MUNICÍPIO DE TOLEDO

Plano de Contingência da Informação

2020

Sumário

1. PLANO DE CONTINGÊNCIA DAS INFORMAÇÕES 3
1.1 Justificativa e Objetivo 3
2. SERVIÇOS ESSENCIAIS 3
3. PRINCIPAIS RISCOS 3
4. RECUPERAÇÃO DE DESASTRES 4
4.1 Ações a Serem Realizadas 4
5. BACKUPS 6
5.1 Backups de Bases de Dados 6
5.2 SIPREV 6

1. PLANO DE CONTINGÊNCIA DAS INFORMAÇÕES

1.1 Justificativa e Objetivo

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

2. SERVIÇOS ESSENCIAIS

Os serviços essenciais utilizados pelos servidores do TOLEDOPREV para o cumprimento de suas obrigações dentro da área de TI são:

- Acesso à Internet;
- Os Sistemas de Cálculo de Benefícios (SICAPWEB) hospedado na nuvem e Folha de Pagamento (SRH) hospedado internamente;
- O acesso aos sistemas e serviços bancários e financeiros;
- Os sistemas governamentais acessados via internet;
- Sistema de Contabilidade (SCP) hospedado internamente;
- Pasta de dados da rede (disco M:/).

3. PRINCIPAIS RISCOS

Os principais riscos avaliados para a continuidade dos serviços de informática identificados são:

a. **Interrupção de energia elétrica:** Como as atividades no âmbito do TOLEDOPREV são realizadas dentro do Paço Municipal, já se utiliza das estruturas existentes neste. Porém, ainda existem riscos externos bem como riscos nos circuitos internos do Paço Municipal.
b. **Indisponibilidade de rede (internet):** Como as atividades no âmbito do TOLEDOPREV são realizadas dentro do Paço Municipal, já se utiliza das estruturas existentes neste. Porém, ainda existem riscos externos bem como riscos nos circuitos internos do Paço Municipal.
c. **Falha humana:** Acidentes ao manusear equipamentos
d. **Ataques Internos:** Ataques intencionais causados por funcionários.
e. **Falha de Hardware:** Falha que necessite de reposição de peça ou reparo cujo reparo ou aquisição dependa de processo licitatório.
f. **Ataques cibernéticos:** Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.
g. **Desastres Naturais / Incêndio:** Desastres que inutilizem equipamentos.

4. RECUPERAÇÃO DE DESASTRES

4.1 Ações a Serem Realizadas

a. Interrupção de Energia Elétrica

O Gerador acionará automaticamente garantindo que os servidores de dados mantenham seu funcionamento.
Acionar o setor de manutenção do Paço Municipal.
Como contingência, pode-se utilizar acesso remoto aos sistemas disponíveis online.

b. Falha no acesso à Internet

Em caso de falhas de acesso à internet superiores a 5 minutos, os seguintes procedimentos devem ser realizados:

✓ **Identificação da origem do problema**

Realizar testes de comunicação com:
• Servidor externo via IP (ping 8.8.8.8) – em caso de sucesso, indica que deve ser um problema na resolução do DNS.
• Servidor externo (ping ww.uol.com.br) – em caso de sucesso, indica que não tem problema, devendo ser aberto chamado para verificar o computador.
• Servidor externo via IP (ping www.toledo.pr.gov.br) – em caso de sucesso, indica que não tem problema, devendo ser aberto chamado para verificar o computador.

c. Problemas na infraestrutura da Prefeitura:

Entrar em contato com a Informática, informar o problema e aguardar uma estimativa de resolução, exemplo de problema (Equipamento queimado, falta de energia elétrica).

d. Falha no sistema de Contabilidade

Verificar a disponibilidade do servidor de Banco de Dados.
Caso haja problemas no servidor, verificar tipo de falha.
Em caso de necessidade, abrir chamado junto a terceirizada (Dbmaster) que gerencia o banco de dados.

e. Falha de acesso à Pasta de dados da rede

Verificar se falha é na estrutura interna da rede ou no servidor AD.
Em caso de falha na estrutura interna da rede, verificar se é problema na rede interna da Prefeitura e verificar se o computador está ligado.
Em caso de falhas na rede interna, verificar se é problema de configuração ou Falha de Hardware (exemplo placa de rede queimada).

f. Comprometimento dos arquivos da Pasta de dados da rede

Verificar causa.
Se Ataques Cibernéticos, Ataques Internos ou Falhas de Hardware, ir para o respectivo item.
Em caso de 'sumiço' de arquivo ou pasta, primeiro verificar se não estão em outra pasta devido a possível 'arrastar' sem querer efetuado por algum usuário.
Em caso de não localização do arquivo, ou arquivo corrompido, restaurar arquivos necessários a partir do último backup válido.

Analisar backups para verificar possível causa do problema.

g. Ataques Cibernéticos

Caso seja detectado um ransonware em atividade (ou grande possibilidade de):
- Comunicar todos os servidores (funcionários) no local;
- Desligar todos os computadores, incluindo os servidores (desligamento bruto, sem finalização do SO);
- Identificar dados corrompidos (criptografados);
- Através de boot com SO 'externo', identificar quais máquinas estão infectadas.
-Providenciar limpeza das máquinas (se possível, removendo o malware, ou caso não seja possível, tentar restaurar backup da máquina virtual se for o caso, e como última alternativa refazer uma instalação limpa no computador);
- Verificar qual último backup íntegro;
- Restaurar arquivos do backup.

Caso seja detectado outro tipo de malware:
- Desconectar computadores dos servidores (funcionários) da rede fisicamente (desligar os switches da Prefeitura);
- Verificar integridade dos servidores
- Identificar todas as máquinas infectadas e iniciar processo de remoção do malware;
- Com servidores limpos, ir reconectar apenas as máquinas 'limpas' à rede, para retomada do serviço;
- Recuperar arquivos danificados pelo malware.

h. Ataques Internos

- Desligar equipamentos com backups (para evitar perda dos backups);
- Identificar origem do ataque;
- Desativar acessos do atacante;
- Checar todas as sessões ativas do atacante e finalizá-las;
- Após certeza de bloqueio dos acessos do atacante, checando com funcionários possibilidade de conhecimento de senha de outros usuários, religar equipamentos de backup;
- Fazer levantamento dos dados danificados e restaurar dos backups.

i. Falhas de Hardware

Falha em desktops
De imediato, qualquer servidor do TOLEDOPREV pode utilizar qualquer desktop do município sem necessidade de configuração (exceto para sistemas específicos que necessitam instalações locais);
Tentar recuperar dados locais do HD do equipamento defeituoso.
Providenciar o conserto ou novo equipamento.

5. BACKUPS

São feitos backups dos dados nos servidores do TOLEDOPREV
Dados das máquinas dos usuários NÃO são armazenados.
Deve ser utilizado o disco da rede para os dados de trabalho.
Arquivos enviados para órgãos de controle (TCE PR) devem ter uma cópia armazenada no disco de rede do Município de Toledo.

5.1 Backups de Bases de Dados

Conforme informado pelo Departamento de informática, eles possuem software e procedimentos de backup sendo executado diariamente que garante o mais alto nível de backup dos arquivos da rede (Dados M) e dos bancos de dados.

5.2 SIPREV

Backup do arquivo de exportação gerado no SIPREV após a importação dos dados do Sistema SRH para o SIPREV. Fica salvo na pasta DADOS M:/Toledoprev da rede. Dados de outubro de 2020.

VALDECIR NEUMANN
Analista de TI

ROBSON JOSÉ VOZNIAKI
Diretor do Departamento de TI

ROSELI FABRIS DALLA COSTA
Diretora Executiva do TOLEDOPREV