

Instituto de Previdência
Do
Município de Teófilo Otoni

**MANUAL DE PROCEDIMENTOS DE
CONTIGÊNCIA**

Teófilo Otoni Fevereiro/2026

Sumário

1. Plano de recuperação de danos	2
1.1. Justificativa e Objetivos	2
1.2. Serviços Essenciais	2
1.3. Classificação de Prioridade e Tempo de Recuperação (RTO e RPO)	3
1.4. Principais Riscos	3
1.5. Governança do Plano de Contingência (Papéis e Responsabilidades)	4
2. Ações a serem tomadas	5
2.1. Interrupção de Energia Elétrica	5
2.2. Falha no acesso à Internet	5
2.3. Falha no sistema de Contabilidade	5
2.4. Falha de acesso à pasta de dados da rede	6
2.5. Comprometimento dos arquivos da pasta de dados da rede	6
2.6. Ataques Cibernéticos	7
2.6.1. Ransomware	7
2.6.2. Outro tipo de <i>malware</i> :	7
2.6.3. Ataques Internos	8
2.7. Falhas de Hardware	8
2.7.1. Falha em desktops:	8
2.7.2. Falha em switch:	8
2.7.3. Falha nos servidores:	9
2.8. Registro de Incidentes	9
3. BACKUPS	9
3.1. Rotinas	9
3.1.1. Backups de Arquivos de Dados	9
3.2. Recuperação	10
3.2.1. Arquivos de Dados	10
3.3. Teste de Restauração de Backup	Erro! Indicador não definido.
4. Fluxograma	11
5. Revisão e Atualização do Plano	Erro! Indicador não definido.

1. Plano de recuperação de danos

1.1. Justificativa e Objetivos

Uma vez que falhas nos serviços de TIC(Tecnologia da Informação e Comunicação) impactam diretamente a continuidade da prestação do serviço, pretende-se com este plano promover medidas ágeis e eficazes de proteção e recuperação para os processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes graves ou desastres.

1.2 Serviços Essenciais

Os serviços essenciais necessários utilizados pelos servidores do SISPREV dentro da área de TI para o cumprimento de suas atividades são:

- Acesso à Internet o Sistema de controle de benefícios e folha de pagamento (ASPPREV) hospedado na nuvem
- Acesso aos sistemas bancários
- Sistemas governamentais acessados via internet
- Sistema de Contabilidade
- Pasta de dados da rede local (disco D:)
- Hardwares

1.3. Classificação de Prioridade e Tempo de Recuperação (RTO e RPO)

Com o objetivo de garantir a continuidade das atividades institucionais, os serviços essenciais foram classificados conforme prioridade e tempo máximo aceitável de indisponibilidade (RTO – Recovery Time Objective) e perda aceitável de dados (RPO – Recovery Point Objective).

Serviço	Prioridade	RTO	RPO
Sistema de Benefícios (ASPPREV)	Crítica	Até 4 horas (mesmo dia útil)	Até 24h
Internet	Crítica	Até 8 horas, condicionado ao provedor	Não aplicável(s/ armazenamento)
Sistema Contábil	Alta	Até 8 horas	Até 24h
Pasta Central da Rede	Alta	Até 4 horas	Até 24h

Nos casos de indisponibilidade decorrentes de fatores externos, como falhas do provedor de internet ou concessionária de energia, os prazos poderão ser impactados, devendo o Instituto adotar todas as medidas cabíveis para restabelecimento no menor tempo possível.

1.4. Principais Riscos

O Plano de Contingência foi desenvolvido para ser acionado quando da ocorrência de cenários que apresentem risco à continuidade dos serviços essenciais. A tabela abaixo define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

Evento	Possíveis causas
Interrupção de energia elétrica	Causada por fator externo à rede elétrica do prédio. Causada por fator interno que comprometa a rede elétrica do prédio, ou do próprio Instituto, como curtos circuitos, incêndio e infiltrações.

Indisponibilidade de rede (Internet)	Rompimento de cabeamento decorrente de execuções de obras, desastres ou acidentes. Assim como falhas nos equipamentos (hardwares), configuração nos computadores, ou interrupções pelo provedor.
Falha humana	Acidente ao manusear equipamento.
Ataques internos (uso indevido proposital)	Ataque aos ativos do Data Center e equipamentos de TI de uso administrativo.
Falha de hardware	Falha que necessite de reposição de peça ou reparo.
Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.
Desastres naturais	Desastres que inutilizem equipamentos.

1.5. Governança do Plano de Contingência (Papéis e Responsabilidades)

- Responsável pelo acionamento e coordenação do Plano: Gerente de TI /Responsável Técnico de TI.
- Responsável pela execução técnica das ações de contingência: TI (mesmo servidor responsável).
- Responsável pela comunicação institucional e decisões extraordinárias (ex.: desligamento geral, contratação emergencial): Diretor Presidente.
- Responsável pelo registro, análise e acompanhamento dos incidentes: Comitê de Política de Segurança da Informação.

Obs: Em razão da estrutura reduzida do Instituto, as funções de coordenação e execução técnica poderão ser exercidas pelo mesmo servidor, sem prejuízo da formalização das responsabilidades e da necessidade de comunicação e registro.

2. Ações a serem tomadas

2.1. Interrupção de Energia Elétrica

- Identificar a origem do problema.
- Caso seja um problema interno na rede do Sisprev verificar, convocar eletricitista.
- Caso seja constatado problema no Edifício Satélite, Acionar o administrador, da Locatto Imóveis.
- Caso seja um problema externo ao Sisprev contatar Empresa Energética fornecedora.

Obs: O Data Center é munido de dois Nobreaks responsáveis por manter o funcionamento dos equipamentos do Data Center e da rede interna até que a Energia Elétrica seja reestabelecida ou até que os nobreaks descarreguem completamente, dando o tempo necessário aos usuários que possuem nobreaks salvarem suas atividades.

- Após verificar origem reestabelecer a energia

2.2. Falha no acesso à Internet

- Identificar se origem do problema é interno ou externo ao Sisprev.
- Caso seja interno, identificar causa do problema, como falhas nos hardwares, computadores ou rede.
- Caso o problema de conexão seja externo ao SISPREV, é acionado o suporte do fornecedor do serviço de Internet.

2.3. Falha no sistema de Contabilidade

- Acionar o suporte do JBBrazil.
- Caso haja problemas no servidor APLICAÇÃO, verificar tipo de falha.
- Em caso de falha no acesso remoto, reconfigurar parâmetros da conexão RDP.

2.4. Falha de acesso à pasta de dados da rede

- Verificar se falha é na estrutura interna da rede ou no servidor APLICAÇÃO.
- Em caso de falha na estrutura interna da rede, verificar se é problema na rede interna do SISPREV.
- Em caso de falhas na rede interna, verificar se é problema de configuração ou falha de hardware.
- Em caso de falha de hardware, verificar o item Falhas de Hardware.
- Restaurar as configurações de rede.

2.5. 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 'desaparecimento' de arquivo ou pasta, primeiro verificar se não estão em outra pasta devido a possibilidade de terem sido 'movidos' ou apagados acidentalmente por algum usuário.
- Em caso de não localização do arquivo, ou arquivo corrompido, restaurar arquivo a partir do último backup válido.

2.6. Ataques Cibernéticos

2.6.1. Ransomware

Caso seja detectado um *malware*(*ransomeware*, *wannacry*) presente na máquina (ou grande possibilidade de ter sido infectado):

- Comunicar todos os servidores (funcionários) no local
- Desligar todos os computadores, incluindo os servidores (desligamento bruto, sem finalização do SO)
- Identificar dados corrompidos (criptografados)
- Providenciar limpeza das máquinas (se possível, removendo o *malware*, ou caso não seja possível, refazer uma instalação limpa no computador)
- Verificar qual último backup íntegro □
- Restaurar arquivos do backup

2.6.2. Outro tipo de *malware*:

- Desconectar computadores dos servidores (funcionários) da rede fisicamente (desligar os switches do SISPREV)
- Verificar integridade dos servidores
- Identificar todas as máquinas infectadas e iniciar processo de remoção do *malware*
- Com servidores limpos, reconectar apenas as máquinas 'limpas' à rede, para retomada das estações de trabalho.
- Recuperar arquivos danificados pelo *malware*

2.6.3. Ataques Internos

- Desligar equipamentos com backups (para evitar perda dos backups)
- Identificar origem do ataque
- Bloquear acessos do atacante
- Checar e finalizar 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

2.7. Falhas de Hardware

2.7.1. Falha em desktops:

- De imediato, qualquer servidor do SISPREV pode utilizar qualquer desktop local sem necessidade de configuração (exceto para sistemas específicos que necessitam instalações locais).
- Recuperar dados locais no HD do equipamento.
- Em caso de dano no desktop, providenciar a manutenção ou disponibilizar um novo equipamento para ingressar no domínio local.

2.7.2. Falha em switch:

- Avaliar o tipo de dano.
- Substituir equipamento por reserva.
- Providenciar manutenção do mesmo.
- Constatando estar o equipamento irrecuperável providenciar novo switch em regime de urgência.

2.7.3. Falha nos servidores:

- Avaliar o tipo de dano.
- Realizar manutenção no servidor que apresentar alguma falha.
- Caso haja a constatação de perda, providenciar novo servidor ou peça (ex: placa de rede) em regime de urgência.

2.8. Registro de Incidentes

Sempre que o Plano de Contingência for acionado, deverá ser elaborado registro simplificado contendo data, tipo de incidente, medidas adotadas e tempo de restabelecimento, devendo o Comitê de Política de Segurança da Informação ser comunicado.

3. BACKUPS

3.1. Rotinas

- São feitos backups diários dos dados armazenados na pasta central nos servidores do SISPREV
- Dados das máquinas dos usuários NÃO são armazenados.
- Para que os arquivos sejam salvos deve se utilizar o local (pasta central) da rede para que os dados de trabalho sejam sincronizados no backup.

3.1.1. Backups de Arquivos de Dados

- O backup da pasta de dados – D:\Pasta Central – é feito pelo Iperius Backup diariamente às 19:00 do servidor para o HD externo no diretório F:.
- Para maior segurança, diariamente é verificado se foi feito o backup do dia anterior, e o HD externo é desconectado e mantido em local seguro até que seja realocado para a próxima seção de backup.

3.2. Recuperação

3.2.1. Arquivos de Dados

Recuperação feita acessando diretamente pela rede. F:\Pasta Central Backup\D

Elaborado por: PERICLES DE OLIVEIRA BARBOSA

Revisado por: JARDEL BATISTA CARVALHO LOPES

Aprovado por: GISLENE PEREIRA SILVA GOMES

4. Fluxograma

