PLANO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Cliente: PREFEITURA MUNICIPAL DE COLÔMBIA

1. APRESENTAÇÃO

Falha nos serviços de TI trazem impactos diretos na prestação de serviços públicos à população, além de prejuízos operacionais e financeiros devido a dependência dos recursos tecnológicos em cada atividade realizada pela Prefeitura por meio das unidades administrativas distribuídas no município.

2. OBJETIVO

O Plano de Continuidade de TI é um documento que descreve as estratégias necessárias à continuidade dos serviços essenciais de TI definidos como críticos para o planejamento dos planos de contingência, de continuidade e de recuperação de forma a garantir a continuidade das operações para os casos de interrupção ou desastre.

3. SERVIÇOS ESSENCIAIS

Os seguintes serviços, por ordem de prioridade, são considerados necessários para ativar e executar este Plano de Continuidade.

Serviço	**Criticidade[1]**	**RPO[2]**	**RTO[3]**	**IMPACTO[4]**			
				FINANCEIRO	**LEGAL**	**IMAGEM**	**OPERACIONAL**
Servidor Dados Local	Alta	24h	12h	Indefinido	Alto	Médio	Alto
Servidor Sistemas Nuvem	Alta	12h	6h	Indefinido	Alto	Alto	Alto
Link Principal	Alta	6h	2h	Indefinido	Alto	Alto	Alto
Sistema Tributário	Alta	12h	8h	Indefinido	Alto	Alto	Alto
Nota Fiscal Eletrônica	Alta	12h	6h	Indefinido	Alto	Alto	Alto

Sistema Contábil	Alta	6h	2h	Indefinido	Alto	Médio	Alto
Sistema Folha	Alta	6h	2h	Indefinido	Alto	Médio	Alto
Sistema Materiais/ Compras	Alta	8h	4h	Indefinido	Alto	Médio	Médio
Sistema Saúde	Alta	8h	4h	Indefinido	Alto	Alto	Alto
Site Corporativo	Alta	12h	6h	Indefinido	Médio	Alto	Médio
Portal Transparência	Média	12h	6h	Indefinido	Médio	Alto	Médio
E-mail Institucional	Alta	12h	6h	Indefinido	Médio	Médio	Médio
Sistema Cemitério	Baixa	24h	12h	Indefinido	Baixo	Baixo	Baixo
Internet Próprios	Alta	12h	6h	Indefinido	Médio	Alto	Médio
Servidor Arquivos	Alta	24h	12h	Indefinido	Médio	Médio	Médio
Sistema de Backup	Baixo	24h	12h	Indefinido	Alto	Médio	Alto
VPN	Alta	24h	12h	Indefinido	Médio	Médio	Médio
Serviços Online	Médio	12h	6h	Indefinido	Alto	Alto	Médio
Boletim Oficial	Médio	24h	12h	Indefinido	Médio	Médio	Médio

1 e 4 – Alto, Médio, Baixo, Indefinido.

2 – **Recovery Point Objective:** Método de controle utilizado em tecnologia de informação para calcular e/ ou estimar a quantidade limite de dados que uma organização toleraria perder em casos de incidentes.

3 – **Recovery Time Objective:** Diretamente relacionado ao tempo máximo que o setor de tecnologia levará para restabelecer os serviços após a parada crítica, devendo ser levado em consideração o tempo de recuperação, testes, reparos, atualizações, reinstalações, etc.

4. PRINCIPAIS AMEAÇAS

O plano deve ser acionado quando da ocorrência de um cenário de desastre que coloque em risco a continuidade dos serviços essenciais.

Desastres	Possíveis Causas
01 – Interrupção Energia Elétrica	- Causada por fator externo à rede elétrica da Prefeitura ou próprios municipais, com duração superior a 1 hora. - Causa por fator interno que comprometa a rede elétrica do próprio público como curtoscircuitos, incêndio ou demais incidentes elétricos.
02 – Falta de Climatização Sala Servidor	- Superaquecimento dos ativos causados devido falha no sistema de refrigeração do ambiente, falha na redundância e/ ou automatização dos aparelhos de climatização dentre outros fatores.
03 – Falha Humana	- Acidente ao manusear equipamentos críticos, como servidores ou processamento de dados.
04 – Falha de Hardware	- Falha que necessite de troca de peças, reparos, ou até mesmo a substituição do equipamento que dependa de processo licitatório.
05 – Desastres Naturais	- Tempestades, alagamentos, caso fortuito, etc.
06 – Ataques Internos	- Ataques aos ativos do(s) servidor(es)
07 – Ataque Cibernético	- Ataques a rede pública municipal que possa comprometer os computadores, servidores locais e em nuvem e/ ou rede de dados.
08 – Indisponibilidade de rede/ circuitos	- Rompimento de cabos de interconexão decorrente da execução de obras públicas, desastres ou acidentes.

09 - Incêndio	- Incêndio que comprometam parcialmente ou completamente a continuidade dos serviços de TI no município.

5. PAPEIS E RESPONSABILIDADES

Comitê de Desastres

A Comissão de Desastres (CD) é responsável por avaliar o plano de continuidade de TI periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução deste e demais ocorrências relacionadas.

Este comitê será responsável por toda a comunicação durante o desastre. Especificamente, se comunicarão com os funcionários, munícipes, autoridades e fornecedores, se necessário.

O comitê será formado pelos membros da DTI e empresa contratada responsável pela gestão dos servidores de dados.

Equipe Técnica

A equipe técnica será responsável pelas instalações físicas que abrigam sistema de TIC e pela garantia de que as instalações de substituição sejam mantidas adequadamente.

Cabe a equipe técnica avaliar os danos específicos de qualquer infraestrutura de rede e fornecer dados e conectividade de rede, incluindo WAN, LAN ou de infraestrutura externa junto a prestadores de serviços. Fornecerá ainda infraestrutura de servidores físicos e virtuais, necessária para que sejam executadas suas operações e processos essenciais durante um desastre garantindo que as aplicações essenciais funcionem como exigido, para atender aos objetivos de negócios em caso de e durante um desastre.

A equipe técnica será a principal responsável por assegurar e validar o desempenho das aplicações essenciais.

Fornecerá aos funcionários as ferramentas de que estes necessitem para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar os trabalhos na solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas à sua atuação.

Por fim, a equipe técnica analisará as perdas e mapeará a quantidade de dados perdidos e o tempo de recuperação desses dados, e formulará a estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.

Invocação do Plano

O plano será acionado quando houver qualquer ocorrência de algum dos cenários de desastres, de risco desconhecido ou de vulnerabilidade que tenha possibilidade de ser explorada.

O plano também poderá ser utilizado nos casos de testes para validação dos processos envolvidos.

Os funcionários da equipe técnica serão os responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente nos casos possíveis.

Macroprocessos

Esse plano tem seus macroprocessos definidos nas atividades a seguir e se desmembra em planos específicos para cada área de atuação, quando da ocorrência de algum desastre.

6. ESTRATÉGIAS DO PLANO DE CONTINUIDADE DOS SERVIÇOS DE TI

A execução do Plano de Continuidade dos Serviços de TI será realizada através das atividades descritas no plano a seguir:

6.1 Backup

Definição da política de backup do município, sendo no mínimo aceito: Completo (full) com arranjos incremental e diferencial bem como a criação de Snapshots para algumas emergências, como recuperação de sistemas de banco de dados. No mínimo os backups dos

sistemas utilizados devem ser enviados por uma conta na nuvem, para garantir a integridade dos dados, lembrando que esses arquivos devem ser testados, para garantir que, se for preciso utilizar eles estarão funcionando corretamente.

6.2 Redundância

A redundância está ligada aos links de internet e servidores físicos e/ ou nuvem, que possa garantir a continuidade do serviço em caso de falha. Cada servidor utilizado em processamento de dados possui um arranjo específico de RAID pela qual garante a tolerância a falhas por redundância de discos.

6.3 Ações de Contingência/ Recuperação

Mapeamento da perda de dados e ativos, restabelecimento de toda a estrutura afetada e, após o ambiente principal estar operacional, provimento da recuperação dos dados em backups. As ações de contingência e recuperação são detalhadas a seguir.

6.4 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.

O principal objetivo é 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 do PCO:

- Prover meios para manter o funcionamento dos principais serviços e a continuidade das operações dos sistemas essenciais.
- Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações durante uma crise ou cenário de desastre.
- Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.
- Orientar os servidores e demais interessados com informações e procedimentos de conduta.

Execução do Plano:

Avaliação de Impacto de Desastre: Identificada a ocorrência de um incidente ou crise, o responsável deverá verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido.

Acionamento do Plano: Convocação de uma reunião de emergência, com o intuito de coordenar prazos e orquestrar as ações de contingência, informar aos envolvidos as ações de contingência com a priorização dos serviços essenciais.

Contingência de Backup: Devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial:

ID	INSTRUÇÃO	DURAÇÃO	OBSERVAÇÃO	RESULTADO
01	Verificar status da aplicação de backup e estimar impacto da perda de dados.			
02	Identificar as rotinas de backup cujos dados em questão foram afetados.			
03	Estimar volume de dados a serem recuperados, tempo de recuperação dos dados e possíveis perdas operacionais.			
04	Atestar retorno do funcionamento do ambiente principal.			
05	Testar a aplicação do backup após desastre.			
06	Validar políticas de backup implementadas.			

Encerramento do PCO: Documentar atividades e informar a todos o retorno das atividades.

6.5 Plano de Administração de Desastre – PAD

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.

Execução do Plano:

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 prioridade será assegurar que os responsáveis pelas áreas afetadas sejam notificados sobre a situação de desastre com as informações dos impactos e serviços afetados e a previsão para o restabelecimento.

Quando o serviço impactado atingir usuários externos deverá ser notificada a área responsável pela Comunicação para que seja tomada a providência quanto a divulgação de nota comunicando a indisponibilidade para o público em geral.

Deverá ser provido um meio de contato específico para este fim, com intuito de que as unidades administrativas se mantenham informadas da ocorrência de um desastre e da inatividade dos serviços essenciais de TI, como também as ações de contingência em andamento para restauração das operações.

Encerramento do Plano: Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade dos servidores serão contactados os departamentos e demais partes descritas neste plano, fornecendo as informações do retorno das operações e dos serviços essenciais.

O Departamento de TI deverá também 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.

6.6 Plano de Recuperação de Desastres

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.

São objetivos do Plano de Recuperação de Desastres:

- Avaliar danos aos ativos e conexões do sistema afetado e prover meios para sua recuperação;
- Evitar desdobramento de outros incidentes na infraestrutura principal; Restabelecer o sistema afetado dentro de um prazo tolerável.

Execução do Plano:

Identificação de ativos danificados ou comprometidos: A equipe técnica deverá identificar e listar todos os ativos danificados da ocorrência do desastre. **Identificação de acessos comprometidos:** A equipe deverá identificar as interrupções de conexões e acessos gerados após o desastre, relatando se trata de um problema interno ou externo ao ambiente, bem como o fornecimento das informações quanto aos sistemas afetados em caso de terceiros.

Listagem dos serviços descontinuados: A equipe técnica deverá mapear quais serviços foram descontinuados, contendo as informações de perda de ativo e de conexão, com intuito de documentar e corrigir os serviços. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, roteadores e switches, bem como respectivas configurações de proxy, DNS, rotas, VLANS, etc.

Elaboração de cronograma de recuperação: Após o mapeamento das perdas e impactos, a equipe técnica elaborará um breve cronograma de recuperação de aplicações, levando em consideração:

1. A priorização dos serviços essenciais, ou determinação de nível institucional;
2. O RTO definido para cada serviço essencial;
3. A força de trabalho disponível.

Substituição de ativos: Em caso de perda de ativos, deverá ser imediatamente informado a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. Deverá ser mensurado quanto tempo o processo licitatório irá impactar o RTO de cada serviço, comunicando os responsáveis se houver alguma solução alternativa a ser tomada enquanto é realizada a aquisição. Deverá ser analisado para os ativos danificados, as coberturas contratuais e/ ou garantias.

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

Ambiente de testes: Deve ser elaborado um ambiente para testes de recuperação garantindo o pleno restabelecimento da aplicação/ serviços afetados pelo incidente e/ ou desastre ocorrido. Os testes incluem a garantia dos níveis de capacidade e disponibilidade dos serviços.

Recuperação dos dados do backup: Proceder a recuperação dos dados para as aplicações afetadas. Validar as configurações e funcionalidades dos sistemas. A validação pode ser realizada pelos testes automatizados de monitoramento dos serviços ou por equipe designada.

Encerramento do Plano de Recuperação de Desastres: Ao término do procedimento de recuperação, as informações serão consolidadas em parecer específico informando o horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

7. PROCESSO DE REVISÃO DO PLANO DE CONTINUIDADE DOS SERVIÇOS DE TI

O Plano de Continuidade dos Serviços de Tecnologia da Informação e Comunicação deverá ser revisado periodicamente pelo Diretoria de Tecnologia da Informação que foi responsável por sua elaboração.

A revisão se faz necessária para o devido acompanhamento dos fatores de risco e necessidades identificadas, assim como para acrescentar melhorias contínuas nas estratégias da execução deste plano, conforme eventuais atualizações e evoluções dos recursos de tecnologia disponíveis na Prefeitura.

8. FATORES CRÍTICOS PARA A EXECUÇÃO DO PLANO DE CONTINUIDADE DOS SERVIÇOS DE TI

São considerados fatores fundamentais para a execução das atividades previstas neste Plano:

a) Acompanhamento dos riscos e necessidades pelo Departamento de TI;
b) O envolvimento dos responsáveis para sustentação das decisões necessárias para atingir os objetivos do plano;
c) O correto alinhamento entre os departamentos técnicos e administrativos envolvidos no plano;
d) Capacitação dos profissionais de TI e dos usuários dos ativos de TI em geral;
e) Disponibilidade orçamentária.

As ações contidas nesse Plano, foram desenvolvidas em parceria com os colaboradores da Prefeitura Municipal de Colômbia, e as informações contidas nele, servem para garantir a integridade das informações e o pleno funcionamento dos equipamentos e consequentemente dos Departamentos da Prefeitura, afim de que possam desenvolver suas funções da melhor maneira possível, sem causar nenhum tipo de danos á população, aos contribuintes, aos prestadores de serviços, aos colaboradores e todos aqueles que de forma direta ou indireta dependem do Poder público Municipal.

Sem mais para o momento, garantimos as informações aqui contidas e certos de que possamos prestar um serviço de excelência, contribuindo com a Administração Pública Municipal.

Colômbia, 10 de Abril de 2024

_____

Leonardo Savio Martins
CNPJ: 27.339.228/0001-67