Lei Geral de Proteção de Dados

Lei Federal nº 13.709/2018

GUIA DE CONFORMIDADE DA LGPD PARA SERVIDORES PÚBLICOS DO MUNICÍPIO DE JOINVILLE

Prefeitura de Joinville

Comitê Municipal de Proteção de Dados Pessoais

Este Guia foi desenvolvido para fornecer orientações práticas e diretas sobre a aplicação da Lei Geral de Proteção de Dados (LGPD) na rotina da Administração Pública, incluindo diretrizes para o uso ético e seguro de tecnologias como a Inteligência Artificial.

Seu conteúdo possui caráter informativo, servindo como material de apoio e conscientização para os servidores. Ele não substitui o aconselhamento jurídico formal, a análise de casos concretos pelas áreas técnicas ou a consulta obrigatória ao Encarregado pelo Tratamento de Dados Pessoais (DPO) em situações específicas.

Sumário

Sumário

CAPÍTULO -01-

O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS?

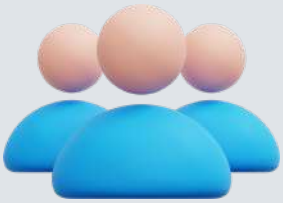
1.1. LGPD - Lei Geral de Proteção de Dados

Lei Federal nº 13.709/2018 – está em plena vigência no Brasil desde agosto de 2021.

Regulamenta o tratamento (uso) de dados pessoais de pessoas naturais (físicas), tanto em meios físicos quanto digitais.

Seu objetivo principal é proteger os direitos fundamentais de liberdade, privacidade e personalidade de todo indivíduo.

A LGPD traz um conjunto de boas práticas e ações para a utilização responsável de dados pessoais.



Essas boas práticas dizem respeito à capacitação e mudança de cultura das equipes de trabalho, documentos jurídicos e segurança da informação.

1.2 A LGPD se Aplica a Quem?

Setor Privado: Todas as empresas, profissionais autônomos, liberais e MEIs que utilizam dados para fins econômicos.

Setor Público: Todos os órgãos federais, estaduais e municipais, como o Município de Joinville.

Territorial: A LGPD se aplica a qualquer operação de tratamento de dados que seja realizada no território nacional brasileiro.

Extraterritorial: A lei também se aplica a qualquer tratamento de dados, mesmo que a empresa ou sistema esteja fora do Brasil se:

O objetivo for ofertar bens ou serviços ou processar dados de indivíduos localizados no Brasil.

O dado pessoal objeto do tratamento tenha sido coletado em território nacional.

1.3. Os 10 Princípios da LGPD

Finalidade

1. O tratamento do dado deve ter um propósito claro, legítimo e específico. Não use dados sem uma justificativa formal. Se não houver razão, o dado não deve ser coletado ou mantido.

Adequação

2. Os dados coletados devem ser relevantes e compatíveis com a finalidade informada. É adequado perguntar o tipo sanguíneo de um cidadão para um cadastro geral? Não. Mas é totalmente adequado e necessário para um atendimento médico de emergência.

Necessidade

3. Colete e use apenas os dados estritamente essenciais para alcançar a finalidade estabelecida. Evite a coleta de dados sob a hipótese de "quem sabe um dia será necessário".

Transparência

4. O titular deve ser informado de forma clara sobre como, onde e por quanto tempo seus dados são tratados. Garanta que as informações sobre o uso e compartilhamento dos dados sejam facilmente acessíveis e compreensíveis.

Livre Acesso

5. Garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados. Todos os pedidos ou dúvidas do titular sobre seus dados devem ser imediatamente direcionados ao Encarregado, que é o canal oficial de comunicação e garante a resposta formal e célere.

1.3. Os 10 Princípios da LGPD

Qualidade dos Dados

6 Garantia de que os dados tratados sejam exatos, claros, relevantes e atualizados. Corrija imediatamente qualquer dado incompleto ou incorreto que você identificar nos sistemas.

Segurança

7 Implementação de medidas técnicas e administrativas (planos de contingência, controle de acesso) contra vazamentos ou perdas. Todo material (digital ou físico) com dados deve estar sob controle. Só acesse, visualize ou modifique se tiver autorização.

Não Discriminação

8 É proibida a realização do tratamento de dados para fins discriminatórios ilícitos ou abusivos. Adote medidas para evitar que os sistemas, incluindo a IA gerem resultados injustos ou tendenciosos.

Prevenção

9 Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Seja proativo. Antes de lançar um novo processo ou sistema, avalie os riscos e adote medidas para evitar vazamentos, perdas ou uso indevido.

Responsabilização

10 Demonstração e comprovação da adoção de medidas eficazes de proteção de dados. Mantenha registros e documentação que prove que o órgão está em conformidade com a LGPD.

CAPÍTULO -02-

DADOS PESSOAIS E DADOS SENSÍVEIS

2. O que são Dados Pessoais e Dados Pessoais Sensíveis?

Dados Pessoais são as informações que identifiquem ou tornam identificáveis, como seu nome, CPF ou endereço. Já os Dados Pessoais Sensíveis são um subgrupo especial com maior potencial de risco, pois se referem a aspectos íntimos como sua saúde, origem racial ou dados biométricos e exigem proteção máxima para prevenir discriminação ou vazamentos graves.

Dados Pessoais

- Nome
- Endereço
- CPF/RG
- Passaporte
- E-Mail
- Telefone
- Currículo
- Outros

Dados Pessoais Sensíveis

- Biometria
- Filiação Politica
- Origem Racial
- Origem Étnica
- Histórico Medico
- Vida Sexual

CAPÍTULO
-03-

DIREITO DOS TITULARES

3.1. Quem é o titular dos dados pessoais?

É a própria pessoa natural (física), ou seja, o indivíduo a quem os dados pessoais se referem. Exemplo: servidor público, munícipe, contribuinte, usuário do SUS, estudante da Rede Pública.

A LGPD foi criada para proteger os direitos deste indivíduo, que tem o poder de exigir transparência e controle sobre seus dados. A lei abrange apenas dados de pessoas físicas; dados de empresas (Pessoas Jurídicas) não são considerados dados pessoais.

3.2. O Direito à Transparência e Acesso

Direito de Confirmação e Acesso: O Titular pode exigir saber se o Controlador (o órgão) ou o Operador (o fornecedor) está tratando dados dele e, em caso positivo, solicitar o acesso e uma cópia integral de todos esses dados.

Direito à Informação de Compartilhamento: O Titular deve ser formalmente informado sobre quais entidades (públicas ou privadas) o Município de Joinville compartilhou os seus dados.

3.3. Direito à Qualidade e Gestão dos Dados

Este conjunto de direitos assegura que os dados sejam precisos e utilizados de forma controlada.

Retificação

O Titular pode solicitar a correção de dados incompletos, inexatos ou desatualizados.

Se você identificar um dado incorreto no sistema, faça a correção imediatamente. Caso não possa, registre o pedido e o encaminhe ao setor responsável.

Anonimização ou Bloqueio

O Titular pode pedir o bloqueio do tratamento de dados desnecessários, excessivos ou que estejam sendo tratados em desacordo com a LGPD.

Caso o Titular solicite o bloqueio ou a eliminação, o pedido deve ser sempre encaminhado ao Encarregado para a análise legal, pois no Serviço Público muitos dados precisam ser mantidos por obrigação legal.

3.4. Direito de Contestação

Permite que o Titular conteste a legalidade do tratamento e exija a revisão de ações ou decisões tomadas sobre seus dados.

Revogação do Consentimento

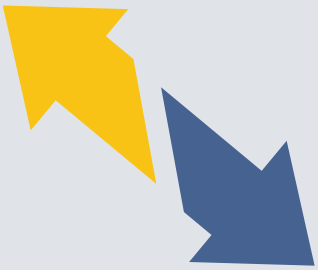
Retirar a qualquer momento o consentimento fornecido para o uso de um dado específico.

Portabilidade de Dados

Pedir a transferência de seus dados para outra instituição ou prestador de serviço.

Oposição ao Tratamento

Contestação formal sobre o tratamento de dados realizado pelo Município se ele for considerado irregular ou ilegal.



3.5. Registro de Pedido de Informações sobre Dados Pessoais do Município de Joinville

O que é?

É o ato formal de requerer informações sobre o tratamento de dados pessoais (acesso, correção, eliminação, etc.) ao Município.

Quem Pode Solicitar?

O próprio titular dos dados (pessoa física, como contribuinte ou servidor) ou seu representante legalmente constituído.

Onde Solicitar?

Utilizando o Formulário de Acesso à Informação no portal da Prefeitura.

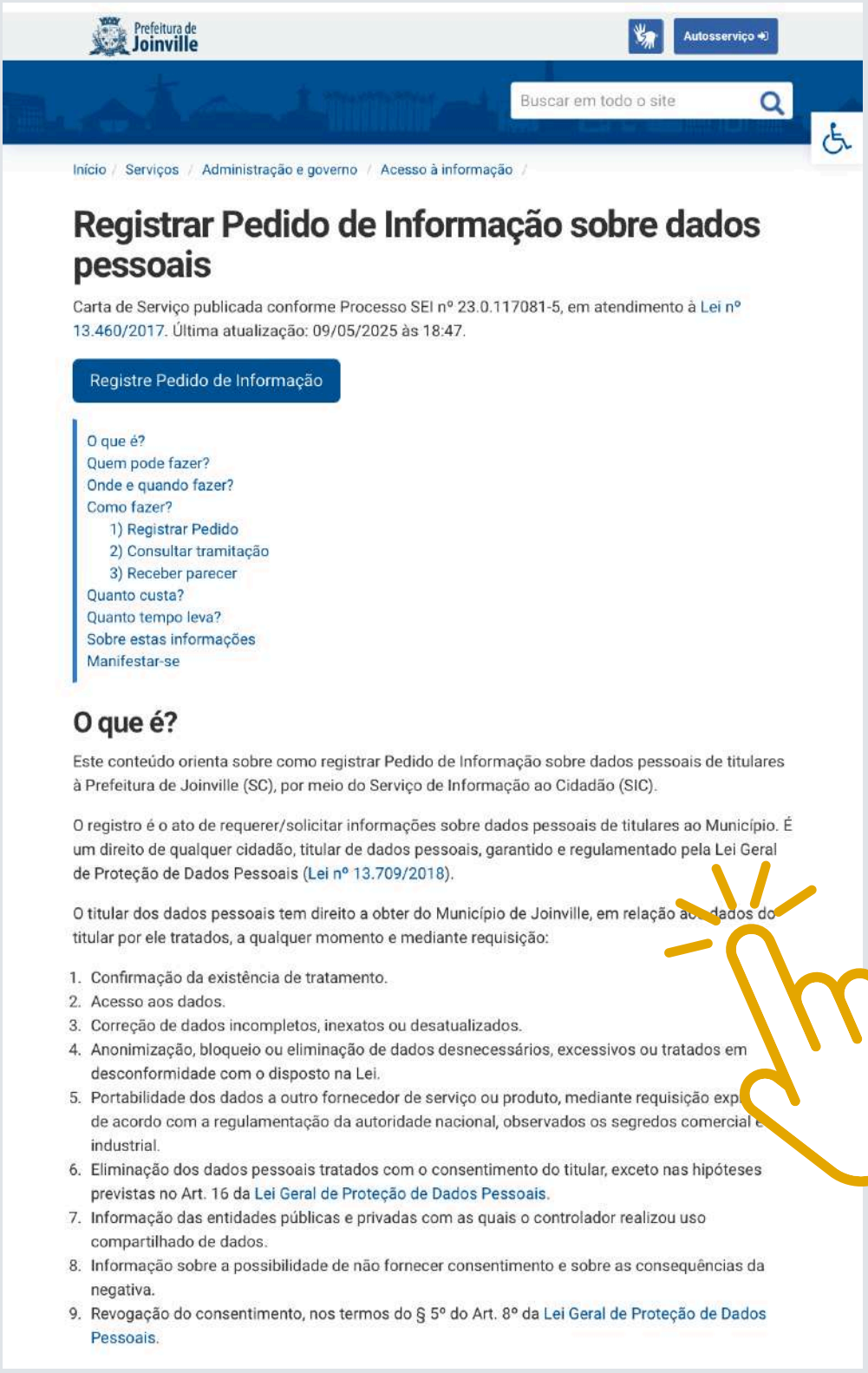
Presencial:

Dirija-se à Unidade de Ouvidoria da Prefeitura:
Av. Hermann August Lepper, 10, 1º andar – Saguaçu.
Segunda a sexta, das 8h às 18h.

On-line:

Formulário de Acesso à Informação

3.5. Registro de Pedido de Informações sobre Dados Pessoais do Município de Joinville



Prefeitura de Joinville

Autosserviço

Buscar em todo o site

Início / Serviços / Administração e governo / Acesso à informação /

Registrar Pedido de Informação sobre dados pessoais

Carta de Serviço publicada conforme Processo SEI nº 23.0.117081-5, em atendimento à Lei nº 13.460/2017. Última atualização: 09/05/2025 às 18:47.

Registre Pedido de Informação

O que é?
Quem pode fazer?
Onde e quando fazer?
Como fazer?
1) Registrar Pedido
2) Consultar tramitação
3) Receber parecer
Quanto custa?
Quanto tempo leva?
Sobre estas informações
Manifestar-se

O que é?

Este conteúdo orienta sobre como registrar Pedido de Informação sobre dados pessoais de titulares à Prefeitura de Joinville (SC), por meio do Serviço de Informação ao Cidadão (SIC).

O registro é o ato de requerer/solicitar informações sobre dados pessoais de titulares ao Município. É um direito de qualquer cidadão, titular de dados pessoais, garantido e regulamentado pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

O titular dos dados pessoais tem direito a obter do Município de Joinville, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

1. Confirmação da existência de tratamento.
2. Acesso aos dados.
3. Correção de dados incompletos, inexatos ou desatualizados.
4. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei.
5. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição exp... de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.
6. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no Art. 16 da Lei Geral de Proteção de Dados Pessoais.
7. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
8. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
9. Revogação do consentimento, nos termos do § 5º do Art. 8º da Lei Geral de Proteção de Dados Pessoais.

CAPÍTULO
-04-

CICLO DE VIDA DOS DADOS

4.1. Da Coleta à Eliminação

O tratamento de dados é um processo contínuo, com um ciclo de vida que envolve o dado desde a sua criação/coleta até o seu descarte final.

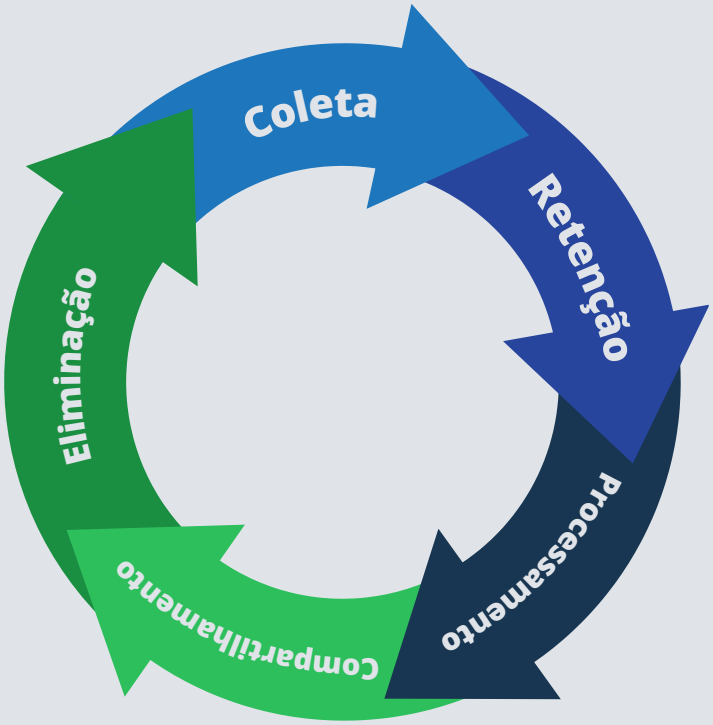
Coleta
Obtenção, recepção ou produção de dados pessoais independente do meio utilizado (documento em papel e eletrônico, sistema de informação, etc.)

Retenção
Arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel e eletrônico, banco de dados, arquivo de aço, etc.)

Processamento
Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.

Compartilhamento
Qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.

Eliminação
Qualquer operação que visa apagar ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.



CAPÍTULO
-05-

TRATAMENTO DE DADOS

5.1. Atribuições e Competências

A LGPD estabelece uma hierarquia de responsabilidade para garantir que o tratamento de dados esteja em conformidade com a lei.

É o principal responsável legal pelos dados, a pessoa jurídica a quem compete as decisões referentes ao tratamento de dados pessoais.
O Controlador decide quais dados serão tratados, como serão tratados e por quê. O Controlador deve responder aos Titulares e à Autoridade Nacional de Proteção de Dados (ANPD).

O Encarregado é a figura central de comunicação e gestão da LGPD dentro da estrutura. É a pessoa (ou área) que atua como canal de comunicação entre o Controlador, os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados (ANPD). Todo pedido de Titular, dúvida de conformidade, ou suspeita de incidente de segurança com dados pessoais, deve ser imediatamente encaminhado ao Encarregado.

O Operador executa o tratamento em nome do Controlador. É a pessoa jurídica ou física que realiza o tratamento de dados em nome do Controlador, seguindo suas instruções. O Operador é obrigado a seguir estritamente as orientações fornecidas pelo Controlador e deve garantir a segurança dos dados sob sua custódia.

5.1. Atribuições e Competências

CAPÍTULO
-06-

O PAPEL DO SERVIDOR MUNICIPAL DE JOINVILLE

6.1 Atuando em nome do Controlador

Na estrutura da LGPD, o Município de Joinville ocupa a posição jurídica de Controladora, sendo a responsável final pelas diretrizes e decisões sobre o tratamento de informações. No entanto, para que a lei não seja apenas um texto no papel, ela precisa de execução, e é aqui que o servidor se torna a figura central.

Finalidade:

As informações e dados pessoais devem ser utilizados exclusivamente para o cumprimento das tarefas oficiais, sendo proibido o uso para fins particulares ou para beneficiar terceiros.

Necessidade:

O servidor deve acessar sistemas e documentos apenas quando for indispensável para o exercício de sua função específica.

Zelo:

É responsabilidade do agente público adotar cuidados que evitem o extravio, a perda ou o acesso não autorizado a documentos e bases de dados.

Sua atuação ética e cuidadosa é o que sustenta o pilar da confiança pública. Quando o cidadão entrega seus dados ao Município, ele espera que o servidor trate essas informações com o máximo de zelo e integridade. Portanto, seu papel vai além do cumprimento de tarefas burocráticas: o servidor é o garantidor de que o direito fundamental à privacidade de cada joinvilense seja respeitado dentro de cada secretaria, gerência e unidade de serviço.

6.2 Termo de Compromisso, Sigilo e Confidencialidade

O Termo de Compromisso, Sigilo e Confidencialidade (TCSC) é o instrumento formal que ratifica a responsabilidade de cada servidor, estagiário ou colaborador no manejo de informações dentro do Município de Joinville. Ele não é apenas um documento administrativo, mas um pacto de confiança que protege o cidadão, a instituição e o próprio agente público.

MINUTA SEI Nº 0017387252/2023 - SAP.UNG.APD

- O dever de guardar sigilo não se limita ao horário de expediente ou ao período de vínculo com o Município. Ele possui caráter perpétuo, permanecendo válido mesmo após a aposentadoria, exoneração ou mudança de cargo.
- É expressamente proibido transferir, copiar, fotografar ou extrair bases de dados para fins pessoais ou para terceiros. O dado público deve permanecer nos canais oficiais do Município.
- O servidor compromete-se a adotar boas práticas de segurança, como não compartilhar senhas, bloquear estações de trabalho ao se ausentar e garantir que documentos digitais e/ou físicos com dados pessoais não fiquem expostos a pessoas não autorizadas.

CAPÍTULO
-07-

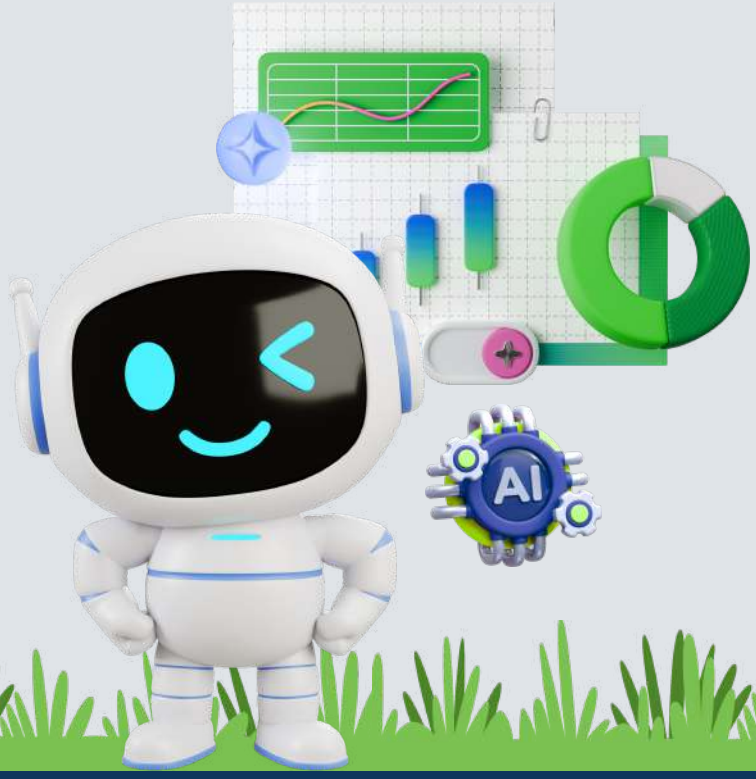
INTELIGÊNCIA ARTIFICIAL

7.1. O que é Inteligência Artificial (IA)?

IA refere-se a sistemas ou programas de computador capazes de aprender, raciocinar, perceber e tomar decisões com base em dados, simulando a inteligência humana.

São sistemas que podem analisar grandes volumes de dados para otimizar a triagem de processos, prever demandas de serviços públicos ou classificar documentos.

Como a IA se alimenta de dados, todo o seu processo de treinamento, execução e saída é considerado Tratamento de Dados e, portanto, deve obedecer à LGPD.



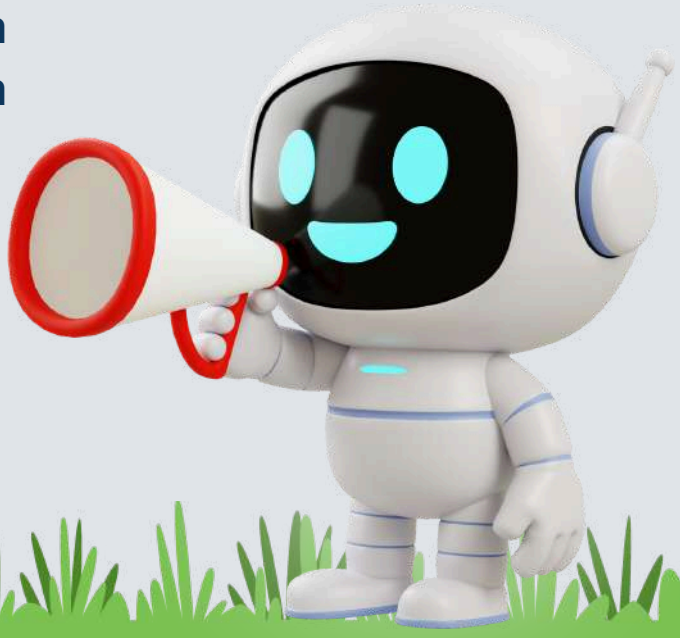
7.2. Regulamentação do uso da Inteligência Artificial no Município de Joinville

Instrução Normativa SEI Nº 228/2025

A Instrução Normativa SEI Nº 228/2025 estabelece o marco legal para o uso da Inteligência Artificial (IA) no Município de Joinville. Ela não apenas define regras, mas atua como um escudo de proteção para o servidor e para os dados do cidadão, garantindo que a inovação caminhe junto com a ética.

A norma visa regulamentar a adoção da IA na administração pública, assegurando conformidade com a Lei Geral de Proteção de Dados (LGPD) e com a Estratégia Brasileira de Inteligência Artificial.

O foco é transformar a tecnologia em uma aliada da eficiência, sem abrir mão da segurança institucional.



7.3. Utilização da IA em Conformidade com a LGPD

Finalidade e Adequação

Certifique-se de que a IA está sendo usada apenas para o propósito público específico para o qual foi projetada.

Limitação de Dados

Nunca insira ou treine o sistema com dados que não são estritamente necessários para alcançar o resultado esperado.

Transparência e Não Discriminação

Mantenha um canal aberto para que as decisões da IA possam ser validadas ou revistas por um agente humano, se necessário.

Segurança e Prevenção

A IA e seus dados de treinamento devem ser protegidos com medidas de segurança da informação rigorosas para evitar vazamentos.

Prestação de Contas

Garanta que o processo e os critérios da IA estejam documentados, facilitando a transparência e a auditoria.

7.4. Risco do Uso de Ferramentas Gratuitas

O uso de ferramentas de IA não oficiais para o trabalho institucional traz desafios que podem comprometer a segurança do servidor e do Município:

Exposição de Dados

Em plataformas gratuitas, as informações inseridas podem ser retidas e utilizadas para treinar modelos da empresa, saindo do controle do Município e tornando-se acessíveis a terceiros.

Vulnerabilidade Jurídica

Ferramentas externas não oferecem garantias contratuais de proteção de dados. Isso pode gerar inconformidades com a LGPD, recaindo a responsabilidade sobre a Administração Pública em caso de incidentes.

Fragilidade Técnica

Versões gratuitas carecem de suporte oficial e camadas avançadas de criptografia, o que aumenta o risco de vazamentos, ataques cibernéticos ou perda de informações críticas.

Incerteza de Segurança

Sem o monitoramento e a infraestrutura de segurança da Prefeitura, o uso dessas ferramentas torna-se uma troca arriscada de conveniência por falta de controle e confidencialidade.

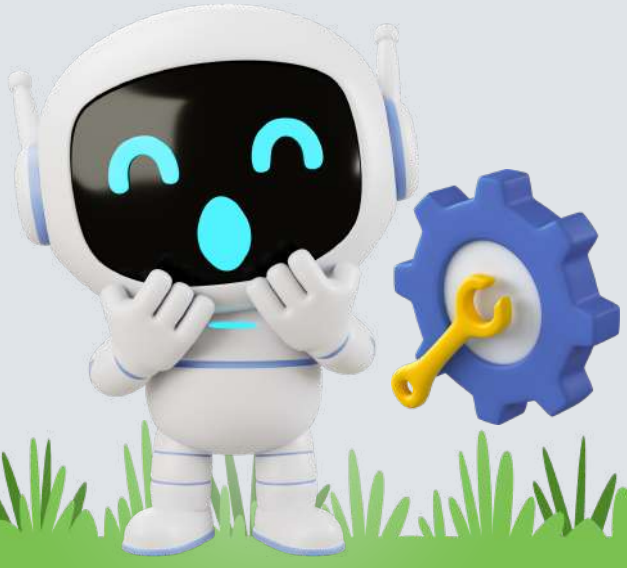
7.5. Decisões Automatizadas

É quando a tecnologia decide sozinha algo que afeta você. Embora eficiente, a IA nunca deve eliminar a transparência. A regra é clara: para cada decisão do sistema, deve existir o direito de recorrer a um ser humano.

A lei não impede o uso de Inteligência Artificial, mas exige que ela seja uma "caixa de vidro", e não uma "caixa-preta". Isso significa que:

O sistema não deve apenas entregar um "sim" ou "não". Ele precisa ser capaz de explicar quais dados foram determinantes para chegar àquele resultado.

Sempre que o Titular se sentir prejudicado por uma decisão robótica, ele tem o direito de solicitar que um ser humano analise o caso novamente.



A tecnologia deve servir como uma ferramenta de suporte para facilitar processos, garantindo que o controle e a responsabilidade final permaneçam, sempre, em mãos humanas.

CAPÍTULO
-08-

COMPARTILHAMENTO DE DADOS

8.1 Compartilhando Dados na Administração Direta e Indireta

Decreto Municipal Nº 55.380, de 02 de junho de 2023

O Decreto Nº 55.380, de 02 de junho de 2023, do Município de Joinville, é o instrumento legal que regulamenta e autoriza o compartilhamento de dados pessoais entre os órgãos da Administração Direta e Indireta do Município.

Este decreto estabelece as regras para o uso e o compartilhamento de dados entre os diversos órgãos da administração direita e indireta do munícipio, garantindo que a administração municipal atue em conformidade com a Lei Geral de Proteção de Dados (LGPD).

Sua importância reside na criação de um ambiente de segurança jurídica, onde o servidor sabe exatamente como tratar as informações e o cidadão tem a garantia de que seus dados não serão usados de forma indevida. Ele transforma a gestão pública em um modelo mais eficiente e transparente, protegendo a privacidade e mitigando riscos de vazamentos.

8.1 Compartilhando Dados na Administração Direta e Indireta

O compartilhamento de dados no Município de Joinville garante a integração de informações de forma direta e indireta entre todas as suas secretarias e autarquias, permitindo que diferentes setores da prefeitura trabalhem de forma integrada para melhorar os serviços prestados à população.

Mecanismos de controle e segurança para garantir a proteção total do compartilhamento de dados

- **Consulta Direta entre Sistemas**
- **Identificação Digital Individual**
- **Proteção por Pseudonimização**
- **Níveis de Acesso Diferenciados**
- **Filtro de Dados Mínimos**
- **Rastro Digital de Uso**

8.1 Compartilhando Dados na Administração Direta e Indireta

O compartilhamento de dados entre órgãos da Administração Direta e Indireta (ex: CAJ e SAMA, ou Hospital São José e SES) deve ocorrer exclusivamente por canais oficiais, como o SEI ou e-mail institucional. É necessário que o solicitante detalhe os dados precisos e justifique sua finalidade. Seguem outras diretrizes para solicitantes e remetentes:

- Finalidade Obrigatória: O compartilhamento só é permitido para a execução de políticas públicas específicas ou para o cumprimento de atribuições legais do órgão solicitante.
- Responsabilidade de Quem Recebe: O órgão que acessa os dados assume automaticamente todos os deveres de sigilo e segurança que o órgão detentor (custodiante) já possuía.
- Segurança Permanente: A obrigação de manter os dados protegidos não termina com o fim da atividade; o sigilo deve ser mantido mesmo após o uso das informações.
- Análise do Controlador: Antes de qualquer liberação, o órgão que guarda os dados (Controlador) deve analisar se o pedido possui fundamentação legal válida.
- Compartilhar com Terceiros: É terminantemente proibido repassar dados recebidos para pessoas, empresas ou entidades fora da administração municipal, sob pena de sanções legais.
- Uso sem Regras: A autorização de acesso é precária e pode ser cancelada imediatamente se as regras de utilização ou a finalidade declarada forem descumpridas.

8.2 Compartilhamento de Dados com outros Órgãos Publicos

Para formalizar o uso compartilhado de dados entre o Município de Joinville e órgãos externos, a exemplo do Governo Federal, Ministério Publico, Órgãos de polícia ou outros Municípios é obrigatória a utilização do instrumento jurídico adequado, podendo ser um Termo ou Acordo de Cooperação, que estabelece as regras e responsabilidades para esse intercâmbio de informações.

O Instrumento jurídico atua como o principal mecanismo de controle e prestação de contas, pois ele define a responsabilidade de cada agente de tratamento e o propósito exato do compartilhamento, tratamento e transferência dos dados.

8.3. Cláusulas Essenciais para Garantir a Conformidade com a LGPD

OBJETO

Define o propósito da cláusula, estabelecendo que o objetivo é regular o tratamento de dados pessoais realizado entre as partes, garantindo a proteção dos direitos fundamentais de liberdade e de privacidade dos titulares, conforme a Lei nº 13.709/2018.

DEFINIÇÃO DAS PARTES (OPERADOR/CONTROLADOR)

Identifica claramente o papel de cada envolvido. O Controlador é quem detém o poder de decisão sobre o tratamento, enquanto o Operador realiza o tratamento em nome e sob as instruções do controlador. Esta distinção é crucial para definir a responsabilidade civil e administrativa.

BASE LEGAL, FINALIDADE E TRANSPARÊNCIA

Estipula que todo dado tratado deve estar vinculado a uma das hipóteses de tratamento (Base Legal) previstas nos arts. 7º ou 11 da LGPD. Além disso, reforça que o dado só pode ser utilizado para a finalidade específica informada ao titular, vedando o uso para fins secundários sem nova autorização ou base legal.

8.3. Cláusulas Essenciais para Garantir a Conformidade com a LGPD

OBRIGAÇÃO DAS PARTES

Lista os deveres práticos, como: manter o registro das operações de tratamento (log), processar dados apenas conforme instruções documentadas e garantir que apenas pessoas autorizadas tenham acesso aos dados.

SEGURANÇA DA INFORMAÇÃO

Obriga a adoção de medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda ou alteração (ex: criptografia, controle de acesso e firewalls).

CONFIDENCIALIDADE

Reforça que o dever de sigilo sobre os dados pessoais tratados permanece mesmo após o término da relação contratual. Todos os envolvidos no tratamento devem assinar termos de confidencialidade específicos.

8.3. Cláusulas Essenciais para Garantir a Conformidade com a LGPD

TREINAMENTO

Cláusula que exige que as partes comprovem que seus funcionários e colaboradores que manuseiam dados pessoais passem por treinamentos periódicos de conscientização sobre a LGPD e segurança da informação.

ENCARREGADO DE DADOS (DPO)

As partes devem indicar quem são seus respectivos Encarregados do Tratamento de Dados (DPO), fornecendo nome e canal de contato direto. Isso garante que comunicações da ANPD ou requisições de titulares sejam atendidas com agilidade.

RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS (RIPD)

Estabelece a obrigação de cooperação. Caso o tratamento ofereça altos riscos às liberdades civis, o Operador deve fornecer ao Controlador todas as informações técnicas necessárias para a elaboração do RIPD, conforme exigido pela ANPD.

8.3. Cláusulas Essenciais para Garantir a Conformidade com a LGPD

AUDITORIA

Assegura ao Controlador o direito de realizar auditorias periódicas ou inspeções nas instalações e sistemas do Operador para verificar o estrito cumprimento das cláusulas de proteção de dados e segurança.

INCIDENTE DE SEGURANÇA

Define o protocolo de crise. Determina que o Operador deve comunicar ao Controlador qualquer incidente de segurança (vazamento ou invasão) em um prazo determinado (ex: 24h ou 48h), detalhando a natureza dos dados afetados e as medidas de mitigação adotadas.

RETENÇÃO E ELIMINAÇÃO

Os dados pessoais devem ser mantidos apenas pelo tempo necessário para cumprir a finalidade ou por obrigação legal. Ao término do contrato, o Operador deve excluir ou devolver os dados ao Controlador, apresentando uma evidência de descarte seguro.

8.4. Compartilhamento de Dados com Fornecedores

Ao contratar serviços que envolvam dados, o Município atua como controlador e a empresa como operadora. O contrato deve obrigatoriamente formalizar as responsabilidades do fornecedor, garantindo o cumprimento das normas de segurança e sigilo previstas na LGPD.

A inclusão de cláusulas específicas é essencial para mitigar riscos e delimitar responsabilidades entre o Município e seus prestadores de serviço. Elas asseguram que o fornecedor utilize os dados estritamente para o objeto contratado, mantenha protocolos rigorosos de segurança e responda legalmente por qualquer incidente.

8.5. Acesso e Instruções do Controlador

Sendo o Município de Joinville o controlador dos dados, cabe a ele definir como as informações devem ser tratadas. O fornecedor (operador) não tem autonomia sobre os dados e deve agir estritamente conforme as orientações recebidas.

Instruções Formalizadas: Toda e qualquer operação de tratamento realizada pelo fornecedor deve estar prevista em contrato ou instrução formal. O operador não pode utilizar os dados para finalidades próprias ou diferentes das contratadas.

Controle de Acesso: O Município precisa ter ciência sobre quem, dentro da estrutura do fornecedor, terá acesso aos dados, garantindo que o privilégio de acesso seja concedido apenas ao pessoal necessário (princípio do menor privilégio).

Poder de Auditoria: O contrato deve assegurar ao Município o direito de realizar auditorias e inspeções nas instalações ou sistemas do fornecedor para verificar se as instruções e normas de segurança estão sendo cumpridas.

Dever de Reporte: O Operador deve ser instruído a comunicar imediatamente ao Município qualquer incidente de segurança ou suspeita de vazamento, bem como qualquer ordem judicial que envolva os dados sob sua guarda.

CAPÍTULO
-09-

GESTÃO DE INCIDENTES

9.1. Gestão de Incidentes e Resposta Rápida

A gestão pública precisa estar preparada para responder a falhas, aplicando a gestão de incidentes, que abrange ações imediatas após a identificação de riscos à segurança ou à privacidade dos dados pessoais. O objetivo é atuar com transparência e eficiência, restabelecendo assim a segurança.

O que é incidente de segurança?

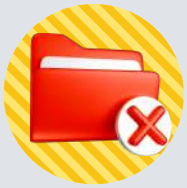
Um incidente de segurança é qualquer evento confirmado que resulte na destruição, perda, alteração, acesso não autorizado ou vazamento de dados pessoais.

Enviar E-Mail com dados sensíveis para o destinatário errado

Deixar o computador desbloqueado e com dados expostos

Perda de dispositivos sem trava de segurança

Descartar documentos que contenham dados pessoais ou sensíveis em lixo comum



9.1. Gestão de Incidentes e Resposta Rápida

Mesmo com todos os mecanismos de controle, a gestão pública deve estar preparada para agir em caso de falhas. A gestão de incidentes é o conjunto de ações tomadas imediatamente após a detecção de uma situação que coloque em risco a segurança ou a privacidade dos dados pessoais. O objetivo da resposta rápida é garantir que, diante de um problema, a prefeitura atue com transparência e eficiência para restabelecer a segurança e manter a confiança dos titulares de dados.

1 Identificação e Notificação

Qualquer suspeita de violação, vazamento ou acesso indevido deve ser reportada imediatamente à UTI (Unidade de tecnologia da SAP)

2 Ação Imediata

A prioridade é conter o incidente para evitar que o dano se propague, podendo incluir o bloqueio temporário de sistemas ou acessos.

3 Análise de Impacto

Avalia-se quais dados foram expostos e quais os riscos reais para o cidadão e para a administração.

4 Transparência

Em caso de risco relevante, o Município deve comunicar a ANPD e os titulares afetados, informando as medidas adotadas para mitigar os danos.

9.2. Como agir?

Qualquer evento adverso confirmado, como acesso não autorizado, vazamento, perda, alteração ou destruição de dados pessoais sob a guarda do Município, é considerado um incidente de segurança. Ao identificar qualquer suspeita ou confirmação dessa natureza, o servidor ou fornecedor deve comunicar imediatamente a Unidade de Tecnologia da Informação (SAP.UTI) e a Área de Proteção de Dados (APD), uma vez que o tempo de resposta é o fator mais crítico para garantir a conformidade legal e preservar os dados.

9.3. O que a ANPD estabelece?

Resolução CD/ANPD Nº 15, de 24 de Abril de 2024

Esta resolução regulamenta o dever de comunicação de incidentes de segurança. Ela estabelece procedimentos e prazos rigorosos, determinando que incidentes que possam acarretar risco ou dano relevante aos titulares devem ser reportados à ANPD e aos cidadãos afetados.

9.4. Fluxograma de Resposta Rápida a Incidentes

CONTATOS
E-MAIL
sap.uti@joinville.sc.gob.br
sap.uti.apd@joinville.sc.gov.br
-
Abrir processo SEI comunicando o incidente de segurança e enviar para SAP.UTI

CAPÍTULO
-10-

GOVERNANÇA E ESTRUTURA

10.1. Comitê Municipal de Proteção de Dados

O Comitê Municipal de Proteção de Dados Pessoais (CMPD) de Joinville é o órgão do Município responsável por regular e fiscalizar a adequação à LGPD (Lei Geral de Proteção de Dados) no município, atuando de forma deliberativa e consultiva, analisando normas, formulando diretrizes e supervisionando a implementação das ações de proteção de dados na administração pública direta e indireta, conforme decretos municipais.

Decreto Municipal Nº 44.844, de 25 de Novembro de 2021

É o marco regulatório que instituiu a estrutura de governança da LGPD no Município de Joinville, definindo as competências do Comitê Municipal de Proteção de Dados e as responsabilidades dos órgãos da administração direta e indireta.

Resolução CD/ANPD nº 18, de 16 de Julho de 2024

Esta resolução, de âmbito nacional, regulamenta especificamente a atuação, as responsabilidades e os deveres do Encarregado de Tratamento de Dados (DPO). Ela reforça a necessidade de autonomia técnica para o exercício da função e estabelece critérios de transparência que devem ser seguidos pelo Município para garantir que o contato entre a ANPD, o cidadão e a prefeitura ocorra de forma eficiente e segura.

10.1. Comitê Municipal de Proteção de Dados

Função

Atuar como o órgão de governança estratégica e consultiva, sendo responsável por centralizar a gestão da proteção de dados e coordenar a conformidade da administração pública municipal com a LGPD.

Atribuição

Incluem o estabelecimento de diretrizes, normas e políticas internas de privacidade, a avaliação de Relatórios de Impacto em novos projetos e a padronização de procedimentos de tratamento de dados entre as Secretarias.

Dever

O Comitê deve promover a cultura de proteção de dados e o treinamento dos servidores, zelar pelo cumprimento dos direitos dos titulares, assegurar que o tratamento de dados observe sempre o interesse público e prestar suporte técnico contínuo às decisões do Encarregado.

10.2. DPO - Encarregado

Função

O Encarregado é o elo oficial entre o Município, os cidadãos (titulares de dados) e a ANPD. Sua função central é garantir um canal de comunicação transparente, podendo ser exercida por um servidor designado ou por uma empresa especializada, desde que sua identidade seja pública e acessível a todos.

Atribuição

Compete a ele o trabalho operacional de receber reclamações e dúvidas dos titulares, prestando os esclarecimentos necessários. Além disso, o Encarregado deve orientar os colaboradores sobre as boas práticas de proteção de dados, apoiar a elaboração de relatórios de impacto e atuar como o ponto de contato direto para as demandas enviadas pela ANPD.

Dever

O Encarregado deve agir com ética, zelo e total autonomia técnica, sem sofrer pressões na sua análise. É seu dever fundamental evitar o conflito de interesses, não podendo ocupar cargos onde ele decida as finalidades do tratamento de dados que deve fiscalizar. Deve ainda garantir uma comunicação clara e em língua portuguesa para com o público.

10.3. Unidade de Tecnologia da Informação (SAP.UTI)

Função

A UTI funciona como o pilar tecnológico central da Secretaria de Administração e Planejamento. Sua missão é gerir a infraestrutura digital e garantir a estabilidade dos sistemas municipais, assegurando que as ferramentas de trabalho e os serviços ao cidadão operem com plena segurança e eficiência tecnológica.

Atribuição

Compete à unidade a gestão dos ativos de hardware, das redes de comunicação e dos sistemas de segurança perimetral. Suas atividades envolvem o monitoramento dos portais institucionais, a atualização constante de equipamentos e o suporte técnico especializado, controlando acessos para prevenir invasões ou vazamentos de informações.

Dever

A unidade tem o dever de zelar pela proteção dos dados em todo o seu ciclo de vida, aplicando a segurança por padrão em cada projeto. É sua obrigação prevenir vulnerabilidades, agir prontamente em incidentes e garantir que o armazenamento ou eliminação de informações ocorra de forma segura e ética.

10.4. Área de Proteção de Dados (APD)

Função

Unidade executiva e operacional, sendo responsável por implementar e monitorar as diretrizes de privacidade no cotidiano da administração pública.

Atribuição

Compreender a gestão do inventário de dados, o suporte técnico na elaboração de mapas de riscos, a verificação de conformidade em sistemas de TI e o auxílio direto ao Encarregado no atendimento às requisições dos titulares.

Dever

Assegurar a manutenção de registros atualizados das operações de tratamento, garantir a aplicação de medidas de segurança em novos projetos de software e atuar na linha de frente para a contenção de incidentes, garantindo que as operações técnicas estejam sempre alinhadas aos princípios de proteção de dados e à transparência administrativa.

10.5. Autoridade Nacional de Proteção de Dados (ANPD)

CANAIS DE ATENDIMENTO ANPD

- CIDADÃO/TITULAR DE DADOS
- AGENTE DE TRATAMENTO
- OUVIDORIA
- ENCARREGADO DE DADOS NA ANPD
- FALE CONOSCO
- PEDIDOS DE ACESSO À INFORMAÇÃO
- DÚVIDAS SOBRE A LGPD OU QUANTO À ATUAÇÃO DA ANPD

CAPÍTULO
-11-

BOAS PRÁTICAS

11.1. Zelo com a informação.

Antes de concluirmos, vamos transformar a teoria em prática. Proteger dados não é sobre burocracia, é sobre o cuidado que dedicamos ao cidadão e a segurança da nossa trajetória profissional. Veja como pequenas atitudes fazem a diferença no dia a dia:

Use apenas o @joinville.sc.gov.br. E-mails pessoais não têm validade oficial, não possuem backup da Prefeitura e deixam você desprotegido juridicamente.

Vai levantar da cadeira? Aperte Windows + L para bloquear seu computador. Isso impede que outras pessoas vejam dados sigilosos ou usem seu sistema enquanto você está fora

Nunca jogue listas com CPFs ou nomes no lixo comum. Pique ou rasgue bem os papéis. Dados pessoais descartados incorretamente são riscos de fraude.

Não anote senhas em post-its ou embaixo do teclado. Sua senha é sua assinatura digital. Só reutilize papéis que não contenham dados de terceiros no verso. Se houver nomes ou CPFs, o destino correto é a fragmentadora.

Ao atender, mantenha processos e fichas virados para baixo. Evite que o cidadão na fila veja informações de quem foi atendido antes.

Não deixe documentos parados na bandeja. Retire suas impressões assim que enviá-las para evitar que dados sensíveis fiquem expostos a quem passa.

Nunca tire fotos da tela do sistema para enviar por mensagem. O registro pode conter dados de outros cidadãos que não têm relação com o assunto.

Evite o uso de pen drives particulares em computadores da Prefeitura. Além do risco de vírus, a transferência de dados para dispositivos externos sem controle é um risco de segurança.

Não clique em links de e-mails suspeitos, mesmo que pareçam urgentes. Na dúvida, use apenas os canais e sistemas oficiais da Prefeitura para realizar seu trabalho.

12. Considerações Finais

A implementação da LGPD e a estruturação dos órgãos de controle, como o Comitê, a APD e a figura do Encarregado, não representam apenas o cumprimento de uma obrigação legal, mas um compromisso ético do Município com a transparência e a cidadania digital. A proteção de dados pessoais é, em última análise, a proteção da dignidade do cidadão.

Esta cartilha serve como um roteiro para que a administração pública municipal transite para um modelo de governança onde a privacidade é a regra, e não a exceção. O sucesso desta jornada depende da colaboração contínua entre todos os setores do município garantindo que o fluxo de informações, essencial para a prestação de serviços públicos, ocorra de forma segura, íntegra e respeitosa.

Ficha Técnica

Titulo:
Titulo: Lei Geral de Proteção de dados - Guia de Conformidade da LGPD para Servidores Públicos do Município de Joinville.

Elaboração:
Danielly Caroline H. A. J. Werneck de Carvalho

Coordenação Geral:
Sahmara Liz Botemberger

Revisão:
Unidade de Tecnologia da Informação – SAP.UTI
Comitê Municipal de Proteção de Dados Pessoais do Município de Joinville

Versão 2.0 – Revisada e Atualizada em 2026