RBPREV
RIO BRANCO PREVIDÊNCIA

Instituto de Previdência do Município de Rio Branco

Plano de Contingência e Manual de Operações de TI

Referência Normativa: Portaria nº 42/2026 (Capítulos VII e VIII) e Lei Federal nº 13.709/2018 (LGPD).

PLANO DE CONTINGÊNCIA E MANUAL DE OPERAÇÕES DE TI – RBPREV

Referência Normativa: Portaria nº 42/2026 (Capítulos VII e VIII) e Lei Federal nº 13.709/2018 (LGPD).

1. ESCOPO E OBJETIVO

Este documento mapeia e manualiza os procedimentos de segurança, backup e contingência dos ativos de informação do Instituto de Previdência do Município de Rio Branco (RBPREV). O objetivo é garantir a continuidade dos serviços previdenciários e a integridade dos dados dos segurados frente a incidentes técnicos ou desastres.

2. MAPEAMENTO DA INFRAESTRUTURA E SISTEMAS

A infraestrutura do RBPREV opera sob um regime de gestão compartilhada e descentralizada entre a DTI/RBPREV e a SDTI.

2.1 Matriz de Ativos e Sistemas Críticos

Sistema / Aplicação	Descrição do Serviço	Natureza da Hospedagem
SISAP	Sistema de Aposentadoria	Virtual (Cluster VMWare)
SIAP	Sistema de Aposentadoria 2.0	Virtual (Cluster VMWare)
DAP / DAP 2.0	Documento de Arrecadação Previdenciária	Virtual (Cluster VMWare)

SITE	Portal Oficial do RBPREV e Transparência	Virtual (Cluster VMWare)
SIMULADOR DE APOSENTADORIA	Ferramenta de Cálculo Previdenciário Web	Virtual (Cluster VMWare)
SERVIDOR	Controlador de Domínio (AD), File Server e SIPREV	Servidor Físico

3. PROCEDIMENTOS DE CÓPIA DE SEGURANÇA (BACKUP)

As rotinas de salvaguarda do RBPREV são integradas aos sistemas de proteção do Datacenter Municipal (SDTI).

I. **Rotinas de Backup**: A execução técnica das cópias de segurança de todas as Máquinas Virtuais (VMs) e bancos de dados é realizada pela infraestrutura da SDTI.
II. **Periodicidade**: São realizados backups integrais (Full), diferenciais e incrementais das imagens dos servidores periodicamente, garantindo a restauração completa em caso de desastre lógico.
III. **Armazenamento**: As cópias são mantidas em dispositivos de storage isolados no Datacenter, garantindo redundância externa ao prédio do RBPREV.
IV. **Validação**: Compete à DTI do RBPREV acompanhar a efetividade das rotinas e solicitar logs de integridade à SDTI para fins de auditoria.

4. CONTROLE DE ACESSO E GOVERNANÇA (FÍSICO E LÓGICO)

O controle de acesso é fundamental para minimizar riscos e garantir a autenticidade das informações.

4.1. Acesso Físico ao Datacenter (SDTI)

Os servidores que hospedam os sistemas do RBPREV possuem as seguintes camadas de segurança física:

I. **Autorização**: Acesso permitido apenas mediante autorização do Diretor da SDTI.
II. **Biometria**: Entrada controlada por leitura de impressão digital.
III. **Monitoramento**: Ambiente sob vigilância contínua por câmeras de segurança (CFTV).
IV. **Resiliência**: Presença de gerador de energia e nobreaks para manter a operação em falhas da rede externa.

4.2. Acesso Lógico e Redes (RBPREV)

I. **Domínio Próprio e Active Directory (AD)**: A gestão de identidades e o controle de acesso aos recursos de rede e servidores são centralizados em um domínio próprio via Active Directory.
II. **Identificação Única**: Todo usuário possui identificação pessoal e intransferível vinculada ao domínio para acesso aos sistemas e estações de trabalho.
III. **Gestão de Rede**: A DTI mantém a gestão direta dos ativos de rede (switches e roteadores) na sede administrativa para assegurar a conectividade com o domínio.
IV. **Privilégios**: O acesso a dados sensíveis (SISAP/SIAP) é restrito através de grupos de segurança no AD, limitando o acesso estritamente à necessidade do serviço público.

5. PLANO DE RESPOSTA A INCIDENTES (CONTINGÊNCIA)

Protocolo para garantia da continuidade dos negócios:

5.1. Falha Crítica ou Corrupção de Dados

1. **Isolamento**: A DTI identifica o sistema afetado e suspende conexões suspeitas.
2. **Restauração (Restore)**: Solicitação formal à equipe da SDTI para o retorno da última imagem íntegra disponível (Full ou Incremental).
3. **Homologação**: A DTI valida o retorno das aplicações e bancos de dados antes da liberação aos usuários do domínio.

5.2. Eventos Externos e Desastres

I. **Queda de Energia/Clima**: As decisões de desligamento preventivo no Datacenter são de competência da SDTI.
II. **Falha de Link**: Em caso de queda de conectividade na sede, a DTI aciona protocolos de contingência local para restabelecer o acesso aos sistemas hospedados.

5.3. Incidentes de Proteção de Dados (LGPD)

1. **Notificação**: Comunicação imediata à Diretoria Executiva e à Comissão de Ética.
2. **Identificação**: A DTI extrai logs de acesso do Active Directory e dos sistemas para mapear a extensão do incidente.

6. DIAGRAMA DE FLUXO INTEGRADO

Este diagrama ilustra a jornada de acesso e salvaguarda, desde a autenticação no domínio até a redundância no Datacenter.

7. REVISÃO E MANUTENÇÃO DO PLANO

7.1. Este Plano de Contingência deverá ser revisado **anualmente ou sempre que ocorrerem alterações críticas** na infraestrutura tecnológica (hardware, topologia de rede ou sistemas), mudanças na estrutura organizacional da DTI/RBPREV ou atualizações na Política de Segurança da Informação (PSI).

7.2. A atualização técnica de nomes de servidores, endereçamentos IP ou fluxos operacionais de backup junto à SDTI pode ser realizada pela DTI sem a necessidade de nova publicação da Portaria principal, desde que mantida a conformidade com as diretrizes da PSI vigente.

8. CONSIDERAÇÕES FINAIS E VALIDAÇÃO OPERACIONAL

O presente **Plano de Contingência e Manual de Operações** constitui o protocolo técnico oficial da Divisão de Tecnologia da Informação (DTI) do **RBPREV**. Sua execução e manutenção visam assegurar que, em caso de sinistro ou falha crítica nos sistemas a interrupção dos serviços previdenciários seja mínima ou inexistente.