

**PREFEITURA MUNICIPAL DE SANTA LÚCIA – SP**



**POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS**

*Versão 1.0 - Documento institucional aprimorado*

*Documento elaborado em conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD, com a Lei de Acesso à Informação, e demais normas aplicáveis à Administração Pública Municipal.*

Santa Lúcia - SP

2026

## POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

<b>Campo</b>	<b>Informação</b>
<b>Título</b>	Política de Privacidade e Proteção de Dados Pessoais
<b>Abrangência</b>	Órgãos, unidades administrativas, servidores, agentes públicos, colaboradores, fornecedores, parceiros e terceiros que tratem dados pessoais em nome da Prefeitura Municipal de Santa Lúcia - SP.
<b>Controlador</b>	Prefeitura Municipal de Santa Lúcia - SP.
<b>Responsável pela elaboração</b>	Encarregado pelo Tratamento de Dados Pessoais, Setor de Tecnologia da Informação e/ou comissão designada.
<b>Responsável pela aprovação</b>	Chefia do Poder Executivo Municipal, por ato formal próprio.
<b>Ato formal de aprovação</b>	Aprovada por [Decreto/Portaria/Resolução] nº [preencher], de [data], publicado(a) no meio oficial de divulgação do Município.
<b>Vigência</b>	Prazo indeterminado a partir da publicação, sem prejuízo de revisões periódicas.
<b>Canal institucional</b>	<a href="https://www.santalucia.sp.gov.br/index">https://www.santalucia.sp.gov.br/index</a>

Versão inicial 1.0 - Revisão ampliada com governança, segurança, cookies, canais institucionais, retenção documental, riscos operacionais e ato formal de aprovação.

## SUMÁRIO

1. Introdução.....	4
2. Objetivo .....	4
3. Abrangência .....	4
4. Fundamentação legal.....	5
5. Definições.....	5
6. Princípios aplicáveis.....	6
7. Coleta e uso de dados pessoais.....	7
8. Coleta e uso de dados .....	7
8.1 Categoria de dados pessoais tratados .....	8
9. Finalidade do tratamento .....	9
10. Tratamento de dados pessoais sensíveis.....	9
11. Dados pessoais de crianças e adolescentes.....	9
12. Compartilhamento de dados e operadores.....	10
13. Transferência internacional de dados.....	10
14. Direitos dos titulares.....	10
15. Segurança da informação e proteção dos dados .....	11
16. Uso de e-mail institucional, aplicativos de mensagens e canais digitais .....	12
17. Cookies, registros de acesso e serviços digitais .....	12
18. Retenção, gestão documental, descarte e anonimização .....	13
19. Incidentes de segurança .....	14
20. Encarregado pelo Tratamento de Dados Pessoais.....	14
21. Riscos prioritários e controles mínimos .....	15
22. Transparência, revisão e atualização .....	15
23. Disposições gerais .....	16

## **1. Introdução**

A Prefeitura Municipal de Santa Lúcia - SP reconhece que a proteção de dados pessoais é condição essencial para a prestação de serviços públicos seguros, transparentes e eficientes. Esta Política estabelece diretrizes institucionais para o tratamento de dados pessoais de cidadãos, servidores, agentes públicos, prestadores de serviços, fornecedores, parceiros, visitantes e demais pessoas que se relacionem com a Administração Municipal.

O documento orienta o tratamento de dados em meios físicos e digitais, incluindo atendimentos presenciais, portais, sistemas, aplicativo, processos administrativos, arquivos eletrônicos, documentos impressos, e-mails institucionais e demais canais oficiais utilizados pelo Município.

A Política busca fortalecer a governança em privacidade e proteção de dados, conciliando a Lei Geral de Proteção de Dados Pessoais com os deveres de transparência pública, arquivo, prestação de contas, segurança da informação e continuidade dos serviços municipais.

## **2. Objetivo**

Esta Política tem por objetivo estabelecer regras e diretrizes para coleta, uso, acesso, armazenamento, compartilhamento, retenção, descarte, anonimização, segurança e demais formas de tratamento de dados pessoais no âmbito da Prefeitura Municipal de Santa Lúcia - SP.

Também busca orientar servidores e colaboradores sobre condutas adequadas no uso de sistemas, documentos, e-mails, aplicativos de mensagens e demais ferramentas de trabalho, reduzindo riscos de vazamento, exposição indevida, compartilhamento informal e acesso não autorizado a dados pessoais.

## **3. Abrangência**

Esta Política aplica-se a todos os órgãos e unidades administrativas da Prefeitura Municipal de Santa Lúcia - SP, bem como a servidores, empregados públicos, agentes políticos, estagiários, conselheiros, colaboradores, prestadores de serviços,

fornecedores, operadores de sistemas, parceiros e terceiros que realizem tratamento de dados pessoais em nome do Município.

As diretrizes abrangem dados tratados em documentos físicos, sistemas internos, bancos de dados, portais, aplicativos, planilhas, formulários, processos administrativos, prontuários, cadastros, imagens, áudios, e-mails institucionais e demais recursos tecnológicos ou administrativos utilizados pela Administração Municipal.

#### 4. Fundamentação legal e normativa

Esta Política observa, entre outras normas aplicáveis:

- Constituição Federal de 1988, especialmente os direitos fundamentais à privacidade, intimidade, acesso à informação e proteção de dados pessoais.
- Emenda Constitucional nº 115/2022, que incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais.
- Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei Federal nº 12.527/2011 - Lei de Acesso à Informação (LAI).
- Lei Federal nº 12.965/2014 - Marco Civil da Internet.
- Lei Federal nº 8.159/1991 - Política Nacional de Arquivos Públicos e Privados.
- Decreto Federal nº 4.073/2002, que regulamenta a Lei nº 8.159/1991, quando aplicável.
- Lei Federal nº 8.069/1990 - Estatuto da Criança e do Adolescente, quando houver tratamento de dados de crianças e adolescentes.
- Normas de gestão documental, tabela de temporalidade documental, normas arquivísticas, atos municipais e orientações da Autoridade Nacional de Proteção de Dados (ANPD), quando aplicáveis.

#### 5. Definições estratégicas

Para fins desta Política, são adotadas as seguintes definições essenciais:

<b>Termo</b>	<b>Definição</b>
<b>Titular</b>	Pessoa natural a quem se referem os dados pessoais tratados pela Prefeitura.
<b>Dado pessoal</b>	Informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, RG, endereço, telefone, imagem, e-mail, cadastro, matrícula ou registro de

	atendimento.
<b>Dado pessoal sensível</b>	Dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, saúde, vida sexual, dado genético ou biométrico, quando vinculado a pessoa natural.
<b>Tratamento</b>	Toda operação realizada com dados pessoais, como coleta, acesso, uso, armazenamento, compartilhamento, arquivamento comunicação ou extração.
<b>Controlador</b>	Agente responsável pelas decisões referentes ao tratamento. Para fins desta Política, a Prefeitura Municipal de Santa Lúcia - SP atua como controladora no âmbito de suas competências.
<b>Operador</b>	Pessoa natural ou jurídica que realiza tratamento de dados pessoais em nome do controlador, conforme contrato, convênio, termo de cooperação ou orientação formal.
<b>Encarregado/DPO</b>	Pessoa ou unidade indicada para atuar como canal de comunicação entre a Prefeitura, os titulares e a ANPD.
<b>Incidente de segurança</b>	Evento que possa comprometer a confidencialidade, integridade ou disponibilidade de dados pessoais, como acesso indevido, perda, vazamento, alteração, destruição ou divulgação não autorizada.

Conceitos técnicos adicionais poderão ser detalhados em glossário, manual interno, procedimento operacional ou norma complementar, sem necessidade de repetição integral nesta Política.

## 6. Princípios aplicáveis

O tratamento de dados pessoais realizado pela Prefeitura observará os princípios previstos na LGPD, especialmente:

- Finalidade: uso dos dados para propósitos legítimos, específicos e compatíveis com as atribuições públicas do Município.
- Adequação: compatibilidade entre o tratamento realizado e o contexto do serviço público prestado.
- Necessidade: limitação do tratamento ao mínimo necessário para atingir a finalidade pública ou administrativa.
- Livre acesso: garantia de consulta facilitada e gratuita, observadas as restrições legais.

- Qualidade dos dados: manutenção de dados corretos, atualizados e pertinentes, quando necessário.
- Transparência: fornecimento de informações claras e acessíveis aos titulares.
- Segurança e prevenção: adoção de medidas técnicas, administrativas e organizacionais para reduzir riscos.
- Não discriminação: vedação de uso de dados para fins abusivos, ilícitos ou discriminatórios.
- Responsabilização e prestação de contas: demonstração de medidas efetivas de conformidade, controle e melhoria contínua.

## **7. Governança, papéis e responsabilidades**

A proteção de dados pessoais deve ser tratada como responsabilidade institucional compartilhada. A chefia do Poder Executivo, secretarias municipais, unidades administrativas, encarregado pelo tratamento de dados, setor de tecnologia da Informação, servidores, colaboradores e operadores externos deverão atuar de forma coordenada para cumprir esta Política.

Compete às secretarias e unidades administrativas identificar dados pessoais tratados em suas rotinas, limitar acessos, manter registros mínimos de operações relevantes, comunicar incidentes, orientar equipes e solicitar apoio técnico ou jurídico quando houver dúvida sobre tratamento de dados.

Prestadores de serviços, fornecedores de sistemas, empresas de tecnologia, consultorias e demais operadores deverão tratar dados pessoais somente conforme finalidade contratada, observando confidencialidade, segurança da informação, dever de sigilo e cláusulas específicas de proteção de dados.

## **8. Coleta e uso de dados pessoais**

A Prefeitura coletará somente os dados necessários para executar serviços públicos, cumprir obrigações legais, administrar políticas públicas, realizar atos administrativos, atender cidadãos, gerir contratos, administrar pessoal e proteger o patrimônio público e a segurança dos sistemas.

Os dados poderão ser obtidos diretamente do titular, de responsável legal, de sistemas municipais, de bases públicas autorizadas, de outros órgãos públicos ou de documentos apresentados em atendimentos presenciais ou digitais, sempre observada a finalidade e a base legal aplicável.

### **8.1 Categorias de dados pessoais tratados**

- Dados de identificação: nome, CPF, RG, data de nascimento, filiação, estado civil, assinatura, fotografia, matrícula ou cadastro municipal.
- Dados de contato: endereço, telefone, e-mail e demais meios de comunicação informados pelo titular.
- Dados profissionais e funcionais: cargo, função, lotação, vínculo, jornada, remuneração, histórico funcional, capacitações e avaliações.
- Dados educacionais: matrícula, frequência, histórico escolar, transporte escolar, responsáveis legais e registros necessários à rede municipal de ensino.
- Dados de saúde: informações necessárias a atendimentos, agendamentos, vacinação, prontuários, regulação, vigilância epidemiológica e programas de saúde pública.
- Dados socioassistenciais: informações para inscrição, avaliação, acompanhamento e concessão de benefícios, programas sociais e políticas públicas.
- Dados financeiros, tributários e patrimoniais: informações necessárias à arrecadação, pagamentos, empenhos, licitações, contratos, compras públicas e prestação de contas.
- Dados de navegação e registros de acesso: endereço IP, data e hora de acesso, navegador, dispositivo, logs e cookies necessários ao funcionamento, segurança e melhoria dos serviços digitais.
- Dados de imagem e áudio: registros de atendimento, eventos oficiais, segurança patrimonial, identificação funcional e divulgação institucional, observadas as bases legais aplicáveis.

## **9. Finalidades do tratamento**

Os dados pessoais poderão ser tratados para identificar cidadãos, emitir documentos, registrar protocolos, executar políticas públicas, efetivar matrículas, realizar atendimentos de saúde, gerir benefícios sociais, administrar tributos, gerir servidores, conduzir licitações, fiscalizar contratos, prestar contas, cumprir determinações legais, proteger sistemas e melhorar a qualidade dos serviços municipais.

O tratamento deverá observar a finalidade informada, a necessidade dos dados, o perfil de acesso autorizado e a compatibilidade com as atribuições da unidade administrativa responsável.

## **10. Tratamento de dados pessoais sensíveis**

Dados pessoais sensíveis serão tratados somente quando indispensáveis ao cumprimento de obrigação legal ou regulatória, execução de políticas públicas, tutela da saúde, proteção da vida, exercício regular de direitos, prevenção à fraude ou demais apontamentos permitidos pela LGPD.

O acesso a dados de saúde, biometria, informações socioassistenciais, dados de crianças e adolescentes e demais informações sensíveis deverá ser restrito a pessoas autorizadas, com registro, justificativa funcional e medidas de segurança proporcionais à criticidade dos dados tratados.

É proibido utilizar dados sensíveis para fins discriminatórios, ilícitos, abusivos ou incompatíveis com a finalidade pública que justificou sua coleta.

## **11. Dados pessoais de crianças e adolescentes**

O tratamento de dados pessoais de crianças e adolescentes será realizado sempre em seu melhor interesse, nos termos da LGPD e do Estatuto da Criança e do Adolescente.

A coleta poderá ocorrer para matrícula, acompanhamento escolar, transporte, alimentação, atividades pedagógicas, vacinação, atendimentos de saúde, programas socioassistenciais, conselhos tutelares, projetos esportivos e culturais, sempre com limitação à finalidade pública e à necessidade do serviço.

Quando a legislação exigir consentimento, este deverá ser específico e destacado, fornecido por pelo menos um dos pais ou responsável legal. Mesmo quando o consentimento não for exigido, a Prefeitura deverá adotar medidas proporcionais para proteção da privacidade de crianças e adolescentes.

## **12. Compartilhamento de dados e operadores**

A Prefeitura Municipal de Santa Lúcia - SP não comercializa dados pessoais. O compartilhamento ocorrerá somente quando houver finalidade pública, previsão legal, obrigação regulatória, execução de política pública, prestação de serviço público, cumprimento de decisão de autoridade competente ou necessidade operacional legítima devidamente justificada.

O compartilhamento poderá ocorrer com secretarias municipais, unidades administrativas, conselhos municipais, órgãos estaduais e federais, Poder Judiciário, Ministério Público, tribunais de contas, órgãos de controle, instituições financeiras, prestadores de serviços, fornecedores de sistemas, operadores de tecnologia e entidades parceiras.

Contratos, convênios, termos de cooperação e instrumentos similares deverão conter, sempre que aplicável, cláusulas de confidencialidade, segurança da informação, dever de sigilo, limitação de finalidade, comunicação de incidentes, regras de subcontratação e obrigações de devolução, eliminação ou retenção segura dos dados ao final da relação.

## **13. Transferência internacional de dados**

Como regra, a Prefeitura buscará manter dados pessoais sob tratamento em território nacional. Caso seja necessária transferência internacional, inclusive por uso de computação em nuvem, hospedagem, suporte técnico ou solução tecnológica com infraestrutura fora do Brasil, a operação deverá observar as hipóteses legais da LGPD, orientações da ANPD e garantias adequadas de proteção.

## **14. Direitos dos titulares**

O titular poderá exercer, nos termos da LGPD e observadas as limitações legais aplicáveis à Administração Pública, os direitos de confirmação da existência de

tratamento, acesso, correção, anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos, informação sobre compartilhamento, revogação de consentimento quando aplicável, oposição a tratamento irregular e peticionamento perante a ANPD.

As solicitações deverão ser apresentadas pelos canais oficiais indicados nesta Política. Para proteção do próprio titular, poderá ser exigida comprovação de identidade antes do atendimento. Pedidos poderão ser total ou parcialmente indeferidos quando houver obrigação legal de guarda, sigilo legal, proteção de interesse público, exercício regular de direitos, segurança de terceiros ou impossibilidade técnica devidamente justificada.

## **15. Segurança da informação e proteção dos dados**

A Prefeitura adotará medidas técnicas, administrativas e organizacionais destinadas a proteger dados pessoais contra acessos não autorizados, perda, destruição, alteração, divulgação indevida, comunicação não autorizada ou qualquer forma de tratamento inadequado ou ilícito, considerando a proporcionalidade, a criticidade dos dados tratados, os riscos envolvidos e a capacidade operacional do Município.

Entre as medidas mínimas recomendadas, observadas as condições de implementação e priorização por risco, incluem-se:

- Controle de acesso físico e lógico a ambientes, sistemas, arquivos e bases de dados.
- Uso de credenciais individuais, senhas fortes, autenticação adicional quando disponível e vedação ao compartilhamento de senhas.
- Perfis de acesso compatíveis com a função do usuário e revisão periódica de permissões.
- Atualização de sistemas, aplicações e mecanismos de proteção conforme plano técnico e priorização de riscos.
- Realização de backups, testes de restauração.
- Inventário e gestão de ativos de tecnologia da informação, incluindo equipamentos, sistemas, bancos de dados e serviços em nuvem.

- Registro e monitoramento de acessos quando necessário à segurança, auditoria e investigação de incidentes.
- Treinamento e orientação periódica de servidores e colaboradores sobre privacidade, sigilo funcional e segurança da informação.
- Procedimentos para descarte seguro de documentos físicos, mídias, equipamentos e arquivos eletrônicos contendo dados pessoais.

## **16. Uso de e-mail institucional, aplicativos de mensagens e canais digitais**

O uso de e-mail institucional, aplicativos de mensagens, ferramentas de comunicação instantânea e demais canais digitais deverá observar finalidade pública, segurança, rastreabilidade, sigilo, necessidade e adequação ao serviço prestado.

Sempre que possível, comunicações oficiais que envolvam dados pessoais deverão ocorrer por canais institucionais, com contas oficiais, controle de acesso e preservação adequada dos registros administrativos. O uso de e-mail pessoal, contas particulares, dispositivos não autorizados ou grupos informais para envio de documentos contendo dados pessoais deve ser evitado e somente ocorrer em situação excepcional, justificada e com medidas de segurança compatíveis.

É vedado compartilhar prontuários, laudos, documentos pessoais, cadastros socioassistenciais, listas com CPF, dados de crianças e adolescentes, senhas, relatórios internos ou informações sensíveis em grupos de mensagens sem autorização, necessidade funcional e proteção adequada.

Quando aplicativos de mensagens forem utilizados para comunicação com cidadãos ou entre equipes, a unidade responsável deverá limitar os dados compartilhados ao mínimo necessário, evitar exposição em grupos, confirmar destinatários, orientar servidores sobre sigilo e preservar registros quando houver relevância administrativa.

## **17. Cookies, registros de acesso e serviços digitais**

Nos portais, sistemas e serviços digitais da Prefeitura, poderão ser utilizados cookies, registros de acesso e tecnologias similares para funcionamento das páginas,

autenticação, segurança, acessibilidade, prevenção a fraudes, registro de protocolos, melhoria da experiência do usuário e produção de estatísticas de acesso.

Os cookies deverão ser classificados, sempre que aplicável, em:

- Cookies essenciais: necessários ao funcionamento do site, autenticação, segurança, acessibilidade e prestação do serviço digital. Em regra, não dependem de consentimento, pois são indispensáveis para a operação do serviço.
- Cookies analíticos ou de desempenho: utilizados para medir audiência, identificar páginas mais acessadas e melhorar os serviços digitais. Quando envolverem dados pessoais ou tecnologias de terceiros, deverão observar base legal adequada e transparência ao usuário.
- Cookies de terceiros: instalados por serviços externos integrados ao portal, como mapas, vídeos, ferramentas estatísticas ou redes sociais, devendo ser informados ao usuário quando aplicável.

A Prefeitura deverá disponibilizar informações claras sobre tipos de cookies, finalidades, responsáveis, prazo de retenção e formas de gerenciamento pelo usuário. Quando necessário, deverá adotar banner ou mecanismo equivalente para consentimento ou preferência, sem impedir o acesso a serviços públicos essenciais em razão da recusa de cookies não essenciais.

Os registros de acesso poderão incluir endereço IP, data e hora, navegador, dispositivo, páginas acessadas e demais informações técnicas necessárias à segurança, auditoria e melhoria dos serviços digitais, observada a legislação aplicável e os prazos de retenção definidos em norma interna, tabela de temporalidade ou procedimento específico.

## **18. Retenção, gestão documental, descarte e anonimização**

Os dados pessoais serão mantidos pelo período necessário ao cumprimento das finalidades que justificaram sua coleta, observados os prazos legais, regulatórios, arquivísticos, fiscais, administrativos, de controle, transparência pública e prestação de contas aplicáveis à Administração Pública.

A retenção e o descarte deverão observar a Lei nº 8.159/1991, normas de arquivo público, tabela de temporalidade documental, plano de classificação, regras de guarda permanente ou temporária e orientações de gestão documental adotadas pelo Município.

Encerrada a finalidade e inexistindo obrigação legal de retenção, os dados poderão ser eliminados, anonimizados ou arquivados de forma segura. O descarte de documentos físicos, mídias, equipamentos e arquivos eletrônicos contendo dados pessoais deverá impedir recuperação indevida e ser realizado conforme procedimento interno.

## **19. Incidentes de segurança**

Toda suspeita ou ocorrência de incidente de segurança envolvendo dados pessoais deverá ser comunicada imediatamente ao Encarregado pelo Tratamento de Dados Pessoais e/ou ao setor responsável por tecnologia e segurança da informação.

Após a comunicação, a Prefeitura deverá avaliar a natureza do incidente, os dados envolvidos, titulares afetados, risco de dano, medidas de contenção, necessidade de preservação de evidências, correção de vulnerabilidades e eventual comunicação à ANPD e aos titulares, conforme a LGPD e orientações da autoridade competente.

Exemplos de incidentes incluem envio de documento ao destinatário errado, perda de pendrive ou computador, acesso indevido a sistema, vazamento de prontuário, exposição de dados, publicação indevida em portal da transparência, ataque cibernético, uso irregular de senha ou compartilhamento informal de dados sensíveis.

## **20. Encarregado pelo Tratamento de Dados Pessoais**

O Encarregado pelo Tratamento de Dados Pessoais atua como canal de comunicação entre a Prefeitura Municipal de Santa Lúcia - SP, os titulares de dados e a Autoridade Nacional de Proteção de Dados.

Enquanto os dados do Encarregado não forem formalmente publicados ou atualizados, as solicitações poderão ser encaminhadas pelos canais oficiais de atendimento da Prefeitura Municipal de Santa Lúcia - SP.

## **21. Riscos prioritários e controles mínimos**

Considerando a realidade operacional de órgãos públicos municipais, a Prefeitura deverá priorizar medidas de prevenção e controle para os seguintes riscos:

- Vazamento, acesso indevido ou compartilhamento irregular de prontuários, exames, laudos e dados de saúde.
- Exposição de dados de assistência social, benefícios, vulnerabilidade econômica, crianças, adolescentes e famílias acompanhadas.
- Publicação indevida de dados pessoais em portal da transparência, site institucional, redes sociais, editais, listas, documentos digitalizados ou diários oficiais.
- Uso de WhatsApp pessoal, e-mail pessoal, grupos informais ou dispositivos particulares para envio de dados pessoais sem controle ou autorização.
- Contratação de sistemas terceirizados sem cláusulas adequadas de proteção de dados, confidencialidade, segurança, suporte e comunicação de incidentes.
- Compartilhamento informal de dados entre secretarias sem finalidade definida, base legal, necessidade funcional ou controle de acesso.
- Acesso irrestrito a sistemas, senhas compartilhadas, perfis genéricos ou manutenção de acesso após mudança de função ou desligamento.

Para esses riscos, recomenda-se adotar controles mínimos como perfis de acesso por função, revisão periódica de permissões, orientação formal aos servidores, termos de confidencialidade quando cabíveis, cláusulas LGPD em contratos, inventário de sistemas, canal de comunicação de incidentes e registro de decisões relevantes sobre tratamento de dados.

## **22. Transparência, revisão e atualização**

A Prefeitura buscará disponibilizar informações claras e acessíveis sobre suas práticas de tratamento de dados pessoais por meio do site institucional, canais de atendimento, avisos de privacidade, formulários, documentos administrativos e demais meios adequados.

Esta Política deverá ser revisada preferencialmente a cada 12 meses ou sempre que houver alteração relevante na legislação, nos serviços prestados, sistemas

utilizados, contratos, riscos identificados, estrutura administrativa ou diretrizes institucionais do Município.

A revisão poderá ser conduzida pelo encarregado pelo tratamento de dados, setor de Tecnologia da Informação, Procuradoria/Assessoria Jurídica, Controle Interno, secretarias municipais e demais unidades envolvidas, conforme ato de designação ou procedimento interno.

### **23. Disposições gerais**

Esta Política não substitui normas específicas de cada secretaria, unidade ou serviço municipal, nem afasta o cumprimento de obrigações legais de transparência pública, controle externo, arquivo público, gestão documental, fiscalização e prestação de contas.

O acesso a sites, sistemas ou serviços de terceiros por meio de links disponibilizados no portal da Prefeitura poderá estar sujeito a políticas próprias desses terceiros, não sendo esta Política aplicável a ambientes externos que não estejam sob responsabilidade direta do Município.

O descumprimento desta Política e das normas de proteção de dados poderá sujeitar os responsáveis às medidas administrativas, civis e legais cabíveis, respeitados o contraditório e a ampla defesa.

A presente Política entra em vigor na data de publicação do ato formal de aprovação e permanecerá válida até sua alteração, substituição ou revogação por ato competente.