MUNICÍPIO DE IBICARÉ | SANTA CATARINA

Manual de Proteção de Dados Pessoais

Guia prático da LGPD para servidores públicos
Como proteger dados comuns e sensíveis

Controle Interno | Responsável pelo Tratamento de Dados

Versão 1.0 | Maio/2025

Sumário

1. Apresentação . . . 3
2. O que é a LGPD . . . 3
3. Conceitos básicos . . . 3
Dado comum x dado sensível: como diferenciar . . . 4
4. Princípios que orientam o tratamento . . . 5
5. Quando a Administração Municipal pode tratar dados . . . 5
Tratamento de dados na Secretaria Municipal de Saúde . . . 6
6. Transparência pública e proteção de dados . . . 6
7. Boas práticas no dia a dia . . . 7
7.1 Documentos em papel . . . 7
7.2 Computador e sistemas . . . 7
7.3 E-mail . . . 7
7.4 WhatsApp e redes sociais . . . 8
7.5 Dispositivos e mídias . . . 8
7.6 Atendimento ao público e por telefone . . . 8
7.7 Terceiros, contratos e compartilhamento . . . 8
7.8 Eliminação e guarda . . . 9
8. Cuidados específicos com dados sensíveis . . . 9
9. Direitos dos titulares . . . 10
10. Incidentes de segurança: o que fazer . . . 10
11. Responsabilidades e consequências . . . 11
12. Papéis e quem procurar . . . 11
13. Checklist rápido do servidor . . . 12
14. Perguntas frequentes . . . 12
15. Glossário . . . 13
16. Base normativa . . . 13

1. Apresentação

Todos os dias, quem trabalha na Administração Municipal lida com informações de pessoas: nome, CPF, endereço, dados de saúde, situação familiar, renda, matrícula escolar, processos administrativos. Esses dados pertencem aos cidadãos, e o Município tem a obrigação legal de protegê-los.

Este manual é um guia prático e de linguagem simples para ajudar você, servidor(a) ou colaborador(a), a entender o que é a Lei Geral de Proteção de Dados Pessoais (LGPD) e a aplicar, na rotina do seu setor, os cuidados necessários com dados pessoais comuns e sensíveis.

> **A regra de ouro**
> Trate os dados dos outros como você gostaria que tratassem os seus.

2. O que é a LGPD

A Lei nº 13.709/2018 (LGPD) estabelece regras sobre como os dados pessoais podem ser coletados, usados, armazenados, compartilhados e eliminados, tanto por empresas quanto pelo poder público. Seu objetivo é proteger a liberdade, a privacidade e o livre desenvolvimento da personalidade das pessoas.

O Capítulo IV da lei (arts. 23 a 30) trata especificamente do tratamento de dados pelo poder público. Ele deixa claro que a Administração Municipal pode tratar dados para executar suas competências legais e políticas públicas, mas deve fazê-lo com transparência, finalidade definida e segurança.

> **A LGPD não impede o trabalho da Administração Municipal.**
> Ela exige que o trabalho seja feito com responsabilidade: usar apenas o que é necessário, para a finalidade correta, e proteger o que for coletado.

3. Conceitos básicos

Termo	O que significa	Exemplo na Administração Municipal
Dado pessoal	Qualquer informação que identifique ou possa identificar uma pessoa	Nome, CPF, RG, endereço, telefone, e-mail, placa de veículo, matrícula funcional
Dado pessoal sensível	Dado que pode gerar discriminação se vazar e por isso exige proteção reforçada	Saúde, origem racial ou étnica, religião, opinião política, filiação sindical, vida sexual, dado genético ou biométrico
Dado de criança e adolescente	Dado de menor de 18 anos, tratado sempre no seu melhor interesse	Matrícula escolar, cadastro em programas sociais, vacinação
Titular	A pessoa a quem os dados se referem	O munícipe, o paciente, o aluno, o servidor

Termo	O que significa	Exemplo na Administração Municipal
Tratamento	Qualquer operação com dados: coletar, consultar, copiar, armazenar, enviar, compartilhar, apagar	Preencher um cadastro, enviar um e-mail com planilha, arquivar um processo
Controlador	Quem decide como e para que os dados são tratados	O Município de Ibicaré, representado pelo Prefeito
Operador	Quem trata dados em nome do controlador	Empresa de software, contabilidade terceirizada, prestadores de serviço
Encarregado	Canal de comunicação entre o Município, os titulares e a ANPD	O(a) Responsável pelo Tratamento de Dados designado(a)
ANPD	Autoridade Nacional de Proteção de Dados, órgão fiscalizador	Recebe comunicações de incidentes e pode aplicar sanções
Anonimização	Retirar a possibilidade de identificar a pessoa	Relatório estatístico sem nomes ou CPFs

Dado comum x dado sensível: como diferenciar

Dados pessoais comuns são os que identificam a pessoa no dia a dia: nome, CPF, RG, CNH, endereço, telefone, e-mail, data de nascimento, estado civil, dados bancários, renda, foto, dados funcionais.

Dados sensíveis são os que revelam características mais íntimas da pessoa e podem causar discriminação ou constrangimento:

- saúde (diagnósticos, CID, atestados, prontuários, receitas, laudos, deficiência);
- origem racial ou étnica;
- convicção religiosa;
- opinião política;
- filiação a sindicato ou organização religiosa, filosófica ou política;
- vida sexual ou orientação sexual;
- dado genético ou biométrico (digital, reconhecimento facial).

Atenção
Alguns dados parecem comuns, mas revelam informação sensível. Um atestado com CID, um pedido de benefício por deficiência ou a lista de pessoas atendidas em um programa de saúde mental devem ser tratados como sensíveis. **Na dúvida, proteja como sensível.** Dados como CPF, dados bancários e informações de crianças não são "sensíveis" pela definição legal, mas exigem cuidado redobrado pelo risco de fraude ou de dano.

4. Princípios que orientam o tratamento

Antes de coletar ou usar qualquer dado, faça-se as perguntas abaixo (art. 6º da LGPD).

1. **Finalidade:** para que estou coletando isso? O propósito é legítimo e informado?
2. **Adequação:** o uso é compatível com a finalidade informada?
3. **Necessidade:** estou pedindo só o mínimo necessário? Preciso mesmo da cópia do RG, da certidão de casamento, da foto?
4. **Livre acesso:** o titular pode consultar os dados que temos sobre ele?
5. **Qualidade dos dados:** os dados estão corretos e atualizados?
6. **Transparência:** o titular sabe quem trata seus dados e para quê?
7. **Segurança:** estou protegendo contra acesso indevido, perda e vazamento?
8. **Prevenção:** estou agindo antes que o problema aconteça?
9. **Não discriminação:** o dado nunca pode ser usado para fins discriminatórios.
10. **Responsabilização e prestação de contas:** consigo demonstrar que cumpro a lei?

5. Quando a Administração Municipal pode tratar dados

Todo tratamento precisa de uma justificativa legal ("base legal"). No serviço público, as mais comuns são:

- **Cumprimento de obrigação legal ou regulatória:** dados enviados ao TCE/SC, e-Social, Receita Federal, RAIS.
- **Execução de políticas públicas:** cadastro em programas sociais, vacinação, matrícula escolar, atendimento na saúde.
- **Exercício regular de direitos em processo:** processos administrativos e judiciais.
- **Execução de contrato ou procedimentos preliminares:** contratos com fornecedores e prestadores.
- **Proteção da vida ou tutela da saúde:** atendimentos de urgência, vigilância sanitária.
- **Consentimento:** é a exceção no serviço público, usado quando não há outra base legal, como no uso de imagem em divulgação institucional ou cadastro de e-mail para newsletter. Deve ser livre, informado e específico.

Para **dados sensíveis**, o art. 11 da LGPD traz hipóteses mais restritas, como cumprimento de obrigação legal, políticas públicas previstas em lei, tutela da saúde por profissionais ou serviços de saúde e proteção da vida.

Tratamento de dados na Secretaria Municipal de Saúde

A Secretaria Municipal de Saúde **pode e deve tratar dados pessoais e sensíveis** dos pacientes, pois isso é indispensável ao atendimento e às políticas públicas de saúde. A LGPD autoriza esse tratamento, em especial nas seguintes situações:

- **Tutela da saúde** (art. 11, II, "f"): atendimento, diagnóstico, tratamento e acompanhamento do paciente, realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- **Execução de políticas públicas** de saúde previstas em lei ou regulamento: vacinação, vigilância epidemiológica e sanitária, programas de saúde da família, regulação de consultas, exames e procedimentos.
- **Cumprimento de obrigação legal ou regulatória**: registro em prontuários e alimentação de sistemas oficiais (e-SUS, SISREG, SINAN, entre outros) e comunicação de doenças de notificação compulsória.
- **Proteção da vida ou da incolumidade física** do titular ou de terceiros, em situações de urgência e emergência.

Essa autorização **não dispensa os cuidados**: o acesso deve ser restrito às equipes que atendem o paciente, deve-se observar o sigilo profissional, coletar apenas o necessário, manter prontuários em local seguro, compartilhar somente com quem tem previsão legal (como Estado, Ministério da Saúde e hospitais de referência) e nunca divulgar dados de pacientes em grupos de mensagens, redes sociais ou portais.

> **Na prática**
> O servidor não precisa decidir sozinho qual é a base legal. Ela será definida no mapeamento de dados do setor. Em caso de dúvida sobre um novo uso de dados, consulte o Responsável pelo Tratamento antes de começar.

6. Transparência pública e proteção de dados

É comum a dúvida: "a Administração Municipal precisa ser transparente, então posso divulgar tudo?" **Não.** A Lei de Acesso à Informação (Lei nº 12.527/2011) e a LGPD funcionam em conjunto.

Pode e deve ser publicado	Não deve ser publicado
Nome e cargo de servidores, remuneração, contratos, licitações, empenhos e pagamentos, nome de fornecedores, atos oficiais, conforme a lei.	CPF completo, endereço residencial, telefone pessoal, dados bancários, dados de saúde, dados de crianças, informações de beneficiários de programas sociais além do exigido por lei.

Como publicar com segurança: mascare o CPF (ex.: ***.123.456-**), publique apenas o necessário e confira documentos digitalizados antes de subir ao portal.

Se um pedido de informação envolver dados pessoais de terceiros, encaminhe à Ouvidoria e ao Responsável pelo Tratamento para análise antes de responder.

7. Boas práticas no dia a dia

7.1 Documentos em papel

- Mantenha a **mesa limpa**: ao sair, guarde documentos com dados pessoais em armários ou gavetas com chave.
- Não deixe processos, fichas e prontuários expostos ao público no balcão de atendimento.
- Não deixe documentos na impressora ou na copiadora. Recolha imediatamente.
- Arquivos com dados sensíveis (saúde, assistência social, RH) devem ficar em local de acesso restrito.
- Descarte correto: papel com dados pessoais deve ser **triturado ou destruído** antes do descarte. Nunca jogue na lixeira comum.
- Ao atender, evite falar dados pessoais em voz alta se houver outras pessoas por perto.

7.2 Computador e sistemas

- Use **senha forte** (mínimo de 12 caracteres, com letras, números e símbolos). Evite datas de nascimento, nomes e sequências como "123456".
- **Nunca compartilhe sua senha** nem seu login. Tudo o que for feito com seu usuário é de sua responsabilidade.
- Não anote senhas em papel colado no monitor ou embaixo do teclado.
- **Bloqueie a tela** (tecla Windows + L) sempre que se ausentar da mesa.
- Mantenha o antivírus e o sistema atualizados. Não desative proteções.
- Não instale programas sem autorização do setor de TI.
- Acesse apenas os dados de que precisa para sua tarefa. Consultar dados por curiosidade (de vizinhos, parentes, colegas, autoridades) é infração, mesmo sem divulgar.
- Não use computadores públicos ou de terceiros para acessar sistemas da Administração Municipal.

7.3 E-mail

- Confira o destinatário antes de enviar. O erro mais comum de vazamento é o e-mail enviado à pessoa errada.
- Ao enviar mensagem para várias pessoas externas, use **cópia oculta (CCO)**.
- Evite enviar planilhas ou documentos com muitos dados pessoais por e-mail. Se necessário, proteja o arquivo com senha e envie a senha por outro canal.
- Desconfie de e-mails com links ou anexos inesperados (**phishing**). Na dúvida, não clique e avise o setor de TI.

- Prefira o e-mail institucional. Evite usar e-mail pessoal para assuntos de trabalho.

7.4 WhatsApp e redes sociais

- Evite tratar dados pessoais e sensíveis por WhatsApp pessoal. Quando o uso for indispensável ao serviço, utilize aparelho e número institucionais e envie apenas o mínimo necessário.
- **Não compartilhe** prints de processos, laudos, receitas, atestados, cadastros ou conversas com munícipes em grupos de WhatsApp, inclusive grupos internos amplos.
- Cuidado com grupos: antes de postar, pense em quem está no grupo e se todos precisam ver aquela informação.
- Não publique nas redes sociais fotos de atendimentos, documentos, telas de sistemas ou crianças sem autorização expressa dos responsáveis.
- Divulgação de eventos e ações: use imagens de caráter geral e, quando houver identificação de pessoas, obtenha autorização (principalmente de crianças e adolescentes).

7.5 Dispositivos e mídias

- Evite salvar dados pessoais em pen drives, HDs externos ou no computador pessoal. Se for inevitável, use dispositivo institucional e, de preferência, criptografado.
- Não deixe notebooks, celulares ou pen drives com dados da Administração Municipal desprotegidos em carros ou locais públicos.
- Se o dispositivo for perdido ou roubado, **comunique imediatamente** o Responsável pelo Tratamento e o setor de TI.

7.6 Atendimento ao público e por telefone

- Confirme a identidade antes de informar dados pessoais. Não passe informação por telefone a quem não puder ser identificado.
- Informações sobre uma pessoa só devem ser dadas ao próprio titular ou a seu representante legal.
- Peça apenas os documentos realmente necessários e **não retenha cópias** sem necessidade.
- Em salas de atendimento, mantenha telas de computador fora da visão de quem aguarda.

7.7 Terceiros, contratos e compartilhamento

- Antes de enviar dados a **empresas, órgãos ou entidades externas**, verifique se existe previsão legal ou contratual e se o compartilhamento é necessário.
- Contratos com fornecedores que tratam dados em nome do Município devem conter **cláusulas de proteção de dados** (conformidade com a LGPD, confidencialidade, comunicação de incidentes).
- Evite enviar a terceiros bases completas. Envie só o necessário e, se possível, anonimizado.

7.8 Eliminação e guarda

- Não guarde dados por tempo indeterminado. Observe as **tabelas de temporalidade** e prazos legais de guarda.
- Terminado o prazo e a finalidade, o dado deve ser eliminado ou anonimizado, seguindo as regras de arquivo público.
- Elimine planilhas, rascunhos e cópias duplicadas que não sejam mais necessárias.

8. Cuidados específicos com dados sensíveis

Os dados sensíveis exigem camada extra de proteção. Em especial:

Situação	Cuidado
Saúde (prontuários, receitas, exames, laudos, CID)	Acesso apenas por profissionais e servidores que necessitem. Nunca compartilhar em grupos de mensagens. Prontuários guardados em local restrito.
Atestados médicos de servidores	O RH deve registrar apenas o necessário (período de afastamento). O CID só deve ser tratado quando indispensável e por quem tem necessidade.
Assistência social (CadÚnico, benefícios, violência, vulnerabilidade)	Acesso restrito à equipe do serviço. Evitar divulgar nomes de beneficiários além do exigido por lei.
Biometria (digital, reconhecimento facial no ponto)	Utilizar somente com base legal e finalidade clara, com armazenamento seguro.
Filiação sindical, religião, opinião política	Não registrar, a menos que seja obrigatório (por exemplo, desconto em folha de contribuição sindical). Nunca usar para decisões de gestão.
Crianças e adolescentes	Tratar sempre no melhor interesse do menor. Evitar divulgação de nomes e imagens. Exigir autorização dos responsáveis para uso de imagem.
Deficiência	Informar apenas a quem precisa para garantir o atendimento ou direito.

Regras gerais para dados sensíveis:

1. Colete somente se for realmente indispensável.
2. Restrinja o acesso a quem precisa saber (princípio do "menor privilégio").
3. Armazene em local seguro (sistema com senha ou armário trancado).
4. Nunca divulgue em portais, murais, grupos ou redes sociais.
5. Quando precisar compartilhar, minimize e, se possível, anonimize.

9. Direitos dos titulares

Qualquer pessoa pode solicitar à Administração Municipal, mediante requerimento (art. 18 da LGPD):

- confirmação de que existe tratamento de seus dados;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade com a lei;
- informação sobre com quem seus dados foram compartilhados;
- informação sobre a possibilidade de não fornecer consentimento e suas consequências;
- revogação do consentimento, quando for a base legal.

> **Se um cidadão fizer esse tipo de pedido a você**
> Não ignore e não responda por conta própria. Registre o pedido e encaminhe imediatamente à **Ouvidoria** e ao **Responsável pelo Tratamento de Dados**, que adotarão as providências nos prazos legais.

10. Incidentes de segurança: o que fazer

Incidente de segurança com dados pessoais é qualquer evento que cause acesso não autorizado, perda, alteração, divulgação ou destruição acidental ou ilícita de dados. Exemplos:

- e-mail com planilha enviado à pessoa errada;
- documento com dados de munícipes deixado em local público;
- perda ou roubo de notebook, celular ou pen drive;
- ataque de vírus, ransomware ou golpe de phishing;
- publicação indevida de dado pessoal no portal ou nas redes sociais;
- acesso indevido por pessoa sem autorização;
- compartilhamento de print de processo em grupo de WhatsApp.

O que fazer imediatamente:

1. **Não esconda.** Quanto mais rápido for comunicado, menor o dano. Comunicar é agir corretamente.
2. **Contenha o problema, se possível:** desconecte o computador da rede, peça a exclusão da mensagem enviada por engano, retire a publicação, troque a senha.

3. **Comunique imediatamente** ao Responsável pelo Tratamento de Dados e ao setor de TI.
4. **Registre o que aconteceu:** data, hora, quais dados, quantas pessoas, como ocorreu.
5. **Aguarde orientação** para as demais providências.

Cabe ao Responsável pelo Tratamento avaliar o risco e, quando houver risco ou dano relevante aos titulares, comunicar à **ANPD** e aos titulares afetados, nos prazos e na forma definidos pela regulamentação vigente.

11. Responsabilidades e consequências

- **Todo servidor** que trata dados pessoais é responsável por observar este manual e a LGPD.
- O descumprimento pode acarretar **responsabilização administrativa** (conforme o Estatuto dos Servidores Municipais) e, conforme o caso, **civil e penal**, além de eventual enquadramento por improbidade administrativa.
- A ANPD pode aplicar ao Município sanções como advertência, publicização da infração, bloqueio ou eliminação dos dados e suspensão do tratamento. Para órgãos públicos, a lei não prevê multa pecuniária, mas os danos à imagem e a eventual indenização aos titulares são reais.
- A LGPD também protege o servidor: quem segue as orientações e comunica falhas prontamente age de forma diligente e demonstra boa-fé.

12. Papéis e quem procurar

Papel	Quem	Função
Controlador	Município de Ibicaré (Prefeito)	Decide sobre o tratamento e garante recursos para a adequação
Responsável pelo Tratamento de Dados (Encarregado)	Fernanda Monaliza Massoco Paz	Orienta servidores, recebe pedidos de titulares e da ANPD, coordena incidentes
Ouvidoria	Dagoberto Primo ouvidoria@ibicare.sc.gov.br	Recebe reclamações e solicitações dos cidadãos
Cada Secretaria/Setor	Secretário(a) e chefias	Garante o cumprimento das regras na sua área

Contato do Responsável pelo Tratamento de Dados
Nome: Fernanda Monaliza Massoco Paz
E-mail: lgpd@ibicare.sc.gov.br
Telefone/ramal: (49) 3538-0222
Local: Rua Dom Pedro II, nº 133, Centro, Ibicaré/SC

13. Checklist rápido do servidor

Use como lembrete diário:

[ ]	Só coleto os dados que realmente preciso?
[ ]	Sei para que vou usar e o cidadão foi informado?
[ ]	Guardei os documentos em local seguro ao sair da mesa?
[ ]	Bloqueei a tela do computador ao me ausentar?
[ ]	Minha senha é forte e só eu a conheço?
[ ]	Conferi o destinatário antes de enviar o e-mail?
[ ]	Evitei enviar dados pessoais por WhatsApp ou redes sociais?
[ ]	Não compartilhei dados sensíveis com quem não precisa?
[ ]	Triturei ou destruí o papel com dados pessoais antes de descartar?
[ ]	Sei a quem avisar em caso de incidente ou dúvida?

14. Perguntas frequentes

Posso passar o telefone de um munícipe para outra pessoa que pediu?

Não, em regra. Se houver necessidade (por exemplo, serviço público em andamento), o encaminhamento deve ser feito pela Administração Municipal, que entra em contato com o munícipe. Em caso de dúvida, consulte o Responsável pelo Tratamento.

Posso tirar foto de um documento do cidadão com meu celular pessoal?

Não é recomendável. Use equipamentos e sistemas institucionais. Se for inevitável, envie ao canal oficial e apague a imagem do aparelho.

Posso publicar a lista de beneficiários de um programa?

Somente se houver exigência legal e, mesmo assim, com o mínimo de dados (por exemplo, nome sem CPF completo, sem endereço). Consulte antes de publicar.

Um colega pediu para ver o cadastro de uma pessoa. Posso mostrar?

Somente se ele precisar do dado para executar sua função. Curiosidade ou interesse pessoal não justificam o acesso.

O vereador, a imprensa ou um advogado pediu informações sobre um cidadão. Posso passar?

Não sem análise. Encaminhe o pedido à Ouvidoria e ao Responsável pelo Tratamento, que avaliarão a base legal e o que pode ser fornecido.

Cometi um erro e enviei um e-mail para a pessoa errada. E agora?

Comunique imediatamente ao Responsável pelo Tratamento. Se possível, peça ao destinatário que apague a mensagem. Comunicar rápido é a atitude correta.

Preciso pedir autorização para fotografar um evento da Administração Municipal?

Para imagens gerais de multidão, em regra não. Quando as pessoas forem identificáveis, especialmente crianças e adolescentes, o ideal é obter autorização. Na dúvida, consulte.

15. Glossário

Termo	Definição
Anonimização	Processo que impede a identificação do titular.
ANPD	Autoridade Nacional de Proteção de Dados.
Base legal	Justificativa prevista em lei que autoriza o tratamento de dados.
Consentimento	Manifestação livre, informada e inequívoca do titular para um tratamento específico.
Criptografia	Técnica que embaralha o dado para que só quem tem a chave consiga ler.
Incidente de segurança	Evento que compromete a confidencialidade, integridade ou disponibilidade de dados pessoais.
Phishing	Golpe por e-mail, mensagem ou site falso para roubar senhas e dados.
RIPD	Relatório de Impacto à Proteção de Dados Pessoais.
Ransomware	Vírus que sequestra os arquivos e exige pagamento para liberá-los.
Titular	Pessoa natural a quem os dados se referem.
Tratamento	Toda operação realizada com dados pessoais.

16. Base normativa

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)
- Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI)
- Lei nº 12.965/2014 – Marco Civil da Internet
- Lei nº 8.069/1990 – Estatuto da Criança e do Adolescente (ECA)
- Regulamentos e guias da ANPD, incluindo a regulamentação sobre o encarregado e sobre comunicação de incidentes de segurança