

**RESOLUÇÃO Nº 932 / 2025.**

**Dispõe sobre a Política de Backup de Dados  
Digitais no âmbito da Câmara Municipal de  
Ouro Preto.**

A Mesa da Câmara Municipal de Ouro Preto, no uso de suas atribuições legais, faz saber que a Câmara Municipal aprovou e ela, em seu nome, promulga a seguinte RESOLUÇÃO:

**CAPÍTULO I  
DISPOSIÇÕES PRELIMINARES**

Art. 1º Esta Resolução institui a Política de Backup e Restauração de Dados Digitais no âmbito da Câmara Municipal de Ouro Preto – CMOP.

Art. 2º A Política de Backup e Restauração de Dados Digitais da CMOP tem o objetivo de estabelecer diretrizes, critérios, responsabilidades e requisitos técnicos mínimos para garantir a integridade, disponibilidade e segurança dos dados digitais da CMOP, assegurando sua recuperação em casos de falha, perda, ataque cibernético, erro humano ou desastre.

Art. 3º Este documento deverá ficar disponível na intranet, em uma área com acesso de leitura para todas as áreas de negócio responsáveis pelos processos de backup na CMOP.

Art. 4º Esta Política se aplica a todos os dados digitais críticos no âmbito da CMOP, incluindo dados digitais fora da organização armazenados em um serviço de nuvem pública ou privada.

Parágrafo único. Entende-se por Dados digitais críticos as bases de dados digitais de sistemas, aplicações, *filesystems* (arquivos) ou drivers de armazenamento de arquivos e sistemas operacionais de servidores.

Art. 5º Quanto aos sujeitos, esta política se aplica:

I - a agentes públicos usuários ou criadores de dados digitais;

II - a terceiros que acessem e usem sistemas e equipamentos de Tecnologia da Informação - TI da CMOP ou que criem, processem e armazenem dados digitais de propriedade da organização.

Art. 6º Para os ambientes em que essa Política seja considerada não aplicável, deve ser conduzida avaliação de risco e documentados os critérios para a escolha de não realização de backup.

Art. 7º A salvaguarda e recuperação dos dados digitais da CMOP abrange exclusivamente repositórios institucionais custodiados pela unidade administrativa de TI.

Art. 8º Não serão salvaguardados nem recuperados dados digitais armazenados localmente.

Art. 9º A salvaguarda dos dados digitais em formato digital pertencentes a serviços de TI da CMOP, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

Parágrafo único. A salvaguarda dos dados digitais de que trata esta Política deve ser acompanhada por meio de relatórios periódicos, conforme contratualmente previsto.

Art. 10 Os serviços de armazenamento de dados digitais e/ou backup fornecidos pela CMOP serão para uso exclusivo de dados digitais institucionais, passíveis de auditoria.

## CAPÍTULO II DAS DEFINIÇÕES

Art. 11 Para os fins desta Política, considera-se:

I - Administrador de backup: agente ou unidade responsável pelo planejamento de soluções de backup, definição de padrões e configurações, bem como pela responsabilidade de proteger a informação e aplicar os níveis de controles de segurança e atendimento avançado de resolução de incidentes e problemas;

II - Área técnica: unidade responsável pela operação técnica dos ativos e serviços de TI;

III - Ativo crítico: equipamento físico, unidade de armazenamento e dados digitais que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização;

IV - Backup: cópia de segurança de dados digitais computacionais, que pode ser utilizada ou consultada após sua restauração, em caso de indisponibilidade, perda ou alteração dos dados digitais originais;

V - Backup completo: modalidade de backup em que todos os dados digitais a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup;

VI - Backup incremental: modalidade de backup em que são salvaguardados apenas os dados digitais novos ou modificados desde o último backup de qualquer modalidade efetuado;

VII - Backup diferencial: modalidade de backup em que são salvaguardados apenas dados digitais novos ou modificados desde o último backup completo efetuado;

VIII - Catálogo de Backup: banco de dados digitais que contém as informações acerca dos próprios planos de backup;

IX - Clientes de backup: todo equipamento servidor no qual é instalada a ferramenta de backup;

X - Disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de titular do dado ou demanda do TI da CMOP;

XI - Eliminação: exclusão de dado ou conjunto de dados digitais armazenados em banco de dados digitais, independentemente do procedimento empregado;

XII - Gestor da informação: agente público formalmente responsável pela administração de serviços de TI e pelas informações produzidas em seu processo de trabalho;

XIII - Imagem de backup: arquivo gerado pela solução de backup, não necessariamente no formato original dos arquivos que contém os dados digitais salvaguardados;

XIV - Janela de backup: período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XV - Mídia: mecanismos em que dados digitais podem ser armazenados:

a) além da forma e da tecnologia utilizada para a comunicação, inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros;

b) um recurso multimídia combina sons, imagens e vídeos;

XVI - Plano de Backup: conjunto de procedimentos que orienta a realização das cópias de segurança em nível operacional;

XVII - Retenção: período de tempo pelo qual os dados digitais devem ser salvaguardados e estar aptos à restauração.

XVIII - *Recovery point objective (RPO)*: ponto no tempo em que os dados digitais dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados digitais no caso de um incidente;

XIX - *Recovery time objective (RTO)*: tempo estimado para restaurar os dados digitais e tornar os serviços de TI novamente operacionais; correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados digitais, após um incidente;

XX – Restauração: restauração dos arquivos de backup;

XXI - Rotina de backup: procedimento utilizado para se realizar um backup;

XXII - Serviço de TI: sistema de informação ou qualquer solução de tecnologia da informação que armazene informações em formato digital;

XXIII - Teste de backup ou teste de integridade: teste dos arquivos de backup de forma a garantir que não estejam corrompidos;

XXIV - Teste de Restauração/Restore: teste do procedimento de restauração visando garantir que os dados digitais de fato possam ser recuperados;

XXV - Unidade de armazenamento de backup: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais.

**CAPÍTULO III**  
**DAS DIRETRIZES**  
**Seção I**  
**Diretrizes Gerais**

Art. 12 A Política de Backup e Recuperação de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 13 As rotinas de backup devem:

I - utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada;

II - possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização;

III - ser orientadas para a restauração dos dados digitais no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Art. 14 Para operadores terceiros, que gerenciam sistemas mediante contrato com a CMOP, deverão documentar as melhores práticas de backup para seus respectivos sistemas.

Art. 15 O armazenamento de backup deve, preferencialmente, ser realizado em um local distinto da infraestrutura crítica.

Art. 16 A infraestrutura de rede de backup deve, preferencialmente, ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Art. 17 Caso não seja possível atender ao disposto nos arts. 15 e 16, o responsável pelo backup deve fazer o registro da impossibilidade nos relatórios de backup.

## **Seção II**

### **Dos instrumentos de backup**

Art. 18 Os ativos envolvidos no processo de backup são considerados de elevada importância para a continuidade das atividades e serviços da CMOP.

Art. 19 Compete ao Departamento de Tecnologia da Informação solicitar, com as justificativas pertinentes, os equipamentos e softwares necessários para manter o parque de ativos computacionais apto ao atendimento da demanda de backup da CMOP.

Art. 20 Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

## **Seção III**

### **Da frequência e do tempo de retenção dos dados digitais**

Art. 21 Os backups devem ser retidos por tempo suficiente para atendimento às legislações relacionadas aos requisitos de negócio.

Art. 22 O tempo de retenção deve ser estabelecido no procedimento de backup e restauração de cada sistema/ambiente, conforme estabelecido por normas complementares expedidas pela CMOP.

Art. 23 Os backups dos serviços de TI críticos da CMOP devem ser realizados, utilizando-se as frequências temporais recomendadas pelo Departamento de Tecnologia da Informação, podendo ser:

I - Diária;

II - Semanal;

III - Mensal;

IV - Anual.

Art. 24 - A retenção dos backups críticos e não críticos da CMOP devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados digitais, podendo ser a estabelecida a seguir:

I - Diária: 1 semana;

II - Semanal: 1 mês;

III - Mensal: 12 meses;

IV - Anual: 2 anos.

Art. 25 Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados e deverão constar em documentos normativos complementares da CMOP.

Art. 26 A solicitação de salvaguarda dos dados digitais referentes aos serviços de TI críticos e aos serviços de TI não críticos será realizada pelo Departamento de Tecnologia da Informação, com a anuência prévia e formal dos gestores das informações, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I - Escopo ou abrangência (dados digitais a serem salvaguardados);

II - Tipo de backup (completo, incremental, diferencial);

III - Frequência temporal de realização do backup (diária, semanal, mensal, anual);

IV - Retenção;

V - RPO;

VI - RTO.

Art. 27 O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados digitais da CMOP, de modo que as rotinas de backup não resultem em indisponibilidade dos demais serviços de TI da organização.

Art. 28 A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

Parágrafo único O período de janela de backup deve ser determinado pelo administrador de backup.

Art. 29 Os responsáveis pelos dados digitais deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

#### **Seção IV**

##### **Do armazenamento**

Art. 30 As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados digitais resguardados:

- I - criticidade do dado salvaguardado;
- II - requisito de segurança da informação;
- III - tempo de retenção do dado;
- IV - probabilidade de necessidade de restauração;
- V - tempo esperado para restauração;
- VI - custo de aquisição da unidade de armazenamento de backup;
- VII - vida útil da unidade de armazenamento de backup.

Art. 31- O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, priorizando a que melhor se adeque a cada caso.

Art. 32 Podem ser utilizadas técnicas de compressão de dados digitais, contanto que o acréscimo no tempo de recuperação dos dados digitais seja considerado aceitável pelos gestores das informações.

Art. 33 As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, uso de criptografia e com acesso restrito a pessoas autorizadas pelo administrador de backup.

Art. 34 Quando da necessidade de descarte, as unidades de armazenamento de backups devem ser fisicamente destruídas de forma a inutilizá-las, atentando-se ao descarte sustentável e ambientalmente correto.

#### **Seção V**

##### **Dos testes de backup e de restore**

Art. 35 Os planos de backup e de restore devem estabelecer diretrizes para a execução dos testes de recuperação de dados digitais, incluindo a periodicidade necessária.

Art. 36 Os backups devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados digitais salvaguardados.

Art. 37 Os testes de restauração dos backups devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis na CMOP.

Art. 38 A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de backup serão definidos em norma específica a ser elaborada pelo Departamento de Tecnologia da Informação, em conjunto com os gestores das informações.

## **Seção VI**

### **Da restauração de backup**

Art. 39 A solicitação de restauração de dados digitais será formulada pelo responsável pelo recurso ao Departamento de Tecnologia da Informação da CMOP.

Art. 40 As solicitações de recuperação ou acesso a imagens de backup deverão ser registradas e armazenadas.

Art. 41 Compete ao administrador de backup negar a restauração de dados digitais quando o conteúdo não for condizente com a atividade do solicitante ou contrarie a missão institucional da CMOP.

## **CAPÍTULO IV**

### **DAS RESPONSABILIDADES DO ADMINISTRADOR DE BACKUP**

Art. 42 Os backups devem ser operados e monitorados pelo administrador de backup.

Art. 43 O administrador de backup deve ser capacitado para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Art. 44 São atribuições do administrador de backup:

I - criar e manter atualizado os planos de backup para cada serviço sob sua administração;

II - providenciar a criação e manutenção dos backups;

III - configurar as soluções de backup;

- IV - manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
- V - efetuar testes de backup e definir os procedimentos de restauração;
- VI - verificar diariamente os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;
- VII - tomar medidas preventivas;
- VIII - restaurar ou recuperar os backups em caso de necessidade;
- IX - reportar imediatamente ao setor a que está subordinado os incidentes, ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de backups;
- X - gerenciar mensagens e registros de auditoria (logs) diários dos backups;
- XI - providenciar a execução dos testes de restauração e validá-los;
- XII - propor modificações visando ao aperfeiçoamento desta Política de Backup e Recuperação de Dados Digitais.

## CAPÍTULO V DISPOSIÇÕES FINAIS

Art. 45 A Política de Backup e Restauração de Dados Digitais será amplamente divulgada na CMOP, preferencialmente com a exposição de link de acesso no site da Câmara.

Art. 46 A Política de Backup e Restauração de Dados digitais deverá ser revista sempre que necessário ou anualmente, observando-se o que ocorrer primeiro.

Art. 47 Compete à CMOP definir a unidade competente ou responsável para decidir sobre questões não previstas nesta Resolução.

Art. 48 Esta Resolução entra em vigor na data de sua publicação.

**Ouro Preto, Patrimônio Cultural da Humanidade, 18 de dezembro de 2025, trezentos e quatorze anos da Instalação da Câmara Municipal e quarenta e cinco anos do Tombamento.**

**Registrada e publicada nesta Secretaria em 18 de dezembro de 2025.**

**Vantuir Antônio da Silva**

Presidente da Câmara Municipal de Ouro Preto

**Renato Zoroastro**

1º Secretário

Projeto de Resolução nº 981/25

Autoria: Mesa Diretora (Vantuir, Renato, Kuruzu e Alex)