MAPEAMENTO E MANUALIZAÇÃO

GESTÃO DE CÓPIAS DE SEGURANÇA E RESTAURAÇÃO DE DADOS

Manual M015

Revisão 01 – Aprovado e validado

5 de outubro de 2026

IDENTIFICAÇÃO	INFORMAÇÃO
Código	M015
Processo	Gestão de cópias de segurança e restauração de dados
Unidade responsável	Departamento de Tecnologia da Informação – DTI, com acompanhamento da Diretoria-Executiva do TOLEDOPREV e da Gestão de Segurança da Informação – GSI.
Unidades participantes	Diretoria-Executiva; DTI; GSI; Comitê de Segurança da Informação – CSI; unidades proprietárias da informação; gestores e fiscais de contratos; fornecedores de sistemas e infraestrutura.
Periodicidade	Execução, monitoramento e retenção conforme a rotina técnica vigente; teste de restauração ao menos anual e após alteração relevante; revisão do manual quando houver alteração relevante no ambiente tecnológico, institucional, contratual ou normativo.
Finalidade	Assegurar disponibilidade, integridade, recuperação e rastreabilidade das informações e dos serviços utilizados pelo TOLEDOPREV.

Revisão	Data	Descrição
00	23/08/2023	Elaboração inicial.
01	05/10/2026	Revisão integral do processo, com atualização do escopo, das responsabilidades, dos controles, das evidências, dos testes de restauração e da integração com a gestão de continuidade e recuperação de desastres.

APROVAÇÃO E VALIDAÇÃO

Etapa	Responsável	Data ou registro
Elaboração técnica	Gestão de Segurança da Informação – GSI e Departamento de Tecnologia da Informação – DTI	04/10/2026
Validação	Diretoria-Executiva do TOLEDOPREV	05/10/2026
Ciência e acompanhamento	Comitê de Segurança da Informação – CSI	Ciência Registrada na Ata nº 002/2026

SUMÁRIO

1. OBJETIVO **4**
2. ABRANGÊNCIA **4**
3. FUNDAMENTAÇÃO NORMATIVA **4**
4. CONCEITOS E SIGLAS **4**
5. DIRETRIZES DO PROCESSO **5**
6. RESPONSABILIDADES **5**
7. ENTRADAS, SAÍDAS, SISTEMAS E REPOSITÓRIOS **5**
8. DESCRIÇÃO DO PROCESSO **6**
8.1. Identificar o escopo e a criticidade 6
8.2. Configurar e programar as rotinas 6
8.3. Executar e monitorar as cópias 6
8.4. Tratar falhas 6
8.5. Armazenar, replicar e proteger 6
8.6. Solicitar e autorizar a restauração 6
8.7. Restaurar e validar 6
8.8. Testar a recuperação 6
8.9. Aplicar retenção e descarte 7
8.10. Revisar a rotina 7
9. LINHA DE BASE TÉCNICA **7**
10. CONTROLES E SEGREGAÇÃO DE FUNÇÕES **7**
11. RISCOS E MEDIDAS DE CONTROLE **8**
12. REGISTROS E EVIDÊNCIAS **8**
13. INDICADORES RECOMENDADOS **9**
14. DISPOSIÇÕES FINAIS **9**
ANEXO I – FLUXOGRAMA DO PROCESSO **10**

1. OBJETIVO

Estabelecer as responsabilidades, os controles e a sequência de atividades para planejar, executar, monitorar, armazenar, testar e utilizar cópias de segurança dos sistemas, bancos de dados, arquivos e demais informações necessárias às atividades do TOLEDOPREV.

O processo deve permitir a recuperação das informações dentro das prioridades definidas para cada serviço, produzir evidências verificáveis e apoiar a continuidade dos serviços e a recuperação de desastres.

2. ABRANGÊNCIA

Aplica-se às informações e aos recursos tecnológicos utilizados pelo TOLEDOPREV, ainda que a infraestrutura, o sistema ou o repositório seja administrado pelo Município, por órgão governamental ou por fornecedor contratado.

O escopo compreende servidores físicos e virtuais, bancos de dados, sistemas institucionais, páginas e serviços web, estações e pastas de rede, arquivos eletrônicos, configurações e outros componentes cuja perda ou indisponibilidade possa afetar as atividades do RPPS.

3. FUNDAMENTAÇÃO NORMATIVA

- Política de Segurança da Informação aplicável ao FAPES/TOLEDOPREV, instituída pelo Decreto Municipal nº 1.802/2026, e seus anexos vigentes.
- Manual M009 – Gestão de Contingências e Recuperação de Desastres.
- Manual M010 – Gestão e Controle de Acessos Físicos e Lógicos.
- Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD.
- Contratos, acordos de nível de serviço, manuais dos sistemas e procedimentos técnicos mantidos pelo DTI, pelos órgãos gestores e pelos fornecedores.

Em caso de divergência, prevalecem a legislação e os atos normativos vigentes. Os procedimentos técnicos devem permanecer alinhados à Política de Segurança da Informação, ao plano de recuperação de desastres e aos contratos aplicáveis.

4. CONCEITOS E SIGLAS

Termo ou sigla	Definição
Cópia de segurança	Cópia de dados, configurações ou ambiente mantida para permitir recuperação após perda, alteração indevida, falha ou indisponibilidade.
Backup completo	Cópia integral do conjunto de dados definido na rotina.
Backup incremental	Cópia das alterações ocorridas após o último backup considerado pela ferramenta.
Snapshot ou shadow copy	Registro do estado de dados ou de ambiente em determinado momento, utilizado como mecanismo complementar de recuperação.
Replicação	Manutenção de cópia sincronizada em outro equipamento, cluster, local ou ambiente.
Restauração	Recuperação de arquivo, banco de dados, sistema, máquina virtual ou ambiente a partir de cópia disponível.
Teste de restauração	Execução controlada destinada a comprovar que a cópia pode ser recuperada e utilizada.
RPO	Ponto máximo de perda de dados admitido, medido entre a última cópia recuperável e o evento de indisponibilidade.
RTO	Tempo esperado para restabelecer o serviço após a decisão de recuperação.
DTI, GSI e CSI	Departamento de Tecnologia da Informação; Gestão de Segurança da Informação; Comitê de Segurança da Informação.

5. DIRETRIZES DO PROCESSO

- As rotinas devem abranger os dados e ambientes necessários à continuidade dos serviços e observar a criticidade, a frequência de alteração e o impacto de perda ou indisponibilidade.

- A execução deve ser automatizada sempre que tecnicamente possível. O DTI ou o fornecedor responsável deve monitorar os resultados e tratar as falhas registradas.
- A cópia deve permanecer separada do ambiente de produção em extensão suficiente para não ser comprometida pelo mesmo evento. Replicação e alta disponibilidade complementam, mas não substituem, a cópia de segurança recuperável.
- O acesso às ferramentas, mídias, repositórios e chaves de proteção deve ser restrito, individualizado e rastreável.
- As cópias que contenham dados pessoais ou informações restritas devem receber proteção compatível com a classificação da informação, inclusive durante transferência e armazenamento.
- A capacidade de recuperação deve ser comprovada por testes periódicos e após alterações relevantes na infraestrutura, no sistema ou na rotina de backup.
- Falha, indisponibilidade de cópia, perda de retenção ou resultado insatisfatório de teste deve gerar registro, análise do risco e providência com responsável e prazo.
- Os horários, ferramentas e comandos podem ser mantidos em procedimentos técnicos próprios. Sua alteração não exige revisão deste manual quando o escopo, os controles e a capacidade de recuperação forem preservados e a mudança for registrada.

6. RESPONSABILIDADES

Responsável	Atribuições no processo
Diretoria-Executiva do TOLEDOPREV	Identificar prioridades institucionais; autorizar restaurações que afetem serviços ou dados do RPPS; validar o resultado com a unidade interessada; encaminhar riscos e providências às instâncias competentes.
Departamento de Tecnologia da Informação – DTI	Administrar as rotinas sob sua responsabilidade; configurar, executar e monitorar cópias; tratar falhas; proteger os repositórios; restaurar dados e ambientes; manter procedimentos técnicos, registros e evidências; informar indisponibilidades relevantes.
Gestão de Segurança da Informação – GSI	Acompanhar a aplicação dos controles; avaliar riscos e exceções; coordenar ou verificar testes de restauração quando atribuídos; registrar achados e acompanhar providências.
Comitê de Segurança da Informação – CSI	Acompanhar riscos relevantes, resultados de testes, exceções e medidas de melhoria, conforme as competências definidas na Política de Segurança da Informação.
Unidade proprietária da informação	Informar os dados e serviços necessários; solicitar restauração por canal verificável; indicar o resultado esperado; validar o conteúdo ou a funcionalidade após a recuperação.
Gestor e fiscal do contrato	Verificar obrigações de backup, retenção, segurança, suporte e restauração previstas no contrato e registrar ocorrências e providências.
Órgãos gestores e fornecedores	Executar as rotinas contratadas ou sob sua administração; proteger as cópias; comunicar falhas; fornecer confirmação, log ou relatório disponível; apoiar testes e restaurações.
Usuários autorizados	Armazenar arquivos nos repositórios institucionais definidos; não manter a única cópia de informação institucional em dispositivo local; comunicar perda, alteração indevida ou necessidade de recuperação.

7. ENTRADAS, SAÍDAS, SISTEMAS E REPOSITÓRIOS

Categoria	Elementos
Entradas	Inventário de sistemas e dados; classificação e criticidade; requisitos de RPO e RTO; agenda de backup; alertas e logs; solicitação de restauração; alteração de infraestrutura ou sistema.
Saídas	Cópia concluída e protegida; falha tratada; dados ou ambiente restaurado; teste registrado; retenção aplicada; risco e medida de melhoria acompanhados.
Ambientes	Infraestrutura física e virtual municipal; servidores de arquivos; bancos de dados; sistemas governamentais e contratados; páginas e serviços web; repositórios institucionais.
Repositórios de evidências	Console ou ferramenta de backup; logs; sistema de chamados; e-mail institucional; SEI; pasta institucional com acesso controlado; relatórios e atas do CSI, quando aplicável.

8. DESCRIÇÃO DO PROCESSO

8.1. Identificar o escopo e a criticidade

O DTI, com apoio da Diretoria-Executiva, da GSI e dos responsáveis pelos sistemas, identifica os dados, ambientes e configurações que precisam de cópia. A avaliação considera o impacto da perda, a frequência de alteração, a dependência de terceiros e as prioridades definidas no plano de recuperação de desastres.

8.2. Configurar e programar as rotinas

O responsável técnico define a origem, o destino, o método, a periodicidade, a retenção, a proteção e a forma de monitoramento. A configuração deve observar a capacidade disponível, a janela de execução e os requisitos de RPO e RTO. Alterações relevantes devem ser registradas e avaliadas antes de entrarem em produção.

8.3. Executar e monitorar as cópias

A ferramenta executa a rotina conforme a programação. O DTI ou o fornecedor acompanha alertas, logs, capacidade e resultado da execução. A conclusão indicada pela ferramenta não dispensa a verificação de erros, arquivos ignorados, retenção interrompida ou outra condição que comprometa a recuperação.

8.4. Tratar falhas

Quando a execução não for concluída, o responsável registra a ocorrência, identifica a causa, corrige a configuração ou a infraestrutura e reexecuta a rotina quando necessário. A falha que reduza a capacidade de recuperação além do limite aceito deve ser comunicada à Diretoria-Executiva e à GSI, com avaliação do risco e definição de prazo para tratamento.

8.5. Armazenar, replicar e proteger

As cópias devem permanecer em repositório destinado à recuperação, com controle de acesso, capacidade, integridade e proteção contra alteração ou exclusão indevida. Sempre que aplicável, deve existir cópia ou réplica em equipamento, área ou ambiente distinto do recurso de produção.

8.6. Solicitar e autorizar a restauração

A unidade interessada identifica o arquivo, o sistema, o período e a finalidade da recuperação e encaminha a solicitação por canal verificável. O DTI confirma a disponibilidade da cópia, avalia o impacto e obtém autorização da autoridade competente quando a restauração puder substituir dados, interromper serviço ou afetar terceiros.

8.7. Restaurar e validar

O DTI ou o fornecedor restaura o arquivo, banco de dados, máquina virtual ou ambiente em local controlado ou diretamente no serviço, conforme o risco e o procedimento técnico. A unidade proprietária valida o conteúdo ou a funcionalidade. O atendimento registra a cópia utilizada, o horário, o executor, o resultado e eventual limitação.

8.8. Testar a recuperação

A capacidade de restauração deve ser testada ao menos uma vez por ano e após alteração relevante que possa afetar o processo. O teste deve abranger amostra representativa dos serviços críticos, preservar o ambiente de produção e registrar o tempo de recuperação, o resultado, as limitações e as providências necessárias.

8.9. Aplicar retenção e descarte

A ferramenta mantém as cópias pelo prazo definido na matriz de retenção. O descarte ocorre de forma automática ou controlada, sem eliminar cópia sujeita a preservação específica. A retenção deve ser revista quando houver mudança de criticidade, capacidade, obrigação legal ou contratual.

8.10. Revisar a rotina

O DTI revisa o escopo e as configurações das rotinas de backup ao menos anualmente e quando houver inclusão, substituição ou descontinuidade de sistema, mudança de fornecedor, incidente, falha recorrente ou resultado insatisfatório de teste. A revisão técnica deve confirmar responsáveis, cobertura, periodicidade, retenção, repositórios, alertas e capacidade de recuperação. Sua realização não exige, por si só, alteração deste manual, salvo quando modificar responsabilidades, controles ou diretrizes institucionalizadas.

9. LINHA DE BASE TÉCNICA

A tabela consolida os parâmetros técnicos adotados como linha de base nesta Revisão 01 do M015. Com a validação desta revisão, esses parâmetros passam a constituir a referência inicial para a execução, o monitoramento e a verificação das rotinas de cópia de segurança. O DTI e os fornecedores responsáveis deverão verificar sua atualidade e aplicabilidade durante a operação, mantendo registro das verificações e das alterações realizadas. A matriz poderá ser mantida como registro técnico controlado e atualizada sempre que necessário, desde que cada alteração seja formalmente registrada e não modifique as diretrizes, as responsabilidades ou os controles estabelecidos neste Manual.

Recurso ou ambiente	Linha de base informada	Pontos de verificação
Máquinas virtuais e bancos de dados municipais	Proteção no cluster e cópia pelo Veeam; execução automatizada; cópias completas e incrementais conforme agenda técnica.	Confirmar escopo, horários, alertas, localização das cópias e responsável pelo monitoramento.
Servidor de arquivos e pasta institucional	Cópia diária pelo Veeam; cópia completa semanal; mecanismo shadow duas vezes ao dia; replicação entre áreas do datacenter.	Confirmar horários, cobertura da pasta atual, redundância entre sites e procedimento de restauração.
Sistema de benefícios administrado pela FAC	Rotina local programada em dias úteis e cópia para repositório institucional.	Confirmar ferramenta, automação, responsável, evidência e destino atualmente utilizados.
Servidor web e banco de dados web	Cópia dos arquivos e exportação do banco de dados, com transferência para repositório local.	Confirmar se a rotina está automatizada, sua periodicidade, retenção, proteção e teste de recuperação.
Retenção	Cópias diárias por 7 dias; semanais por 30 dias; mensais e anuais por 1 ano.	Confirmar adequação aos serviços críticos, capacidade, contratos, RPO, RTO e regras de temporalidade.

10. CONTROLES E SEGREGAÇÃO DE FUNÇÕES

Controle	Aplicação mínima
Cobertura	Inventário relaciona sistemas, dados, responsável, periodicidade, retenção e repositório.
Monitoramento	Logs e alertas identificam conclusão, falha, capacidade insuficiente e retenção interrompida.
Acesso restrito	Administração das ferramentas e repositórios é limitada a usuários autorizados e rastreáveis.
Separação do ambiente	A cópia recuperável não depende exclusivamente do mesmo equipamento ou área do ambiente de produção.
Integridade e proteção	Cópias são verificadas e recebem proteção compatível com a informação armazenada.
Autorização de restauração	Restaurações com impacto são autorizadas e validadas pela unidade competente.
Teste periódico	Teste anual e após alteração relevante comprova recuperação e registra resultado e tempo.
Segregação	Quem solicita e valida a recuperação não substitui o executor técnico; alterações críticas exigem registro e autorização.

11. RISCOS E MEDIDAS DE CONTROLE

Risco	Medida de controle
Dados ou sistemas fora do escopo	Manter inventário, revisar cobertura e vincular a rotina às prioridades do plano de recuperação.
Falha não identificada	Monitorar alertas e logs, definir responsável e registrar correção e reexecução.
Cópia comprometida pelo mesmo evento	Manter cópia ou réplica separada e restringir credenciais administrativas.

Risco	Medida de controle
Cópia íntegra mas não recuperável	Realizar testes periódicos de restauração com evidência e tratamento dos achados.
Acesso indevido a dados copiados	Aplicar controle de acesso, rastreabilidade e proteção durante transferência e armazenamento.
Retenção insuficiente	Manter matriz de retenção e revisar prazos conforme criticidade, contratos e capacidade.
Restauração incorreta ou destrutiva	Exigir solicitação, autorização, ambiente controlado quando aplicável e validação da unidade proprietária.
Dependência de fornecedor	Definir obrigação contratual, evidências, suporte, prazos, teste e procedimento de transição ou encerramento.

12. REGISTROS E EVIDÊNCIAS

Registro ou evidência	Responsável principal	Repositório
Inventário e matriz das rotinas de backup	DTI	Procedimento técnico ou pasta controlada.
Logs, relatórios e alertas de execução	DTI ou fornecedor	Console da ferramenta e repositório definido.
Registro de falha, correção e reexecução	DTI ou fornecedor	Chamado, log, e-mail institucional ou sistema aplicável.
Solicitação e autorização de restauração	Unidade solicitante e autoridade competente	Chamado, SEI ou e-mail institucional.
Comprovação da restauração e validação	DTI e unidade proprietária	Chamado, relatório ou pasta controlada.
Plano e relatório de teste	DTI e GSI	SEI ou pasta institucional com acesso controlado.
Achados, riscos e providências	GSI e CSI	Relatório, plano de ação e ata, quando aplicável.
Evidências contratuais	Gestor e fiscal do contrato	Processo administrativo ou SEI.

As evidências devem permanecer em repositório institucional autorizado, com acesso restrito, integridade, disponibilidade e prazo de guarda compatível com a finalidade, a gestão documental e a segurança da informação.

13. INDICADORES RECOMENDADOS

Indicador	Critério
Cobertura das rotinas	Percentual de sistemas e repositórios críticos incluídos em rotina de cópia validada.
Execuções concluídas	Percentual de rotinas concluídas sem erro no período.
Falhas tratadas no prazo	Percentual de falhas corrigidas dentro do prazo definido conforme o risco.
Testes realizados	Percentual de serviços críticos testados no ciclo anual.
Sucesso da restauração	Percentual de testes e solicitações concluídos com dados ou serviço validados.
Atendimento do RTO	Percentual de recuperações concluídas dentro do tempo definido para o serviço.

Quando não houver dados suficientes para calcular o indicador, a limitação e a providência necessária deverão ser registradas. As metas serão definidas com base na matriz técnica e nos parâmetros de recuperação vigentes.

14. DISPOSIÇÕES FINAIS

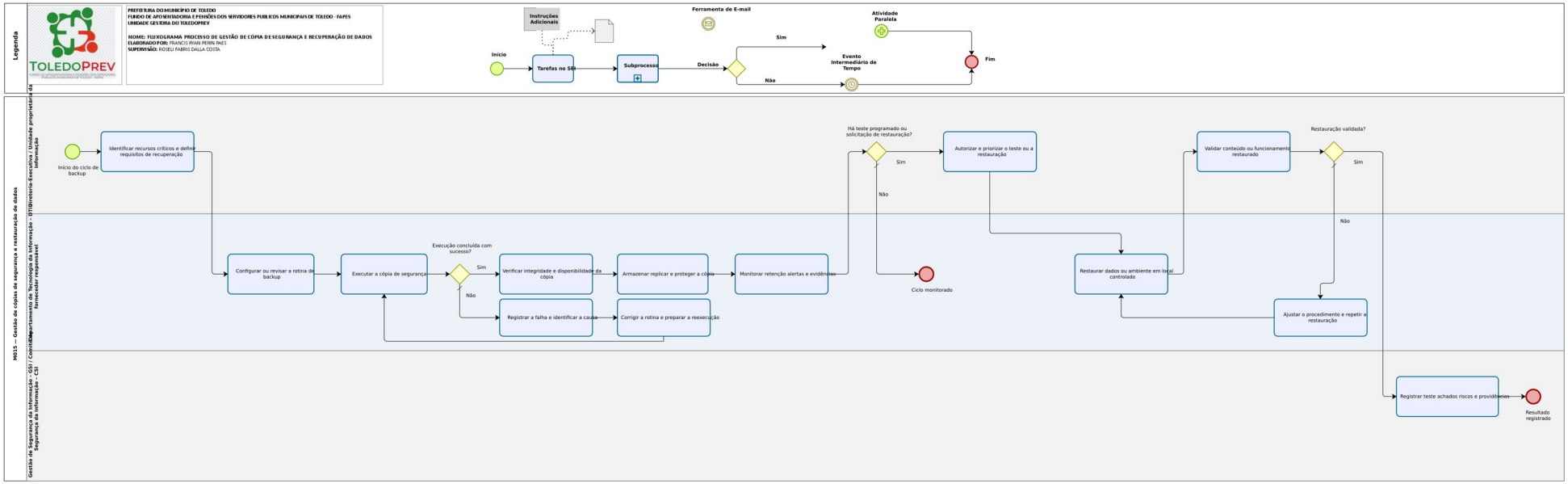
Este manual deverá ser revisto quando houver alteração relevante na Política de Segurança da Informação, no plano de recuperação de desastres, na infraestrutura, nos sistemas, nos fornecedores, nas responsabilidades, nos requisitos legais ou nos controles do processo, bem como quando incidentes, testes, auditorias ou avaliações de risco indicarem necessidade de atualização.

Os procedimentos técnicos detalhados permanecem sob responsabilidade do DTI, dos órgãos gestores e dos fornecedores, conforme o recurso. Eles podem ser atualizados sem alterar a essência deste manual, desde que a mudança seja registrada, preserve a capacidade de recuperação e seja comunicada aos responsáveis afetados.

Os casos omissos e as exceções serão submetidos à Diretoria-Executiva, com apoio da GSI e do DTI. Riscos relevantes, falhas recorrentes e medidas de melhoria serão encaminhados ao CSI conforme a Política de Segurança da Informação.

ANEXO I – FLUXOGRAMA DO PROCESSO

Processo de Gestão de Cópias de Segurança e Restauração de Dados



Fluxo aplicável à execução, ao monitoramento, à restauração e aos testes das cópias de segurança.