POLÍTICA DE BACKUP E DE RESTAURAÇÃO

CÂMARA MUNICIPAL DE INDIAPORÃ

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 1.0

Indiaporã, 18 de julho de 2025

Encarregada LGPD: Adriana Ushijima

1. OBJETIVO

O objetivo do presente documento consiste em divulgar os procedimentos adotados para a realização de backup e de restauração de dados (em casos de desastre ou outros eventos de fortuitos externos ou de força maior) no ambiente administrativo da Câmara Municipal de Indiaporã.

2. AMPLITUDE DO DOCUMENTO

A política de backup engloba os seguintes itens do processo de cópia:

✓ Estratégia de backup;

✓ Tipos de backup;

✓ Rotinas de backup;

✓ Fluxo de segurança;

✓ Tempo de retenção das cópias e Restauração;

✓ Gerenciamento dos Backup;

✓ Requisitos de armazenamento em nuvem;

✓ Armazenamento de Logs de Acesso para fins de Auditoria;

✓ Confidencialidade dos Dados Pessoais

3. ESTRATÉGIA DE BACKUP

Será operacionalizado por intermédio de backup híbrido local (on-premise) e cloud (em nuvem), com base na Estratégia 3-2-1-1-0[1], abrangendo o fornecimento em regime de comodato de servidor dedicado (específico para backup), a ser instalado na Câmara Municipal de Indiaporã, com armazenamento local, em nuvem e air-gapped, que suporte volumetria total estimada de dados de 3.5TB (*terabytes*).

Diretivas de Segurança do servidor a ser instalado na Câmara Municipal de Indiaporã:

a) O equipamento deverá estar conectado a nobreak e equipamento de monitoramento de energia, também fornecido pela contratada;

b) Desconexão automática do equipamento (CPU) da rede de compartilhamento após o término da realização de cada backup;

c) Reinicialização automática em caso de quedas de energia ou conexão com a internet, monitoramento do sistema via internet.

4. FLUXO DE SEGURANÇA

- Dados são salvos no servidor de produção da Câmara Municipal;
- Backup é gerado e criptografado no servidor/equipamento local para backup;
- Cópia é replicada automaticamente para o armazenamento em nuvem;
- Verificações automáticas são feitas diariamente e reportadas;
- Testes de restauração são executados periodicamente;
- Redundância da infraestrutura;
- Monitoramento ativo com relatórios de status de backup e falhas;
- Scripts automatizados de verificação.

[1] ESTRATÉGIA 3-2-1-1-0, a qual é lida como: 3 (três) cópias dos dados, em 2 (dois) formatos diferentes e independentes, em pelo menos 1 (um) local fora do ambiente (offsite), com o último 1 (um) representando 1 (uma) cópia isolada de rede (air-gapped) e 0 (zero) falhas durante as testagens periódicas.

5. TIPOS DE BACKUP:

a) Backup Completo: Realizar o backup completo de todos os tipos de documentos, planilhas, imagens, vídeos, sistemas e bancos de dados, a serem indicados pela contratante;

b) Backup Incremental: Após o backup completo, o sistema deverá ter a capacidade de identificar e realizar o backup apenas dos arquivos novos e modificados (deduplicação);

c) Backup Agendado: Permitir a criação de **múltiplos agendamentos** do tipo: diário, semanal, mensal, anual ou políticas personalizadas conforme demanda do solicitante.

6. TEMPO DE RETENÇÃO DAS CÓPIAS E RESTAURAÇÃO DE DADOS:

Os backups ficarão à disposição da Câmara Municipal (em servidor local e na nuvem) para a restauração por até 30 (trinta) dias, onde os dados poderão ser solicitados de forma completa ou apenas de arquivos específicos, conforme a necessidade.

Em caso de contratação de solução de backup, deverão constar nos contratos medidas que evitem o aprisionamento tecnológico, tais como:

a) garantia de portabilidade e migração de dados e informações ao final do contrato;

b) destruição integral dos dados por terceiros após extinção contratual;

c) obrigação de Relatório Técnico As-Built;

d) sanções contratuais detalhadas como medidas de prevenção.

7. GERENCIAMENTO DOS BACKUPS

Gerenciamento dos backups por e-mail: O sistema deverá disponibilizar os seguintes recursos de gerenciamento através de e-mail: alerta de falhas de execução, de tamanho do backup e tipo de backup.

Deverá ser implantada solução que permita:

a) a criação de múltiplos agendamentos do tipo: diário, semanal, mensal, anual ou políticas personalizadas conforme demanda do solicitante; completo e incremental;

b) Retenção de múltiplas versões;

c) Transferência SSH: Os dados deverão ser transferidos através de conexões da internet utilizando um canal seguro de comunicação (VPN) criptografado e autenticado;

d) Compressão e desduplicação;

e) Integração com armazenamento em nuvem por servidores de alta confiabilidade com dados e tráfego criptografados;

f) A licença de software de backup deverá, nativamente, ser capaz de emitir relatórios com informações completas;

g) Permitir a geração de relatórios sobre os testes automatizados do backup de nível de aplicação, incluindo a quantidade de rotinas de verificação, status das rotinas e quantidade de máquinas virtuais verificadas;

h) Criptografia dos dados, oferecendo a possibilidade de armazenar os arquivos de backup de forma criptografada, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário.

8. REQUISITOS DO ARMAZENAMENTO EM NUVEM

- Uso de Data Centers com, no mínimo, TIER Nível III (três), com disponibilidade 24/7/365;

• Para evitar transferência internacional de dados sem consentimento para países que não atendam às diretrizes e regras da LGPD – Lei Geral de Proteção de Dados Pessoais, deverá ser exigido aos contratantes a comprovação de que o Data Center que hospeda a solução de TI opera em território nacional;

• O provedor estará obrigado a assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras brasileiras.

9. ARMAZENAMENTO DE LOGS DE ACESSO PARA FINS DE AUDITORIA

• Os logs deverão ser mantidos durante toda a vigência das contratações de backup, devendo ser entregues à Contratante quando solicitados e no encerramento do contrato;

• Os serviços devem observar os preceitos da Lei Geral de Proteção de Dados, sendo vedada a transferência internacional de dados até a publicação da lista da ANPD de países cujas legislações estão de acordo com a LGPD;

• Sujeição da Câmara de Vereadores a auditorias externas do Tribunal de Contas do Estado de São Paulo, bem como a necessidade de resguardo de todas as garantias da legislação brasileira quanto ao regime jurídico-administrativo.

10. CONFIDENCIALIDADE DOS DADOS:

• Exigir a assinatura de Termo de Confidencialidade dos Dados pelas empresas prestadoras do serviço de solução de backup;

• Prever sanções específicas nos contratos para as condutas que envolvam a alimentação de sistemas de Inteligência Artificial com dados da Câmara Municipal e de transferência não autorizada a terceiros.

Versão	1.0
Data da elaboração	18/07/2025
Elaborado por	Adriana Ushijima (encarregada pela proteção de dados)