MAPEAMENTO E MANUALIZAÇÃO

GESTÃO E CONTROLE DE ACESSOS FÍSICOS E LÓGICOS

Manual M010

Revisão 01 – Aprovado e validado

5 de outubro de 2026

IDENTIFICAÇÃO	INFORMAÇÃO
Código	M010
Processo	Gestão e controle de acessos físicos e lógicos
Unidade responsável	Diretoria-Executiva do TOLEDOPREV, com apoio da Gestão de Segurança da Informação – GSI
Unidades participantes	Departamento de Tecnologia da Informação – DTI; Secretaria Municipal de Recursos Humanos – SMRH; Coordenação de Contabilidade – COORDCONT; Comitê de Segurança da Informação – CSI; órgãos gestores e fornecedores de sistemas, conforme o recurso.
Periodicidade	Revisão anual dos acessos; revisão semestral da pasta compartilhada; revisão extraordinária quando houver mudança funcional, incidente, alteração do sistema ou risco identificado.
Finalidade	Assegurar que os acessos sejam autorizados, compatíveis com a necessidade funcional, rastreáveis e revogados quando deixarem de ser necessários.

Revisão	Data	Descrição
00	09/11/2020	Elaboração inicial.
01	05/10/2026	Revisão integral do processo, com atualização do escopo, das responsabilidades, dos canais de solicitação, dos controles, das evidências e dos fluxos de acesso físico e lógico.

APROVAÇÃO E VALIDAÇÃO

Etapa	Responsável	Data
Elaboração técnica	Gestão de Segurança da Informação – GSI e Departamento de Tecnologia da Informação – DTI	03/10/2026
Validação	Diretoria-Executiva do TOLEDOPREV	05/10/2026

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....6
8. DESCRIÇÃO DO PROCESSO....6
8.1. Identificar a necessidade de acesso ou alteração....6
8.2. Definir e autorizar o perfil....6
8.3. Encaminhar a solicitação....6
8.4. Conceder, alterar ou restabelecer o acesso....7
8.5. Confirmar o atendimento e registrar a evidência....7
8.6. Bloquear ou cancelar o acesso....7
8.7. Realizar a revisão periódica....7
8.8. Auditar os acessos....7
8.9. Controlar o acesso físico....8
8.10. Controlar o acesso de terceiros....8
9. CONTROLES E SEGREGAÇÃO DE FUNÇÕES....8
10. RISCOS E MEDIDAS DE CONTROLE....8
11. REGISTROS E EVIDÊNCIAS....8
12. INDICADORES RECOMENDADOS....9
13. DISPOSIÇÕES FINAIS....9
ANEXO I – FLUXOGRAMA DA GESTÃO DO ACESSO LÓGICO....10
ANEXO II – FLUXOGRAMA DO CONTROLE DE ACESSO FÍSICO....11

1. OBJETIVO

Estabelecer as responsabilidades, os critérios, os controles e a sequência de atividades para solicitar, autorizar, conceder, alterar, revisar, bloquear e cancelar acessos físicos e lógicos relacionados às atividades do TOLEDOPREV. O processo busca assegurar que cada usuário tenha acesso somente aos ambientes, sistemas, informações e recursos necessários ao desempenho de suas atribuições, pelo período necessário e com evidências suficientes para comprovar as decisões e providências adotadas.

Este manual complementa a Política de Segurança da Informação – PSI e seus anexos, especialmente o Manual de Auditoria de Acessos. Os procedimentos técnicos mantidos pelo Município, pelo Ministério da Previdência Social – MPS, pela Dataprev ou pelos fornecedores permanecem aplicáveis aos recursos sob sua administração.

2. ABRANGÊNCIA

Aplica-se aos servidores e demais usuários autorizados que acessem instalações, arquivos físicos, equipamentos, estações de trabalho, redes, pastas compartilhadas, sistemas, bases de dados ou informações utilizadas pelo TOLEDOPREV, ainda que o recurso seja administrado pelo Município, por órgão governamental ou por fornecedor contratado.

O escopo compreende, conforme aplicável, CADPREV, COMPREV/Novo COMPREV, GESCON, Pronto, SIRC, sistemas de simulação e concessão de benefícios, plataforma de investimentos, SCP/contabilidade, SRH/folha, SEI, SIAP/TCE, Consignet, FAC Sistemas, sistemas corporativos municipais, internet, VPN e pastas de rede. A relação é exemplificativa e deve ser atualizada sempre que houver inclusão, substituição ou descontinuidade de recurso.

3. FUNDAMENTAÇÃO NORMATIVA

- Política de Segurança da Informação aplicável ao FAPES/TOLEDOPREV, instituída pelo Decreto Municipal nº 1.802/2026, e seus anexos vigentes, inclusive o Manual de Auditoria de Acessos e o Plano de Recuperação de Desastres.
- Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD.
- Normas municipais de gestão de pessoas, uso de recursos tecnológicos, administração de sistemas, gestão documental e controle patrimonial.
- Contratos, termos de uso, manuais e procedimentos dos sistemas governamentais e dos fornecedores que administram recursos utilizados pelo TOLEDOPREV.
- Relatório de Levantamento dos Controles de Acesso Físico e Lógico – 2026 e respectivos registros de execução e acompanhamento das medidas de melhoria.

Em caso de divergência, prevalecem a legislação e os atos normativos vigentes, seguidos da PSI e dos documentos institucionais específicos.

4. CONCEITOS E SIGLAS

Termo ou sigla	Definição
Acesso físico	Entrada ou permanência em edifício, sala, arquivo ou área em que estejam pessoas, documentos, equipamentos ou infraestrutura tecnológica.
Acesso lógico	Autenticação e autorização para utilizar sistema, rede, equipamento, base de dados, pasta ou serviço digital.
Perfil de acesso	Conjunto de permissões atribuídas ao usuário de acordo com suas atividades e responsabilidades.
Revisão de acesso	Verificação da necessidade de manutenção do acesso e da adequação das permissões concedidas.
Auditoria de acesso	Avaliação dos controles, permissões e registros de acesso segundo a PSI e o Manual de Auditoria de Acessos.
Menor privilégio	Concessão somente das permissões indispensáveis ao desempenho da atividade, pelo período necessário.
GSI	Gestão de Segurança da Informação.
CSI	Comitê de Segurança da Informação.
DTI	Departamento de Tecnologia da Informação do Município.

5. DIRETRIZES DO PROCESSO

- Todo acesso deve decorrer de necessidade funcional identificada e de solicitação ou autorização da unidade competente.
- As credenciais são individuais e intransferíveis. É vedado compartilhar senhas ou contornar mecanismos de autenticação.
- O perfil deve observar o princípio do menor privilégio e, quando aplicável, a segregação de funções.
- Permissões de consulta, inclusão, alteração, exclusão e administração devem ser diferenciadas quando o sistema oferecer essa possibilidade.
- Solicitações, autorizações, concessões, alterações, revisões, bloqueios e cancelamentos devem produzir registro verificável.
- Mudança de atribuição, lotação, substituição, transferência, afastamento relevante, aposentadoria, exoneração, desligamento ou incidente de segurança exige revisão do acesso.
- A comunicação automática do SRH aplica-se aos acessos integrados à matrícula e não dispensa a conferência e o bloqueio dos recursos não integrados.
- O acesso de terceiro deve ser previamente autorizado, limitado ao escopo e ao período necessários e encerrado após a prestação do serviço.

6. RESPONSABILIDADES

Responsável	Atribuições no processo
Diretoria-Executiva / UG do RPPS	Validar a necessidade funcional; solicitar ou autorizar os acessos sob sua competência; definir ou confirmar o perfil; solicitar alterações, bloqueios e cancelamentos; coordenar as revisões periódicas e extraordinárias; acompanhar pendências e manter as evidências institucionais.
SMRH	Solicitar os acessos ao sistema de recursos humanos sob sua gestão e comunicar as movimentações funcionais conforme os procedimentos municipais; apoiar a inativação dos acessos integrados à matrícula.
COORDCONT / chefia da Contabilidade	Solicitar ou confirmar os acessos aos sistemas contábeis de sua competência, indicando o usuário, a finalidade e o perfil necessário.
Departamento de TI – DTI	Receber e executar os chamados relativos aos recursos sob administração municipal; validar a existência de solicitação autorizada; conceder, alterar, bloquear ou remover permissões; registrar o atendimento; fornecer relações de usuários e apoiar as adequações aprovadas.
Gestão de Segurança da Informação – GSI	Acompanhar a aplicação dos controles da PSI; coordenar ou realizar as revisões e auditorias que lhe forem atribuídas; registrar achados, recomendações e providências e encaminhá-los às instâncias competentes.
Comitê de Segurança da Informação – CSI	Acompanhar os resultados das avaliações, os riscos identificados e as medidas de melhoria, conforme suas competências e os registros de reunião.
Órgãos gestores e fornecedores	Processar as solicitações autorizadas; administrar as credenciais dos sistemas sob sua responsabilidade; manter os controles técnicos aplicáveis; fornecer confirmação ou registro das providências, quando disponível e cabível.
Usuário autorizado	Utilizar o acesso exclusivamente para fins institucionais; proteger credenciais e equipamentos; comunicar perda, suspeita de uso indevido ou excesso de permissão; não compartilhar contas; deixar de utilizar o recurso quando cessar a necessidade funcional.

7. ENTRADAS, SAÍDAS, SISTEMAS E REPOSITÓRIOS

Categoria	Elementos
Entradas	Necessidade funcional; designação ou movimentação do servidor; solicitação autorizada; relação de usuários e perfis; alerta de incidente; relatório de auditoria; inclusão, alteração ou descontinuidade de sistema.
Saídas	Acesso concedido, alterado, bloqueado ou cancelado; perfil revisado; divergência tratada; registro de atendimento; relatório de revisão ou auditoria; medida de melhoria acompanhada.
Sistemas governamentais	CADPREV, COMPREV/Novo COMPREV, GESCON, Pronto e SIRC, conforme disponibilidade, atribuições e procedimentos do órgão gestor.
Sistemas municipais	SCP/contabilidade, SRH/folha, SEI, SIAP/TCE, Consignet, rede, internet, VPN, pastas compartilhadas

Categoria	Elementos
	e demais sistemas corporativos.
Sistemas contratados	FAC Sistemas, sistemas de simulação e concessão de benefícios, plataforma de investimentos e outras soluções contratadas pelo RPPS.
Repositórios	Sistema municipal de chamados; protocolos e formulários do MPS/Dataprev; e-mail institucional; SEI; pastas institucionais com acesso controlado; relatórios e atas do CSI.

8. DESCRIÇÃO DO PROCESSO

8.1. Identificar a necessidade de acesso ou alteração

A unidade competente identifica o usuário, o sistema ou recurso, a atividade que fundamenta o acesso, a finalidade, o perfil necessário e o tipo de providência: inclusão, alteração, bloqueio, cancelamento ou restabelecimento. O pedido deve observar as atribuições atuais do usuário e evitar a manutenção automática de permissões anteriores.

8.2. Definir e autorizar o perfil

A autoridade competente confirma a necessidade funcional e define o perfil mínimo. A Diretoria-Executiva/UG do RPPS solicita ou autoriza os acessos aos sistemas do MPS, da Dataprev, aos sistemas contratados pelo RPPS e aos recursos sob sua competência. A SMRH atua nos acessos ao sistema de recursos humanos e a COORDCONT ou a chefia da Contabilidade nos sistemas contábeis, conforme as competências institucionais.

Quando o acesso envolver atividades críticas, a autorização deve considerar a segregação de funções, especialmente nas operações de autorização, movimentação financeira, liquidação, pagamento e registro contábil.

8.3. Encaminhar a solicitação

A solicitação é encaminhada por canal que permita comprovar a autoria, a data, o objeto e a providência requerida:

Tipo de recurso	Autoridade solicitante	Canal e executor
Sistemas do MPS e governamentais	Diretoria-Executiva/UG do RPPS, observados os requisitos do órgão gestor.	Formulário, protocolo ou procedimento oficial do MPS/Dataprev; execução pelo órgão gestor responsável.
Sistema de RH municipal	SMRH, conforme sua competência e a necessidade funcional.	Sistema municipal de chamados; execução pelo DTI ou administrador municipal.
Sistemas contábeis municipais	COORDCONT ou chefia da Contabilidade, conforme a competência.	Sistema municipal de chamados; execução pelo DTI ou administrador municipal.
Demais sistemas e recursos municipais	Diretoria-Executiva, SMRH ou COORDCONT, conforme o recurso.	Sistema municipal de chamados; execução pelo DTI.
Sistemas contratados pelo RPPS	Diretoria-Executiva/UG do RPPS.	E-mail institucional ou canal oficial do fornecedor; execução pelo fornecedor ou administrador do sistema.

O pedido deve identificar o usuário, o recurso, o perfil, a finalidade e a providência solicitada. Senhas não devem ser incluídas no chamado, formulário ou e-mail.

8.4. Conceder, alterar ou restabelecer o acesso

O administrador do sistema verifica a solicitação e a autorização recebidas e executa a providência dentro de sua competência. O perfil concedido deve corresponder ao perfil aprovado. Limitações técnicas, divergências ou necessidade de complementação devem ser comunicadas ao solicitante antes do encerramento do atendimento.

A credencial deve ser disponibilizada diretamente ao usuário por meio seguro. Contas administrativas ou técnicas devem permanecer restritas aos agentes autorizados e ter utilização rastreável sempre que a solução permitir.

8.5. Confirmar o atendimento e registrar a evidência

O executor registra a providência no chamado, protocolo, formulário, e-mail ou comprovante equivalente e comunica o solicitante. O solicitante ou o usuário confirma o funcionamento quando o canal permitir e comunica imediatamente falha, ausência ou excesso de permissão. A evidência deve permanecer vinculada à solicitação que originou a providência.

8.6. Bloquear ou cancelar o acesso

A inativação da matrícula funcional aciona os procedimentos de bloqueio dos acessos integrados ao ambiente municipal. Para os sistemas e serviços não integrados, a unidade responsável deve solicitar diretamente o bloqueio ou o cancelamento ao órgão gestor, ao DTI ou ao fornecedor, conforme o recurso.

Aposentadoria, exoneração, desligamento, transferência, afastamento relevante, substituição ou perda da necessidade funcional exige revisão imediata. Quando houver risco de segurança, o bloqueio deve ser solicitado pelo canal mais rápido disponível e formalizado posteriormente, se necessário. A solicitação e a confirmação da execução devem ser arquivadas.

8.7. Realizar a revisão periódica

A Diretoria-Executiva coordenará, com apoio da GSI e das unidades gestoras, revisão geral anual dos acessos lógicos utilizados pelo TOLEDOPREV. A revisão deve confrontar os usuários e as permissões existentes com as atribuições atuais, identificando contas sem uso ou sem necessidade, perfis excessivos e situações funcionais alteradas.

A pasta compartilhada do TOLEDOPREV no servidor municipal terá revisão semestral de usuários e permissões, com diferenciação entre leitura e leitura/escrita conforme a necessidade funcional. Também será realizada revisão extraordinária sempre que houver mudança funcional, incidente de segurança, alteração relevante do sistema ou risco identificado.

A revisão deve registrar a data, os recursos avaliados, o responsável pela validação e a decisão aplicável a cada usuário: manter, ajustar, bloquear ou cancelar. Quando a relação de usuários não estiver disponível diretamente, a unidade responsável deve solicitá-la ao administrador do sistema e manter o pedido e a resposta como evidência.

8.8. Auditar os acessos

A auditoria de acesso lógico será realizada conforme o Manual de Auditoria de Acessos, Anexo IV da PSI. A GSI realiza ou coordena a atividade dentro das atribuições definidas na política, com apoio do DTI e dos administradores dos sistemas para obtenção das relações de usuários, permissões e registros disponíveis.

A auditoria poderá verificar a autorização, a aderência do perfil à função, contas inativas, privilégios elevados, evidências de concessão e revogação, registros de autenticação e eventos relevantes. Limitações de logs ou de acesso a relatórios devem ser registradas. Os achados, recomendações, responsáveis e prazos de tratamento serão encaminhados à Diretoria-Executiva e ao CSI, conforme a PSI. A auditoria não substitui a revisão funcional periódica; os controles são complementares.

8.9. Controlar o acesso físico

O acesso às dependências do Paço Municipal segue os controles gerais administrados pelo Poder Executivo, com monitoramento por câmeras e atuação da Guarda Municipal. A área ocupada pelos servidores do RPPS integra a estrutura da SMRH e possui recepção compartilhada. Documentos e telas com informação restrita devem permanecer protegidos, e as estações de trabalho devem ser bloqueadas quando o usuário se ausentar.

O arquivo físico de processos de benefícios e documentos de aposentados e pensionistas integra o arquivo funcional municipal e permanece sob acompanhamento de servidor responsável durante o expediente. A consulta, a retirada, a movimentação ou a reprodução de documentos deve atender à finalidade do serviço, às regras de gestão documental e à proteção de dados pessoais. A movimentação deve ser registrada quando o procedimento aplicável assim determinar.

O acesso à infraestrutura tecnológica e ao ambiente de servidores é restrito e administrado pelo DTI. A entrada de técnico ou fornecedor para manutenção deve ser previamente autorizada e acompanhada pelo responsável municipal, conforme as regras locais.

8.10. Controlar o acesso de terceiros

A manutenção da infraestrutura pelos fornecedores não constitui autorização geral para consulta às informações institucionais. Sempre que o serviço exigir acesso de terceiro a conta, ambiente, base ou informação do RPPS, a Diretoria-Executiva deverá autorizar previamente, definir o escopo e o período, exigir identificação individual quando tecnicamente possível e manter registro da autorização, da execução e do encerramento. Encerrada a necessidade, a credencial ou permissão temporária deve ser bloqueada ou cancelada.

9. CONTROLES E SEGREGAÇÃO DE FUNÇÕES

Controle	Aplicação mínima
Autorização prévia	O pedido identifica usuário, recurso, finalidade, perfil e autoridade competente.
Menor privilégio	As permissões concedidas são compatíveis com a atividade e limitadas ao necessário.
Segregação de funções	Perfis críticos não concentram etapas incompatíveis de autorização, movimentação, liquidação, pagamento e registro contábil.
Rastreabilidade	Solicitação, autorização, execução, alteração, revisão e cancelamento permanecem vinculados a evidências verificáveis.
Revisão periódica	Revisão geral anual; pasta compartilhada semestral; revisão extraordinária após evento relevante.
Auditoria lógica	Procedimento executado conforme o Anexo IV da PSI, com registro dos achados e do tratamento.
Bloqueio e cancelamento	Acessos desnecessários, excessivos ou de usuários desligados são bloqueados ou cancelados e a execução é confirmada.
Acesso físico	Áreas, arquivos e infraestrutura seguem controles municipais, restrição e acompanhamento conforme o ambiente.

10. RISCOS E MEDIDAS DE CONTROLE

Risco	Medida de controle
Acesso sem autorização ou sem necessidade	Exigir solicitação autorizada, justificativa funcional e validação do perfil.
Permissão excessiva ou incompatível	Aplicar menor privilégio, diferenciar perfis e realizar revisão periódica.
Manutenção de acesso após mudança funcional	Revisar imediatamente e solicitar alteração, bloqueio ou cancelamento nos recursos integrados e não integrados.
Compartilhamento ou comprometimento de credencial	Proibir o compartilhamento, orientar os usuários, bloquear a conta e acionar a resposta a incidentes quando aplicável.
Acesso de terceiro além do necessário	Autorizar previamente, limitar escopo e período, acompanhar a execução e encerrar a permissão.
Ausência de evidência da providência	Utilizar canal verificável e manter solicitação, autorização e confirmação em repositório institucional.
Exposição física de documentos ou telas	Restringir a consulta, guardar documentos, bloquear estações e acompanhar o acesso ao arquivo e à infraestrutura.
Logs ou relatórios insuficientes	Registrar a limitação, avaliar o risco e encaminhar medida de melhoria ao responsável e ao CSI.

11. REGISTROS E EVIDÊNCIAS

Registro ou evidência	Responsável principal	Repositório
Chamados de TI e respostas de atendimento	Solicitante / DTI	Sistema municipal de chamados.
Formulários, protocolos e confirmações do	Diretoria-Executiva / UG do	Sistema governamental, SEI ou pasta

Registro ou evidência	Responsável principal	Repositório
MPS/Dataprev	RPPS	institucional.
E-mails e confirmações de fornecedores	Diretoria-Executiva	E-mail institucional e pasta controlada.
Relações de usuários, perfis e permissões	Administrador do sistema / GSI	Pasta institucional com acesso controlado.
Registros de revisão anual, semestral e extraordinária	Diretoria-Executiva / GSI	SEI ou pasta institucional.
Solicitações e confirmações de alteração, bloqueio e cancelamento	Unidade competente / executor	Chamado, protocolo, e-mail ou SEI.
Relatórios de auditoria e tratamento dos achados	GSI / CSI	SEI, pasta controlada e ata do CSI, quando aplicável.
Registros de acesso físico, movimentação documental ou manutenção	Unidade responsável / DTI	Repositório previsto no procedimento municipal aplicável.

As evidências devem permanecer em repositório institucional autorizado, com acesso restrito, integridade, disponibilidade e prazo de guarda compatíveis com as regras de gestão documental, temporalidade e segurança da informação.

12. INDICADORES RECOMENDADOS

Indicador	Critério
Cobertura da revisão anual	Percentual de sistemas e recursos revisados em relação ao universo de acessos identificado.
Revisão da pasta compartilhada	Percentual de revisões semestrais realizadas no prazo.
Tratamento das divergências	Percentual de ajustes, bloqueios e cancelamentos concluídos no prazo definido.
Tempo de bloqueio após desligamento ou risco	Prazo entre a comunicação e a confirmação do bloqueio nos recursos aplicáveis.
Tratamento dos achados de auditoria	Percentual de providências de auditoria concluídas no prazo.
Evidências completas	Percentual de solicitações amostradas que contêm autorização e confirmação da execução.

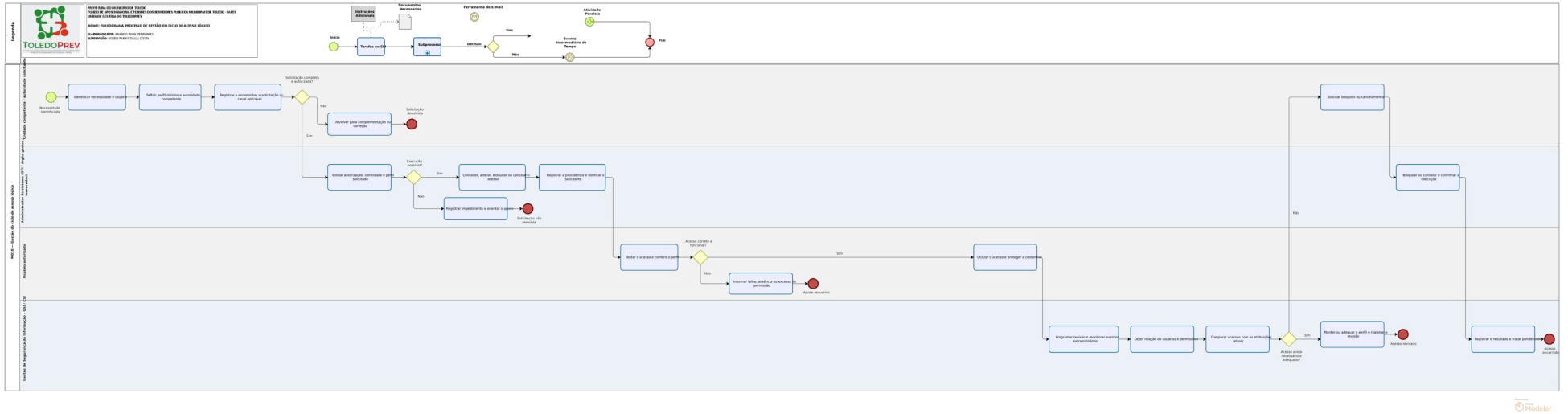
Quando não houver dados suficientes para o cálculo, a limitação e a providência necessária devem ser registradas. Os indicadores não substituem as evidências individualizadas do processo.

13. DISPOSIÇÕES FINAIS

Este manual deve ser revisto sempre que houver alteração relevante na legislação, na Política de Segurança da Informação, na estrutura administrativa, nos sistemas utilizados, nos responsáveis ou nos controles do processo. A relação de sistemas e canais operacionais poderá ser atualizada sem alteração da essência do processo, desde que a mudança seja registrada e comunicada aos responsáveis.

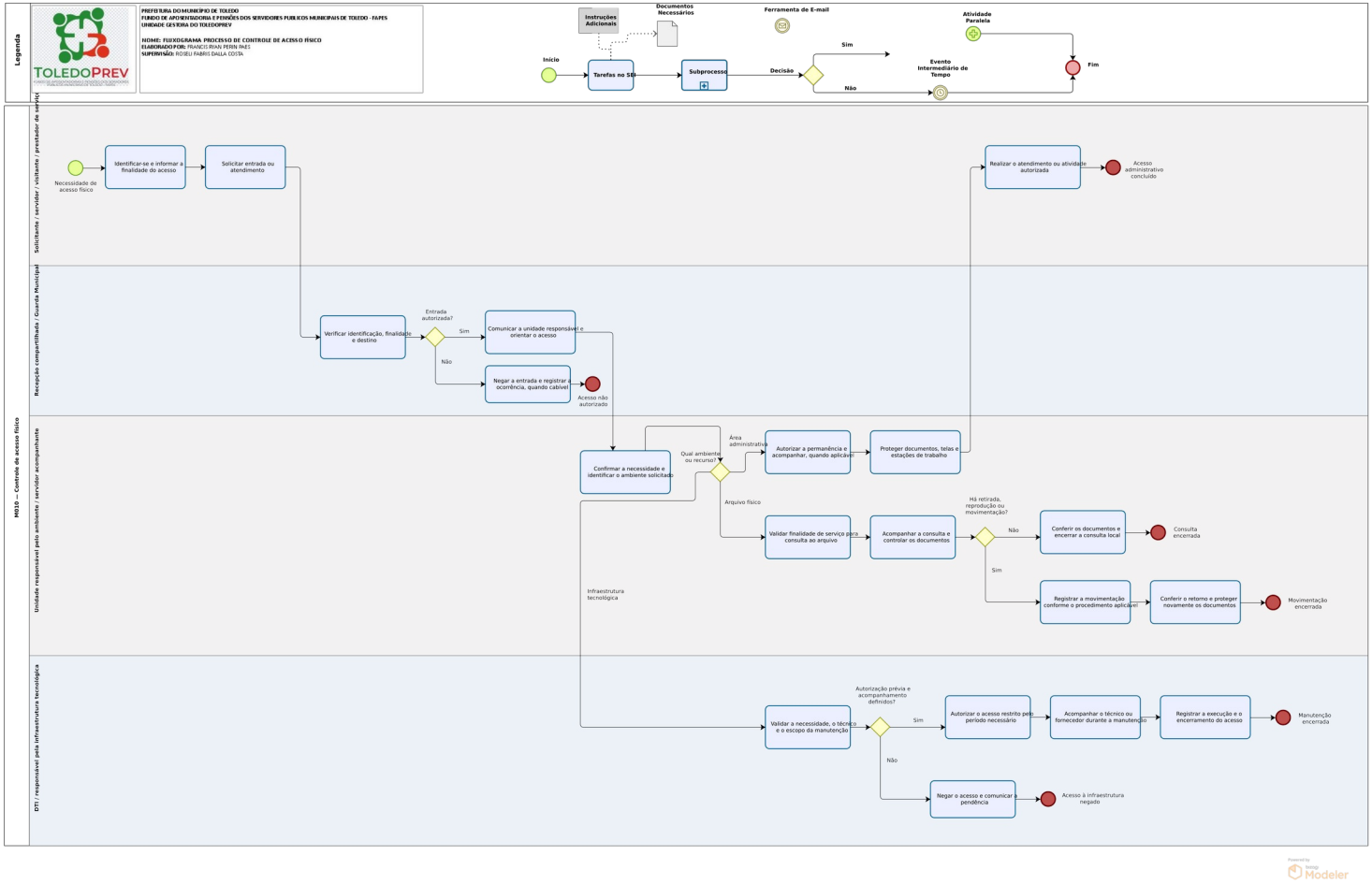
Os casos omissos e as situações excepcionais serão submetidos à Diretoria-Executiva, com apoio da GSI e, quando necessário, do DTI e do CSI, observadas as competências de cada unidade. A aplicação deste manual deverá produzir evidências suficientes para demonstrar autorização, adequação do perfil, rastreabilidade, revisão e encerramento dos acessos.

ANEXO I – FLUXOGRAMA DA GESTÃO DO ACESSO LÓGICO



Fluxo aplicável à inclusão, alteração, revisão, bloqueio e cancelamento de acessos lógicos.

ANEXO II – FLUXOGRAMA DO CONTROLE DE ACESSO FÍSICO



Fluxo aplicável às instalações, ao arquivo físico, aos documentos e à infraestrutura tecnológica.