Plano de Continuidade de TI do CRCAP

(versão 1.0)

Plano de Continuidade de TI do CRCAP

Conservação, ininterrupção dos sistemas essenciais de TI do Conselho Regional de Contabilidade do Amapá

Coordenadoria de Gestão de TI (CGTI)
Departamento de Informática (Deinf)
Macapá, AP

SUMÁRIO

Histórico de Alterações

Data	Versão	Descrição da versão	Responsável
17/10/2022	1.0	Elaboração da primeira versão	Deinf
17/10/2022	1.0	Revisão	Cgti
17/10/2022	1.0	Aprovação do documento	CTI
17/10/2022	1.0	Aprovação do documento	CSI
27/10/2022	1.0	Aprovação do PCTI	Plenário do CRCAP
27/10/2022	1.0	Publicação Portal da Transparência	CTransparência
27/10/2022	1.0	Divulgação	Ccom/Direx

1. JUSTIFICATIVA E OBJETIVO

O Plano de Continuidade de Tecnologia da Informação (PCTI) contém medidas preventivas, procedimentos de recuperação em eventuais interrupções de negócios, além de assegurar a identificação, avaliação, monitoramento e controle dos recursos que dão suporte à realização das operações (equipamentos, sistemas de informações, pessoal, instalações e informações). O PCTI atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos.

Gestão de Continuidade de TI

A estrutura estratégica e operacional adequada ao CRCAP:

- ✓ Obter capacidade de gerenciar uma interrupção no negócio de forma a evitar impactos para o registro, a fiscalização do exercício da profissão contábil, a normalização e a educação profissional continuada, a fim de proteger a reputação da organização;
- ✓ Melhorar proativamente a resiliência da organização em momentos necessários, mitigar os riscos de interrupções e diminuindo o tempo de resposta a possíveis incidentes; e
- ✓ Assegurar através de método sistemático o retorno de operacionalização, em um tempo aceitável dos serviços críticos, após um incidente.

2. ESCOPO

O Plano de Continuidade de Tecnologia da Informação (PCTI) abrange as estratégias necessárias à continuidade dos serviços de TI essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a TI do CRCAP e serviços essenciais, de acordo com o Decreto-Lei n.º 9.295/46 e alterações, para o registro, a fiscalização do exercício da profissão contábil, a normatização e a educação profissional continuada.

O PCTI é executado tanto no âmbito da CGTI quanto isoladamente, ou como parte de um Plano de Continuidade de Negócios (PCN) do CRCAP.

3. SERVIÇOS ESSENCIAIS

São os seguintes os serviços essenciais, por ordem de priorização para o acionamento e execução do PCTI.

Serviço	Criticidade	RPO[1]	RTO[2]	Impacto			
				Financeiro	Legal	Imagem	Operacional
Sistema de Registro	Alta	24 horas	8 horas	Alto	Alto	Alto	Alto
Arrecadação	Alta	24 horas	8 horas	Crítico	Crítico	Crítico	Crítico
Serviços On Line	Alta	4 dias	8 horas	Baixo	Médio	Alto	Baixo
Sistemas de Gestão	Alta	24 horas	8 horas	Crítico	Alto	Baixo	Alto
Sistema de Fiscalização	Alta	24 horas	8 horas	Baixo	Baixo	Médio	Médio
Sistema CNAI, CNPC e CNAI-PJ	Alta	7 dias	7 dias	Alto	Médio	Alto	Médio
EPC	Alta	72 horas	7 dias	Baixo	Médio	Alto	Alto
Decore	Alta	7 dias	8 horas	Médio	Médio	Alto	Médio
CRE	Alta	7 dias	7 dias	Baixo	Médio	Alto	Médio

[1] RPO: ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura

[2] RTO: período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção.

CONSIDERAÇÕES:

Os sistemas gerenciados pelo CRCAP estão listados em Sistema e Serviços do CRCAP,página 28.

Além dos serviços descritos anteriormente, existem as contigências de infraestruturas físicas, as quais abrangem serviços críticos como falha no gerador em caso de ausência de energia elétrica, desastres e catástrofes naturais. Todas as situações naturais devem ser previstas e planejadas para que não ocorram maiores prejuízos a organização.

3.1. DESASTRES E CATÁSTROFES NATURAIS OU NÃO

Abrangência: Casos de incidentes ou ações da natureza, tais como incêndio, inundação, não acesso, pandemia, falta de energia elétrica e outros desastres naturais ou acidentais.

Contingência: Acionar o Plano de Administração de Crises (PAC), em seguida os outros planos para resolver o problema.

Procedimento:

- ✓ Sempre que ocorrer um incidente que gere a descontinuidade das atividades. O Comitê *Disaster Recovery* (DR) deverá analisar o incidente, definindo se o Plano de Continuidade será acionado ou não;
- ✓ O Comitê DR deverá acompanhar todo o processo de restabelecimento das atividades normais; e
- ✓ As respectivas equipes, coordenadas pelo líder, devem seguir os procedimentos estabelecidos no Plano de Continuidade.

Retorno à normalidade: Após todo e qualquer processo de ativação de Plano de Continuidade ou de gestão de crise, cabe ao líder da equipe registrar a descrição do incidente, o que foi bem sucedido, o que falhou e os aprimoramentos implementados para correção das fragilidades identificadas, bem como as ações com os responsáveis e prazo para implementação, se necessário.

É necessário emitir relatórios para encaminhar aos Gestores para conhecimento e adoção de medidas julgadas necessárias.

3.2. SITUAÇÕES DE CONTIGÊNCIA DE PESSOAL

Abrangência: No caso de um colaborador se ausentar, os procedimentos e senhas operacionais dos sistemas devem estar disponíveis aos outros colaboradores, visto que os substitutos devem ser devidamente treinados, e/ou contratar recursos humanos terceirizados.

Contigência: Estratégias para manter as habilidades e conhecimentos fundamentais, tais como: documentação dos procedimentos de execução das atividades críticas, segregação das atividades fundamentais, uso de recursos humanos terceirizados, planejamento de sucessão, gestão do conhecimento (adequada capacitação), entre outras opções.

Procedimento:

- ✓ Submeter os funcionários e prestadores de serviços a treinamentos multidisciplinares;
- ✓ Separar as atividades fundamentais (a finalidade é reduzir a concentração do risco);
- ✓ Planejar a sucessão;
- ✓ Uso de terceirizados; e
- ✓ Retenção e gestão do conhecimento.

Retorno à normalidade: No caso de necessidade de deslocamento físico, a retomada será feita mediante eliminação dos efeitos motivadores da contingência. O Comitê DR avisará aos Gestores o retorno das atividades.

3.3. INFRAESTRUTURAS TECNOLÓGICAS

Abrangência: Compreende-se gerenciamento de servidores, gerenciamento de falhas de redes, gerenciamento de desempenho de redes, *Storage*, gerenciamento de Banco de Dados e *Backup* lógico e físico, se necessário.

Contigência: Estratégias de tecnologia devem considerar o tempo máximo que a entidade esteja disposta a esperar a restauração das atividades críticas (tempo objetivado de recuperação), onde as estratégias podem incluir: distribuição geográfica da tecnologia, adotar o equipamento ou solução similar como substituto em caso de emergências, utilização de redundância de equipamentos, acesso remoto, etc.

Procedimento: Os planos devem ser ativados com base na estratégia selecionada para gerenciar o incidente, devem ser seguidos total ou parcialmente em qualquer estágio de resposta ao incidente.

Retorno à normalidade: Comunicar aos líderes e gestores o retorno das atividades.

4. ÁREA

O PCTI será administrado, avaliado e acionado no âmbito da Coordenadoria de Gestão de Tecnologia da Informação (CGTI) do CRCAP tendo sua manutenção, organização e melhoria revistas, atualizadas periodicamente pelo Departamento de Informática (DEINF) e aprovadas pelo Comitê de Segurança da Informação (CSI).

5. PRINCIPAIS RISCOS

O PCTI foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam riscos à continuidade dos serviços essenciais.

O quadro a seguir define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
01- Interrupção de energia elétrica	- Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 24 (vinte e quatro) horas; - Causada por fator interno que comprometa a rede elétrica do prédio com curtos-circuitos, incêndio e infiltrações; - Impossibilidade de acionar o Grupo gerador no momento de uma queda de energia.
02 - Falha na Climatização do CPD	- Superaquecimento dos ativos devido à falha no dimensionamento de carga; - Falha na unidade de climatização e não emissão de alertas de monitoração.
03 - Indisponibilidade de Backup	- Cópia de segurança dos dados não disponível ou sem integridade.
04 - Indisponibilidade de rede/circuitos	- Rompimento de fibra ótica decorrente de execução de obras públicas, desastres ou acidentes; - Mal funcionamento de *switch* gerenciador de segmento de rede; - Interrupção dos serviços de conectividade com as operadoras de telecomunicação por mais de 12 (doze) horas.
05 - Falha humana	- Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível.

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
06 - Ataques internos	- Ataque aos ativos do *Data Center e à rede CRCAP.*
07 - Incêndio	- Falhas nos equipamentos ou por ação humana.
08 - Desastres Naturais	- Alagamento.
09 - Falha de hardware	- Falha que necessite reposição de hardware crítico ou reparo, e cujo reparo ou aquisição dependa de processo licitatório.
10 - Ataque cibernético	- Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais, assim como a indisponibilização dos dados por meio de deleção ou mesmo sequestro virtual.

6. PAPÉIS E RESPONSABILIDADES

Comitê de *Disaster Recovery* (DR):

- ✓ Avaliar o plano periodicamente;
- ✓ Decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas; e
- ✓ Incluir autoridades em nível institucional e tomadores de decisão da CGTI.

Equipe de instalações/ambiente:

- ✓ Garantir que as instalações de alternativa são mantidas adequadamente; estas são as responsáveis pelas instalações físicas que abrigam sistemas de TI;
- ✓ Avaliar os danos e supervisionar os reparos para o local principal no caso de

a localização primária sofrer destruição ou danos; e

- ✓ Administrar e manter o Plano de Recuperação de Desastre (PRD), responsabilidade do líder da equipe.

Equipe de rede:

- ✓ Avaliar os danos específicos de qualquer infraestrutura de rede; e
- ✓ Fornecer dados e conectividade de rede de voz, incluindo WAN, LAN, e quaisquer conexões de telefonia, dentro do CRCAP ou de infraestrutura externajunto aos prestadores de serviço.

Equipe de servidores/aplicações:

- ✓ Fornecer a infraestrutura de servidor físico e virtual necessária, para que a TI execute suas operações e processos essenciais durante um desastre; e
- ✓ Garantir que as aplicações essenciais funcionem como exigido, a fim de atender aos objetivos de negócios em caso de desastre e durante o mesmo. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais, também podem ajudar outras equipes de TI/DR conforme necessário.

Equipe de operações:

- ✓ Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções de forma mais rápida e eficiente possível. Eles precisarão provisionar todos os funcionários do CRCAP na solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas à sua atuação; e
- ✓ Administrar e manter o Plano de Continuidade Operacional (PCO), responsabilidade do líder da equipe.

Equipe de comunicação:

- ✓ Responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário; e
- ✓ Administrar e manter o Plano de Administração de Crise, responsabilidade do líder da equipe.

Equipe de backup:

- ✓ Analisar as perdas; e
- ✓ Mapear a quantidade de dados perdidos, tempo de recuperação desses

dados e formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.

Equipe de segurança da informação:

- ✓ Prover mecanismos de segurança no ambiente principal e alternativo; e
- ✓ Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.

7. INVOCAÇÃO DO PLANO

O Plano de Continuidade será acionado quando ocorrer algum dos cenários de desastres, insurgência ou ocorrência de um risco desconhecido, e ainda se houver uma vulnerabilidade que tenha grande possibilidade de ser explorada. Poderá invocar o PCTI em casos de testes, ou por determinação do Comitê DR juntamente com a alta administração do CRCAP.

O acionamento das demais equipes será realizado pelo Líder da Equipe de Operações, de acordo com as características de cada ocorrência. Deverá registrar o evento onde serão consignados informações como data do incidente, descrição sucinta do ocorrido e as devidas equipes acionadas.

Os planos de continuidade serão encaminhados para aprovação da Alta Gestão e pelo responsável da Infraestrutura de TI, inseridos os incidentes de interrupção. Interação com áreas provedoras de recursos para operacionalização (TI, Comunicação Social, entre outras).

Os integrantes das equipes, após acionados, iniciarão a avaliação e investigação do ocorrido, podendo acionar outras equipes, caso necessário.

Abaixo, segue o planejamento da árvore de acionamento de contatos, que estabelece o registro das informações dos principais atores, na eventualidade de acionamento do plano.

- ✓ Árvore de Acionamento de Contatos Equipe de Conectividade

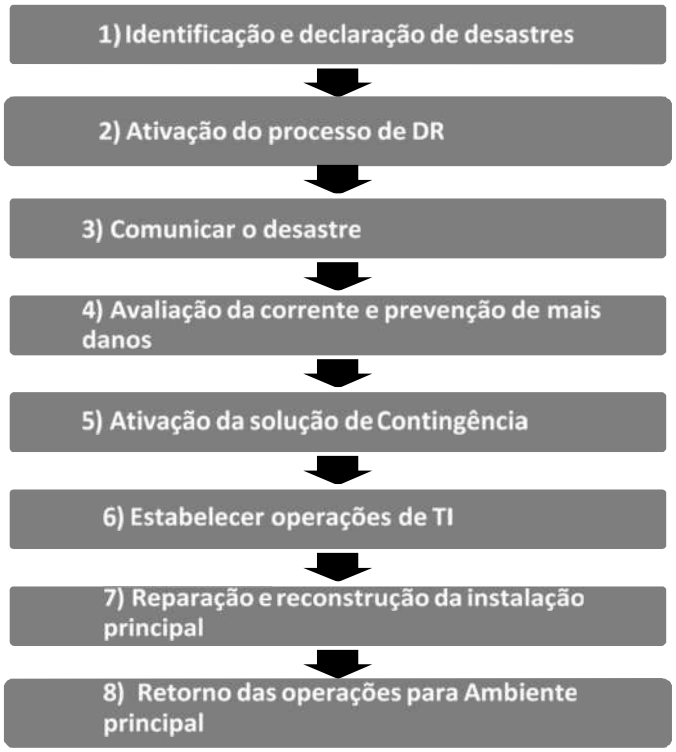
FUNCIONÁRIO	RAMAL	CONTATO ALTERNATIVO
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

- ✓ Empresa Terceirizada

NOME	TELEFONE	CONTATO ALTERNATIVO
Colaborador Terceirizado	99999-9999	xxx@xxx.com.br

8. MACROPROCESSOS DO PCTI

O PCTI tem seus macroprocessos definidos nas atividades a seguir, que se desmembram em planos específicos para cada área de atuação no momento da ocorrência de um desastre.



Os subplanos do PCTI consistem em:

- ✓ **Plano de Continuidade Operacional (PCO)**:
  - Garantir a continuidade dos serviços essenciais de TI críticos na ocorrência de um desastres, enquanto recupera-se o ambiente principal. O PCO é fortemente orientado aos processos (sistemas) e serviços.
  - Cada serviço identificado como crítico pelo documento

“Avaliação de Impacto de Desastre” terá seu PCO.

- ✓ **Plano de Administração de Crise (PAC):**
  - Definir as atividades das equipes envolvidas e orquestrar as ações de contingência e comunicação durante e depois da ocorrência de um desastre, com intuito de minimizar impactosaté a superação da crise.

- ✓ **Plano de Recuperação de Desastre (PRD):**
  - Planejar e agir para que, uma vez controlada a contingênciae passada a crise, a TI do CRCAP retome seus níveis originais de operação no ambiente principal; e
  - Cada serviço identificado como crítico deverá possuir um “Procedimento de Continuidade”.

- ✓ **Plano de Testes e Validação (PTV):**
  - Um Plano de Continuidade de Negócios só está apto afuncionar, após ser testado e exercitado. O plano define a periodicidade e tipos de teste que serão realizados.

PLANO DE CONTINUIDADE OPERACIONAL

9. PLANO DE CONTINUIDADE OPERACIONAL (PCO)

Este plano descreve os cenários de inoperância, os respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais.

O plano deve ser revisado, no mínimo anualmente, ou quando ocorrer mudanças significativas no CRCAP.

9.1. APLICABILIDADE

É aplicável para:

a) Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações de TI, dos sistemas essenciais;
b) Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre;
c) Estabelecer uma equipe para cada plano PCO, PRD e PAC; e
d) Definir os formulários, *checklists* e relatórios a serem entregues pelas equipes ao executar a contingência.

9.2. EQUIPES ENVOLVIDAS

EQUIPES	LÍDER	MEMBROS
REDE		
SOFTWARE		
HARDWARE		
SERVIDORES/ APLICAÇÕES		
BANCO DE DADOS		
COMUNICAÇÃO		
BACKUP		
SEGURANÇA DA INFORMAÇÃO		

9.3. GESTÃO

A CGTI é a unidade responsável por implementar, manter e melhorar o PCO e toda

documentação inerente.

9.4. EXECUÇÃO DO PLANO

ID	RESPONSÁVEL	PROCEDIMENTO
1	CGTI	Acionar o líder da equipe BACKUP para verificar a dimensão do impacto e possíveis desdobramentos do ocorrido. Preencher o documento "AVALIAÇÃO DE IMPACTO DE DESASTRE"
2	Comitê DR	Avaliar e decidir sobre o acionamento do plano e iniciar as ações de contingência. Divulgar a informação para as equipes envolvidas.
		Acionar a Equipe de Operações que deverá convocar reunião de emergência com os líderes do PRD e PAC.
3	Equipe de Operações	Coordenar prazos, orquestrar as ações de contingência e informar as equipes as ações de contingência com a priorização dos serviços essenciais.

9.5. ENCERRAMENTO DO PCO

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do Datacenter deverá emitir um parecer ao Comitê DR com o relato das atividades realizadas no PCO.

Outra ação é informar o retorno das atividades à equipe de comunicação.

Caso seja necessário, implementar procedimentos de aprimoramento dos respectivos planos.

PLANO DE ADMINISTRAÇÃO DE CRISES

10. PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

Este plano especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos, inerente ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

O PAC deve ser revisado, anualmente ou em caso de mudança na organização, atualizado e gerenciado pelo Gestor, ou por algum membro da CGTI.

10.1. OBJETIVO ESPECÍFICOS

São objetivos específicos do PAC:

- ✓ Garantir a segurança à vida das pessoas;
- ✓ Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise;
- ✓ Orientar os funcionários e demais colaboradores com informações, além de procedimentos de conduta; e
- ✓ Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido.

10.2. EQUIPES ENVOLVIDAS

A gestão de crises é estruturada em três níveis de atuação: Estratégico, Tático e Operacional.

NÍVEIS	RESPONSÁVEL	INSTRUÇÕES
1- ESTRATÉGICO	**CGTI**	São deliberadas as decisões estratégicas do negócio, as respostas aos incidentes de impactos críticos, a comunicação às alçadas superiores da organização e todas as partes interessadas durante a crise.
2- TÁTICO	**Líderes de Equipes**	No início é realizada a avaliação e resolução do incidente, que dependendo do tipo escolhem convocar ou não outras pessoas para identificação e tratamento do incidente. Neste nível decide-se pela ativação ou não do Plano de Continuidade em conformidade com as instruções da CGTI. Age na avaliação e resolução de incidentes, mantendo a informação atualizada a todos os envolvidos, analisando o impacto nas áreas afetadas, monitorando o incidente até a resolução. O nível tático tem autonomia de convocar a CGTI quando entender que o incidente tratado atingiu o cenário de crise.

NÍVEIS	RESPONSÁVEL	INSTRUÇÕES
3- OPERACIONAL	**Analistas e Técnicos**	Após o início da execução do PAC, os membros da equipe devem informar ao nível tático o status da resolução do incidente. São os responsáveis pela atualização do PCO e PRD de cada incidente definido como crítico para o CRCAP.

10.3. COMUNICAÇÃO

Na ocorrência de um desastre será necessário entrar em contato com diversas áreas, principalmente as afetadas. Enfim, deve informá-las de seu efeito na continuidade dos serviços e tempo de recuperação. A equipe de comunicação será responsável por contatar estas unidades, passar as informações pertinentes a cada grupo, setor ou segmento.

A comunicação com cada parte ocorrerá da seguinte forma:

10.3.1. COMUNICAR ÀS AUTORIDADES

A prioridade da equipe de comunicação será assegurar que as autoridades competentes sejam notificadas do incidente, principalmente se envolver risco às pessoas, fornecendo as seguintes informações de localização, natureza, magnitude e impacto do desastre.

Autoridade	Número paraContato	Data/Hora do Registro	Número da Ocorrência
Polícia Civil	197		
Polícia Miitar	190		
Bombeiros	193		
SAMU	192		

10.3.2. COMUNICAÇÃO APÓS UM DESASTRE

Ao término da reunião com os líderes do PRD e PCO, a equipe de comunicação elaborará um breve programa de comunicação para acionar as partes envolvidas e afetadas de modo a manter todos informados.Por fim, deve transmitir aos envolvidos a perspectiva dos esforços necessários para o reestabelecimento dos serviços inativos.

10.3.3. COMUNICAÇÃO COM OS FUNCIONÁRIOS

A equipe de comunicação deverá prover meio de contato específico para este fim, com intuito de que as unidades do CRCAP mantenham-se informadas da ocorrênciade um desastre e da inatividade dos serviços essenciais de TI.

Números de contato a serem disponibilizados:

Telefone: [redacted]
Contatos de E-mail: [redacted]

Telefone: [redacted]
Contatos de E-mail: [redacted]

Caso não haja conectividade ou linha telefônica disponível, as informações serão cedidas por meio de publicações de comunicação interna, aplicativos de mensagens instantâneas ou outra estratégia disponível no momento.

As informações a serem dadas irão se referir a:

- ✓ Se é seguro os usuários entrarem no ambiente afetado;
- ✓ Onde os usuários devem ir se não puderem ter acesso ao CRCAP;
- ✓ Quais serviços ainda estão disponíveis aos usuários; e
- ✓ Expectativas de trabalho durante o desastre.

10.3.4. COMUNICAR UNIDADES E SETORES DO CRCAP

- ✓ Acionar diretamente às Unidades Organizacionais (UO) afetadas pelo desastre e fornecer contatos;
- ✓ Descrever a natureza, impacto e abrangência da catástrofe;
- ✓ Informar as ações de contingência em andamento; e
- ✓ Esclarecer quais os processos/sistemas e serviços que são cobertos pelo plano de continuidade (serviços essenciais).

Unidade Organizacional / Setor	Número para Contato	Data/Hora do Contato	Local
[redacted]	[redacted]		
[redacted]	[redacted]		

10.3.5. COMUNICAR FORNECEDORES E PRESTADORES DE

SERVIÇO

LISTA DOS PRINCIPAIS FORNECEDORES	
Empresa: [redacted] Nº Contato: Email:	**Pessoa/Contato:** ________________ **Data/Hora Acionamento:** ____/____/______ ___:___:___
Empresa: [redacted] Nº Contato: Email:	**Pessoa/Contato:** **Data/Hora Acionamento:** ____/____/______ ___:___:___
Empresa: [redacted] Nº Contato: Email:	**Pessoa/Contato:** ________________ **Data/Hora Acionamento:** ____/____/______ ___:___:___
Empresa: [redacted] Nº Contato: Email:	**Pessoa/Contato:** ________________ **Data/Hora Acionamento:**
Empresa: [redacted] Nº Contato: Email:	**Pessoa/Contato:** ________________ **Data/Hora Acionamento:**
Empresa: [redacted] Nº Contato: Email:	**Pessoa/Contato:** ________________ **Data/Hora Acionamento:**
Empresa: [redacted] Nº Contato: Email:	**Pessoa/Contato:** ________________ **Data/Hora Acionamento:**
Empresa [redacted] Nº Contato: Email:	**Pessoa/Contato:** ________________ **Data/Hora Acionamento:**
Empresa: [redacted] Nº Contato: Email:	**Pessoa/Contato** [redacted] ________________ **Data/Hora Acionamento:**

10.3.6. COMUNICAR COLABORADORES EXTERNOS, CIDADÃOS E MÍDIA

A equipe de comunicação, em consonância com a Coordenadoria de Comunicação (CCOM) do CRCAP, deve fornecer informações pertinentes aos colaboradores externos: profissionais da contabilidade, cidadãos e demais autoridades competentes.

A equipe citada deve validar a situação de acordo com o cenário e, em seguida, publicar em meios oficiais e de ampla divulgação, com a concordância do Comitê DR e gestores do CRCAP, informações sobre o ocorrido.

10.4. ACIONAMENTO DA CRISE

O nível operacional (analistas e técnicos) comunica ao nível estratégico (CGTI) sobre o evento que pode evoluir para uma crise, então a CGTI aciona o nível tático (líderes de equipes) para que este avalie a gravidade do evento, depois deve acionar o Plano de Continuidade mais adequado. Caso o evento evolua para uma situação de crise, deve-se acionar o PAC, o nível tático juntamente com o nível estratégico convocarão o Comitê DR, e este, se necessário envolverá os demais Unidades Organizacionais de acordo com o evento.

Critérios para ativação do PAC:

- ✓ Incêndio no Centro de Processamento de Dados;
- ✓ Falta de energia no Centro de Processamento de Dados;
- ✓ Indisponibilidade dos sistemas; e
- ✓ Ataques por vírus ou *hackers*.

10.5. RETORNO DAS OPERAÇÕES

Comunicar a todas as partes supracitadas quando as operações retornarem à normalidade.

PLANO DE RECUPERAÇÃO DE DESASTRES

11. PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, todavia define as atividades prioritárias com o objetivo de reestabelecer o nível de operação dos serviços no ambiente afetado, dentro de um prazo tolerável.

11.1. OBJETIVO ESPECÍFICOS

São objetivos específicos do PRD:

- ✓ Avaliar danos aos ativos e conexões do Datacenter e prover meios para sua recuperação; e
- ✓ Reestabelecer o Datacenter dentro do prazo tolerável.

11.2. EXECUÇÃO DO PLANO

CENÁRIO 1:	Indisponibilidade de equipamentos do Centro de Processamento de Dados.
Área Responsável pelo Plano:	Departamento de Informática
Responsável pelo Plano:	[redacted]
Contato:	[redacted]; [redacted]
Objetivo:	Identificar os ativos danificados e contatar os fornecedores para realizar a substituição ou reparo.
Ambiente de Contingência:	Conselho Regional de Contabilidade do Amapá
Prazo de Operação:	Até 48h
CONTRAMEDIDAS/ PREMISSAS:	
CONTRAMEDIDAS	**PREMISSAS**
Contrato Vigente	Contrato de manutenção com substituição de peças.
PROCEDIMENTO DE CONTINUIDADE	
PROCEDIMENTO 001	Reparo de equipamentos.
INSTRUÇÕES	
1	Verificar a falha do equipamento.
2	Entrar em contato com o fornecedor.
3	O fornecedor deve prover novo equipamento ou reparar o usado.
4	Após a instalação do novo equipamento ou reparo do usado, o Departamento de Informática deve comunicar a equipe que o sistema está operante e encerrar o incidente.

PLANO DE TESTES E VALIDAÇÃO

12. PLANO DE TESTES E VALIDAÇÃO (PTV)

Cumprindo o propósito de reavaliar os procedimentos planejados visando a melhoria contínua, o Plano de Continuidade será testado e validado em reunião entre os líderes de cada subplano anualmente ou com a insurgência de novos fatores de risco, mudança na análise de impacto, ou com a inclusão de um novo serviço no Plano de Continuidade.

12.1. TIPOS DE TESTES E VALIDAÇÃO

A execução dos passos planejados deve ser registrada, contendo data de execução, tipo do teste, descrição de motivo e *status*, respeitando os seguintes critérios a serem informados no registro:

- ✓ **Teste de mesa: Geralmente realizado em uma mesa de reunião.**
  Teste de complexidade simples no qual é realizada uma análise (crítica dos ensaios de execução) dos procedimentos e informações descritas, com o objetivo de atualizar e/ou validar os procedimentos e as informações contidas no plano.

- ✓ **Simulação no ambiente: Simular uma situação real de interrupção.**
  Teste de complexidade média no qual uma situação "artificial" é criada. Por exemplo, é realizada a parada de um processo em horários diferentes das operações diárias (finais de semana, após expediente, etc.), sendo o resultado utilizado para validar se os planos possuem as informações necessárias e suficientes, de forma a permitir recuperação de determinado arranjo de contingência ou processo com sucesso.

- ✓ **Teste real: testar em tempo real os Planos de Continuidade, o que envolve alta complexidade.**
  Os testes gerados devem ser documentados e validados pelos responsáveis, pois esses indicarão os procedimentos de cada plano e o resultado do teste. O programa de testes deve ser consistente com o escopo dos subplanos, incluindo as devidas considerações legais e/ou normativas. O ambiente de testes será controlado de maneira a não interromper as atividades principais.

SISTEMAS E SERVIÇOS HOSPEDADOS NO CRCAP

- Acervo Digital – Banco de fotos do CRCAP;
- Banco de Palestrantes;
- Bens patrimoniais;
- Carteira Digital;
- Carteira Fisica;
- CNAI;
- CNPC;
- COAF;
- Consulta de cursos e eventos EPC;
- CRE;
- DECORE;
- EQT (Sistema de Exames);
- E-sic;
- GLENIF – Site;
- Intranet CRCAP;
- Portal da Transparência;
- Portal do CRCAP;
- PVCC – Site e sistema;
- QUANTOS SOMOS - Dados Estatísticos de profissionais;
- Revista Brasileira de Contabilidade (RBC);
- Replicação de dados dos CRCs – SPW;
- SEI;
- Servidor de Arquivos (J, K, L e Arquivo Digital);
- Servidor de e-mail;
- Sispag – Sistema de pagamentos;
- Sistemas administrativos – Contabilidade, Financeiro, Diárias e Passagens, Protocolo, Plano de Trabalho e o Sistema de Estoque;
- Sistema de Balancetes – CCI;
- Sistema CNAI- PJ;
- Sistema de Comunicação;
- Sistema de Consulta Cadastral nacional dos profissionais;
- Sistema de emissão de certificados aprovados nos exames de suficiência;
- Sistema EPC;
- Sistema de Eventos;
- Sistema GIT e RedMine – TI;
- Sistema de helpdesk;
- Sistema Jira – TI;
- Sistema de ouvidoria;
- Sistema de Reembolso – CDPO;
- Sistema de Registro;
- SPER;
- SRE - Sistema de Resoluções; e
- STP – Sistema de tramitação de processo – SPW.

GLOSSÁRIO

CCI	Coordenadoria de Controle Interno
CCOM	Coordenadoria de Comunicação
CDPO	Sistema de Reembolso
CGTI	Coordenadoria de Gestão de TI
CFC	Conselho Federal de Contabilidade.
CNAI	Cadastro Nacional de Auditores Independentes
CNAI-PJ	Cadastro Nacional de Auditores Independentes – Pessoa Jurídica
CNPC	Cadastro Nacional de Peritos Contábeis
COAF	Conselho de Controle de Atividades Financeiras
CPD	Centro de Processamento de Dados
CRCs	Conselhos Regionais de Contabilidade
CRE	Comitê Administrador do Programa de Revisão Externa de Qualidade
CSI	Comitê de Segurança da Informação
Decore	Declaração Comprobatória de Percepção de Rendimentos
Deinf	Departamento de Informática
Direx	Diretoria Executiva
DOU	Diário Oficial da União
e-SIC	Sistema Eletrônico de Informações ao. Cidadão
EPC	Educação Profissional Continuada
EQT	Exame de Qualificação Técnica
Glenif	*Grupo Latinoamericano de Emisores de Normas de Información Financiera*
LAN	Local area network
N/D	Não definido
PAC	Plano de Administração de Crises
PCN	Plano de Continuidade de Negócios
PCO	Plano de Continuidade Operacional
PCTI	Plano de Continuidade de Tecnologia da Informação
PRD	Plano de Recuperação de Desastres
PTV	Plano de Testes e Validação
PVCC	Programa de Voluntariado da Classe Contábil
RBC	Revista Brasileira de Contabilidade
RPO	Ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura
RTO	Período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção
SAMU	Serviço de Atendimento Móvel de Urgência
SEI	Sistema Eletrônico de Informações
Sispag	Sistema de Pagamentos
SPER	Sistema de Processo Eletrônico de Registro
SPW	Spiderware – SPW Informática
SRE	Sistema de Resoluções
STP	Sistema de Tramitação de Processo
TI	Tecnologia da Informação
WAN	*Wide Área Network*