

* Publicada no DOETCE-MS n.º 4.331, de 16 de março de 2026 – páginas 5-12.

RESOLUÇÃO TCE-MS N.º 285, DE 12 DE MARÇO DE 2026.

Dispõe sobre a Política de Backup e *Restore* de informações eletrônicas do Tribunal de Contas do Estado de Mato Grosso do Sul.

O TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL, no uso das atribuições conferidas pelo inciso XI do art. 21 da Lei Complementar n.º 160, de 2 de janeiro de 2012, e pela alínea 'a' do inciso I do § 2º do art. 17 do Regimento Interno, aprovado pela Resolução TCE-MS n.º 98, de 5 de dezembro de 2018,

RESOLVE:

CAPÍTULO I DISPOSIÇÕES GERAIS

Art. 1º Esta Resolução estabelece a Política de Backup e *Restore* de informações eletrônicas no âmbito do TCE-MS, com o objetivo de definir diretrizes para cópia, armazenamento e recuperação de dados sob a responsabilidade da Diretoria de Tecnologia da Informação - DTI, a fim de garantir a segurança, a integridade e a disponibilidade das informações.

CAPÍTULO II DEFINIÇÕES

Art. 2º Para os fins desta Resolução considera-se:

- I - Administrador de backup: servidor do TCE-MS responsável pelos procedimentos de configuração, execução, monitoramento e testes de backup e *restore*;
- II - Administrador do recurso: servidor do TCE-MS ou colaborador responsável pela operação de determinados serviços ou equipamentos da Diretoria de Tecnologia da Informação;
- III - Backup full ou completo: modalidade de backup em que todos os dados são copiados integralmente;
- IV - Backup diferencial ou incremental: modalidade de backup em que somente os arquivos novos ou modificados, desde o último backup completo, são copiados;
- V - Backups de primeiro e segundo estágio: modalidade de backup dividida em duas etapas, armazenadas em meios diferentes, sendo o primeiro em disco e o segundo em fita ou equivalente;
- VI - Clientes de backup: equipamento servidor no qual é instalado o agente de backup;

- VII - Disaster recovery: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;
- VIII - File library: biblioteca de arquivos utilizada para armazenamento de backup em disco;
- IX - Mídia: meio físico no qual são armazenados os dados de um backup;
- X - Object storage: serviço de armazenamento de objetos em nuvem ou local utilizado para backup;
- XI - Retenção: período de tempo em que o conteúdo da mídia de backup deve ser preservado;
- XII - Recovery Manager (RMAN): ferramenta de backup e *disaster recovery* de banco de dados Oracle; e
- XIII - *Restore*: processo de restauração dos dados que foram objeto de sinistro ou exclusão acidental.

CAPÍTULO III

ESTRUTURA E COMPETÊNCIAS

Art. 3º O titular do setor de infraestrutura e segurança de tecnologia da informação será o administrador de backup.

Parágrafo único. As atribuições do administrador de backup poderão ser delegadas, por ato formal, a servidor do TCE-MS lotado na Diretoria de Tecnologia da Informação.

Art. 4º São atribuições do administrador de backup:

- I - propor modificações visando o aperfeiçoamento contínuo da política de backup;
- II - criar, configurar e manter os backups conforme as diretrizes desta Resolução;
- III - gerir a ferramenta de backup, incluindo sua atualização e otimização;
- IV - criar, testar e manter scripts de backup e *restore*;
- V - criar e gerenciar as mídias de backup;
- VI - realizar testes periódicos de backup e *restore*;
- VII - criar, configurar e monitorar notificações e relatórios automatizados;
- VIII - verificar diariamente os relatórios gerados pela ferramenta de backup;
- IX - restaurar os backups quando necessário, conforme procedimentos estabelecidos;
- X - analisar mensagens e logs diários dos backups, implementando ações corretivas para eliminação de erros;
- XI - realizar manutenções preventivas e corretivas dos dispositivos de backup;
- XII - garantir o carregamento das mídias necessárias para os backups programados;
- XIII - comunicar imediatamente ao administrador do recurso as falhas e ocorrências relevantes nos backups;
- XIV - armazenar as mídias de backup em cofre de segurança apropriado;
- XV - manter documentação atualizada dos procedimentos de backup e *restore*; e
- XVI - elaborar relatórios gerenciais sobre o status dos backups.

Art. 5º São responsabilidades do administrador do recurso:

- I - aprovar formalmente os testes de *restore* realizados;
- II - manter atualizado o cadastro de dados críticos sob sua gestão;
- III - comunicar ao administrador de backup qualquer alteração em sistemas, aplicações ou bases de dados que impacte a política de backup; e
- IV - participar dos testes de recuperação de desastres quando convocado.

CAPÍTULO IV

INCLUSÃO E EXCLUSÃO DE DADOS

Art. 6º Todos os dispositivos que armazenam dados institucionais deverão ser avaliados para inclusão no backup.

§ 1º O responsável por cada recurso da DTI deverá definir quais diretórios e arquivos serão incluídos no backup, tendo como prioridade:

- I - arquivos de configuração de sistemas operacionais e aplicativos instalados em servidores;
- II - arquivos de log dos aplicativos, incluindo logs da ferramenta de backup e *restore*;
- III - informações e configurações de bancos de dados;
- IV - arquivos de usuários, incluindo documentos e e-mails institucionais;
- V - arquivos de aplicações desenvolvidas pelo Tribunal ou por terceiros; e
- VI - demais arquivos cuja perda gere prejuízo operacional, legal ou estratégico ao TCE-MS.

§ 2º O administrador de backup ou o responsável pela aplicação deverá definir quais diretórios e arquivos não serão incluídos na rotina, tendo como referência:

- I - arquivos de sistemas operacionais ou aplicações que possam ser reinstalados;
- II - arquivos temporários e de cache;
- III - arquivos salvos em unidades locais de estações de trabalho;
- IV - arquivos de áreas de transferência temporária; e
- V - arquivos particulares não institucionais dos usuários.

§ 3º Para aplicativos e bancos de dados, devem ser seguidas as recomendações do desenvolvedor ou fabricante, adaptadas às necessidades do TCE-MS.

Art. 7º Os procedimentos de backup deverão ser atualizados quando houver:

- I - implementação de novas aplicações;
- II - criação de novos locais de armazenamento de dados;
- III - instalação de novos bancos de dados;
- IV - instalação de novos aplicativos críticos;
- V - mudança na criticidade ou classificação de informações existentes; e
- VI - migração para novos ambientes tecnológicos, incluindo nuvem.

CAPÍTULO V

SOLICITAÇÃO E IMPLEMENTAÇÃO DE BACKUPS

Art. 8º Para a especificação de um backup, o administrador do recurso deverá formalizar solicitação por meio de documento ou sistema apropriado, contendo minimamente:

I - identificação do servidor e localização dos dados;

II - tipo de dados a serem incluídos; e

III - classificação das informações.

§ 1º O backup deverá ser configurado em ferramenta apropriada, seguindo as orientações do documento de solicitação e as diretrizes desta Resolução.

§ 2º Todos os backups criados deverão ser testados antes da aplicação da programação definitiva, incluindo teste completo de restauração para comprovar sua eficácia.

§ 3º O administrador do recurso deverá definir os diretórios e arquivos a serem incluídos no backup da sua área de responsabilidade.

§ 4º O administrador do recurso deverá atestar formalmente a aprovação do backup após o teste de restauração.

CAPÍTULO VI

ARMAZENAMENTO E RETENÇÃO

Art. 9º Os backups realizados em mídias móveis do tipo cartucho de fita, ou equivalente, que necessitem de armazenamento para *disaster recovery*, serão guardados no cofre de segurança do Tribunal, observando sua capacidade.

§ 1º Na ausência de solução do tipo cartucho de fita, deverá ser adotada solução equivalente ou superior que permita *disaster recovery* com as mesmas características de segurança e confiabilidade.

§ 2º O ambiente de armazenamento das mídias deverá atender às seguintes especificações:

I - temperatura mantida em 21°C (vinte e um graus Celsius);

II - umidade relativa mantida em 40% (quarenta por cento);

III - proteção contra umidade excessiva e acesso não autorizado; e

IV - controle de acesso físico e registro de movimentações.

Art. 10. A retenção dos backups observará os seguintes prazos mínimos:

I - backups diários: sete últimos dias;

II - backups semanais: quatro últimas semanas;

III - backups mensais: doze últimos meses; e

IV - backups anuais: cinco últimos anos.

§ 1º Expirado o prazo de retenção, a mídia poderá ser reutilizada ou destruída, observando-se seu estado de conservação e número de ciclos de leitura e gravação.

§ 2º As mídias de fita não deverão ultrapassar trinta anos de armazenamento, devendo ser copiadas para nova mídia antes do descarte.

§ 3º O descarte de mídias deverá observar as normas ambientais vigentes e garantir a impossibilidade de recuperação dos dados.

§ 4º Para dados sujeitos à legislação específica de retenção, prevalecerão os prazos legais.

CAPÍTULO VII

OPERAÇÃO DOS BACKUPS

Art. 11. A criação e operação dos backups observarão as seguintes diretrizes:

I - programação de backups:

- a) os backups serão programados para execução automática em horários de menor utilização dos sistemas e da rede;
- b) serão priorizados horários noturnos e finais de semana para backups completos; e
- c) backups que impactem a performance deverão ser agendados para horários não comerciais;

II - monitoramento de backups:

- a) o administrador de backup monitorará diariamente a execução dos backups;
- b) para backups realizados com sucesso, será gerado extrato automatizado pela ferramenta, enviado por e-mail aos respectivos responsáveis; e
- c) para backups com falhas, o administrador de backup elaborará relatório de acompanhamento contendo: data, horários de início e término, objetos afetados, clientes de backup, causa da falha, ação corretiva adotada e impacto da falha;

III - tratamento de falhas:

- a) as falhas identificadas deverão ser tratadas em até vinte e quatro horas;
- b) falhas recorrentes deverão ser objeto de análise aprofundada e implementação de solução definitiva; e
- c) falhas críticas que comprometam a segurança dos dados deverão ser comunicadas imediatamente à Diretoria de Tecnologia da Informação.

Art. 12. Os backups serão realizados conforme as seguintes modalidades e periodicidades:

I - backups diários em dispositivos apropriados para armazenamento de dados;

II - backups semanais, mensais e anuais na modalidade FULL, possibilitando recuperação integral sem necessidade de outros backups;

III - backup semanal realizado às sextas-feiras, referente à semana encerrada;

IV - backup mensal realizado na primeira sexta-feira de cada mês, referente ao mês anterior; e

V - backup anual realizado na primeira sexta-feira de janeiro, referente ao ano anterior.

Parágrafo único. Em caso de falha em procedimento de backup ou impossibilidade de execução, o administrador de backup adotará providências alternativas para salvaguardar as informações, tais como: cópia para outro servidor, execução em horário de produção ou uso de mídia alternativa,

priorizando sempre a segurança dos dados.

CAPÍTULO VIII

BACKUP DE SERVIDORES DE ARQUIVOS

Art. 13. O backup do servidor de arquivos será realizado segundo a seguinte estratégia:

I - armazenamento em *file library* ou *object storage*, conforme disponibilidade:

- a) backup diferencial diário, de domingo a sábado, com retenção de sete dias;
- b) backup FULL mensal, na primeira sexta-feira do mês, com retenção de trezentos e sessenta e cinco dias; e
- c) backup FULL anual, na primeira sexta-feira do ano, com retenção de cinco anos;

II - em segundo estágio, a *file library* ou *object storage* poderá ser copiada diariamente para até duas mídias diferentes:

- a) primeira mídia armazenada em cofre de segurança, compondo o backup diário; e
- b) segunda mídia mantida na *tape library*, quando aplicável, permitindo recuperação rápida e sequência de gravações;

III - as informações gravadas em *file library* deverão ser preservadas pelo maior período possível, conforme disponibilidade de espaço em disco;

IV - backups de logs e bancos de dados de aplicativos de infraestrutura seguirão a mesma política do servidor de arquivos; e

V - o backup do servidor de arquivos será executado diariamente.

Parágrafo único. Para ambientes em nuvem, deverão ser implementados mecanismos de backup nativos ou compatíveis, garantindo os mesmos níveis de segurança e retenção.

CAPÍTULO IX

RECUPERAÇÃO DE BACKUPS

Art. 14. A recuperação de backups observará os seguintes procedimentos:

I - usuários que necessitem recuperar arquivos deverão registrar solicitação no sistema de controle de atendimento, informando:

- a) nome e setor do solicitante;
- b) identificação completa do(s) arquivo(s) a ser(em) recuperado(s);
- c) localização (diretório e subdiretório); e
- d) data da versão a ser recuperada;

II - a equipe de atendimento encaminhará o chamado ao administrador de backup;

III - o administrador de backup executará a restauração e registrará a conclusão no sistema de controle;

IV - será mantido registro histórico de todas as restaurações solicitadas;

V - bancos de dados serão restaurados pelo administrador de banco de dados, com auxílio do administrador de backup quando necessário; e

VI - a restauração de arquivos de rede somente será possível para arquivos capturados pela estratégia de backup, não sendo passíveis de recuperação arquivos criados e excluídos no mesmo dia.

§ 1º O prazo para conclusão da restauração será de até quarenta e oito horas úteis, podendo ser ampliado em casos de disaster recovery ou grandes volumes.

§ 2º Em situações de urgência devidamente justificadas, a restauração poderá ser priorizada.

§ 3º Restaurações de grande volume que possam impactar a operação deverão ser agendadas em conjunto com o solicitante.

CAPÍTULO X

BACKUP DE BANCOS DE DADOS ORACLE

Art. 15. O backup do banco de dados Oracle será realizado por meio do *Oracle RMAN* nas seguintes modalidades:

I - backup FULL diário com retenção de sete dias;

II - backup FULL mensal (incluindo logs), realizado na primeira sexta-feira do mês, com retenção de um ano;

III - backup FULL anual (logs e dados), realizado na primeira sexta-feira de janeiro, com retenção de cinco anos; e

IV - backup dos arquivos de log do *Oracle RMAN*, realizado no mínimo três vezes ao dia, com retenção de sete dias.

Art. 16. Os recursos de alta disponibilidade do *Oracle* deverão estar habilitados e configurados conforme segue:

I - Oracle Flash Back: para recuperação de dados a partir de ponto específico no tempo, configurado para recuperação dos últimos sete dias; e

II - Oracle Data Guard: para proteção contra falhas, desastres, erros e corrupção de dados:

a) instalado em ambiente tecnológico separado do data center principal (site de backup);

b) mantendo réplica exata do banco de dados principal; e

c) acionado em caso de falha no ambiente principal, funcionando como banco principal até restauração do ambiente original.

Parágrafo único. A configuração e monitoramento das funcionalidades do banco de dados Oracle são de responsabilidade do administrador de banco de dados.

CAPÍTULO XI

BACKUP DE BANCOS DE DADOS POSTGRESQL E MYSQL

Art. 17. O backup dos bancos de dados *PostgreSQL* e *MySQL* será realizado nas seguintes modalidades:

- I - backup FULL diário com retenção de sete dias;
- II - backup FULL mensal, realizado na primeira sexta-feira do mês, com retenção de um ano; e
- III - backup FULL anual, realizado na primeira sexta-feira de janeiro, com retenção de cinco anos.

Parágrafo único. Deverão ser implementados mecanismos de backup específicos para cada sistema gerenciador de banco de dados, respeitando suas peculiaridades técnicas.

CAPÍTULO XII TESTES E VALIDAÇÃO

Art. 18. Os backups mensais e anuais deverão ser testados no prazo máximo de uma semana após sua execução.

§ 1º Caso seja detectada falha ou incompletude do backup, novo backup deverá ser executado imediatamente.

§ 2º Os testes de restauração de bancos de dados serão supervisionados pelo administrador de banco de dados.

§ 3º Para todos os testes realizados será elaborado relatório apresentado ao diretor de tecnologia da informação.

§ 4º Anualmente deverá ser realizado teste completo de disaster recovery, simulando cenário de perda total do ambiente principal.

CAPÍTULO XIII SEGURANÇA E CONTROLES

Art. 19. Procedimentos programados em servidores que impliquem riscos ao funcionamento ou a dispositivos de armazenamento somente serão executados após realização de backup dos dados.

Art. 20. Os backups deverão atender aos seguintes requisitos de segurança:

- I - criptografia de dados sensíveis, conforme classificação da informação;
- II - controle de acesso às mídias e sistemas de backup;
- III - registro de logs de todas as operações de backup e *restore*;
- IV - segregação de funções entre administradores de backup e outros administradores; e
- V - proteção contra *ransomware* e *malware*, incluindo backups offline ou em nuvem isolada.

Art. 21. O descarte de mídias de backup inservíveis ou inutilizáveis será precedido de proposta do administrador de backup ao diretor de tecnologia da informação.

Parágrafo único. As mídias descartadas deverão ser fisicamente destruídas de forma a impedir reutilização ou acesso indevido às informações.

CAPÍTULO XIV
DISPOSIÇÕES FINAIS

Art. 22. O descumprimento das disposições desta Resolução sujeitará o responsável às sanções administrativas cabíveis, sem prejuízo de outras medidas legais.

Art. 23. A Diretoria de Tecnologia da Informação elaborará manual técnico complementar detalhando os procedimentos operacionais de backup e *restore*.

Art. 24. Esta Resolução poderá ser atualizada periodicamente para adequação a novas tecnologias e melhores práticas de mercado.

Art. 25. Os casos omissos serão resolvidos pela Diretoria de Tecnologia da Informação, com aprovação do Comitê de Segurança da Informação do Tribunal.

Art. 26. Esta Resolução entra em vigor na data de sua publicação.

Campo Grande, 12 de março de 2026.

Conselheiro Flávio Kayatt

Presidente

Conselheiro Sérgio de Paula

Relator

Conselheiro Iran Coelho das Neves

Conselheiro Waldir Neves Barbosa

Conselheiro Osmar Domingues Jeronymo

Conselheiro Marcio Campos Monteiro

Conselheiro Substituto Leandro Lobo Ribeiro Pimentel

Procurador-Geral de Contas João Antônio de Oliveira Martins Júnior

Alessandra Ximenes
COORDENADORIA DE SESSÕES
Chefe