MAPEAMENTO E MANUALIZAÇÃO

# GESTÃO DE CONTINGÊNCIAS E RECUPERAÇÃO DE DESASTRES

**Manual M009**

Revisão 02 – Aprovado e validado

5 de outubro de 2026

# IDENTIFICAÇÃO

| Campo | Informação |
|---|---|
| **Código** | M009 |
| **Processo** | Gestão de contingências e recuperação de desastres |
| **Unidade responsável** | Diretoria-Executiva do TOLEDOPREV e Gestão de Segurança da Informação – GSI |
| **Unidades participantes** | Departamento de Tecnologia da Informação – DTI, Comitê de Segurança da Informação – CSI, unidades usuárias, gestores dos sistemas e fornecedores, quando aplicável |
| **Periodicidade** | Processo contínuo; teste do DRP, no mínimo, anual; revisão do Manual quando houver alteração relevante no ambiente tecnológico, institucional ou normativo, ou em consonância com a revisão do DRP e da PSI. |
| **Finalidade** | Estabelecer o fluxo operacional de identificação, comunicação, acionamento, continuidade, recuperação, validação, encerramento e melhoria após incidentes graves ou desastres |

# CONTROLE DE REVISÕES

| Revisão | Data | Descrição |
|---|---|---|
| 00 | 12/11/2020 | Elaboração inicial. |
| 01 | 01/03/2023 | Atualização da logomarca. |
| 02 | 05/10/2026 | Revisão integral do processo, com atualização do escopo, das responsabilidades, dos procedimentos de contingência e recuperação, dos controles, das evidências, dos indicadores e do fluxograma, em alinhamento ao Decreto Municipal nº 1.802/2026 e ao DRP. |

# APROVAÇÃO E VALIDAÇÃO

| Etapa | Responsável | Data/Registro |
|---|---|---|
| Elaboração técnica | Gestão de Segurança da Informação – GSI e Departamento de Tecnologia da Informação – DTI | 02/10/2026 |
| 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....5
5. DIRETRIZES DO PROCESSO....5
6. RESPONSABILIDADES....6
7. SERVIÇOS CRÍTICOS E PRIORIDADES....7
    7.1. Classificação para acionamento....7
8. DESCRIÇÃO DO PROCESSO....7
    8.1. Identificação e registro inicial....7
    8.2. Avaliação e decisão de acionamento....7
    8.3. Comunicação e mobilização....7
    8.4. Contenção e continuidade....7
    8.5. Definição da estratégia de recuperação....8
    8.6. Recuperação e restauração....8
    8.7. Validação e retorno à operação....8
    8.8. Encerramento e relatório....8
    8.9. Testes periódicos....8
    8.10. Acompanhamento das melhorias....8
9. PARÂMETROS DE RECUPERAÇÃO E ESTRATÉGIAS....8
10. CONTROLES E SEGREGAÇÃO DE FUNÇÕES....9
11. REGISTROS E EVIDÊNCIAS....9
12. RISCOS E MEDIDAS DE CONTROLE....9
13. INDICADORES RECOMENDADOS....10
14. DISPOSIÇÕES FINAIS....10
ANEXO I – FLUXOGRAMA DO PROCESSO....11

## 1. OBJETIVO

Estabelecer os procedimentos operacionais para identificação, comunicação, acionamento, continuidade, recuperação, validação e encerramento de incidentes graves ou desastres que afetem os sistemas, as bases de dados, os equipamentos e os serviços tecnológicos utilizados pelo FAPES/TOLEDOPREV.

O Manual complementa o Plano de Recuperação de Desastres – DRP, previsto no Anexo III do Decreto Municipal nº 1.802/2026, e orienta a execução prática do processo sem substituir as competências técnicas do Departamento de Tecnologia da Informação – DTI nem as rotinas específicas de cópia de segurança disciplinadas no M015.

## 2. ABRANGÊNCIA

Aplica-se às unidades do TOLEDOPREV, à Gestão de Segurança da Informação – GSI, ao DTI, ao Comitê de Segurança da Informação – CSI, aos gestores dos sistemas, aos usuários e aos fornecedores que participem da sustentação ou recuperação de serviços tecnológicos.

Abrange os sistemas previdenciários, a folha de pagamento de benefícios, as bases previdenciárias e cadastrais, os sistemas administrativos essenciais, o site institucional, os servidores de arquivos, as máquinas virtuais, a conectividade e os demais componentes necessários à continuidade das atividades essenciais. Para serviços externos, o Manual aplica-se às providências sob controle do TOLEDOPREV, como registro, comunicação, acionamento do fornecedor, acompanhamento e validação do retorno.

## 3. FUNDAMENTAÇÃO NORMATIVA

| Referência | Aplicação ao processo |
|---|---|
| **Decreto Municipal nº 1.802/2026** | Política de Segurança da Informação do FAPES/TOLEDOPREV e Anexo III – Plano de Recuperação de Desastres. |
| **Lei Federal nº 13.709/2018** | Lei Geral de Proteção de Dados Pessoais – LGPD, especialmente quanto à segurança e ao tratamento de incidentes que envolvam dados pessoais. |
| **Manual do Pró-Gestão RPPS** | Dimensão Controles Internos, requisitos de segurança da informação, continuidade, auditoria e evidências aplicáveis ao nível de certificação pretendido. |
| **M010** | Gestão e controle de acessos físicos e lógicos, inclusive acessos emergenciais, temporários e registros de concessão ou bloqueio. |
| **M015** | Cópias de segurança, restauração e proteção das bases de dados, incluindo rotinas, retenção, monitoramento e testes técnicos de restauração. |

## 4. CONCEITOS E SIGLAS

| Termo | Definição |
|---|---|
| **Backup válido** | Cópia íntegra, disponível e apta a ser utilizada em procedimento de restauração. |
| **Continuidade** | Manutenção das atividades essenciais em nível aceitável durante a indisponibilidade ou recuperação. |
| **Desastre** | Evento que provoque interrupção prolongada ou indisponibilidade total de sistemas e serviços críticos. |
| **DRP** | Plano de Recuperação de Desastres. |
| **GSI** | Gestão de Segurança da Informação. |
| **Incidente grave** | Evento que comprometa significativamente a disponibilidade, a integridade ou a confidencialidade das informações ou dos sistemas. |
| **RPO** | Ponto Objetivo de Recuperação: limite máximo aceitável de perda de dados, medido em tempo, a partir do último backup válido. |
| **RTO** | Tempo Objetivo de Recuperação: tempo máximo aceitável para restabelecimento do serviço após incidente grave ou desastre. |

## 5. DIRETRIZES DO PROCESSO

- A proteção da vida, da segurança das pessoas e da integridade do ambiente físico prevalece sobre a recuperação tecnológica.
- A ativação do DRP deve ser proporcional ao impacto, à criticidade do serviço e à estimativa de indisponibilidade.
- A recuperação deve observar as prioridades institucionais, os parâmetros de RTO e RPO e a utilização de cópia tecnicamente validada.
- Toda ação relevante deve ser registrada, inclusive decisões, responsáveis, horários, sistemas afetados, pontos de restauração, testes e resultados.
- O retorno à operação exige validação técnica e validação funcional pela unidade responsável pelo serviço ou pela informação.
- As credenciais emergenciais e os acessos extraordinários devem seguir o M010, com prazo, finalidade, rastreabilidade e revogação após o uso.
- Os detalhes sensíveis do incidente devem circular apenas entre os responsáveis e pelos canais institucionais autorizados.
- Cada incidente ou teste deve resultar em aprendizado, plano de ação e acompanhamento das melhorias necessárias.

## 6. RESPONSABILIDADES

| Responsável | Atribuições |
|---|---|
| **Diretoria-Executiva** | Definir prioridades institucionais quando houver conflito entre serviços; autorizar medidas administrativas extraordinárias; acompanhar impactos relevantes; decidir sobre comunicação institucional externa, quando necessária. |
| **Gestão de Segurança da Informação – GSI** | Coordenar a ativação e a condução do DRP; registrar o incidente; articular GSI, DTI, unidades e fornecedores; consolidar registros e relatórios; submeter resultados e melhorias ao CSI. |
| **Departamento de Tecnologia da Informação – DTI** | Avaliar tecnicamente o incidente; conter danos; executar recuperação, restauração e validação técnica; assegurar disponibilidade dos recursos e backups; registrar procedimentos, tempos, logs e resultados. |
| **Comitê de Segurança da Informação – CSI** | Acompanhar a aplicação do DRP; tomar ciência dos incidentes relevantes e dos testes; avaliar resultados; recomendar melhorias e acompanhar providências. |
| **Unidade responsável pelo serviço ou dado** | Comunicar a indisponibilidade; informar impacto e prioridade operacional; apoiar a continuidade; validar funcionalidades e consistência das informações após a recuperação. |
| **Usuários** | Interromper ações que possam ampliar o dano; preservar evidências; comunicar imediatamente pelos canais definidos; seguir orientações do GSI e do DTI. |
| **Fornecedores** | Atender ao acionamento conforme contrato; apoiar diagnóstico e recuperação; fornecer registros e evidências; comunicar limitações e previsão de restabelecimento. |

Quando uma mesma pessoa exercer formalmente as funções de GSI e de responsável técnico pela execução, cada atuação deverá ser registrada de forma distinta, e os resultados serão submetidos à Diretoria-Executiva e ao CSI para assegurar supervisão e rastreabilidade.

# 7. SERVIÇOS CRÍTICOS E PRIORIDADES

| Prioridade | Sistema ou serviço | RTO máximo | RPO máximo |
|---|---|---|---|
| 1 | Sistema previdenciário | Até 24 horas | Até 24 horas |
| 1 | Folha de pagamento de benefícios | Até 24 horas | Até 24 horas |
| 1 | Bases de dados previdenciárias e cadastrais | Até 24 horas | Até 24 horas |
| 2 | Sistemas administrativos essenciais | Até 48 horas | Até 24 horas |
| 2 | Site institucional | Até 48 horas | Até 24 horas |

A prioridade indicada é a referência inicial. A GSI e o DTI poderão ajustar a ordem de recuperação conforme o impacto concreto, a dependência entre serviços, a proximidade de fechamento de folha ou de obrigação legal, a existência de solução alternativa e a disponibilidade dos recursos técnicos. A alteração deverá ser registrada.

## 7.1. Classificação para acionamento

| Classificação | Critério | Tratamento |
|---|---|---|
| **Ocorrência operacional** | Falha localizada, com solução pelo atendimento regular e sem comprometimento significativo de serviço crítico. | Registrar no canal técnico; não ativar o DRP, salvo agravamento. |
| **Incidente grave** | Comprometimento significativo da disponibilidade, integridade ou confidencialidade, com risco de ultrapassar a tolerância do serviço. | Comunicar imediatamente ao GSI e ao DTI; avaliar ativação parcial ou total do DRP. |
| **Desastre** | Interrupção prolongada, indisponibilidade total ou impacto simultâneo em serviços críticos ou na infraestrutura essencial. | Ativar o DRP; priorizar continuidade e recuperação; informar a Diretoria-Executiva e o CSI. |

# 8. DESCRIÇÃO DO PROCESSO

## 8.1. Identificação e registro inicial

Qualquer usuário, unidade, ferramenta de monitoramento ou fornecedor que identifique indisponibilidade, comportamento anormal, corrupção de dados ou evento de segurança deverá comunicar imediatamente ao DTI e ao GSI. O registro inicial deve conter, quando disponível: data e horário, comunicante, serviço afetado, sintomas, usuários impactados, evidências e ações já realizadas.

## 8.2. Avaliação e decisão de acionamento

O DTI realiza o diagnóstico inicial e estima impacto, abrangência, dependências, possibilidade de correção imediata e tempo provável de restabelecimento. A GSI classifica a ocorrência e decide pela ativação parcial ou total do DRP, registrando a decisão e a prioridade. Medidas técnicas urgentes de contenção podem ser executadas antes da formalização quando a espera puder ampliar o dano, com comunicação imediata ao GSI.

## 8.3. Comunicação e mobilização

Confirmada a ativação, a GSI comunica a Diretoria-Executiva, mobiliza DTI, unidade responsável e fornecedores necessários e informa ao CSI nos casos relevantes. As comunicações aos usuários devem apresentar impacto, orientação temporária e atualizações de situação, sem divulgar credenciais, vulnerabilidades ou informações técnicas sensíveis.

## 8.4. Contenção e continuidade

O DTI deve isolar componentes comprometidos, preservar logs e evidências e impedir propagação ou perda adicional. A unidade responsável aplica alternativas temporárias previamente definidas, quando disponíveis, mantendo controles de acesso, proteção de dados e registro das operações realizadas durante a contingência.

### 8.5. Definição da estratégia de recuperação

O DTI identifica a última cópia válida compatível com o RPO, verifica dependências e define a sequência técnica de restauração. Sempre que viável, a recuperação deve ocorrer em ambiente controlado ou isolado, especialmente em testes de máquina virtual, para evitar sobreposição com o ambiente de produção.

### 8.6. Recuperação e restauração

A recuperação deve ser executada por pessoal autorizado, conforme procedimentos técnicos aplicáveis. Devem ser registrados: origem e data da cópia, sistemas e componentes restaurados, horários de início e término, responsáveis, comandos ou ferramentas relevantes, falhas encontradas e medidas adotadas.

### 8.7. Validação e retorno à operação

O DTI valida infraestrutura, inicialização, conectividade, logs, permissões e integridade técnica. A unidade responsável valida funcionalidades, dados essenciais e continuidade do processo de negócio. O retorno à produção somente será confirmado após registro das validações e comunicação da GSI aos envolvidos.

### 8.8. Encerramento e relatório

Após a normalização, a GSI consolida a linha do tempo, o impacto, os tempos observados, a aderência a RTO e RPO, a causa conhecida ou provável, as decisões adotadas, as evidências, as falhas e as ações corretivas. O relatório deve ser encaminhado à Diretoria-Executiva e submetido à ciência do CSI, com responsáveis e prazos para as medidas de melhoria.

### 8.9. Testes periódicos

O DRP deve ser testado, no mínimo, uma vez ao ano, por simulação e/ou restauração controlada. O plano do teste deve definir escopo, ambiente, responsáveis, critérios de sucesso, medidas para evitar impacto na produção e evidências esperadas. O relatório do teste conterá, no mínimo, data, sistemas testados, tempo de recuperação, aderência a RTO e RPO, falhas, ações corretivas e assinaturas previstas no DRP.

### 8.10. Acompanhamento das melhorias

A GSI mantém controle das medidas decorrentes de incidentes e testes. O CSI acompanha o cumprimento dos prazos e avalia a necessidade de atualização do DRP, deste Manual, do M010, do M015 ou de procedimentos técnicos do DTI.

## 9. PARÂMETROS DE RECUPERAÇÃO E ESTRATÉGIAS

| Objeto | Estratégia mínima |
|---|---|
| **Arquivos e pastas** | Restauração de versão anterior ou cópia válida, preferencialmente em local alternativo para validação antes da substituição. |
| **Máquina virtual** | Snapshot ou imagem de backup, com inicialização e validação controladas; recovery integral deve ser testado em ambiente isolado quando houver risco de conflito com a produção. |
| **Base de dados** | Restauração coordenada com verificação de integridade, consistência e ponto temporal, observadas dependências com aplicações. |
| **Serviço externo** | Registro e acionamento do fornecedor; acompanhamento de status; adoção de alternativa operacional, quando existente; validação após retorno. |
| **Conectividade ou infraestrutura** | Acionamento do DTI e dos prestadores; priorização dos serviços críticos; uso de recursos alternativos autorizados, quando disponíveis. |

As frequências, tecnologias, locais de armazenamento, retenções e verificações de backup são mantidas no M015 e nos documentos técnicos do DTI. O M009 utiliza essas cópias no processo de recuperação e exige comprovação de validade e rastreabilidade.

## 10. CONTROLES E SEGREGAÇÃO DE FUNÇÕES

| Ponto de controle | Regra |
|---|---|
| **Ativação** | Decisão coordenada pela GSI, com diagnóstico técnico do DTI e registro da classificação. |
| **Execução técnica** | Realizada pelo DTI ou fornecedor autorizado; usuários não devem executar restauração por iniciativa própria. |
| **Validação** | Validação técnica pelo DTI e funcional pela unidade responsável; a mesma evidência deve identificar ambas. |
| **Acesso emergencial** | Concessão temporária, com finalidade, prazo, registro, monitoramento e revogação conforme M010. |
| **Retorno à produção** | Confirmado após validação e comunicação formal aos envolvidos. |
| **Supervisão** | Resultados submetidos à Diretoria-Executiva e ao CSI; acumulação de funções deve ser explicitada nos registros. |

## 11. REGISTROS E EVIDÊNCIAS

| Registro | Conteúdo mínimo | Responsável |
|---|---|---|
| Registro inicial do incidente | Data, horário, comunicante, serviço, descrição, impacto e evidências disponíveis. | GSI/DTI |
| Registro de ativação | Classificação, decisão, escopo, prioridades e responsáveis mobilizados. | GSI |
| Registros técnicos | Logs, tickets, cópia utilizada, comandos, horários, falhas, capturas e resultados. | DTI/fornecedor |
| Validação pós-recuperação | Checklist técnico e validação funcional dos dados e serviços. | DTI/unidade responsável |
| Relatório de incidente ou teste | Linha do tempo, RTO/RPO, resultados, limitações, causas e ações corretivas. | GSI e responsável técnico |
| Plano de ação | Medida, responsável, prazo, situação e evidência de conclusão. | GSI/CSI |
| Ciência da governança | Encaminhamento, ata ou registro de ciência da Diretoria-Executiva e do CSI. | GSI/Secretaria do CSI |

Os registros deverão ser mantidos em repositório institucional com controle de acesso, integridade, disponibilidade e prazo de guarda compatível com as normas aplicáveis, permanecendo disponíveis para auditoria, certificação e prestação de contas.

## 12. RISCOS E MEDIDAS DE CONTROLE

| Risco | Possível consequência | Medida de controle |
|---|---|---|
| Demora na identificação ou no acionamento | Indisponibilidade prolongada e descumprimento do RTO. | Canais definidos, comunicação imediata, contatos atualizados e escalonamento. |
| Cópia inválida ou indisponível | Perda de dados e impossibilidade de restauração. | Monitoramento, testes periódicos e estratégia de backup prevista no M015. |
| Restauração em ponto incorreto | Perda adicional ou inconsistência de dados. | Confirmar RPO, origem, data e integridade antes da restauração. |
| Sobreposição do ambiente de produção | Conflito, interrupção ou perda de evidência. | Preferir ambiente isolado e aprovar previamente o procedimento. |
| Validação insuficiente | Retorno com falhas técnicas ou funcionais. | Checklist técnico e validação pela unidade responsável. |
| Acesso emergencial excessivo | Exposição ou alteração indevida de informações. | Aplicar M010, limitar prazo e privilégio, monitorar e revogar. |
| Registros incompletos | Baixa rastreabilidade e fragilidade perante auditoria. | Modelos padronizados, consolidação pela GSI e ciência do CSI. |

## 13. INDICADORES RECOMENDADOS

| Indicador | Cálculo | Periodicidade | Referência |
|---|---|---|---|
| Execução do teste anual do DRP | Testes realizados ÷ testes previstos × 100 | Anual | 100% |
| Aderência ao RTO | Recuperações dentro do RTO ÷ recuperações executadas × 100 | Por evento e anual | 100% |
| Aderência ao RPO | Recuperações dentro do RPO ÷ recuperações executadas × 100 | Por evento e anual | 100% |
| Conclusão das ações de melhoria | Ações concluídas no prazo ÷ ações previstas × 100 | Trimestral | Tendência de evolução |
| Cobertura dos serviços críticos | Serviços críticos testados no ciclo ÷ serviços críticos mapeados × 100 | Anual | Ampliar progressivamente |

As metas poderão ser ajustadas pelo CSI e pela Diretoria-Executiva conforme a maturidade do processo e os resultados dos testes, sem reduzir os parâmetros mínimos estabelecidos no DRP.

## 14. DISPOSIÇÕES FINAIS

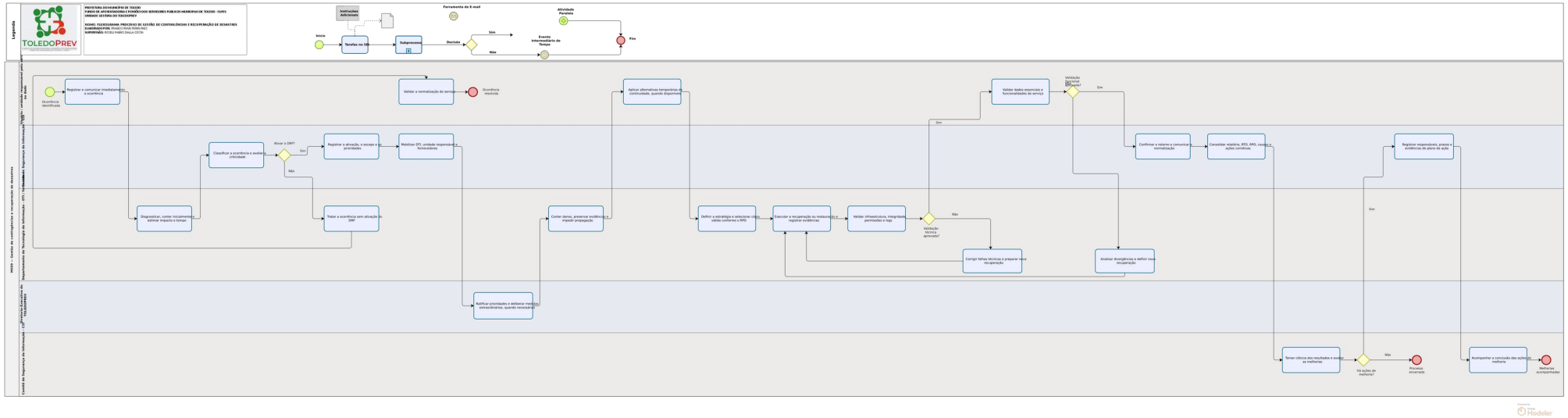
Este Manual deve ser revisto sempre que houver alteração relevante no ambiente tecnológico, institucional ou normativo, ou em consonância com a revisão do Plano de Recuperação de Desastres – DRP e da Política de Segurança da Informação – PSI. A necessidade de revisão deve ser avaliada após incidentes graves e testes do DRP.

Os procedimentos técnicos detalhados poderão ser mantidos pelo DTI em documentos próprios, desde que permaneçam alinhados ao Decreto Municipal nº 1.802/2026, ao DRP, ao M010, ao M015 e às deliberações da governança de segurança da informação.

Os casos omissos serão avaliados pela GSI em conjunto com o DTI e a Diretoria-Executiva, com posterior ciência do CSI quando envolverem risco relevante, alteração permanente do processo ou medida de melhoria institucional.

# ANEXO I – FLUXOGRAMA DO PROCESSO

## Processo de Gestão de Contingências e Recuperação de Desastres



Fluxograma do processo – Revisão 02 | Aprovado e validado em 05/10/2026