CAAPSML – Manual de Procedimentos de Contingência em Tecnologia da Informação

---

Sumário

- 1. Introdução
- 2. Objetivo
- 3. Escopo
- 4. Serviços Essenciais
- 5. Principais Riscos
- 6. Procedimentos de Contingência
  - 6.1 Interrupção de Energia Elétrica
  - 6.2 Falha no Acesso à Internet
  - 6.3 Falha em Sistemas Críticos
    - 6.3.1 Sistema de Contabilidade
    - 6.3.2 Sistema de Gestão de Benefícios
    - 6.3.3 SEI (Sistema Eletrônico de Informações)
  - 6.4 Acesso e Integridade dos Arquivos da Rede
  - 6.5 Ataques Cibernéticos
  - 6.6 Ataques Internos
  - 6.7 Falhas de Hardware
- 7. Política de Backup e Recuperação
- 8. Monitoramento e Verificação
- 9. Responsabilidades
- 10. Considerações Finais

1. Introdução

A continuidade dos serviços da CAAPSML depende da operação segura e ininterrupta dos recursos de Tecnologia da Informação (TI). Este manual define os procedimentos de contingência em caso de falhas, ataques ou desastres.

2. Objetivo

Estabelecer diretrizes para restaurar os serviços essenciais de TI em situações críticas, minimizando impactos à operação institucional.

3. Escopo

Este plano abrange todos os sistemas, dados, equipamentos e redes utilizados pela CAAPSML.

4. Serviços Essenciais

- Acesso à Internet.
- Sistema de Contabilidade – EQUIPLANO.
- Sistema de Gestão de Benefícios – SOFTPREV.
- SEI (Sistema Eletrônico de Informações)
- Pastas e arquivos de rede (disco compartilhado)

5. Principais Riscos

- Interrupção de energia elétrica
- Indisponibilidade de Internet
- Falha humana (erro de operação ou configuração)
- Ataques cibernéticos (ransomware, malware)
- Ataques internos (sabotagem ou acesso indevido)
- Falhas de hardware
- Desastres naturais (enchentes, incêndios)

6. Procedimentos de Contingência

6.1 Interrupção de Energia Elétrica

Comunicar a COPEL.

Verificar funcionamento dos nobreaks.

Alertar usuários sobre a autonomia limitada e orientar a finalização de sessões.

6.2 Falha no Acesso à Internet

Comunicar à DTI – SMPOT.

À DTI caberá:

Realizar testes de conectividade e verificação do gateway da rede.

Identificar se a falha é de DNS, link ou roteador.

Contatar provedores, se necessário.

6.3 Falha em Sistemas Críticos

6.3.1 Sistema de Contabilidade

Comunicar setores envolvidos.

Contatar suporte técnico.

6.3.2 Sistema de Gestão de Benefícios

Contatar suporte técnico.

6.3.3 SEI (Sistema Eletrônico de Informações)

Verificar se a falha é local ou externa.

Caso necessário, contatar o suporte técnico do órgão responsável (SMGP – DGIAP).

A DGIAP deverá executar a correção imediata da falha, sempre que possível.

Documentar falha para histórico.

6.4 Acesso e Integridade dos Arquivos da Rede

Comunicar à DTI – SMPOT.

À DTI caberá:

Verificar conectividade com servidor.

Conferir movimentação indevida de arquivos.

Restaurar a partir de backup.

Avaliar integridade.

6.5 Ataques Cibernéticos

Comunicar à DTI – SMPOT.

Desligar máquinas afetadas.

À DTI caberá:

Identificar origem.

Identificar dados corrompidos (criptografados)

Restaurar sistemas com backup seguro.

Isolar equipamentos e reconectar apenas após verificação.

6.6 Ataques Internos

Comunicar à DTI – SMPOT.

À DTI caberá:

Verificar histórico de atividades.

Restaurar dados danificados.

Reforçar autenticação e auditoria.

6.7 Falhas de Hardware

Usar equipamentos reserva (ex: notebooks).

7. Política de Backup e Recuperação

A Diretoria de Tecnologia da Informação (DTI) da SMPOT, e as empresas gestoras dos sistemas utilizados — Equiplano (contábil) e Softprev (previdenciário) — deverá observar as seguintes diretrizes:

1. Backup

É obrigatória a realização de backups automáticos diários de todos os dados críticos e sistemas, assegurando a continuidade das operações e a proteção das informações institucionais.

2. Validação

Deverá ser realizada, de forma periódica, a verificação da integridade dos arquivos de backup, garantindo que os dados armazenados estejam completos, livres de corrupção e prontos para serem restaurados.

3. Restauração Rápida

A DTI e os fornecedores responsáveis devem manter procedimentos testados e documentados para a restauração rápida e eficaz dos dados e sistemas em caso de falhas, perda de dados ou incidentes de segurança.

8. Monitoramento e Verificação

A Diretoria de Tecnologia da Informação (DTI) – SMPOT, e as gestoras dos sistemas contábil (Equiplano) e previdenciário (Softprev), deverá adotar as seguintes medidas:

1. Implementação de Sistema de Monitoramento

Implantar sistema automatizado de monitoramento que possibilite a geração de alertas imediatos em caso de falhas nos processos de backup.

2. Verificação Diária

Realizar verificação diária dos relatórios de backup, garantindo que a equipe de TI acompanhe o status e a integridade das rotinas executadas.

3. Correção Imediata de Falhas

Proceder à correção imediata de qualquer falha identificada nos processos de backup, assegurando a continuidade e a confiabilidade das operações de salvaguarda dos dados.

9. Responsabilidades

DTI – SMPOT- supervisionar plano e executar ações.

Gestores de setores: comunicar falhas e colaborar.

Empresas contratadas: prestar suporte conforme contrato.

10. Considerações Finais

Este manual deve ser atualizado anualmente ou após mudanças na infraestrutura de TI.