URBES
TRÂNSITO E TRANSPORTES

Prefeitura de SOROCABA

MANUAL DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) – URBES

1. APRESENTAÇÃO E DISPOSIÇÕES GERAIS

1.1 Objetivo

O presente Manual tem por objetivo estabelecer as diretrizes de privacidade e proteção de dados pessoais aplicáveis a todos os processos operacionais, administrativos e fiscais da Urbes - Empresa de Desenvolvimento Urbano e Social de Sorocaba, doravante denominada URBES. Este documento constitui a política de governança de dados da empresa pública, orientando o tratamento de dados pessoais no âmbito de suas atividades finalísticas e meio.

As regras aqui contidas visam assegurar o cumprimento integral da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), bem como das legislações municipais pertinentes, promovendo a transparência, a segurança jurídica e o respeito aos direitos fundamentais de liberdade e privacidade dos titulares de dados.

1.2 Escopo de Aplicação

Este Manual é de observância obrigatória para todos os empregados públicos da URBES, incluindo aqueles ocupantes de cargos de provimento efetivo, comissionados, função de confiança, estagiários, menores aprendizes, bem como para prestadores de serviços terceirizados, consultores, diretores, conselheiros e qualquer pessoa física ou jurídica que, em nome da URBES, realize operações de tratamento de dados pessoais.

O descumprimento das disposições deste Manual sujeitará o infrator às sanções administrativas, civis e penais previstas na legislação aplicável, sem prejuízo das medidas disciplinares internas.

1.3 Fundamentação Jurídica

Este Manual fundamenta-se nos seguintes diplomas legais e normativos:

- Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), com as alterações introduzidas pela Lei nº 13.853/2019.

- Lei Municipal nº 12.924, de 21 de dezembro de 2023 - Dispõe sobre a reestruturação administrativa e funcional da URBES e a criação de cargos efetivos e funções de carreira.
- Decreto Municipal nº 29.075, de 15 de março de 2024 - Institui a Política Geral de Proteção de Dados Pessoais no âmbito do Poder Executivo do Município de Sorocaba.
- Constituição Federal de 1988, art. 5º, incisos X e LXXIX (direito à privacidade e à proteção de dados).
- Regulamentação da Autoridade Nacional de Proteção de Dados (ANPD), em especial a Resolução CD/ANPD nº 1/2021 (adequação de agentes de tratamento).

2. AGENTES DE TRATAMENTO E GOVERNANÇA

2.1 A URBES como Controladora

A URBES figura como Controladora de dados pessoais, nos termos do art. 5°, VI, da LGPD, uma vez que detém o poder de decisão referente ao tratamento de dados pessoais de munícipes, empregados públicos, prestadores de serviços e terceiros no exercício de suas atribuições legais. Compete à Controladora:

- Definir as finalidades, os meios e os procedimentos de tratamento de dados;
- Garantir a observância dos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização prestação de contas;
- Responder perante os titulares e a ANPD por eventuais violações decorrentes de tratamentos realizados sob sua responsabilidade direta.

2.2 Operadores Terceirizados

Todos os fornecedores, parceiros e prestadores de serviços que realizem tratamento de dados pessoais em nome da URBES são considerados Operadores. A contratação desses operadores deve obrigatoriamente conter cláusulas contratuais específicas que definam as finalidades do tratamento, a duração, a natureza dos dados, as obrigações de confidencialidade e segurança, bem como a vedação ao tratamento para finalidades próprias ou incompatíveis com o objeto contratual.

A URBES manterá registro atualizado de todos os operadores e realizará auditoria periódica de conformidade com os termos contratuais e a legislação aplicável.

2.3 Do Encarregado pelo Tratamento de Dados Pessoais (DPO)

O Encarregado pelo Tratamento de Dados Pessoais (DPO/DATA PROTECTION OFFICER) será formalmente designado por ato administrativo do Diretor-Presidente da URBES, mediante Portaria interna publicada no Diário Oficial do Município. A designação recairá sobre um profissional, que poderá ser servidor efetivo ou comissionado da empresa, ou, excepcionalmente, pessoa física ou jurídica contratada para essa finalidade.

Compete ao Encarregado, nos termos do art. 41, §2º, da LGPD e do art. 12 do Decreto Municipal nº 29.075/2024:

- Atuar como canal de comunicação entre a URBES, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- Receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Orientar os empregados e demais agentes da URBES quanto às práticas de proteção de dados;
- Coordenar o processo de resposta a incidentes de segurança;
- Elaborar relatórios anuais de impacto à proteção de dados pessoais (RIPD) e submetê-los à DAU;
- Representar a URBES junto ao Comitê Gestor de Proteção de Dados Pessoais do Município de Sorocaba, instituído pelo Decreto nº 29.075/2024.

Nota: O nome e os contatos oficiais do Encarregado (e-mail corporativo e telefone) serão divulgados no site institucional da URBES e na seção de Proteção de Dados do Portal da Transparência do Município de Sorocaba.

3. CANAIS DE ATENDIMENTO E DIREITOS DOS TITULARES

3.1 Direitos dos Titulares (Art. 18 da LGPD)

A URBES assegura a todos os titulares de dados pessoais o exercício dos direitos previstos no art. 18 da LGPD, mediante requisição formal, a saber:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial;
- Eliminação dos dados tratados com o consentimento do titular, exceto nas hipóteses legais de guarda obrigatória;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revisão de decisões automatizadas.

O exercício desses direitos é gratuito, salvo quando excessivo, manifestações infundadas ou repetitiva, casos em que poderá ser cobrado custo administrativo, conforme regulamentação da ANPD no Art. 18, § 5° da Lei nº 13.709, de 14 de agosto de 2018.

3.2 Integração com a Ouvidoria da URBES e Canais Municipais

A URBES estabelece fluxo integrado de atendimento aos titulares de dados, com a Ouvidoria da URBES atuando como porta de entrada preferencial para as solicitações. O canal de Ouvidoria é acessível por meio do site institucional www.urbes.com.br/ouvidoria, e presencialmente na sede da empresa.

O fluxo operacional obedecerá às seguintes etapas:

1. O titular protocola sua solicitação no canal da Ouvidoria da URBES indicando tratar-se de pedido relativo a dados pessoais.
2. A Ouvidoria tria a solicitação e a encaminha via sistema ao Encarregado pelo Tratamento de Dados (DPO).
3. O DPO analisa o pedido e, fundamentadamente, responde ao titular, informando se o direito será exercido ou, se indeferido, a razão legal do indeferimento.
4. Caso a solicitação envolva dados de terceiros ou informações classificadas como sigilosas, o DPO aplicará as hipóteses legais de restrição ao exercício do direito (art. 4º, III, e art. 11, I, da LGPD).

4. TRATAMENTO DE DADOS DE EMPREGADOS PÚBLICOS E COLABORADORES (CONFORMIDADE COM A LEI MUNICIPAL N° 12.924/2023)

4.1 Contexto Normativo

A Lei Municipal nº 12.924/2023 reestruturou o quadro de pessoal da URBES, criando novas comissões e instâncias administrativas com competência para avaliar e decidir sobre a evolução funcional e recursos dos empregados públicos. Em seus Artigos 141 e 143, I, a lei determina que essas comissões devem observar rigorosamente as disposições da LGPD no acesso e tratamento de dados pessoais dos servidores.

4.2 Comissão Permanente de Evolução Funcional (Art. 141)

A Comissão Permanente de Evolução Funcional, composta por empregados efetivos designados pelo Diretor-Presidente, terá acesso a dados funcionais (histórico de avaliações, frequência, titulação, tempo de serviço, sanções disciplinares) exclusivamente para instruir e decidir sobre progressão horizontal, vertical ou por mérito. Ficam estabelecidas as seguintes regras específicas para o tratamento desses dados:

- Minimização: A Comissão somente acessará os dados estritamente necessários à análise do caso concreto, vedada a consulta indiscriminada a prontuários ou bases de dados.
- Confidencialidade: Cada membro da Comissão assinará Termo de Compromisso e Confidencialidade antes de iniciar suas atividades, comprometendo-se a não divulgar, copiar ou utilizar as informações para fins alheios ao processo de evolução.
- Registro de acesso: Todos os acessos aos sistemas de gestão de pessoas (RH) serão registrados em logs de auditoria, identificando o usuário, data, horário e dados consultados.
- Vedação de compartilhamento externo: É expressamente proibido repassar a terceiros, inclusive a outros setores da URBES, informações pessoais obtidas no âmbito da Comissão, salvo quando exigido por ordem judicial ou pela Controladoria-Geral do Município.

4.3 Comissão Recursal (Art. 143, I)

A Comissão Recursal, instância de julgamento de recursos administrativos interpostos pelos empregados contra decisões relativas à evolução funcional, também observará as mesmas regras de proteção de dados estabelecidas no item 4.2, acrescidas das seguintes garantias:

- Direito ao contraditório e à ampla defesa: O empregado recorrente terá acesso a todos os dados pessoais utilizados na decisão recorrida e poderá impugnar sua veracidade ou pertinência.
- Decisão fundamentada: A Comissão Recursal deve explicitar em seus acórdãos quais dados foram considerados, vedando a referência a informações sensíveis (saúde, vida sexual, orientação política, etc.), salvo quando imprescindíveis para a decisão e com anuência expressa do titular.
- Prazo de guarda: Os documentos relativos aos recursos (inclusive aqueles contendo dados pessoais) serão arquivados pelo período de 10 anos, na forma da legislação municipal de arquivos, e após esse prazo serão eliminados de forma segura, sob supervisão do DPO.

4.4 Vedação Expressa

Fica expressamente vedado a qualquer membro das Comissões, bem como aos empregados da URBES em geral, utilizar dados pessoais de colegas, subordinados ou superiores para fins de assédio moral, perseguição política, discriminação ou qualquer outra finalidade estranha ao interesse público e ao regular processo administrativo. A infração a esta vedação constituirá falta grave, passível de demissão por justa causa, sem prejuízo das sanções previstas na LGPD (advertência, multa, bloqueio ou eliminação dos dados).

5. ATRIBUIÇÕES DA T.I. E SEGURANÇA DA INFORMAÇÃO

5.1 Medidas técnicas e organizacionais de proteção de dados

Na área de Tecnologia da Informação (TI), a Urbes conta com um contrato de prestação de serviços acompanhado por um funcionário gestor responsável por sua fiscalização. Este profissional atua em conjunto com o Encarregado pelo Tratamento de Dados

Pessoais (DPO) na implementação das medidas técnicas e organizacionais voltadas à proteção de dados. As atribuições específicas da TI no âmbito da LGPD são:

- Implementar e manter as políticas de senhas, controle de acesso lógico e criptografia.
- Gerenciar a infraestrutura de redes e servidores, garantindo a segregação de ambientes de produção, desenvolvimento e teste.
- Realizar backups periódicos e testar a restauração de dados, conforme política de retenção definida pelo DPO e pela Comissão de Adequação a LGPD da URBES.
- Auditar semestralmente os logs de acesso aos sistemas corporativos (SIG, RH, financeiro e transporte), gerando relatórios de acessos não autorizados ou suspeitos.
- Coordenar a resposta técnica a incidentes de segurança, isolando sistemas comprometidos e preservando evidências digitais.

5.2 Política de Acesso Remoto e VPN

O acesso remoto à rede interna da URBES somente será permitido mediante conexão via VPN (Virtual Private Network) corporativa, com autenticação de múltiplos fatores (MFA). Cada usuário receberá credenciais individuais e intransferíveis, e o acesso será registrado com IP de origem, horário e duração da sessão.

Fica proibido o uso de redes Wi-Fi públicas ou não seguras para realizar trabalho remoto que envolva tratamento de dados pessoais. Os dispositivos utilizados (notebooks, tablets, smartphones) deverão ter software antivírus corporativo instalado e atualizado.

5.3 Auditoria de Logs

A TI manterá sistema centralizado de gestão de logs e eventos (SIEM - Security Information and Event Management) que coleta e armazena, por no mínimo 6 meses, todos os registros de acesso a sistemas que tratam dados pessoais.

Trimestralmente, serão gerados relatórios de auditoria para o DPO, indicando tentativas de acesso não autorizado, acessos fora do horário de expediente, ou consultas a dados de terceiros sem justificativa funcional. Identificado qualquer padrão anômalo, a TI comunicará imediatamente o DPO, que determinará a abertura de processo investigatório interno.

6. LGPD, A TRANSPARÊNCIA ATIVA E OS CRITÉRIOS DE SIGILO

6.1. Da Transparência Ativa e Execução Contratual e Orçamentária

A observância às diretrizes de proteção de dados pessoais estabelecidas neste Manual não obsta, restringe ou limita o cumprimento das obrigações de transparência ativa impostas pela legislação vigente. A URBES manterá a disponibilização pública, por meio eletrônico e com atualização mensal, das informações completas referentes à sua execução orçamentária, financeira e à execução de seus contratos, em estrito cumprimento ao caput do artigo 88 da Lei Federal nº 13.303, de 30 de junho de 2016 (Lei das Estatais). Nas hipóteses em que a divulgação pública desses relatórios envolver dados de pessoas físicas, aplicar-se-á tão somente a técnica de ocultação ou anonimização pontual de dados estritamente pessoais (como CPF, dados bancários individuais e contatos), de modo a preservar a privacidade do titular sem prejuízo do pleno acesso público aos valores, objetos, aditivos e pagamentos efetuados.

6.2. Dos Critérios de Classificação de Informações Sigilosas

Em observância ao artigo 86, § 5º, da Lei Federal nº 13.303/2016 e ao artigo 25 da Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), este Manual estabelece as diretrizes e procedimentos para o enquadramento de informações em sigilo no âmbito da URBES, sendo adotados os seguintes critérios objetivos para a classificação de informações sigilosas ou reservadas:

I - Segredo Comercial, Industrial e Estratégico: Informações mercadológicas, planos de negócios e propostas técnicas/comerciais cuja divulgação possa representar vantagem competitiva indevida a terceiros ou prejuízo financeiro e operacional às atividades da empresa pública;
II - Proteção de Dados Pessoais: Informações que se enquadrem nas definições de dados pessoais ou dados pessoais sensíveis nos termos do art. 5º da Lei Federal nº 13.709/2018 (LGPD);
III - Segurança Operacional e de Infraestrutura: Dados e documentos cuja revelação ponha em risco a segurança física das instalações, a arquitetura dos sistemas de tecnologia da informação ou a operação do sistema de transporte coletivo e trânsito do Município de Sorocaba.

6.3. Do Rol Exemplificativo de Documentos de Acesso Restrito

Ficam resguardados por sigilo ou acesso restrito, não estando sujeitos à divulgação irrestrita no Portal da Transparência:

- Prontuários funcionais, fichas médicas, registros de frequência e dados cadastrais sensíveis de empregados públicos e colaboradores;
- Códigos-fonte, credenciais de acesso, arquitetura de redes e dados de auditoria técnica mantidos pela Tecnologia da Informação;
- Propostas comerciais e/ou cobertas por sigilo industrial em procedimentos licitatórios, até a respectiva fase de abertura pública;
- Dados bancários e fiscais de pessoas físicas e jurídicas mantidos nos sistemas financeiros.

§ 1º Qualquer dado ou documento considerado sigiloso por motivos estratégicos, comerciais ou industriais deverá ser formalmente classificado como sigiloso por meio de um Termo de Classificação. Esse termo será elaborado pela Diretoria responsável pela informação, deverá apresentar a justificativa financeira e precisará ser aprovado pela Diretoria-Presidente.

§ 2º Toda e qualquer negativa de acesso a dados ou documentos não listados expressamente neste item demandará parecer motivado e conjunto do Encarregado de Dados (DPO) e da Diretoria Jurídica (DJU).

7. GESTÃO DE INCIDENTES E SANÇÕES

7.1 Fluxo de Resposta a Incidentes

Define-se como incidente de segurança qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais, incluindo acesso não autorizado, perda, destruição, alteração, vazamento ou qualquer outra forma de tratamento ilícito ou acidental.

O fluxo de resposta seguirá as seguintes fases:

1. Detecção e Comunicação Interna: Qualquer empregado que tome ciência de incidente deverá comunicá-lo imediatamente, por e-mail ou canal de emergência, ao DPO e à TI. O prazo máximo para comunicação é de 2 (duas) horas do conhecimento do fato.
2. Contenção e Mitigação: A TI, em coordenação com o DPO, adotará as medidas técnicas para conter o incidente (bloqueio de acessos, isolamento de sistemas, revogação de credenciais).
3. Análise Forense: Em até 48 horas, a equipe de segurança da informação realizará a coleta de evidências digitais, preservação dos logs e identificação da causa raiz.
4. Comunicação à ANPD e aos Titulares: Se o incidente puder acarretar risco ou dano relevante aos titulares, o DPO comunicará o fato à ANPD no prazo de 72 horas (art. 48 da LGPD) e informará individualmente cada titular afetado, detalhando a natureza do incidente, os dados envolvidos e as medidas de proteção adotadas.
5. Relatório Final: Em até 30 dias corridos, o DPO elaborará relatório circunstanciado com as conclusões da investigação, as ações corretivas implementadas e as recomendações para evitar recorrência.

Atenção: A comunicação tardia ou omissão dolosa do incidente constitui violação grave das obrigações do DPO e dos gestores envolvidos, sujeitando-os a sanções administrativas e civis.

7.2 Sanções Administrativas Internas

O descumprimento das normas deste Manual ou da LGPD por empregados públicos da URBES será apurado em processo administrativo disciplinar, observando o contraditório e a ampla defesa, e poderá resultar nas seguintes sanções, aplicadas de forma cumulativa ou isolada, conforme a gravidade:

- Advertência verbal ou escrita — para infrações leves, como acesso indevido a dados sem consequências materiais.
- Suspensão de 1 a 30 dias — para reincidência ou infração moderada, como compartilhamento não autorizado de senha.

- Penalidades administrativas e demissão por justa causa – para infrações graves, como vazamento deliberado de dados, uso de dados para assédio ou discriminação, ou obstrução de investigação.
- Multa contratual - para prestadores de serviços terceirizados, conforme cláusula contratual específica.
- Comunicação ao Ministério Público e à Polícia - quando houver indícios de infração penal (art. 325 do Código Penal - violação de sigilo funcional; crimes previstos na LGPD, art. 52, §3°).

As sanções administrativas internas não excluem a responsabilidade civil ou as penalidades aplicáveis pela ANPD. Também poderá ter limitação de tratamento de dados, proibição parcial ou total do exercício de atividades com dados.

8. DISPOSIÇÕES FINAIS

Este Manual entra em vigor na data de sua aprovação pelo Diretor-Presidente da URBES e será revisado periodicamente, no mínimo a cada 2 (dois) anos, ou sempre que houver alteração significativa na legislação ou nas práticas de tratamento de dados da empresa. Dúvidas de interpretação ou omissões serão dirimidas pela Comissão de Adequação a LGPD, por intermédio do Encarregado pelo Tratamento de Dados Pessoais da URBES.

Sorocaba/SP, 08 de junho de 2026.

Adriano Aparecido Almeida Brasil
Diretor-Presidente da URBES

gov.br
Documento assinado digitalmente
ADRIANO APARECIDO ALMEIDA BRASIL
Data: 11/09/2026 14:36:11-0300
Verifique em https://validar.iti.gov.br

Jonathan Conrado Proença
Encarregado pelo Tratamento de Dados Pessoais

gov.br
Documento assinado digitalmente
JONATHAN CONRADO PROENCA
Data: 11/09/2026 14:00:45-0300
Verifique em https://validar.iti.gov.br