Universidade Federal do Rio Grande do Norte
Superintendência de Tecnologia da Informação

PLANO DE CONTINUIDADE DE TI DA SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Conservação, ininterrupção dos sistemas essenciais de TI da Superintendência de Tecnologia da Informação da Universidade Federal do Rio Grande do Norte - UFRN.

Maio
2021

1. Sumário

HISTÓRICO DE VERSÕES 4
HISTÓRICO DE ALTERAÇÃO E INCLUSÃO 5
REGISTRO DE ACIONAMENTO DO PCTI 6
1. JUSTIFICATIVA 7
2. OBJETIVO 7
3. ABRANGÊNCIA E CONTROLE DE CÓPIAS 7
4. ESCOPO 7
5. SERVIÇOS ESSENCIAIS 8
6. ÁREA 10
7. PRINCIPAIS RISCOS 10
8. PAPÉIS E RESPONSABILIDADES 11
9. INVOCAÇÃO DO PLANO 12
10.MACROPROCESSO DO PCTI 13
11. ESTRATÉGIAS DE CONTINUIDADE 13
1.PLANO DE CONTINUIDADE OPERACIONAL (PCO) 16
2. OBJETIVO E ESCOPO 16
3. EQUIPES ENVOLVIDAS. 16
4. GESTÃO 16
5. EXECUÇÃO DO PLANO 16
A. AVALIAÇÃO DE IMPACTO DE DESASTRE 16
B. ACIONAMENTO DO PLANO 16
C. CONTINGÊNCIA DE WARM SITE T1 17
6. ENCERRAMENTO DO PCO 17
1.PLANO DE ADMINISTRAÇÃO DE CRISES (PAC) 19
2.OBJETIVO 19
3. EXECUÇÃO DO PLANO 19
A. COMUNICAÇÃO NA OCORRÊNCIA DE UM DESASTRE 20
3.A.1. COMUNICAR ÀS AUTORIDADES 20
B. COMUNICAÇÃO APÓS UM DESASTRE 20
3. B.1. COMUNICAÇÃO COM OS FUNCIONÁRIOS 20
3.B.2. COMUNICAR UNIDADES E SETORES DA UFRN 21
3.B.3. COMUNICAR FORNECEDORES E PRESTADORES DE SERVIÇO 21
3.B.4. COLABORADORES EXTERNOS, CIDADÃOS E MÍDIA 21
C. COMUNICAR RETORNO DAS OPERAÇÕES 21

4.ENCERRAMENTO DO PAC 22
1. PLANO DE RECUPERAÇÃO DE DESASTRES (PRD) 24
2. OBJETIVO E SCOPO 24
3. EXECUÇÃO DO PLANO 24
A. IDENTIFICAR ATIVOS DANIFICADOS 24
B. IDENTIFICAR ACESSOS INTERROMPIDOS 24
C. LISTAR SERVIÇOS DESCONTINUADOS 24
D. ELABORAR CRONOGRAMA DE RECUPERAÇÃO 24
3.D.1. SUBSTITUIÇÃO DE ATIVOS E EQUIPAMENTOS 25
3.D.2. RECONFIGURAÇÃO DE ATIVOS E EQUIPAMENTO 25
3.D.3. TESTE DE AMBIENTE 25
3.D.4. RECUPERAR DADOS DO BACKUP 26
4. ENCERRAMENTO DO PRD 26
10. VALIDAÇÃO E TESTE DE PCTI 27
11. APROVAÇÃO DO PCTI 28

HISTÓRICO DE VERSÕES

Versão	Descrição	Responsável
1.0	Criação da primeira versão do PCTI	Julio Cesar R.L. Gonçalves
1.0	Aprovação	28/05/2021 – Comitê de Governança, Riscos e Controles
1.1	Revisão	
1.2	Publicação	16/06/2021 – Comitê de Governança, Riscos e Controles

HISTÓRICO DE ALTERAÇÃO E INCLUSÃO

Data	Inclusão/Alteração	Modificado por

REGISTRO DE ACIONAMENTO DO PCTI

Data/Hora ___/___/___ Início: ____:____	Data/Hora ___/___/___ Fim ____:____
Descrição	
Resultado	

Data/Hora ___/___/___ Início: ____:____	Data/Hora ___/___/___ Fim ____:____
Descrição	
Resultado	

Data/Hora ___/___/___ Início: ____:____	Data/Hora ___/___/___ Fim ____:____
Descrição	
Resultado	

1. JUSTIFICATIVA

Uma vez que falhas nos serviços de TI impactam diretamente na continuidade da prestação dos serviços, almeja-se com este plano prover medidas de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais utilizados pelas comunidades acadêmica e administrativa da UFRN, em casos de incidentes graves ou desastres.

2. OBJETIVO

O objetivo desse plano é estabelecer as ações e procedimentos necessários para garantir que os serviços essenciais sejam assegurados no plano de continuidade operacional. A paralisação considerada se dá em função de qualquer incidente ou desastre de grandes proporções. Os cenários de recuperação contemplados nesta versão do plano são para prover restabelecimento destes serviços.

3. ABRANGÊNCIA E CONTROLE DE CÓPIAS

Este plano é de propriedade da Superintendência de Tecnologia da Informação da Universidade Federal do Rio Grande do Norte (STI-UFRN). Em função das informações sensíveis nele contidas, este documento está disponível apenas para as pessoas designadas como membros de um ou mais grupos funcionais aqui indicados, ou quem desempenhe função direta no processo de continuidade operacional. Pelo menos um dos integrantes dos grupos funcionais relacionados deve receber e manter atualizadas duas cópias deste documento, uma física na área a que pertence e outra na nuvem de documentos da STI.

4. ESCOPO

O Plano de Continuidade de TI (PCTI) abrange as estratégias necessárias à continuidade dos serviços de TIC essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a STI (Superintendência de Tecnologia da Informação da UFRN).

Este plano pode ser executado tanto no âmbito da STI isoladamente, ou como parte de um Plano de Continuidade de Negócio (PCN) da UFRN.

5. SERVIÇOS ESSENCIAIS

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

Serviço	Criticidade	RPO*	RTO*	Descrição
Firewall Fortigate	Crítico	3 dias	4 horas	Sem acesso a redes, sistemas e internet
Firewall Linux	Crítico	3 dias	4 horas	Sem acesso a redes, sistemas e internet
DHCP	Crítico	24 horas	4 horas	Sem acesso a redes, sistemas e internet
DNS	Crítico	24 horas	4 horas	Sem acesso a redes, sistemas e internet
Email	Alta	24 horas	4 horas	Serviço de e-mail indisponível
SIPAC	Crítico	24 horas	4 horas	Sistema indisponível
SIGRH	Alta	24 horas	4 horas	Sistema indisponível
SIGPP	Baixo	24 horas	4 horas	Sistema indisponível
Memo	Médio	24 horas	4 horas	Sistema indisponível
SIGAA	Crítico	24 horas	9 horas	Sistema indisponível
SIGeleição	Crítico	24 horas	9 horas	Sistema indisponível
Intellectus	Baixo	24 horas	9 horas	Sistema indisponível
SIGAdmin	Médio	24 horas	4 horas	Sistema indisponível
CAUS	Médio	24 horas	4 horas	Sistema indisponível
Olar	Baixo	24 horas	4 horas	Sistema indisponível
SIGEventos	Baixo	24 horas	4 horas	Sistema indisponível
Cronus	Crítico	24 horas	2 horas	Sistema indisponível
Acervus	Baixo	24 horas	2 horas	Sistema indisponível
Gestore	Baixo	24 horas	2 horas	Sistema indisponível
SIEDI	Baixo	24 horas	2 horas	Sistema indisponível
EMEI	Baixo	24 horas	2 horas	Sistema indisponível
Reuse	Baixo	24 horas	2 horas	Sistema indisponível
SIGProjetos	Baixo	24 horas	2 horas	Sistema indisponível
Sites	Alta	24 horas	4 horas	Serviço de hospedagem indisponível

VPN	Alto	24 horas	4 horas	Acesso remoto via VPN indisponível
VoIP	Crítico	24 horas	4 horas	Telefonia fixa indisponível
LDAP	Crítico	7 dias	4 horas	Sem acesso a VPN, rede sem fio, Federação Café, Periódicos CAPES
Radius	Crítico	7 dias	4 horas	Sem acesso a rede sem fio
EduROAM	Alto	7 dias	24 horas	Sem acesso a rede sem fio
Fed. Café	Alto	7 dias	24 horas	sem acesso ao Mconf, periódicos CAPES
Controladoras Wi-Fi	Alto	24 horas	4 horas	Rede sem fio indisponível
Site CeTRIS	Médio	24 horas	8 horas	Repositório de informações de segurança do site indisponível
Emissão Certificados Sites (EXT: RNP)	Médio	4 horas	24 horas	Sem emissão/revogação de certificados
Emissão certificados pessoais (EXT: RNP)	Baixo	4 horas	24 horas	Sem emissão/revogação de certificados

RPO(Recovery Point Objective) Ponto de Recuperação do Objetivo: ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura.

RTO (Recovery Time Objective) Tempo de Recuperação do Objetivo: período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção.
Impacto: Irrelevante, Baixo, Médio, Alto, Crítico ou N/D(não definido)

CONSIDERAÇÕES:

i. Os sistemas SIGs UFRN essenciais estão detalhados nos documentos anexo do PCTI: MAPEAMENTO DOS SERVIÇOS ESSENCIAIS.

ii. A priorização dos serviços essenciais, os níveis de impacto no negócio e tempos toleráveis de recuperação serão definidos a partir da Análise de Impacto de Negócio (AIN).

6. ÁREA

O PCTI será administrado, avaliado e acionado no âmbito da Superintendência de Tecnologia da Informação da UFRN (STI) tendo sua manutenção, organização e melhoria revistas e atualizadas periodicamente pelas Coordenações da STI.

7. 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 abaixo define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
01-Interrupção de Energia	Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 12 horas. Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndio e infiltrações. Impossibilidade de acionar o Grupo Moto-gerador no momento de uma queda de energia.
02 - Falha Climatização da sala segura	Superaquecimento dos ativos devido a falha no dimensionamento de carga na sala segura
03 - Indisponibilidade de rede/circuitos	Rompimento de fibra óptica decorrente da execução de obras públicas,desastres ou acidentes.
04 - Falha humana	Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível.
05 - Ataques internos (funcionários insatisfeitos)	Ataque aos ativos do DataCenter.
06 - Incêndio	Incêndios que comprometam os hardwares.
07- Desastres Naturais	Terremotos, tempestades, alagamentos e etc.
08 - Falha de hardware/Software	Falha que necessite reposição de peça ou correção de aplicações, cujo reparo ou aquisição dependa de processo licitatório ou de suporte do fabricante.
09 - Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou a configuração dos serviços essenciais.

8. PAPÉIS E RESPONSABILIDADES

COMITÊ DE DISASTER/RECOVERY (DR):

- Avaliar o plano periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.

- Inclui autoridades em nível institucional e tomadores de decisão da STI.

EQUIPE DE INSTALAÇÕES/AMBIENTE:

- Responsável pelas instalações físicas que abrigam sistemas de TI e pela garantia que as instalações de alternativa são mantidas adequadamente. Avalia os danos e supervisiona os reparos para o local principal no caso da localização primária sofra destruição ou danos.

- O líder desta equipe administrará e manterá o Plano de Recuperação de Desastres.

EQUIPE DE CONECTIVIDADE:

- Avaliar os danos específicos de qualquer infra-estrutura de rede, fornecer dados e conectividade de rede incluindo WAN, LAN e conexões de telefonia VoIP internamente na UFRN ou de infraestrutura externa junto aos prestadores de serviço.

EQUIPE DE SERVIDORES/APLICAÇÕES:

- Fornecer a infraestrutura de servidores físicos e virtuais necessária para que a TI execute suas operações e processos essenciais durante um desastre.

- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos dos negócios em caso de e durante um desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TI DR conforme necessário.

EQUIPE DE OPERAÇÕES:

- Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar todos os funcionários necessários, da Superintendência de Tecnologia da Informação da UFRN (STI) na solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas à sua atuação.

- O líder desta equipe administrará e manterá o Plano de Continuidade Operacional.

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.

- O líder desta equipe administrará e manterá o Plano de Administração de Crise.

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. Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.

9. INVOCAÇÃO DO PLANO

O PCTI será acionado quando da ocorrência de algum dos cenários de desastres, a insurgência ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada.

O plano também poderá ser invocado em casos de testes ou por determinação do COMITÊ DE DR em conjunto com a alta administração da Superintendência de Tecnologia da Informação da UFRN (STI).

Os integrantes da EQUIPE DE COMUNICAÇÃO serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente, caso seja possível. A árvore de acionamento de contatos consta no arquivo Anexo I.

10. MACROPROCESSOS DO PCTI

O PCTI tem seus macroprocessos definidos nas atividades a seguir e se desmembra em planos específicos para cada área de atuação quando da ocorrência de um desastre.

1) Identificação e declaração de desastres

2) Ativação do processo de DR

3) Comunicar o desastre

4) Avaliação da corrente e prevenção de mais danos

5) Ativação da solução de Contingência

6) Estabelecer operações de TI

7) Reparação e reconstrução da instalação principal

8) Retorno das operações para Ambiente principal

Os sub-planos do PCTI consistem em:

- Plano de Continuidade Operacional (PCO):
  - Garantir a continuidade dos serviços essenciais de TI críticos na ocorrência de desastres, enquanto recupera-se o ambiente principal.

- Plano de Administração de Crise (PAC):
  - Definitividade das equipes envolvidas e orquestrar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos até a superação da crise.

- Plano de Recuperação de Desastre (PRD):
  - Planejar e agir para que, uma vez controlada a contingência e passada a crise, a TI da Superintendência de Tecnologia da Informação da UFRN (STI), retome seus níveis originais de operação no ambiente principal.

11. ESTRATÉGIAS DE CONTINUIDADE

A estratégia de continuidade para o cenário atual da TI e serviços essenciais acadêmicos e administrativos, está estabelecida da seguinte forma:

TIPO : Warm site T1

DESCRIÇÃO:

Replicação e cópias de backup dos sistemas essenciais armazenadas em local alternativo:

- Data Center do Instituto Metrópole Digital.
- Ter infraestrutura de hardware no site secundário, para disponibilizar os serviços.
- Link redundante ativo
- Downtime médio-baixo

AÇÕES DE CONTINGÊNCIA/RECUPERAÇÃO:

Mapear perda de dados e ativos, restabelecer toda a estrutura afetada e, após o ambiente principal estar operacional, prover a recuperação dos dados em backups.

OBSERVAÇÕES:

- As ações de contingência e recuperação são detalhadas nos sub planos a seguir.

PLANO DE CONTINUIDADE OPERACIONAL

1. PLANO DE CONTINUIDADE OPERACIONAL (PCO)

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

2. OBJETIVO E ESCOPO

É escopo deste plano garantir ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre, tratando-se apenas das ações de contingência definidas na estratégia.

São objetivos PCO:

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

D. Definir os formulários, check lists e relatórios a serem entregues pelas equipes ao executar a contingência.

3. EQUIPES ENVOLVIDAS.

Equipe de: operações, Backup, instalações/Ambientes, conectividade.

4. GESTÃO

A STI é a unidade responsável por implementar, manter e melhorar o PCO e toda documentação inerente.

5. EXECUÇÃO DO PLANO

A. Avaliação de Impacto de Desastre

Identificada a ocorrência de um incidente ou crise, o Líder da Equipe de Operação e Backup deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido. O documento Anexo I “AVALIAÇÃO DE IMPACTO DE DESASTRE” deve ser preenchido e submetido ao Comitê de DR para decisão sobre o acionamento do plano e início das ações de contingência.

Divulgar a informação a todas as equipes envolvidas.

B. Acionamento do plano

Dado o aval pelo COMITÊ DE DR acionamento do plano a EQUIPE DE OPERAÇÕES convocará reunião de emergência com os líderes do PRD e PAC com o intuito de:

- Coordenar prazos e orquestrar as ações de contingência.
- Informar as equipes ações de contingência com a priorização dos serviços essenciais.

C. Contingência de Warm Site T1

Devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial.

6. ENCERRAMENTO DO PCO

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter deverá ser emitido um parecer ao comitê relatando as atividades realizadas neste PCO. Tabela no arquivo Anexo I.

Informar à equipe de COMUNICAÇÃO o retorno das atividades.

PLANO DE ADMINISTRAÇÃO DE CRISES

1.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, inerentes ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

2. OBJETIVO

Instituir e documentar procedimentos de comunicação, respostas e soluções frente ao(s) incidente(s) que possam trazer impactos negativos a STI-UFRN junto aos seus principais públicos de interesse, prejudicando sua imagem institucional e suas operações.

Definir o procedimento para identificação e tratamento de crises, bem como as atividades das equipes envolvidas e sua dinâmica de atuação.

Integrado ao Plano de Gerenciamento de Incidentes, ao Plano de Recuperação de Desastres, ao Plano de Continuidade Operacional e outros procedimentos da STI-UFRN, o Plano de Administração de Crises contribui para aumentar sua capacidade de atuar de maneira organizada e eficaz, frente a ameaças de qualquer natureza, garantindo a sustentabilidade da prestação de serviços essenciais, de ensino, pesquisa e extensão. A STI-UFRN deve trabalhar de acordo com sua realidade, mapeando os riscos e ameaças, bem como definindo os critérios de crise, que podem identificar os pontos iniciais (Incidentes) causadores das crises e indicar o modo de tratar esses riscos.

Os objetivos específicos do PAC:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos do incidente e estimular o esforço em conjunto para superação da crise.
- Orientar os funcionários e demais colaboradores com

  informações e procedimentos de conduta.

- Informar a sociedade em tempo e com esclarecimentos

  condizentes com o ocorrido.

3. EXECUÇÃO DO PLANO

A. Comunicação na ocorrência de um Desastre

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

A comunicação com cada parte ocorrerá da seguinte forma:

3.A.1.COMUNICAR ÀS AUTORIDADES

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

Autoridade	Número	Data/Hora do Registro	Num. Ocorrência
Polícia	190		
Bombeiros	193		
SAMU	192		

B. Comunicação após um Desastre

Após reunião com 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 bem informados e passar a todos a perspectiva dos esforços necessários para o restabelecimento dos serviços inativos.

3.B.1.COMUNICAÇÃO COM OS FUNCIONÁRIOS

A equipe de comunicação deverá prover um meio de contato específico para este fim, com intuito de que os funcionários da Superintendência de Tecnologia da Informação da UFRN (STI) mantenham-se informados da ocorrência de um desastre e da inatividade dos serviços essenciais de TI.

Números de Contato a serem disponibilizados:

Telefone: (84) 33422210 ou (84)99193-6477

Contatos de E-mail: suporte@info.ufrn.br redes@info.ufrn.br

Central de Serviços (service desk)

*Caso não haja conectividade ou linha telefônica disponível, ceder essas informações por meio de publicações, ou outra estratégia definida no momento.

As informações a serem dadas irão se referir a:

- Se é seguro para eles entrarem no ambiente afetado
- Onde eles devem ir se não puderem ter acesso ao Prédio da STI..
- Que serviços ainda estão disponíveis para eles
- Expectativas de trabalho durante o desastre

3.B.2.COMUNICAR UNIDADES E SETORES DA UFRN

- Acionar diretamente às unidades afetadas pelo desastre e fornecer contato.
- Natureza, impacto e abrangência da catástrofe.
- Ações de contingência em andamento.
- Processos/sistemas e serviços cobertos pelo plano de continuidade (serviços essenciais)

As informações constam no arquivo Anexo I deste documento.

3.B.3.COMUNICAR FORNECEDORES E PRESTADORES DE SERVIÇO

As informações constam no arquivo Anexo I deste documento.

3.B.4.COLABORADORES EXTERNOS, CIDADÃOS E MÍDIA

A equipe de comunicação, em consonância com a Assessoria de Comunicação da UFRN, deverá fornecer informações pertinentes aos colaboradores externos: cidadãos e outros órgãos.

- Validar a situação passada de acordo com o cenário
- Buscar publicar em meios oficiais e de ampla divulgação, com aval do comitê de continuidade e institucional, informações sobre o ocorrido.

Colaborador/ Rede/ Empresa / Pessoa	Contato	Publicação	E-mail

C. COMUNICAR RETORNO DAS OPERAÇÕES

3.C.1. Comunicar a todas as partes acima supracitadas quando ocorrer o retorno das operações à normalidade

4. ENCERRAMENTO DO PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do Datacenter a EQUIPE DE COMUNICAÇÃO entrará em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

Compor relatório com relação das atividades necessárias após a ocorrência do desastre como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

PLANO DE RECUPERAÇÃO DE DESASTRES

1. Plano De Recuperação de Desastres (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para restabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

2. OBJETIVO E ESCOPO

É escopo deste plano garantir o retorno das operações do ambiente principal depois da ocorrência de uma crise ou cenário de desastre, tratando-se apenas dos ativos, conexões e configurações deste ambiente.

São objetivos PRD:

A. Avaliar danos aos ativos e conexões do datacenter e prover meios para sua recuperação.

B. Evitar desdobramentos de outros incidentes no site principal.

C. Restabelecer o datacenter dentro do prazo tolerável

3. EXECUÇÃO DO PLANO

A. Identificar ativos danificados

As equipes de INSTALAÇÃO/BACKUP/SERVIDORES/ CONECTIVIDADE deverão identificar e listar todos os ativos danificados da ocorrência do desastre. As informações de cada ativo que encontram-se no prédio da Superintendência de Tecnologia da Informação da UFRN (STI)

B. Identificar acessos interrompidos

A equipe de CONECTIVIDADE deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, rede WAN ou com o provedor de serviços.

C. Listar serviços descontinuados

A equipe do PRD deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento do Comitê de DR.

O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de proxy, dns, rotas, vlans e etc.

D. Elaborar cronograma de recuperação

O líder do PRD após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação das aplicações levando em consideração:

? A priorização dos serviços essenciais, ou de acordo com determinação de nível institucional.

? O RTO definido para cada serviço essencial.

? A força de trabalho disponível.

3.D.1.Substituição de ativos e equipamentos

Em caso de perda de ativos, deverá ser imediatamente informado ao comitê de DR a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço comunicando ao COMITÊ DE DR se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.

A equipe de INSTALAÇÕES deve verificar quais ativos foram danificados estão cobertos por garantia e se poderá ser acionada neste caso através da lista de fornecedores [3.B.3].

As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC.

3.D.2.Reconfiguração de ativos e equipamento

A equipe de Instalações deverá verificar que as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Caso não estejam, prover cronograma estimado para configurar estes ativos informando à EQUIPE DE COMUNICAÇÃO e COMITÊ DE DR.

3.D.3.Teste de ambiente

O ambiente principal do data center antes do recovery dos dados do backup deverá ser testado a fim de garantir que o processo de recuperação ocorra conforme o planejado.

Os testes incluem:

- Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre ref.: mapeamento serviços essenciais.
- Validar as configurações

Sistema	**Instrução**	**Duração**	**Observação**	**Resultado**
1				□
2				□
3				□
4				□
5				□
6				□
7				□
8				□

3.D.4.Recuperar dados do backup

Proceder à recuperação dos dados para as aplicações, seja do storage ou fitas de backup.

4. ENCERRAMENTO DO PRD

Ao término do procedimento de recuperação, as informações da recuperação de serviços serão consolidadas em parecer específico informando horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

10.VALIDAÇÃO E TESTE DE PCTI

O PCTI será testado e validado em reunião entre os líderes de cada subplano a cada semestre 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.

Tipos de testes a serem realizados:

- Teste de mesa:
- Caminho percorrido: Assegurar que cada integrante de processo crítico se familiarize com o PCTI
- Simulação: Simular uma situação real de interrupção.

Status:

- Programado
- Executado
- Planejado
- Agendado

Data	Tipo	Motivo	Status

11. APROVAÇÃO DO PCTI

A versão 1 do PCTI fica aprovada em 28/05/2021 por deliberação do Comitê de Governança, Riscos e Controles.