Plano de Continuidade de Negócios

Recuperação de Desastres

e

Serviços de TI

	Política	Código	POL-05
PREFEITURA DE SÃO JOSÉ DO RIO PARDO	Plano de Continuidade de Negócios / Recuperação de Desastres e Serviços de TI	Classificação	Pública
		Revisão	0

SUMÁRIO

1. INTRODUÇÃO

O Plano de Continuidade de Negócios (PCN) assegura à PREFEITURA DE SÃO JOSÉ DO RIO PARDO a continuidade de seus processos em caso de paralisação decorrente de sinistro de um ou mais processos considerados críticos, devendo estabelecer cenários de situações inesperadas ou incidentes, quer sejam operacionais, desastres ou crises.

O plano de continuidade atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos, tendo o dever de gerenciá-los, dando a devida atenção para:
a. alternativas estratégicas, táticas e operacionais para responder à interrupção;
b. prevenção de novas perdas ou indisponibilidade de atividades prioritárias;
c. detalhes sobre como e em que circunstâncias a prefeitura irá se comunicar com as partes interessadas.

2. OBJETIVO

Almeja-se com este Plano de Continuidade de Negócios (PCN), promover estratégias e medidas de proteção eficazes e rápidas para os processos críticos de TI, a fim de garantir sua preservação após a ocorrência de um desastre, até a retomada em tempo hábil.

3. ESCOPO

Esta política se aplica aos recursos computacionais e/ou sistêmicos para o perfeito funcionamento da PREFEITURA MUNICIPAL DE SÃO JOSÉ DO RIO PARDO, incluindo sistemas, processos e pessoal, e abrange todas as ameaças potenciais que podem interromper as operações organizacionais, que são de responsabilidade do departamento de Tecnologia da Informação.

4. TERMOS E DEFINIÇÕES

Continuidade de Negócios (CN): Capacidade de uma organização para continuar suas operações essenciais durante e após um incidente ou interrupção significativa.

Recuperação de Desastres (RD): Processo de restauração de sistemas, dados e infraestrutura após um desastre ou interrupção que afeta as operações normais da organização.

Plano de Continuidade de Negócios (PCN): Documento que descreve os procedimentos, processos e responsabilidades para manter a continuidade das operações críticas durante e após um incidente.

Plano de Recuperação de Desastres (PRD): Documento que descreve os procedimentos e processos para restaurar sistemas, dados e infraestrutura após um desastre ou interrupção.

Ponto de Recuperação Objetivo (RPO - Recovery Point Objective): O período de tempo aceitável durante o qual a perda de dados pode ocorrer como resultado de um incidente antes

que os sistemas e serviços precisam ser restaurados.

Ponto de Tempo Objetivo (RTO - Recovery Time Objective): O período de tempo máximo permitido para a recuperação de sistemas, dados e serviços após um incidente para garantir a continuidade das operações.

Teste de Continuidade de Negócios e Recuperação de Desastres: Processo planejado para avaliar a eficácia dos planos de continuidade de negócios e recuperação de desastres por meio de simulações e exercícios práticos.

Avaliação de Riscos: Processo sistemático para identificar, avaliar e priorizar os riscos potenciais que podem afetar a continuidade das operações e a recuperação de desastres da organização.

Equipe de Resposta a Incidentes: Grupo designado de indivíduos responsáveis por coordenar e executar as ações necessárias para responder a incidentes e garantir a continuidade das operações.

Backup e Recuperação de Dados: Processo de cópia de dados críticos e sua restauração em caso de perda ou corrupção, como parte dos planos de continuidade de negócios e recuperação de desastres.

5. DIRETRIZES

O PCN atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos, provendo quais as ações serão realizadas em cada etapa do plano.

Este plano divide-se em outras 4 (quatro) etapas, as quais são:

1. **Plano de Administração de Crises (PAC) -** Define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência;

2. **Plano de Contingência (PC) -** Define as necessidades e ações mais imediatas. Deve ser utilizado somente quando todas as prevenções tiverem falhado;

3. **Plano de Recuperação de Desastres (PRD) -** Determina o planejamento para que, uma vez controlada a contingência e passada a crise, sejam retomados os níveis originais de operação e;

4. **Plano de Continuidade Operacional (PCO) -** Seu objetivo é restabelecer o funcionamento dos principais ativos que suportam as operações da organização, reduzindo o tempo de queda e os impactos provocados por um eventual incidente.

Dentre os objetivos do PCN, destacam-se os seguintes procedimentos:

a) Identificar todos os processos deTI, definindo atividades críticas e classificá-las.

b) Identificar e documentar os riscos que possam comprometer a continuidade das atividades críticas;
c) Identificar ameaças, vulnerabilidades e estimar os riscos;
d) Identificar controles existentes;
e) Identificar, documentar e avaliar os possíveis impactos à continuidade das atividades críticas, caso tais riscos se concretizem;
f) Determinar e calcular o tempo e o custo de parada e da recuperação do negócio;
g) Definir, implementar e manter um processo formal e documentado para a Análise de Impacto nas atividades;
h) Avaliação dos impactos de não realização das atividades críticas ao longo do tempo;
i) Fixação dos prazos de forma priorizada para a retomada das atividades, em um nível mínimo de execução tolerável, levando em consideração o tempo em que os impactos da interrupção tornem-se inaceitáveis;
j) Identificação de interdependências e recursos que suportam as atividades, incluindo fornecedores, terceiros e demais partes interessadas relevantes;
k) Determinar estratégias de continuidade das atividades adequada para proteger, estabilizar, continuar, retomar e recuperar as atividades prioritárias, bem como suas interdependências e recursos de apoio (Plano de Administração de Crises);
l) Estabelecer níveis adequados de autoridade e competência, no intuito de assegurar a comunicação efetiva às partes interessadas, bem como assegurar a continuidade das atividades críticas (Plano de Continuidade Operacional);
m) Viabilizar a continuidade e a recuperação das atividades críticas, em caso de interrupção (Plano de Recuperação de Desastres e Contingência);
n) Realizar treinamentos e avaliações do PCN periodicamente para garantir a manutenção e o bom funcionamento dos planos de continuidade;
o) Realizar testes para garantir a eficiência da continuidade das operações;
p) Promover a conscientização dos servidores;
q) Identificar oportunidades para melhorar a continuidade das operações.

6. MODELO DO PLANO (PDCA)

Os planos aqui definidos seguirão o Modelo “PLAN-DO-CHECK-ACT” (PDCA) para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente a eficácia do Sistema.

Modelo PDCA: O modelo PDCA ajudará na melhoria contínua do Plano de Continuidade de Negócios:

a) PLAN (estabelecer) - Seguir uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimento pertinentes para a melhoria da continuidade das atividades, de forma a ter resultados alinhados com os objetivos.
b) Do (Implementar e operar) - Implementar e operar a política de continuidade de negócios, controles, processos e procedimentos.
c) CHECK (Monitorar e analisar criticamente) - Monitorar e analisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a

administração para análise crítica, definir e autorizar ações de melhorias e correções.
d) ACT (Manter e Melhorar) - Manter e melhorar o PCN, tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica da administração e reavaliando o escopo, as políticas e objetivos de continuidade das atividades.

Para cada uma das etapas, deverá ser feito Planos de Ações, e estes deverão ser elaborados assim que dar-se os ocorridos, com base na sua temporalidade e impacto. Estes devem formar um log ou registro de ações, para que para cada acontecimento seja possível verificar o que foi feito em outros momentos similares.

7. INVOCAÇÃO DO PLANO

O presente plano será acionado quando houver ocorrência de algum desastre, na ocorrência de um risco não conhecido ou caso uma vulnerabilidade tenha grande probabilidade de ser explorada. Também poderá ser acionado o plano quando ocorrer a necessidade de testes ou por determinação do PREFEITURA DE SÃO JOSÉ DO RIO PARDO.

8. PRINCIPAIS RISCOS

O PCN foi elaborado para ser acionado quando houver alguma ocorrência de desastres que apresentem riscos à continuidade das atividades ou serviços essenciais. Abaixo segue o quadro que define estes riscos, bem como aponta quais os parâmetros para reportar as possíveis causas das ocorrências.

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
Interrupção de energia elétrica	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-circuito, incêndio e infiltração
Indisponibilidade de rede/circuitos	Rompimento de fibra ótica decorrente de execução de obras públicas, desastres ou acidentes
Falha humana	Qualquer ato causado por negligência, imprudência e/ou imperícia
Ataques internos (servidor mal intencionado)	Ataques aos ativos do Data Center ou aos servidores internos

Incêndio	Incêndios com classificação A, B, C, D e K (Classificação feita pelo Corpo de Bombeiros)
Desastres naturais	Afundamento, colapso, ciclones, tufões, tornados, deslizamento ou escorregamento de terra, inundações, tempestades e outros fenômenos
Falha de hardware	Falha que necessite reposição de peça ou cujo reparo ou aquisição dependa de orçamento
Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou as configurações dos serviços essenciais
Pandemias e epidemias	Paralisação de alguns serviços como atendimento ao público em decorrência de causas biológicas, fatores ambientais, causas humanas, fatores econômicos e políticos

9. PAPÉIS E RESPONSABILIDADES

9.1. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

- 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.

9.2. EQUIPE DE INSTALAÇÕES/AMBIENTE/SERVIDORES/APLICAÇÕES

- Responsável pelas instalações físicas que abrigam as estações de trabalho e servidores locais;
- Avaliar os danos e supervisionar os reparos para um local secundário, no caso de a localização primária sofrer destruição ou danos.
- O líder desta equipe administrará, manterá e reavaliará o Plano de Recuperação de Desastre.
- Avaliar os danos específicos de infraestrutura de rede interna, incluindo WAN, LAN e quaisquer outra infraestrutura externa junto aos prestadores de serviço.
- Fornecer a infraestrutura de servidores físicos e virtuais necessárias para que a equipe responsável execute suas operações e processos essenciais durante um desastre.
- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos das atividades em caso de um desastre. Eles serão os principais responsáveis por assegurar e

validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TI.

9.3. EQUIPE DE OPERAÇÕES

- Fornecer aos servidores as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível.
- São responsáveis em provisionar ferramentas para que, no caso de um desastre, os servidores possam trabalhar remotamente com as ferramentas específicas à sua atuação.
- O líder desta equipe administrará e manterá o Plano de Continuidade Operacional.

9.4. EQUIPE DE COMUNICAÇÃO

- Responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os servidores, munícipes e com quem mais se fizer necessário.
- O líder desta equipe administrará e manterá o Plano de Administração de Crise.

9.5. EQUIPE DE BACKUP

- Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégias de recuperação de dados de acordo com as políticas pré-estabelecidas.

9.6. EQUIPE DE SEGURANÇA DA INFORMAÇÃO

- Promover mecanismos de segurança, tanto nas estações de trabalho, quanto nos acessos remotos, em caso de acionamento do PCN.
- Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade.
- Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégias de recuperação de dados.

10. PROCESSOS E SISTEMAS CRÍTICOS

Processos e sistemas críticos podem ser definidos como um processo de trabalho que, uma vez paralisado por um tempo superior ao definido pelos gestores da atividade, irá afetar sensivelmente as operações, gerando impacto às pessoas.

Esse impacto é definido pela seguinte fórmula: MTD = RTO + WRT

1- MTD (Maximum Tolerable Downtime) = Define a quantidade total de tempo que um processo pode ser interrompido sem causar quaisquer consequências inaceitáveis. Esse valor deve ser definido pelo Comitê de Desastres. Diferentes funções de atividades terão diferentes MTD's.

2- RTO (Recovery Time Objective) = Determina a quantidade máxima tolerável de tempo necessária para colocar todos os sistemas críticos novamente on-line (por exemplo, restaurar dados de backup ou consertar uma falha).

3- WRT (Work Recovery Time) = Determina a quantidade de tempo tolerável necessária para verificar o sistema e/ou a integridade dos dados (verificar os bancos de dados e logs, por exemplo). Quando todos os sistemas afetados pelo desastre são verificados e / ou recuperados, o ambiente está pronto para retomar a produção novamente.

PROCESSO CRÍTICO	MTD	RTO	WRT
Defeito de hardware	52hs	48hs	4hs
Danos, perda ou corrupção dos servidores, computadores e sistemas operacionais	80hs	72hs	8hs
Falha no Backup	12hs	8hs	4hs
Falha humana (imprudência, negligência e/ou imperícia)	12hs	8hs	4hs
Falha no equipamento interno	12hs	8hs	4hs
Falha estrutural (danos físicos ao edifício/escritório)	52hs	48h	4hs
Absenteísmo de servidor essencial	12hs	8hs	4hs

11. ANÁLISE DE IMPACTO DE NEGÓCIOS (BIA)

I. Uma análise de impacto de negócios (BIA) prevê as consequências da interrupção de uma função e processos e reúne informações necessárias para desenvolver estratégias de recuperação.
II. Cenários potenciais de perda devem ser identificados durante uma avaliação de risco. As operações também podem ser interrompidas pela falha de um fornecedor de bens ou serviços.
III. A BIA deve identificar os impactos operacionais e financeiros resultantes da interrupção das funções e processos organizacionais. Os possíveis cenários e impactos a considerar no caso de interrupção do processo, incluem:

a) Receita perdida;
b) Penalidades contratuais;
c) Insatisfação do usuário de serviços;
d) Danos físicos ao edifício;
e) Danos ou quebras de máquinas, sistemas ou equipamentos;
f) Acesso restrito a um local ou edifício;
g) Paralisação dos serviços públicos (por exemplo, queda de energia elétrica);
h) Danos, perda ou corrupção dos servidores, computadores, sistemas operacionais, aplicativos e dados;
i) Absenteísmo de servidores essenciais.

11.1. TEMPO E DURAÇÃO DA INTERRUPÇÃO

A análise de impacto das atividades existe para definir parâmetros sobre o prazo requerido na recuperação dos serviços (indisponibilidade máxima aceitável/objetivo para o tempo de recuperação) e o momento requerido para suas cópias de segurança (objetivo para Ponto de recuperação / perda máxima de dados). Parâmetros estes que serão calculados após a elaboração de questionários e tabulação de levantamento de riscos.

Os questionários são pensados para obter informações para a elaboração dos:

a) Sistemas /processos críticos de processos sob responsabilidade da prefeitura;
b) Levantar o investimento e custeio para implantação das alternativas para evitar a interrupção e /ou recuperar as operações;
c) Impactos a serem considerados;
d) Grau de criticidade dos sistemas/processos críticos;
e) Tempo objetivado e tempo máximo de paralisação, bem como o seu ponto positivo;
f) Decidir sobre as alternativas, recursos e seus custos com base em análise de custo x benefício;

11.2. CONDUÇÃO DA BIA

Para que se dê uma condução correta da BIA, primeiramente se faz necessário a análise da criticidade e após, a avaliação de todos os impactos (financeiro, legal, operacional,

administrativo, imagem e recursos humanos).

A tabela abaixo serve como referência para que se identifique as ameaças, seus impactos, qual o valor sobre as operações, sua importância e qual o procedimento será adotado para correção desta ameaça.

A revisão desta tabela deve ser feita anualmente, ou sempre que houver mudanças significativas das atividades, devendo, nesse caso, a PREFEITURA DE SÃO JOSÉ DO RIO PARDO solicitar a revisão.

AMEAÇAS	IMPACTO	VALOR	IMPORTÂNCIA
Defeito de Hardware	Direto	Alto	1
Danos, perda ou corrupção dos servidores, computadores e sistemas operacionais	Direto	Alto	1
Falha no Backup	Direto	Alto	1
Perda de dados vitais a prefeitura	Direto	Alto	1
Ataques à sistemas	Direto	Alto	2
Falha humana (imprudência, negligência e/ou imperícia	Direto	Alto	2
Desatualização de Softwares	Indireto	Médio	3
Falha no equipamento interno	Direto	Médio	3
Falha estrutural (danos físicos ao edifício/escritório)	Indireto	Baixo	4
Absenteísmo de servidor essencial	Direto	Baixo	4

11.3. RELATÓRIO DA BIA

Para verificação do nível de criticidade do risco, será utilizada a seguinte fórmula: AMEAÇA +

IMPORTÂNCIA = IMPACTO DE NEGÓCIO

Para cálculo desta formula, serão utilizados os seguintes parâmetros de pontuação:

• Importância 1 – 15 pontos para cada processo;
• Importância 2 – 10 pontos para cada processo;
• Importância 3 – 07 pontos para cada processo;
• Importância 4 – 03 pontos para cada processo.

O resultado desta fórmula, sinaliza o grau de impacto da não implementação de contingência e/ou sua demora, no caso de desastre ou paralisação do serviço.

RESULTADO	SEVERIDADE	IMPACTO DA NÃO IMPLEMENTAÇÃO DE CONTINGÊNCIA
70 a 100	Crítico	Alto
40 a 70	Moderado	Médio
10 a 40	Leve	Baixo

12. PLANO DE ADMINISTRAÇÃO DE CRISES - (PAC)

Este plano especifica as ações ante os cenários de desastres. As ações incluem administrar, gerir, eliminar ou neutralizar os impactos inerentes ao relacionamento entre os envolvidos e/ou afetados, até a superação da crise.

12.1. OBJETIVO

O objetivo do PAC é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de um desastre.

São objetivos específicos do PAC:

a) Garantir a segurança à vida das pessoas;
b) Orientar os servidores e outras partes envolvidas sobre as condutas que serão tomadas;
c) Informar as pessoas interessadas com esclarecimentos condizentes com o ocorrido em tempo hábil;
d) Minimizar transtornos sobre os desdobramentos do incidente e estimular o esforço em

conjunto para a superação da crise.

12.2. EXECUÇÃO DO PLANO

Na ocorrência de um desastre será necessário entrar em contato com as áreas afetadas para informá-las de seu efeito na continuidade dos serviços e tempo para recuperação. O plano deve incluir ações para redirecionar as chamadas telefônicas recebidas para um segundo número.

A equipe de comunicação será responsável por contatar as pessoas prejudicadas e passar as informações pertinentes.

A comunicação ocorrerá da seguinte forma:
a) COMUNICAR ÀS AUTORIDADES: Deve-se comunicar às autoridades competentes em caso de desastre que envolva risco às pessoas, fornecendo informações de localização, natureza, magnitude e impacto do desastre.

- Polícia Militar - 190
- SAMU – 192
- Corpo de Bombeiros – 193
- Defesa Civil – 199

b) COMUNICAR OS SETORES RESPONSÁVEIS: Além da comunicação aos responsáveis, deverá informar também:

- Natureza, impacto e abrangência da catástrofe
- Ações de contingência em andamento
- Processos / sistemas e serviços cobertos pelo plano de continuidade (serviços essenciais)

c) COMUNICAR FORNECEDORES / PRESTADORES DE SERVIÇOS
d) COMUNICAR SERVIDORES
e) COMUNICAR TODAS AS PARTES ACIMA QUANDO OCORRER O RETORNO DAS OPERAÇÕES À NORMALIDADE

12.3. ENCERRAMENTO DO PAC

Uma vez validado o retorno das funções essenciais do sistema e sua total estabilidade, bem como a estabilidade do Data Center, se esse for o caso, a Equipe de comunicação entrará em contato com todos os envolvidos descritos neste plano, provendo as informações de retorno e o status dos serviços essenciais, devendo emitir um parecer relatando as atividades realizadas para restabelecimento dos serviços.

13. PLANO DE CONTINGÊNCIA – (PC)

13.1. OBJETIVO

Este plano visa estabelecer uma recuperação após um desastre, com o objetivo de assegurar o restabelecimento dos sistemas essenciais e suas respectivas atividades.

Tem como principal objetivo listar os procedimentos definidos para permitir que serviços de processamento e armazenamento de dados continuem a operar, mesmo que com um certo grau de degradação.

13.2. DEFINIÇÃO DA ESTRATÉGIA

O plano de contingência, tem como definição três pilares macros, aos quais se baseiam:

a) PESSOAS: trata dos recursos humanos envolvidos nas atividades em contingência;
b) ORGANIZAÇÃO: trata a disponibilidade e segurança dos recursos estruturais organizacionais para suportar as atividades necessárias em contingência
c) TECNOLOGIA: trata dos recursos de hardware e software apoiados em tecnologias e complementam para atender a contingência.

Seguindo esta linha, temos como referência quatro grupos, distribuídos da seguinte forma:

a) Contingência de infraestruturas físicas: compreende as situações de catástrofe, naturais ou não, tais como inundações, desabamentos, incêndios, falhas no fornecimento de energia, entre outros. Em termos gerais, são ocorrências que impeçam o acesso e/ou utilização das instalações, como também danos físicos relevantes a instalações e/ou equipamentos, intencionais ou não.

b) Contingência de pessoas: são aquelas onde os servidores chaves não estão presentes por motivos de greves, doenças, licenças e etc.

c) Contingência de Infraestruturas Tecnológicas: compreende as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, telecomunicações, rede e segurança.

d) Contingência de serviços Externos: compreende as situações de não prestação de serviço contratado considerado crítico aos processos.

13.3. ETAPAS DA CONTINGÊNCIA

Para que a contingência siga seu fluxo, são recomendadas que essas etapas estejam presentes. São elas:

a) Diagnóstico: consiste na identificação dos pontos fracos que poderiam ser foco de problemas

para o setor de TI da prefeitura
b) Análise de riscos: a partir das vulnerabilidades, deve-se considerar as possíveis ameaças e os fatores que possam levar à concretização desses riscos, como o ataque de vírus e a ausência de um antivírus corporativo.
c) Definição de prioridades: identificar os processos vitais da prefeitura e apontar quais os sistemas que precisam ser recuperados primeiro ou preferencialmente em casos de problemas
d) Determinação de estratégias: esse é o caminho para se definir como cada sistema deve ser recuperado (usando softwares ou aplicações), quando e quem são os responsáveis por isso.

13.4. ENCERRAMENTO DO PLANO DE CONTINGÊNCIA

O plano será encerrado assim que todos os serviços estiverem estáveis e o funcionamento dos sistemas essenciais operando normalmente.

A equipe responsável pelo retorno deve emitir um parecer relatando as atividades realizadas, que por sua vez deverá fornecer um comunicado de retorno às atividades.

14. PLANO DE RECUPERAÇÃO DE DESASTRES – (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos, para que, uma vez definindo as atividades prioritárias para restabelecer o nível de operação dos serviços, controlada a contingência e passada a crise, a organização retorne aos seus níveis normais de operação.

Para garantir o retorno das operações depois da ocorrência de uma crise ou desastre, são objetivos do plano de recuperação:

a) Avaliar danos aos ativos e conexões do Data Center e prover meios para sua recuperação.
b) Evitar desdobramento de outros incidentes.
c) Restabelecer o Data Center dentro do prazo tolerável.

14.1. EXECUÇÃO DO PLANO DE RECUPERAÇÃO

Para que o plano transcorra como planejado, deve-se executar os seguintes passos:

a) A equipe responsável pelos BACKUPS e SERVIDORES, deverá identificar e listar todos os ativos danificados da ocorrência do desastre;
b) A equipe de rede deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, WAN ou com o provedor de serviços;
c) Os responsáveis pelo PRD deverão mapear quais os serviços foram descontinuados contendo as informações de perda de ativo e de conexão;
d) O comitê responsável pelo PRD, após o mapeamento das perdas e impactos elaborará um

cronograma de recuperação das aplicações, levando em consideração as seguintes aplicações para recuperação:

- Substituição dos ativos e equipamentos;
- Reconfiguração de ativos e equipamentos;
- Teste de ambiente.

14.1.1. SUBSTITUIÇÃO DOS ATIVOS E EQUIPAMENTOS

Em caso de perda de ativos, deverá ser imediatamente informado a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar cada serviço, comunicando se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição. As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes de PCO e PAC.

14.1.2. RECONFIGURAÇÃO DE ATIVOS E EQUIPAMENTOS

A equipe responsável deverá verificar se as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Caso não estejam, prover cronograma estimado para configurar estes ativos.

14.1.3. TESTE DE AMBIENTE

O ambiente principal (local e/ou Data Center), deverá ser testado antes da recuperação dos dados, a fim de garantir que o processo de recuperação ocorra conforme o planejado. Os testes e recuperações deverão:

a) Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre;
b) Garantir a integridade dos dados, que podem estar corrompidos ou defasados;
c) Validar todas as configurações anteriores;
d) Suportar o retorno dos sistemas de acordo com a demanda;
e) Verificar a integridade dos dados e restaurar os backups, caso necessário.

14.2. ENCERRAMENTO DO PLANO

O plano será encerrado assim que os procedimentos de recuperação forem realizados por todas as equipes. Ao término de todos os procedimentos, as informações de recuperação de serviços serão consolidadas em parecer específico, informando o horário de restabelecimento de cada serviço, equipamentos adquiridos e/ou realocados, se for o caso, fornecedores que tiveram de ser acionados procedimentos de recuperação realizados, entre outras informações relevantes

15. 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 e restabelecer o funcionamento dos principais ativos que suportam as operações de TI, reduzindo o tempo de queda e os impactos provocados por um eventual desastre.

15.1. OBJETIVO

I. Garantir ações de continuidade durante e depois da ocorrência de uma crise ou desastre, tratando-se apenas de ações de contingência, destinados a manter a continuidade dos processos e serviços vitais. É através deste, que as equipes de processos saberão como agir na falta ou na falha de algum componente que o suporte, garantindo assim a continuidade do processo, reduzindo os seus impactos.
II. Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações e sistemas essenciais;
III. Estabelecer controles, regras e procedimentos alternativos que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre;
IV. Definir os formulários, checklist e relatórios a serem entregues pelas equipes ao executar a contingência.

15.2. EXECUÇÃO DO PLANO

Identificada a ocorrência de um incidente, crise ou desastre, a equipe de operações e backups deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido. Após a avaliação de impacto de desastre, a equipe responsável deverá preencher um questionário para avaliação e decisão sobre o acionamento do plano e início das ações de contingência. Este questionário deve ser divulgado para todas as equipes envolvidas.

Dado o aval para o acionamento do plano pelos responsáveis, será convocada uma reunião de emergência com os líderes com o intuito de:
a) Coordenar prazos e orquestrar as ações de contingência;
b) Informar as equipes de ações de contingência com a priorização dos serviços essenciais.

15.3. PROCEDIMENTOS DE RETOMADA

Para que se tenha a retomada das operações, será necessário a verificação das seguintes etapas:

a) Estimar o impacto de perda de dados;
b) Identificar ativos afetados;
c) Mapear ativos a serem recuperados;
d) Estimar volume dos dados a serem recuperados;
e) Tempo de recuperação e possíveis perdas operacionais;
f) Implantar procedimento de recuperação;
g) Testar procedimentos realizados;
h) Repassar os procedimentos aos servidores e verificar melhorias.

15.4. ENCERRAMENTO DO PLANO

O plano será encerrado assim que for validado o funcionamento dos sistemas essenciais, bem como o Data Center, se esse for o caso, relatando a sua estabilidade e a sua normalidade. Após esse processo, será emitido um parecer da equipe responsável, informando o que ensejou o acionamento do plano, as atividades realizadas e os recursos que foram utilizados para então, comunicar a todos os setores a estabilidade do sistema.

16. HISTÓRICO DE REVISÕES

Revisão	Data	Histórico de Revisões
0	27-11-2024	Emissão Inicial

EqPDTIC

Libércio Donizete Martins
Cooordenador do Setor de Tecnologia da Informação