser retomado ou os recursos recuperados (retorno à normalidade).

2.9 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.

2.10 REGISTRO

Formalização dos resultados atingidos durante e após a execução de um **PCGR**.

2.11 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.

2.12 IMPACTO

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

3. PLANOS DE CONTINGÊNCIA E GESTÃO DE RISCOS PARA INCIDENTES DE IMPACTO GLOBAL NA EMPRESA

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

INCIDENTE	TOMADORES DE DECISÃO
Falha em Ativos de TI e Comunicação	Diretor Administrativo + Diretor Operacional
Incidente nas Instalações Prediais	Diretor Administrativo + Diretor-Presidente
Incidente nas Instalações Elétricas	Diretor Administrativo + Diretor-Operacional
Incidente com envolvimento de Colaboradores	Diretor Administrativo + Diretor-Presidente

ATIVO: LINK DE DADOS (WAN) - INTERNET

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

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO – INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Estabelecer contato com o responsável contratado para serviços manutenção preventiva e corretiva de TI.	Gerência Administrativa	Mínimo possível de acordo com o Termo de Contrato	Imediata
Estabelecer contato com a operadora e solicitar o reestabelecimento de forma emergencial.	Gerência Administrativa	Mínimo possível de acordo com a operadora	Imediata
Mensurar com a operadora a previsão do reestabelecimento.	Gerência Administrativa		Imediata
Informar a interrupção e a previsão de retorno às Diretorias.	Gerência Administrativa		Imediata

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 meios de comunicação paralelos como e-mail, ou aplicativos de chamada disponibilizados, como o Teams.	Colaboradores portadores dos recursos	Interrupção não tolerável	Implantar ações imediatamente
Manter contato com a empresa de telefonia para viabilizar o retorno o mais rápido possível.	Gerência Administrativa		
Informar a interrupção e a previsão de retorno às Diretorias.	Gerência Administrativa		

ATIVO: BANCO DE DADOS EM NUVEM

AMEAÇAS	VULNERABILIDADE	RISCOS	
Impossibilidade de acesso aos arquivos em nuvem	Interrupção do acesso aos arquivos da empresa	Falta de acesso disponibilizado pelo responsável ou algum usuário apagar os arquivos	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Tentar reestabelecer o acesso e verificar se não é falha no fornecimento de internet	Gerente da área e responsável de TI (contratado)	Interrupção não tolerável	Implantar ações imediatamente
Buscar último backup realizado e mensurar perdas	Gerente da área e responsável de TI (contratado)		
Disponibilizar novamente os arquivos, ora recuperados mediante a busca do último backup	Gerente da área e responsável de TI (contratado)		

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 do prédio	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 à administração do prédio e os órgãos competentes (SAMU, Bombeiros, Defesa Civil, Polícia etc.), conforme a natureza do incidente/desastre	Diretor Administrativo e Gerência Administrativa		
Nas situações extremas (por exemplo: existência de vítimas), informar aos familiares. ANEXO I			
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.)	Diretores das áreas		
Providenciar junto aos órgãos competentes os documentos necessários para as medidas de reestabelecimento da empresa junto às seguradoras (financeiro e operacional)	Diretor Administrativo		
Informar aos funcionários como se dará a continuidade das atividades e o prazo para reestabelecimento do funcionamento regular da empresa.	Diretores das áreas		

ATIVO: ENERGIA ELÉTRICA

AMEAÇAS	VULNERABILIDADE	RISCOS	
---------	-----------------	--------	--

Falha na prestação de 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. Caso o prédio não acione o gerador, entrar em contato com a administração.	Gerência Administrativa	1 hora	Implantar ações imediatamente
Executar medidas para preservação dos equipamentos de TI	Gerência Administrativa e responsável de TI (contratado)		
Caso a interrupção não seja solucionada, viabilizar medidas alternativas, como atividades em home office.	Diretorias das áreas		

ATIVO: COLABORADORES

AMEAÇAS	VULNERABILIDADE	RISCOS	
Ausência em massa por motivo adverso; Movimentos sociais (greves, passeatas etc.)	Demandas descobertas	Operação da empresa interrompida parcial ou totalmente	

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Para os casos de ausência em massa, utilizar os recursos de setores remanescentes com atividades afins, estabelecendo um acordo de ajuda mútua.	Diretores das áreas impactadas	4 horas	Implantar ações imediatamente
Fornecer informações e aparatos para os funcionários desempenharem os trabalhos em home office.	Diretores das áreas impactadas		

4. 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 Executiva da CADA:

4.1 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, e levar a conhecimento geral as orientações de fuga e emergência do prédio no qual a CADA está instalada.

4.2 REVISÃO PERIÓDICA DE EQUIPAMENTOS DE COMBATE A INCÊNDIOS

Checar com o prédio no qual a CADA está instalada se a revisão periódica dos equipamentos de incêndio está em dias.

4.3 SIMULAÇÕES

Checar com o prédio no qual a CADA está instalada a periodicidade das simulações e informar aos colaboradores.

4.4 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.

4.5 IDENTIFICAÇÃO DE VISITANTES

Todos os visitantes devem se identificar na recepção do prédio onde funciona a CADA e somente após autorização poderá acessar as dependências da sede administrativa.

4.6 CIRCULAÇÃO DE PRESTADORES DE SERVIÇOS DE TERCEIROS

A prestação de serviços de terceiros dar-se em dia programado com a Gerência Administrativa, que enviará um email: admtheplace@gmail.com à administração do condomínio solicitando a autorização de Ordem de Serviços – OS. Observando que os serviços que fazem barulho só poderão ser realizados em dias úteis após às 22h, e durante feriado, sábado e domingo após às 14h.

4.7 MONITORAMENTO DO AMBIENTE CORPORATIVO

O monitoramento da câmera deverá ser realizado pela Diretoria Executiva.

4.8 MELHORIA OPERACIONAL NA CENTRAL DE CONTROLE DE DOCUMENTOS

Em função da natureza da atividade (manuseio e guarda de documentos), oferece-se 03 meios, quais sejam: Sistema de Gestão de Documentos – SIGED; Junta Comercial – JUCEA e arquivos físicos; recomenda-se que cada diretoria de área administre os documentos para controle da guarda e manuseio de documentos físicos e digitais.

4.9 AVALIAÇÃO PERIÓDICA DOS CIRCUITOS ELÉTRICOS

Verificação periódica para mitigar o risco de curto-circuito.

4.10 AVALIAÇÃO PERIÓDICA DAS INSTALAÇÕES HIDRÁULICAS

Verificação periódica de registros, válvulas e pontos de infiltração.

4.11 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.

5. MONITORAMENTO DO PCGR E MELHORIAS

5.1 REVISÕES:

O **PCGR** deve ser revisado **anualmente** ou, eventualmente, na ocorrência de nova regulação ou nas seguintes situações:

EVENTO	AÇÃO	RESPONSÁVEL
Alteração em processos (otimização ou adaptação a alterações na legislação)	Analisar impacto no PCGR e, se necessário, atualizá-lo	Gerência da área
Introdução de nova tecnologia	Analisar risco de falha, impacto nos processos, definir contingência e atualizar PCGR	Gerentes das áreas afetadas com auxílio do Prestador de serviços de TI

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

ETAPA	AÇÃO	RESPONSÁVEL
Análise crítica do PCGR	Leitura prévia e análise do conteúdo do PCGR	Gerente das áreas
Validação da revisão	Reunião da Diretoria Executiva com os Gerentes, para apresentação de sugestões	Diretor-Presidente

Ao final do processo de revisão, os seguintes produtos serão gerados:

- **PCGR** 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 **PCGR** foi revisado e que seu conteúdo atende aos requisitos de negócio para o próximo período).

- Caso ocorra atualização/correção no **PCGR**, a Gerência Executiva procederá à devida atualização nos meios de comunicação interna disponíveis.

5.2 TESTES

A realização de testes do **PCGR** 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.)	De acordo com a administração do condomínio	Diretor Administrativo
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)	Diretor da área
Home Office: liberar, por um dia, colaboradores cuja atividade principal possa ser executada de casa, estabelecendo controles de atuação remota	Eventual	Diretor da 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)	Diretor da área

ANEXO I

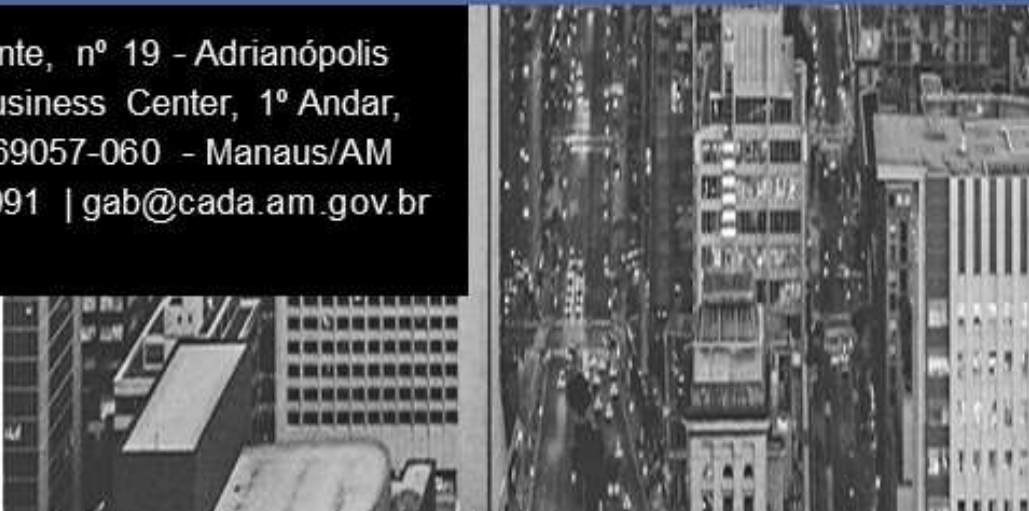
LISTA DOS CONTATOS DE FAMILIARES DOS FUNCIONÁRIOS CADA - 2024				
ITEM	FUNCIONÁRIO	CONTATO	TELEFONE	GRAU DE PARENTESCO
1	ACRAM SALAMEH ISPER JR		(	ESPOSA
2	ALBERTO PACHECO LADEIRA			ESPOSA
3	CAMILLA MORAES			MÃE
4	CAROLINE SEBBEN			MÃE
5	FLÁVIA DE PAIVA BRANDI			MÃE
6	HELLEN BALDINO			MÃE
7	JORGE ARAÚJO DA COSTA			FILHO
8	JULIANA GIRARDI VARGAS			ESPOSO
9	JULIANA GOMES			PAI
10	KARLA MARTINS			IRMÃ
11	LAÍZA BEZERRA MACIEL		(	MÃE
12	MÉRCIA NOGUEIRA MONTEIRO			MÃE
13	RENATA BEZERRA DE MELO			FILHO

Plano de Contingências e Gestão de Riscos Aprovado em 29/11/2024 na 39ª Reunião da Diretoria Executiva da CADA, com ata anexa sob o Processo nº 01.01.014501.000013/2024-80 – SIGED.



CADA

COMPANHIA AMAZONENSE
DE DESENVOLVIMENTO E
MOBILIZAÇÃO DE ATIVOS



Rua Belo Horizonte, nº 19 - Adrianópolis
Ed. The Place Business Center, 1º Andar,
Sala 107 | CEP:69057-060 - Manaus/AM
Fone: (92) 3022-1091 | gab@cada.am.gov.br