ITAPEVI
PREFEITURA

Cartilha sobre a Lei Geral de Proteção de Dados

ITAPEVI
PREFEITURA

Cartilha sobre a Lei Geral de Proteção de Dados

Contatos:

***DPO*: Patrícia Jordão Marques**

(11) 4143-7500 – Ramal: 2323

***DPO*: Maria Claudia Chaluppe Galvão**

(11) 4143-7500 – Ramal: 2321

Apresentação

Esta cartilha tem como objetivo fornecer um guia prático com orientações de boas práticas sobre a segurança da privacidade de dados pessoais e estabelecer diretrizes dos processos referentes às obrigações estabelecidas na Lei Geral de Proteção de Dados (LGPD – Lei Federal n° 13.709/18 e Decreto Municipal n° 5.676/21) para a Administração Pública do Município de Itapevi. Abordaremos os principais pontos da legislação, definições, responsabilidades e penalidades, visando capacitar os servidores públicos para a adequada proteção dos dados pessoais.

Sumário

PREFEITURA MUNICIPAL DE ITAPEVI
CONTROLADORIA GERAL DO MUNICIPIO
Rua.Isola Belli Leonardi, 08 – Vila Nova | Itapevi | São Paulo | CEP: 06694-110
Tel.: (11) 4143-7500 | controladoriageral@itapevi.sp.gov.br

1. RESUMO SOBRE A LGPD

A Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), representa um marco na proteção da privacidade e no tratamento de dados pessoais no Brasil. Sua abrangência alcança todos os setores, incluindo a Administração Pública Municipal, que lida diariamente com uma vasta quantidade de informações sensíveis dos cidadãos.

A LGPD regulamenta o tratamento de dados pessoais, por pessoa natural ou jurídica, de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. A lei se aplica a qualquer operação realizada com dados pessoais, desde a coleta até a eliminação.

A legislação também estabelece dez princípios basilares para o tratamento de dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. No âmbito municipal, a observância desses princípios é crucial para garantir a confiança da população e o exercício pleno da cidadania. Afinal, as prefeituras coletam e processam dados relacionados à saúde, educação, assistência social, tributação, entre outros, demandando responsabilidade e transparência em sua gestão.

Um desafio significativo para os municípios é a adequação à LGPD, considerando as limitações de recursos e a complexidade da legislação. A criação de uma estrutura de governança em proteção de dados, com a nomeação de um Encarregado pelo Tratamento de Dados Pessoais (DPO), é fundamental. O DPO atua como um elo entre o município, os titulares dos dados e a

Autoridade Nacional de Proteção de Dados (ANPD), orientando e fiscalizando a aplicação da lei. A capacitação dos servidores municipais também é essencial para disseminar a cultura da proteção de dados e garantir a conformidade com a LGPD.

A lei prevê diferentes bases legais para o tratamento de dados pessoais, sendo o consentimento do titular uma das mais importantes. No entanto, no contexto da Administração Pública, o consentimento não é sempre a base legal aplicável. A execução de políticas públicas previstas em leis e regulamentos, por exemplo, autoriza o tratamento de dados sem a necessidade de consentimento explícito. Compreender as bases legais aplicáveis a cada situação é fundamental para evitar tratamentos indevidos e garantir a legalidade das ações da Administração Pública.

A LGPD também estabelece direitos aos titulares dos dados, como o acesso, a correção, a portabilidade e a eliminação dos seus dados. Os municípios devem implementar mecanismos que facilitem o exercício desses direitos pelos cidadãos, assegurando a transparência e o controle sobre suas próprias informações. A lei prevê sanções para o descumprimento de suas disposições, que podem variar de advertências a multas significativas. Portanto, a adequação à LGPD não é apenas uma questão ética, mas também uma necessidade legal, visando evitar penalidades e prejuízos à imagem do município.

2. PRINCIPAIS NOMENCLATURAS

2.1. Dado Pessoal

É qualquer informação relacionada a uma pessoa natural identificada ou identificável. Essa definição abrange uma ampla gama de informações que, direta ou indiretamente, permitem a individualização de uma pessoa.

2.1.1. Aspectos importantes da definição:

- Pessoa natural: A LGPD protege apenas os dados de pessoas físicas, não se aplicando a pessoas jurídicas.
- Identificada ou identificável: A pessoa pode ser identificada diretamente (ex: nome, CPF) ou indiretamente (ex: data de nascimento, endereço, características físicas, placa de veículo etc.), através da combinação de diferentes informações. A identificabilidade não precisa ser imediata ou fácil, basta que seja possível, por qualquer meio, associar a informação a um indivíduo.

2.1.2. Exemplos de dados pessoais na Administração Pública Municipal:

- Dados cadastrais: Nome, CPF, RG, endereço, data de nascimento, estado civil, filiação, etc.
- Dados de contato: Telefone, e-mail, endereço residencial, etc.
- Dados biométricos: Impressões digitais, reconhecimento facial, etc.
- Dados de saúde: Informações sobre o estado de saúde, prontuários médicos, etc.
- Dados educacionais: Histórico escolar, notas, frequência, etc.

- Dados financeiros: Renda, patrimônio, dados bancários, etc.
- Dados de localização: Registros de GPS, informações de câmeras de segurança, etc.
- Dados de navegação: Histórico de acesso a sites, cookies, etc. (quando coletados por sistemas municipais).
- Imagens e gravações: Fotos, vídeos, áudios que permitam a identificação de indivíduos.
- Dados sensíveis: Dados sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicato, saúde ou a vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural. Esses dados possuem proteção ainda mais rigorosa e exigem justificativas e cuidados especiais para o tratamento.

2.1.3. Implicações para a Administração Pública Municipal:

A definição de dado pessoal é fundamental para que a Administração Pública Municipal possa:

- Mapear os dados pessoais tratados: Identificar quais informações sob sua guarda são consideradas dados pessoais.
- Implementar medidas de segurança adequadas: Proteger os dados pessoais de acordo com os requisitos da LGPD.
- Atender aos direitos dos titulares: Garantir o exercício dos direitos dos cidadãos em relação aos seus dados pessoais.

- Demonstrar a conformidade com a LGPD: Comprovar que o tratamento de dados pessoais está de acordo com a lei.

2.2. Dado Pessoal Sensível

É uma categoria especial de dados pessoais que recebem proteção ainda mais rigorosa devido à sua natureza e ao potencial de discriminação ou violação de direitos fundamentais. A LGPD define dados pessoais sensíveis como aqueles que se referem a:

- Origem racial ou étnica: Informações sobre a raça, cor, etnia, ancestralidade ou origem nacional de um indivíduo.
- Convicção religiosa: Crenças, práticas e dogmas religiosos de uma pessoa.
- Opinião política: Ideologias, filiações partidárias e posicionamentos políticos de um indivíduo.
- Filiação a sindicato ou a organização de caráter religioso, filosófico ou político: Associação a grupos que representem interesses específicos, como sindicatos, igrejas ou partidos políticos.
- Dado referente à saúde ou à vida sexual: Informações sobre o estado de saúde física ou mental, histórico médico, tratamentos, exames, laudos, vida sexual, orientação sexual, etc.
- Dado genético: Informações sobre a composição genética de um indivíduo.
- Dado biométrico: Características físicas ou comportamentais únicas de uma pessoa, como impressões digitais, reconhecimento facial, íris, voz, etc., quando vinculado a uma pessoa natural.

2.2.1. Aspectos importantes sobre dados sensíveis:

Maior proteção: Exigem cuidados redobrados no tratamento e medidas de segurança mais robustas.

Regras específicas para o tratamento: O tratamento de dados sensíveis é, em regra, proibido, exceto em situações específicas previstas na LGPD, como:

- Cumprimento de obrigação legal ou regulatória pelo poder público.
- Proteção da vida ou da incolumidade física do titular ou de terceiros.
- Tutela da saúde, exclusivamente, em procedimentos realizados por profissionais de saúde, serviços de saúde ou órgão de pesquisa.
- Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de acesso a sistemas eletrônicos.
- Para a defesa de direitos em processo judicial, administrativo ou arbitral.
- Consentimento específico e inequívoco do titular, em alguns casos.

Consentimento: Embora o consentimento seja uma das bases legais para o tratamento de dados pessoais, a LGPD estabelece restrições e requisitos específicos para o consentimento em relação a dados sensíveis. O consentimento deve ser específico, informado e inequívoco, demonstrando claramente a finalidade do tratamento.

2.2.2. Exemplos na Administração Pública Municipal:

- Dados de saúde de pacientes em hospitais municipais: Prontuários médicos, resultados de exames, laudos, etc.
- Informações sobre religião e filiação sindical em cadastros de servidores: Coletados apenas quando estritamente necessário e com base legal específica.
- Dados biométricos para controle de acesso a sistemas: Impressões digitais para identificação de funcionários ou usuários de serviços públicos.

2.2.3. Implicações para a Administração Pública:

A correta identificação e tratamento dos dados pessoais sensíveis é crucial para a conformidade com a LGPD e a proteção dos direitos fundamentais dos cidadãos. A Administração Pública Municipal deve:

- Mapear os dados sensíveis tratados: Identificar quais informações sob sua guarda se enquadram nessa categoria.
- Implementar medidas de segurança reforçadas: Adotar medidas de proteção mais rigorosas para esses dados.
- Justificar o tratamento: Basear o tratamento em uma das hipóteses legais previstas na LGPD.
- Obter consentimento específico quando necessário: Assegurar que o consentimento seja livre, informado e inequívoco.

- Treinar os servidores: Capacitar os funcionários sobre as regras específicas para o tratamento de dados sensíveis.

2.3. Titular

É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Em outras palavras, é o indivíduo que pode ser identificado, direta ou indiretamente, pelas informações coletadas e utilizadas pela Administração Pública.

2.3.1. Características do titular:

Pessoa natural: Somente pessoas físicas podem ser titulares de dados pessoais, excluindo-se pessoas jurídicas.

Identificação: O titular é o indivíduo que pode ser identificado pelos dados, seja diretamente (nome, CPF) ou indiretamente (características, combinação de informações).

Dono dos dados: Embora a Administração Pública colete e utilize os dados, o titular é o "dono" das informações e possui direitos sobre elas.

2.3.2. Exemplos de titulares na Administração Pública:

- Cidadãos: Dados coletados em cadastros municipais, sistemas de saúde, educação, assistência social, etc.
- Servidores públicos: Dados cadastrais, funcionais, de saúde, etc.

- Fornecedores e prestadores de serviços: Dados cadastrais, contatos, informações contratuais, etc.
- Usuários de serviços públicos: Dados coletados em portais, aplicativos e plataformas digitais.

2.3.3. Direitos do titular:

A LGPD garante aos titulares uma série de direitos em relação aos seus dados pessoais, incluindo:

- Confirmação da existência de tratamento: O titular pode solicitar a confirmação de que a Administração Pública está tratando seus dados.
- Acesso aos dados: O titular tem o direito de acessar seus dados pessoais, obtendo cópia das informações em formato acessível.
- Correção de dados incompletos, inexatos ou desatualizados: O titular pode solicitar a correção de informações incorretas ou desatualizadas.
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD: O titular pode solicitar a anonimização, o bloqueio ou a eliminação de dados que não estejam sendo tratados de acordo com a lei.
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa: O titular pode solicitar a transferência de seus dados para outra organização.
- Eliminação dos dados pessoais tratados com o consentimento do titular: O titular pode solicitar a

eliminação dos dados que foram coletados com base em seu consentimento.

- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados: O titular pode solicitar informações sobre o compartilhamento de seus dados com outras organizações.
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa: A Administração Pública deve informar o titular sobre a possibilidade de recusar o consentimento para o tratamento de dados e as consequências dessa recusa.
- Revogação do consentimento: O titular pode revogar o consentimento para o tratamento de dados a qualquer momento.

2.3.4. Importância da identificação do titular:

A correta identificação do titular é essencial para que a Administração Pública possa:

Atender aos direitos dos titulares: Garantir o exercício dos direitos previstos na LGPD.

Implementar medidas de segurança adequadas: Proteger os dados pessoais de cada indivíduo.

Demonstrar a conformidade com a LGPD: Comprovar que o tratamento de dados pessoais está de acordo com a lei.

2.4. Controlador

É a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Na prática, dentro da Administração Pública, o controlador é o órgão ou entidade pública que define a finalidade e os meios de tratamento dos dados pessoais.

2.4.1. Características do Controlador:

Responsabilidade: O controlador tem a responsabilidade final pela proteção dos dados pessoais e pelo cumprimento da LGPD.

Autonomia: Decide quais dados serão coletados, para qual finalidade, por quanto tempo e quais medidas de segurança serão implementadas.

Transparência: Deve fornecer informações claras e acessíveis aos titulares sobre o tratamento de seus dados.

Prestação de contas: Deve ser capaz de demonstrar à ANPD (Autoridade Nacional de Proteção de Dados) a conformidade com a LGPD.

2.4.2. Exemplos de controladores na Administração Pública:

- Prefeituras: Controlam os dados dos cidadãos em cadastros municipais, sistemas de saúde, educação, etc.

- Secretarias Municipais: Controlam os dados relacionados às suas áreas de atuação (ex: Secretaria de Saúde controla os dados dos pacientes).
- Câmaras Municipais: Controlam os dados de vereadores, funcionários e cidadãos que interagem com a Câmara.
- Autarquias e Fundações Públicas Municipais: Controlam os dados relacionados às suas atividades específicas.

2.4.3. Importância da identificação do controlador:

A correta identificação do controlador é fundamental para:

- Definir responsabilidades: Esclarecer quem é o responsável pela proteção dos dados pessoais.
- Garantir a conformidade com a LGPD: Assegurar que o tratamento de dados pessoais esteja de acordo com a lei.
- Facilitar o exercício dos direitos dos titulares: Permitir que os titulares saibam a quem se dirigir para exercer seus direitos.

2.5. Operador

É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Em outras palavras, o operador processa os dados seguindo as instruções e sob a autoridade do controlador.

2.5.1. Características do operador:

Subordinação ao Controlador: Age sob as determinações do controlador, não tendo autonomia para decidir sobre a finalidade e os meios do tratamento.

Responsabilidade Limitada: Embora tenha responsabilidades específicas em relação à segurança dos dados, a responsabilidade final pelo tratamento permanece com o controlador.

Obrigações Contratuais: O relacionamento entre controlador e operador deve ser formalizado em contrato, com cláusulas específicas sobre a proteção de dados.

Sigilo e Segurança: Deve garantir a confidencialidade, integridade e disponibilidade dos dados pessoais.

2.5.2. Exemplos de operadores na Administração Pública:

- Empresas de Tecnologia da Informação (TI): Que prestam serviços de armazenamento, processamento ou análise de dados para a Administração Pública.
- Empresas de terceirização de serviços: Que realizam atividades que envolvem o tratamento de dados pessoais, como *call centers*, empresas de cobrança, etc.
- Órgãos ou Entidades Públicas que tratam dados em nome de outro órgão: Por exemplo, uma autarquia que processa dados para uma secretaria municipal.

2.5.3. Importância da identificação do operador:

A correta identificação do operador é fundamental para:

- Definir responsabilidades: Esclarecer as obrigações do operador e do controlador em relação à proteção de dados.
- Garantir a segurança dos dados pessoais: Assegurar que o operador implemente medidas de segurança adequadas.
- Facilitar a fiscalização e a responsabilização: Permitir que a ANPD e os titulares identifiquem os responsáveis pelo tratamento de dados.

2.6. Encarregado (*DPO - Data Protection Officer*)

É o profissional indicado pelo controlador para atuar como um ponto focal para assuntos relacionados à proteção de dados pessoais. Ele tem a responsabilidade de orientar o controlador e o operador sobre as melhores práticas para garantir a conformidade com a LGPD. O *DPO*, sigla para *Data Protection Officer* ou Encarregado pelo Tratamento de Dados Pessoais, atua também como um canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

2.6.1. Obrigatoriedade da designação de *DPO*:

A LGPD determina que a designação de um *DPO* é obrigatória em alguns casos, como quando o tratamento de dados envolver:

- Dados sensíveis;
- Tratamento em larga escala de dados pessoais;

- Monitoramento regular e sistemático de titulares de dados.

Mesmo quando não for obrigatória, a designação de um *DPO* é altamente recomendável para a Administração Pública, considerando a grande quantidade de dados pessoais que são tratados e a complexidade das operações.

2.6.2. Características importantes do *DPO*:

Conhecimento especializado em Proteção de Dados: O *DPO* deve possuir conhecimento técnico e jurídico sobre a LGPD e as melhores práticas de proteção de dados.

Imparcialidade e independência: O *DPO* deve atuar com isenção e independência, sem sofrer interferências indevidas do controlador.

Sigilo Profissional: O *DPO* deve manter a confidencialidade das informações a que tem acesso.

Acesso aos Dados Pessoais: O *DPO* deve ter acesso aos dados pessoais para poder desempenhar suas funções.

2.6.3. Importância do *DPO* na Administração Pública:

A presença de um *DPO* na Administração Pública é fundamental para:

- Garantir a conformidade com a LGPD: O *DPO* auxilia a organização a cumprir as obrigações legais e evitar sanções.
- Promover a cultura de proteção de dados: O *DPO* conscientiza os servidores sobre a importância da privacidade e da proteção de dados.
- Fortalecer a confiança dos cidadãos: A designação de um *DPO* demonstra o compromisso da Administração Pública com a proteção dos dados pessoais.
- Mitigar riscos e evitar incidentes de segurança: O *DPO* auxilia na identificação e prevenção de vazamentos de dados e outros incidentes.

2.7. **Tratamento de Dados**

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Em termos mais simples, qualquer ação que a Administração Pública realize com os dados pessoais dos cidadãos, desde a coleta até a eliminação, é considerada tratamento.

2.7.1. Exemplos de tratamento de dados na Administração Pública:

- Coleta de dados em cadastros municipais: Registro de informações como nome, endereço, CPF, etc.
- Armazenamento de dados de pacientes em sistemas de saúde: Manutenção de prontuários médicos eletrônicos.
- Utilização de dados para análise estatística: Processamento de dados para gerar indicadores de saúde, educação, etc.
- Compartilhamento de dados entre órgãos públicos: Transferência de informações entre diferentes secretarias ou entidades.
- Eliminação de dados após o término da finalidade: Descarte seguro de informações que não são mais necessárias.

2.7.2. Princípios que regem o tratamento de dados:

A LGPD estabelece princípios que devem ser observados em todas as operações de tratamento de dados:

- Finalidade: Os dados devem ser coletados para finalidades legítimas, específicas, explícitas e informadas ao titular.
- Adequação: Os dados coletados devem ser pertinentes, adequados e não excessivos em relação à finalidade do tratamento.
- Necessidade: Os dados coletados devem ser limitados ao mínimo necessário para atingir a finalidade do tratamento.

- Livre Acesso: Deve ser garantida aos titulares consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como a integralidade de seus dados pessoais.
- Qualidade dos Dados: Os dados devem ser exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
- Transparência: O titular deve ser informado de forma clara e acessível sobre o tratamento de seus dados.
- Segurança: Devem ser implementadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
- Prevenção: Devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
- Não Discriminação: O tratamento de dados não pode ser utilizado para fins discriminatórios, ilícitos ou abusivos.
- Responsabilização e Prestação de Contas: O controlador deve ser capaz de demonstrar a conformidade com a LGPD.

2.7.3. Bases legais para o tratamento de dados:

A LGPD define as bases legais que autorizam o tratamento de dados pessoais. A Administração Pública pode tratar dados com base em, por exemplo:

- Cumprimento de Obrigação Legal ou Regulatória: Quando a lei exige a coleta e o tratamento de dados.
- Execução de Políticas Públicas: Quando o tratamento é necessário para a implementação de políticas públicas previstas em leis e regulamentos.
- Tutela da Saúde: Em procedimentos realizados por profissionais de saúde.
- Consentimento: Autorização livre, informada e inequívoca do titular. No entanto, o consentimento não é a base legal mais adequada para a Administração Pública, pois deve ser utilizado apenas quando as outras bases legais não se aplicarem.

2.7.4. Importância do conceito de tratamento:

Compreender o conceito de tratamento de dados é fundamental para que a Administração Pública possa:

- Cumprir a LGPD: Assegurar que todas as operações com dados pessoais estejam de acordo com a lei.
- Proteger os direitos dos titulares: Garantir a privacidade e a segurança das informações pessoais dos cidadãos.
- Promover a transparência e a confiança: Demonstrar aos cidadãos como seus dados estão sendo tratados.

2.8. Consentimento

O consentimento é uma das bases legais que autorizam o tratamento de dados pessoais. Ele é definido como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

A utilização do consentimento como base legal para o tratamento de dados pessoais na Administração Pública deve ser excepcional e criteriosamente avaliada. A preferência deve ser dada a outras bases legais, como o cumprimento de obrigação legal e a execução de políticas públicas, sempre que possível. Quando o consentimento for utilizado, é fundamental garantir que ele seja livre, informado, inequívoco, específico e facilmente revogável, conforme os requisitos da LGPD.

2.8.1. Características do consentimento:

Livre: O titular deve ter a liberdade de escolher se consente ou não com o tratamento de seus dados, sem sofrer qualquer tipo de coação ou pressão. A recusa não pode implicar em discriminação ou prejuízo para o titular.

Informado: O titular deve receber informações claras e precisas sobre a finalidade do tratamento, os dados que serão coletados, o período de armazenamento, os destinatários dos dados e seus direitos como titular.

Inequívoco: O consentimento deve ser demonstrado por meio de uma ação afirmativa do titular, que indique de forma clara sua concordância com o tratamento dos dados. Silêncio, inação ou pré-marcação de opções não configuram consentimento.

Específico: O consentimento deve ser dado para finalidades determinadas. O controlador não pode utilizar os dados para finalidades diferentes daquelas para as quais o consentimento foi obtido.

Revogável: O titular pode revogar o consentimento a qualquer momento, da mesma forma e com a mesma facilidade com que o concedeu.

2.8.2. Consentimento na Administração Pública:

Embora o consentimento seja uma base legal prevista na LGPD, a sua aplicação na Administração Pública é restrita e deve ser utilizada com cautela. Isso ocorre porque, em muitos casos, a Administração Pública trata dados pessoais com base em outras bases legais, como o cumprimento de obrigação legal ou regulatória e a execução de políticas públicas.

O consentimento só deve ser utilizado pela Administração Pública quando as outras bases legais não se aplicarem e quando for realmente necessário para a execução de suas atividades. É importante ressaltar que o poder hierárquico da Administração Pública pode influenciar a liberdade do titular em consentir, tornando o consentimento questionável em certas situações.

2.8.3. Exemplos de situações em que o consentimento pode ser utilizado na Administração Pública:

- Pesquisas Científicas: Coleta de dados para fins de pesquisa, com a autorização expressa dos participantes.
- Programas Sociais com Benefícios Adicionais: Oferecimento de benefícios que não são obrigatórios por

lei, condicionados ao consentimento do titular para o tratamento de seus dados.

- Serviços Personalizados: Oferta de serviços que exigem o tratamento de dados além do estritamente necessário para o cumprimento da obrigação legal, como envio de comunicados informativos.

2.8.4. Recomendações para o uso do consentimento na Administração Pública:

- Utilizar o consentimento apenas quando estritamente necessário: Priorizar outras bases legais, como o cumprimento de obrigação legal.
- Fornecer informações claras e completas ao titular: Explicar de forma transparente a finalidade do tratamento, os dados que serão coletados e os direitos do titular.
- Documentar o consentimento: Manter registros que comprovem a obtenção do consentimento do titular.
- Facilitar a revogação do consentimento: Oferecer mecanismos simples e acessíveis para que o titular possa revogar o consentimento a qualquer momento.

2.9. ANPD (Autoridade Nacional de Proteção de Dados)

ANPD é a sigla para Autoridade Nacional de Proteção de Dados, órgão da administração pública federal, integrante da Presidência da República, responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei n° 13.709/2018).

2.9.1. Funções da ANPD:

A ANPD exerce diversas funções, entre as quais destacam-se:

- Fiscalizar e aplicar sanções: A ANPD tem o poder de fiscalizar o cumprimento da LGPD por parte de órgãos públicos e entidades privadas, podendo aplicar sanções em caso de descumprimento da lei. Essas sanções podem variar de advertências a multas.
- Elaborar regulamentos e diretrizes: A ANPD é responsável por criar normas complementares à LGPD, detalhando procedimentos e requisitos para o tratamento de dados pessoais.
- Promover a conscientização sobre a proteção de dados: A ANPD desenvolve campanhas educativas e materiais informativos para orientar a sociedade sobre a importância da proteção de dados pessoais.
- Emitir pareceres e recomendações: A ANPD pode emitir pareceres sobre questões relacionadas à proteção de dados, orientando órgãos públicos e entidades privadas sobre a melhor forma de cumprir a LGPD.
- Fomentar a adoção de boas práticas: A ANPD incentiva a implementação de medidas de segurança da informação e a adoção de boas práticas para o tratamento de dados pessoais.
- Julgar recursos contra decisões de controladores: A ANPD atua como instância recursal para decisões tomadas por controladores de dados.
- Cooperar com autoridades de proteção de dados de outros países: A ANPD mantém relações com autoridades

internacionais para promover a cooperação na área de proteção de dados.

- Requerer informações e documentos: A ANPD pode solicitar informações e documentos a controladores e operadores para verificar o cumprimento da LGPD.

2.9.2. Importância da ANPD para a Administração Pública:

A ANPD desempenha um papel fundamental na regulação e fiscalização do tratamento de dados pessoais na Administração Pública. Sua atuação contribui para:

- Garantir a conformidade com a LGPD: A ANPD auxilia os órgãos públicos a interpretarem e aplicarem corretamente a LGPD, evitando sanções e promovendo a proteção dos dados dos cidadãos.
- Aumentar a segurança dos dados pessoais: A fiscalização da ANPD incentiva a adoção de medidas de segurança da informação, reduzindo o risco de vazamentos de dados e outros incidentes.
- Promover a transparência e a prestação de contas: A ANPD exige que os órgãos públicos sejam transparentes sobre o tratamento de dados pessoais, prestando contas à sociedade sobre suas práticas.
- Fortalecer a confiança dos cidadãos: A atuação da ANPD contribui para aumentar a confiança dos cidadãos na Administração Pública, demonstrando o compromisso com a proteção de seus dados pessoais.

2.9.3. Relação entre a Administração Pública e a ANPD:

Os órgãos e entidades da Administração Pública estão sujeitos à fiscalização e às sanções da ANPD, devendo cumprir as suas determinações e regulamentos. A ANPD atua como um órgão regulador independente, garantindo a aplicação da LGPD em todos os setores, inclusive no âmbito público.

Em resumo, a ANPD é uma peça-chave na implementação e fiscalização da LGPD no Brasil, assegurando a proteção de dados pessoais e a privacidade dos cidadãos, inclusive em relação à Administração Pública. Sua atuação é fundamental para a construção de uma cultura de proteção de dados no país.

3. PAPEIS E RESPONSABILIDADES

3.1. Do Controlador

O Controlador na Administração Pública Municipal tem a responsabilidade de estabelecer e implementar uma cultura de proteção de dados, garantindo que os dados pessoais dos cidadãos sejam tratados de forma segura, ética e em conformidade com a LGPD. A implementação correta dessas responsabilidades é crucial para evitar sanções e manter a confiança da população na gestão municipal.

Na Administração Pública Municipal, o Controlador, geralmente representado pela própria prefeitura. Suas atribuições envolvem a tomada de decisões sobre o tratamento de dados e a implementação de medidas para garantir sua segurança e conformidade com a lei. A seguir, detalhamos os principais papéis e responsabilidades do Controlador no contexto municipal:

3.1.1. Definição da Finalidade e dos Meios do Tratamento:

O Controlador determina por que e como os dados pessoais serão tratados. Isso inclui especificar a finalidade da coleta de dados (ex: cadastro de contribuintes, gestão de programas sociais, etc.) e os métodos utilizados para o tratamento (ex: armazenamento em bancos de dados, compartilhamento com outros órgãos etc.). Essa definição deve ser clara, específica e documentada.

3.1.2. Implementação de Medidas de Segurança:

O Controlador é responsável por implementar as medidas de segurança técnicas e administrativas necessárias para proteger os dados pessoais contra acessos não autorizados, vazamentos, uso indevido e outras ameaças. Isso inclui a adoção de práticas como criptografia, controle de acesso, firewalls, backups e treinamentos para os servidores.

3.1.3. Nomeação do Encarregado (DPO):

O Controlador deve designar um *Data Protection Officer* (*DPO*) para atuar como canal de comunicação entre a prefeitura, os titulares dos dados e a ANPD. A escolha do DPO deve considerar sua expertise em proteção de dados e LGPD. A nomeação e os dados de contato do DPO devem ser comunicados à ANPD.

3.1.4. Elaboração de Políticas e Procedimentos:

O Controlador é responsável por criar e implementar políticas internas de proteção de dados, incluindo a Política de Privacidade, que deve ser pública e acessível aos cidadãos. Também deve estabelecer procedimentos para o atendimento dos direitos dos titulares, como acesso, correção, portabilidade e eliminação de dados.

3.1.5. Gestão de Riscos e Incidentes de Segurança:

O Controlador deve realizar avaliações de riscos para identificar as vulnerabilidades e ameaças aos dados pessoais. Em caso de incidentes de segurança, como vazamentos de dados, o Controlador é responsável por tomar as medidas cabíveis, incluindo a notificação à ANPD e aos titulares afetados, conforme previsto na LGPD.

3.1.6. Garantia da Conformidade com a LGPD:

O Controlador deve assegurar que todas as atividades de tratamento de dados pessoais realizadas pela prefeitura estejam em conformidade com a LGPD. Isso inclui a observância dos princípios da lei, como finalidade, necessidade, livre acesso, transparência e segurança.

3.1.7. Responsabilização e Prestação de Contas:

O Controlador é responsável perante a ANPD e os titulares dos dados pelo tratamento de dados realizado pela prefeitura. Deve ser capaz de demonstrar a conformidade com a LGPD e prestar contas sobre suas ações.

3.1.8. Gestão de Contratos com Terceiros:

Ao contratar empresas que tratam dados pessoais em nome da prefeitura (operadores), o Controlador deve garantir que os contratos incluam cláusulas específicas sobre a proteção de dados, assegurando a conformidade com a LGPD por parte do operador.

3.2. Dos Operadores

O Operador atua como um parceiro do Controlador na proteção de dados pessoais. Suas responsabilidades focam na execução segura e conforme das instruções do Controlador, garantindo a confidencialidade, integridade e disponibilidade dos dados. A compreensão e o cumprimento dessas responsabilidades são essenciais para evitar sanções e garantir um ambiente seguro para o tratamento de dados pessoais no município.

Na Administração Pública Municipal, um Operador é uma pessoa física ou jurídica, pública ou privada, que realiza o tratamento de dados pessoais em nome do Controlador (a prefeitura). Isso significa que o Operador não define a finalidade nem os meios do tratamento, mas executa as instruções do Controlador. Empresas contratadas para serviços de TI, desenvolvimento de sistemas, armazenamento de dados, entre outros, podem atuar como Operadores. A LGPD estabelece responsabilidades específicas para os Operadores, visando garantir a segurança e a conformidade no tratamento de dados.

3.2.1. Seguir as Instruções do Controlador:

O Operador deve tratar os dados pessoais estritamente de acordo com as instruções do Controlador. Qualquer atividade fora do escopo definido pelo Controlador deve ser previamente autorizada.

3.2.2. Implementar Medidas de Segurança:

O Operador é responsável por implementar as medidas de segurança técnicas e administrativas necessárias para proteger os dados pessoais sob sua responsabilidade. Essas medidas devem ser adequadas aos riscos envolvidos no tratamento e atender aos padrões estabelecidos pela LGPD e pela ANPD.

3.2.3. Auxiliar o Controlador:

O Operador deve auxiliar o Controlador no cumprimento de suas obrigações, como o atendimento dos direitos dos titulares e a resposta a incidentes de segurança. Isso pode incluir fornecer informações, implementar mecanismos de acesso aos dados e colaborar na elaboração de Relatórios de Impacto à Proteção de Dados (RIPD).

3.2.4. Confidencialidade dos Dados:

O Operador deve garantir a confidencialidade dos dados pessoais, restringindo o acesso apenas aos funcionários autorizados e implementando medidas para evitar vazamentos e acessos indevidos.

3.2.5. Subcontratação:

Caso o Operador precise subcontratar outras empresas para auxiliar no tratamento de dados, deve obter autorização prévia do Controlador e garantir que o subcontratado também cumpra as obrigações da LGPD.

3.2.6. Notificação de Incidentes de Segurança:

Em caso de incidentes de segurança que possam comprometer os dados pessoais, o Operador deve notificar o Controlador imediatamente, fornecendo informações detalhadas sobre o ocorrido e as medidas adotadas para conter os danos.

3.2.7. Eliminação ou Devolução dos Dados:

Ao término do contrato de prestação de serviços, o Operador deve, conforme instrução do Controlador, eliminar ou devolver todos os dados pessoais tratados, garantindo que não retenha cópias, exceto se houver obrigação legal de armazenamento.

3.2.8. Demonstrar a Conformidade:

O Operador deve ser capaz de demonstrar ao Controlador e à ANPD que está cumprindo suas obrigações em relação à LGPD. Isso pode incluir a apresentação de documentos, relatórios e auditorias.

3.3. Do Encarregado (DPO - Data Protection Officer)

O *Data Protection Officer* (*DPO*), ou Encarregado pelo Tratamento de Dados Pessoais, desempenha um papel crucial na conformidade com a LGPD na Administração Pública, a prevenção de incidentes de segurança e a promoção de uma cultura de privacidade no serviço público. Suas responsabilidades abrangem a orientação, o monitoramento e a comunicação em relação à proteção de dados. A seguir, detalhamos os principais papéis e responsabilidades do DPO no contexto da Administração Pública:

3.3.1. Orientação e Supervisão:

O *DPO* orienta e supervisiona a implementação da LGPD no órgão público. Isso inclui a elaboração de políticas e procedimentos, a realização de treinamentos para os servidores e a avaliação da conformidade das atividades de tratamento de dados com a lei.

3.3.2. Canal de Comunicação:

O *DPO* atua como canal de comunicação entre o órgão público, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Responde a consultas e solicitações dos titulares sobre seus direitos e esclarece dúvidas dos servidores sobre a aplicação da LGPD.

3.3.3. Gestão de Riscos e Incidentes:

O *DPO* participa da avaliação de riscos relacionados ao tratamento de dados pessoais e auxilia na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD). Em caso de incidentes de segurança, como vazamentos de dados, o *DPO* coordena as ações de resposta e notifica a ANPD e os titulares afetados, conforme previsto na lei.

3.3.4. Monitoramento e Auditoria:

O *DPO* monitora a conformidade do órgão público com a LGPD e realiza auditorias internas para verificar a eficácia das medidas de proteção de dados. Recomenda melhorias nos processos e sistemas para garantir a segurança e a privacidade das informações.

3.3.5. Treinamento e Conscientização:

O *DPO* promove a conscientização sobre a importância da proteção de dados pessoais e realiza treinamentos para os

Rua.Isola Belli Leonardi, 08 – Vila Nova | Itapevi | São Paulo | CEP: 06694-110
Tel.: (11) 4143-7500 | controladoriageral@itapevi.sp.gov.br

servidores públicos sobre a LGPD e as melhores práticas para o tratamento de dados.

3.3.6. Consultoria e Assessoria:

O *DPO* atua como consultor interno para as áreas do órgão público que tratam dados pessoais, fornecendo orientações sobre a aplicação da LGPD em situações específicas.

3.3.7. Interação com a ANPD:

O *DPO* mantém contato com a ANPD, respondendo a questionamentos e comunicando informações relevantes sobre o tratamento de dados pessoais no órgão público.

3.3.8. Manutenção de Registros:

O *DPO* mantém registros das atividades de tratamento de dados pessoais, incluindo as bases legais utilizadas, as medidas de segurança implementadas e os incidentes de segurança registrados.

3.3.9. Qualificações e Características Importantes do DPO:

- Conhecimento da LGPD e de proteção de dados: Domínio da legislação e das melhores práticas em privacidade e segurança da informação.

Rua.Isola Belli Leonardi, 08 – Vila Nova | Itapevi | São Paulo | CEP: 06694-110
Tel.: (11) 4143-7500 | controladoriageral@itapevi.sp.gov.br

- Experiência profissional relevante: Experiência em áreas como direito, segurança da informação, compliance ou gestão de riscos.
- Imparcialidade e Independência: Capacidade de atuar de forma independente e imparcial, sem sofrer interferências indevidas.
- Boas habilidades de comunicação: Capacidade de se comunicar de forma clara e eficaz com diferentes públicos (titulares, servidores, ANPD).
- Proatividade e capacidade de organização: Habilidade para antecipar problemas, planejar ações e gerenciar múltiplas tarefas.

4. MAPEAMENTO DE DADOS PESSOAIS

É o processo de identificação, classificação e documentação de todos os dados pessoais tratados pelo município. Ele envolve um levantamento detalhado das informações pessoais coletadas, armazenadas, utilizadas e compartilhadas pela prefeitura, incluindo a finalidade do tratamento, a base legal, os fluxos de dados e as medidas de segurança aplicadas.

O mapeamento consiste em um inventário detalhado de todos os dados pessoais tratados pela Administração Pública Municipal. Deve-se identificar:

- Quais dados pessoais são coletados? (Nome, CPF, endereço, telefone, dados de saúde, etc.)
- Onde esses dados são armazenados? (Sistemas, arquivos físicos, etc.)

- Como esses dados são coletados? (Formulários, sistemas online, etc.)
- Para que finalidade esses dados são utilizados?
- Com quem esses dados são compartilhados?
- Qual a base legal para o tratamento desses dados? (Consentimento, cumprimento de obrigação legal, etc.)

O mapeamento de dados é uma etapa essencial para a adequação da Administração Pública Municipal à LGPD. Ele permite identificar, classificar e documentar os dados pessoais tratados, garantindo maior segurança, transparência e conformidade com a lei.

4.1. **Como deve ser feito o Mapeamento de Dados**

O mapeamento de dados deve ser realizado de forma sistemática e abrangente, envolvendo as seguintes etapas:

- Definição do escopo: Determinar quais áreas, departamentos e sistemas da prefeitura serão incluídos no mapeamento.
- Identificação dos Dados Pessoais: Listar todos os tipos de dados pessoais tratados pelo município, como nome, CPF, endereço, dados de saúde, etc.
- Classificação dos Dados: Categorizar os dados pessoais de acordo com sua natureza (dados simples, sensíveis) e nível de criticidade.
- Definição da finalidade do tratamento: Descrever para qual propósito cada dado pessoal é coletado e utilizado.

- Identificação da Base Legal: Indicar a base legal que autoriza o tratamento de cada dado pessoal (cumprimento de obrigação legal, execução de políticas públicas, consentimento, etc.).
- Mapeamento dos Fluxos de Dados: Documentar o caminho percorrido pelos dados pessoais, desde a coleta até o descarte, incluindo os sistemas, departamentos e entidades envolvidas.
- Identificação dos riscos e medidas de segurança: Avaliar os riscos associados ao tratamento de dados pessoais e as medidas de segurança implementadas para mitigá-los.
- Documentação: Registrar todas as informações coletadas em um relatório ou sistema específico, mantendo-o atualizado.

4.1.1. Melhores práticas para a classificação de Dados Sensíveis:

A classificação de dados sensíveis na Administração Pública é crucial para a conformidade com a LGPD e para a proteção da privacidade dos cidadãos. Dados sensíveis, por sua natureza, exigem maior cuidado e medidas de segurança mais robustas. Aqui estão algumas melhores práticas para a classificação desses dados:

- Conhecimento profundo da LGPD: A base para a classificação correta é o entendimento preciso da definição de dados sensíveis conforme o Art. 5°, II da LGPD: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Treinamentos e consultas com especialistas em proteção de dados são essenciais.

- Inventário detalhado: Antes da classificação, é fundamental realizar um inventário completo de todos os dados pessoais tratados pela Administração Pública. Esse inventário deve especificar onde os dados estão armazenados, como são utilizados, com quem são compartilhados e qual a finalidade do tratamento.
- Criação de categorias específicas: Além das categorias definidas na LGPD, a Administração Pública pode criar categorias adicionais para classificar os dados sensíveis de acordo com seu nível de criticidade e com as especificidades de cada órgão. Por exemplo, dados de saúde podem ser subdivididos em prontuários médicos, resultados de exames, etc.
- Critérios claros e objetivos: A classificação deve ser baseada em critérios claros e objetivos, documentados e acessíveis a todos os envolvidos no tratamento de dados. Esses critérios devem considerar a sensibilidade dos dados, o impacto potencial de um vazamento e as obrigações legais aplicáveis.
- Revisão periódica: A classificação dos dados sensíveis não é estática. É importante realizar revisões periódicas para garantir que a classificação continue adequada, considerando mudanças na legislação, nos processos e nos sistemas.
- Minimização da coleta: A Administração Pública deve coletar apenas os dados sensíveis estritamente necessários para o cumprimento de suas finalidades. A

coleta excessiva de dados aumenta os riscos e a complexidade da gestão da informação.

- Medidas de segurança reforçadas: Dados sensíveis exigem medidas de segurança mais rigorosas, como criptografia, controle de acesso, autenticação multifator e monitoramento constante. A implementação dessas medidas deve ser proporcional à sensibilidade dos dados.
- Transparência com o titular dos dados: A Administração Pública deve ser transparente com os cidadãos sobre a coleta e o tratamento de dados sensíveis, informando a finalidade, as bases legais e os direitos dos titulares.
- Consulta ao Encarregado pelo Tratamento de Dados Pessoais (*DPO*): O *DPO*, preferivelmente, deve ser consultado na definição dos critérios de classificação e nas medidas de segurança a serem implementadas.
- Documentação completa: Todo o processo de classificação de dados sensíveis deve ser documentado, incluindo os critérios utilizados, as categorias criadas e as medidas de segurança implementadas. Essa documentação é fundamental para demonstrar a conformidade com a LGPD.

Implementando essas melhores práticas, a Administração Pública pode garantir a proteção dos dados sensíveis, minimizar os riscos de vazamentos e incidentes de segurança, e fortalecer a confiança dos cidadãos na gestão da informação.

4.1.2. Ferramentas que podem facilitar a classificação de Dados Sensíveis:

A escolha das ferramentas mais adequadas depende das necessidades e dos recursos de cada órgão da Administração Pública. É importante avaliar as funcionalidades, os custos e a complexidade de implementação de cada ferramenta antes de tomar uma decisão.

Diversas ferramentas podem auxiliar na classificação de dados sensíveis, facilitando o processo de adequação à LGPD na Administração Pública. Essas ferramentas podem ser agrupadas em algumas categorias:

Softwares de Governança de Dados:

Essas ferramentas oferecem funcionalidades para catalogar, classificar, gerenciar e proteger dados sensíveis. Algumas funcionalidades comuns incluem:

- Descoberta de dados: Identificam automaticamente dados sensíveis em diferentes fontes de dados, como bancos de dados, sistemas de arquivos e e-mails.
- Classificação automatizada: Utilizam algoritmos e regras predefinidas para classificar os dados de acordo com sua sensibilidade.
- Mapeamento de fluxos de dados: Rastreiam o caminho percorrido pelos dados sensíveis dentro da organização.
- Gestão de políticas de acesso: Controlam o acesso aos dados sensíveis, garantindo que apenas usuários autorizados possam visualizá-los e modificá-los.
- Relatórios e dashboards: Fornecem relatórios e dashboards com informações sobre a classificação dos dados, os

riscos identificados e as medidas de segurança implementadas.

Exemplos de softwares de governança de dados: Collibra, Alation, Informatica, IBM Information Governance Catalog etc.

Ferramentas de Data Loss Prevention (*DLP*):

As ferramentas de DLP ajudam a prevenir a perda ou o vazamento de dados sensíveis, monitorando e controlando o fluxo de informações. Elas podem:

- Identificar dados sensíveis em trânsito: Analisam o tráfego de rede, e-mails e outras comunicações para identificar dados sensíveis que estão sendo transmitidos.
- Bloquear o envio de dados sensíveis: Impedem que dados sensíveis sejam enviados para fora da organização sem autorização.
- Alertar sobre possíveis vazamentos: Notificam os responsáveis pela segurança da informação sobre possíveis tentativas de vazamento de dados.

Exemplos de ferramentas DLP: Symantec Data Loss Prevention, McAfee DLP, Forcepoint DLP etc.

Ferramentas de Gestão de Risco:

Essas ferramentas ajudam a identificar, avaliar e gerenciar os riscos associados ao tratamento de dados sensíveis. Elas podem:

- Realizar análises de risco: Avaliam a probabilidade e o impacto de diferentes cenários de risco, como vazamentos de dados, ataques cibernéticos e falhas de segurança.
- Priorizar os riscos: Classificam os riscos de acordo com sua gravidade, permitindo que a organização direcione seus esforços para as áreas mais críticas.
- Monitorar os controles de segurança: Verificam se os controles de segurança implementados estão funcionando corretamente.

Planilhas e Documentos:

Em cenários com recursos limitados, planilhas e documentos podem ser utilizados para registrar e classificar os dados sensíveis. No entanto, essa abordagem pode ser menos eficiente e mais propensa a erros do que o uso de ferramentas especializadas. É importante garantir a segurança desses documentos, com controle de acesso e backups regulares.

Consultoria especializada:

Empresas de consultoria especializadas em proteção de dados podem auxiliar na classificação de dados sensíveis, fornecendo expertise e metodologias específicas. Elas podem ajudar na implementação de ferramentas, na definição de políticas e na capacitação da equipe.

4.2. Quem deve fazer o Mapeamento de dados

Todos os entes que compõem a Administração Pública Municipal, sem exceção, devem efetuar o mapeamento de dados conforme a LGPD. Isso inclui:

- Prefeitura Municipal: Órgão central da administração, responsável pela gestão municipal.
- Secretarias Municipais: Responsáveis por áreas específicas da administração, como saúde, educação, finanças, etc.
- Órgãos da Administração Indireta: Autarquias, fundações, empresas públicas e sociedades de economia mista controladas pelo município.
- Câmaras Municipais: Responsáveis pelo poder legislativo municipal.
- Conselhos Municipais: Órgãos colegiados com participação da sociedade civil, que atuam em áreas específicas como saúde, educação, assistência social, etc.

4.2.1. Abrangência:

A LGPD se aplica a qualquer operação de tratamento de dados pessoais realizada por pessoa natural ou jurídica de direito público ou privado. Portanto, todos os entes da municipalidade, independentemente de sua natureza jurídica ou área de atuação, que realizam tratamento de dados pessoais, estão obrigados a cumprir a lei, incluindo a realização do mapeamento de dados.

4.2.2. Importância do mapeamento em todos os entes:

O mapeamento de dados é fundamental para que a Administração Pública Municipal, como um todo, esteja em conformidade com a LGPD. A falta de mapeamento em qualquer um dos entes pode gerar riscos para a segurança dos dados pessoais e expor o município a sanções.

4.2.3. Considerações adicionais:

Entes terceirizados: Mesmo que a prefeitura contrate empresas terceirizadas para realizar o tratamento de dados pessoais, a responsabilidade pela conformidade com a LGPD continua sendo do município. Portanto, é importante que a prefeitura exija que as empresas contratadas também realizem o mapeamento de dados e adotem as medidas de segurança necessárias.

Dados compartilhados: O mapeamento deve considerar os dados pessoais compartilhados entre diferentes entes da municipalidade, garantindo a transparência e a segurança nesses fluxos de informações.

Atualização constante: O mapeamento de dados não é uma atividade pontual, mas um processo contínuo. É importante que os entes da municipalidade mantenham o mapeamento atualizado, refletindo as mudanças nos processos de tratamento de dados.

4.3. Principais desafios enfrentados na implementação do Mapeamento de Dados

Os entes da Administração Pública enfrentam diversos desafios na implementação do mapeamento de dados conforme a LGPD. Alguns dos principais desafios são:

- Complexidade e volume de dados: A Administração Pública lida com uma grande quantidade de dados pessoais, muitas vezes dispersos em diferentes sistemas e departamentos. Essa complexidade e volume dificultam a identificação, classificação e documentação de todos os dados.
- Resistência à mudança: A implementação da LGPD e do mapeamento de dados exige mudanças nos processos e na cultura organizacional. Alguns servidores podem resistir a essas mudanças, dificultando a implementação do projeto.
- Integração de sistemas legados: Muitos órgãos públicos utilizam sistemas antigos (legados) que não foram projetados para atender aos requisitos da LGPD. A integração desses sistemas com novas tecnologias e a migração de dados podem ser complexas.
- Falta de conhecimento sobre a LGPD: A compreensão da LGPD e de seus requisitos técnicos pode ser um desafio para os servidores públicos. A falta de conhecimento dificulta a correta classificação dos dados, a identificação das bases legais e a implementação das medidas de segurança necessárias.
- Definição de papéis e responsabilidades: É fundamental definir claramente os papéis e responsabilidades de cada setor e servidor envolvido no mapeamento de dados. A

falta de clareza pode gerar conflitos e atrasos no projeto.

- Cultura de compartilhamento de dados: Em alguns casos, a cultura organizacional pode dificultar o compartilhamento de informações entre diferentes departamentos e órgãos. Essa falta de colaboração pode prejudicar o mapeamento dos fluxos de dados.
- Dificuldade em manter o mapeamento atualizado: O mapeamento de dados não é uma atividade pontual, mas um processo contínuo. Manter o mapeamento atualizado, refletindo as mudanças nos processos e sistemas, pode ser um desafio.
- Classificação de dados sensíveis: A correta classificação dos dados sensíveis, como dados de saúde, biométricos, etc. exige cuidado redobrado e conhecimento específico, representando um desafio adicional.
- Entendimento das bases legais: A escolha da base legal adequada para cada tratamento de dados pode ser complexa, exigindo análise jurídica e conhecimento profundo da LGPD.

Superar esses desafios exige planejamento, investimento em recursos, capacitação e o comprometimento de todos os envolvidos. A implementação de um projeto de mapeamento de dados bem-sucedido é fundamental para a adequação à LGPD e para a proteção dos dados pessoais dos cidadãos. Importante ressaltar, que qualquer dificuldade encontrada no decorrer do processo de mapeamento de dados, o controlador e o *DPO* devem ser acionados para que eles possam dar todo apoio e suporte necessário.

4.4. Medidas para manter a Segurança e Privacidade dos Dados no processo de Mapeamento

Princípio da Minimização: Coletar apenas os dados estritamente necessários para o mapeamento, evitando informações excessivas ou irrelevantes para a finalidade.

Controle de Acesso: Restringir o acesso aos dados coletados apenas às pessoas autorizadas e envolvidas diretamente no processo de mapeamento. Implementar mecanismos de autenticação forte, como senhas robustas e autenticação multifator.

Armazenamento Seguro: Armazenar os dados coletados em ambientes seguros, com medidas de proteção física e lógica, como criptografia, firewalls e sistemas de detecção de intrusão. Utilizar servidores e dispositivos com acesso controlado e monitorado.

Classificação da Informação: Classificar os dados mapeados de acordo com seu nível de sensibilidade (público, interno, confidencial, restrito), aplicando medidas de segurança proporcionais à classificação.

Treinamento da Equipe: Treinar os envolvidos no mapeamento sobre a importância da segurança e privacidade dos dados, as regras da LGPD e as políticas internas de segurança da informação.

Contratos com Terceiros: Se houver contratação de empresas terceirizadas para auxiliar no mapeamento, garantir que os contratos incluam cláusulas específicas sobre a proteção de dados pessoais, a confidencialidade das informações e a conformidade com a LGPD.

Registro das Atividades: Manter registros detalhados de todas as atividades realizadas durante o mapeamento, incluindo acessos aos dados, modificações e transferências. Esses registros são importantes para auditorias e investigações em caso de incidentes.

Plano de Resposta a Incidentes: Elaborar um plano de resposta a incidentes de segurança da informação, que defina os procedimentos a serem adotados em caso de vazamento de dados ou outros incidentes relacionados ao mapeamento.

Avaliação e Revisão Periódica: Realizar avaliações periódicas das medidas de segurança implementadas, revisando os processos e as políticas para garantir a sua eficácia e a conformidade com a LGPD.

Encarregado (*DPO*): Envolver o Encarregado (preferivelmente) em todas as etapas do mapeamento, desde o planejamento até a execução, garantindo a supervisão e a orientação em relação à proteção de dados.

4.5. Vantagens e Benefícios do Mapeamento Dados

Conformidade com a LGPD: O mapeamento é fundamental para demonstrar a conformidade com a lei, evitando sanções e multas.

Maior segurança dos dados pessoais: A identificação dos fluxos de dados e das medidas de segurança permite identificar vulnerabilidades e implementar melhorias na proteção das informações.

Transparência e prestação de contas: O mapeamento facilita a transparência sobre o tratamento de dados pessoais, permitindo que os cidadãos tenham acesso às informações sobre como seus dados estão sendo utilizados.

Visão clara do fluxo de dados: O mapeamento permite entender como os dados pessoais são tratados em cada ambiente da Administração Pública Municipal.

Otimização dos processos: O mapeamento pode revelar ineficiências nos processos de tratamento de dados, permitindo a otimização e a redução de custos.

Identificação de riscos: O mapeamento facilita a identificação de vulnerabilidades e possíveis descumprimentos da LGPD.

Melhoria na tomada de decisão: O conhecimento sobre os dados pessoais tratados pela Municipalidade permite uma tomada de decisão mais embasada e eficiente.

Facilidade na resposta a incidentes de segurança: Em caso de vazamento de dados ou outros incidentes, o mapeamento facilita a identificação dos dados afetados e a adoção de medidas corretivas.

Base para a implementação de outras medidas de proteção de dados: O mapeamento serve como base para a elaboração de políticas de privacidade, a implementação de controles de acesso e outras medidas de segurança.

5. TRATAMENTO DE DADOS PESSOAIS

O artigo 5°, inciso X, da LGPD define tratamento de dados pessoais como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Em termos práticos, qualquer ação realizada com dados pessoais, desde a sua coleta até a sua eliminação, configura tratamento de dados.

O tratamento de dados pessoais deve ser realizado de forma lícita, leal e transparente, para finalidades determinadas, explícitas e legítimas, com base em uma das hipóteses legais previstas na LGPD (art. 7°), como:

- Consentimento do titular;
- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Execução de políticas públicas previstas em leis e regulamentos;
- Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;

- Proteção da vida ou da incolumidade física do titular ou de terceiros;
- Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- Proteção do crédito, inclusive para fins de proteção a crédito consignado.

5.1. Como deve ser feito o tratamento de dados

O tratamento de dados pessoais pela Administração Pública Municipal deve observar os princípios da LGPD (Art. 5°), como:

- Finalidade: Deve haver uma finalidade legítima, específica, explícita e informada ao titular para o tratamento dos dados (inciso II).
- Adequação: Os dados coletados devem ser compatíveis com a finalidade informada ao titular, não podendo ser utilizados para outras finalidades sem o seu consentimento (inciso II).
- Necessidade: Os dados coletados devem ser limitados ao mínimo necessário para atingir a finalidade do tratamento (inciso III).

- Livre acesso: Deve ser garantido ao titular o acesso facilitado às informações sobre o tratamento de seus dados (inciso V).
- Qualidade dos dados: Os dados devem ser exatos, atualizados e relevantes em relação à finalidade para a qual foram coletados (inciso VI).
- Transparência: Deve haver transparência sobre o tratamento dos dados, informando ao titular sobre a finalidade, os dados coletados, os procedimentos utilizados e os responsáveis pelo tratamento (inciso VI).
- Segurança: Devem ser implementadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (inciso VII).
- Prevenção: Devem ser adotadas medidas para prevenir a ocorrência de danos em decorrência do tratamento de dados pessoais (inciso VIII).
- Não discriminação: O tratamento de dados não pode ser utilizado para fins discriminatórios, ilícitos ou abusivos (inciso IX).
- Responsabilização e prestação de contas: Os agentes de tratamento devem demonstrar que estão adotando medidas eficazes para a proteção de dados pessoais (inciso XI).

5.2. **Precauções a serem adotadas**

Além da observância dos princípios, algumas precauções específicas devem ser adotadas:

- Medidas de segurança: Implementar medidas de segurança da informação, como criptografia, controle de acesso, firewalls e backups regulares.
- Consentimento: Obter o consentimento do titular para o tratamento de dados sensíveis, exceto nas hipóteses previstas em lei (Art. 11).
- Minimização da coleta: Coletar apenas os dados estritamente necessários para a finalidade do tratamento.
- Transparência: Informar ao titular sobre a finalidade do tratamento, os dados coletados e seus direitos.
- Treinamento: Capacitar os servidores públicos sobre a LGPD e as melhores práticas para o tratamento de dados pessoais.
- Gestão de incidentes: Implementar um plano de resposta a incidentes de segurança da informação.

5.3. **Exclusão ou Descarte de Dados**

A exclusão ou descarte de dados na Administração Pública Municipal, conforme a LGPD, deve seguir rigorosamente as diretrizes da lei para garantir a proteção dos dados pessoais e evitar sanções. A LGPD prevê a eliminação dos dados pessoais em diversas situações, e a forma como essa eliminação ocorre depende do contexto.

A eliminação de dados na Administração Pública Municipal é um processo complexo que exige cuidado e atenção aos detalhes. A implementação de procedimentos adequados e o acompanhamento do Encarregado (*DPO*) são fundamentais para garantir a conformidade com a LGPD e a proteção dos dados pessoais dos cidadãos.

5.3.1. Base Legal para a Eliminação (Art. 17):

O artigo 17 da LGPD define as hipóteses em que os dados pessoais devem ser eliminados:

I. Finalidade atingida: Quando a finalidade para a qual os dados foram coletados for atingida. Exemplo: Dados coletados para um programa social específico, após o término do programa.

II. Término do prazo de conservação legal: Após o término do prazo de conservação previsto em lei ou regulamentação. Exemplo: Dados fiscais, que possuem prazos de guarda definidos pela legislação tributária.

III. Retirada do consentimento: Quando o titular dos dados retirar o seu consentimento para o tratamento, exceto se houver outra base legal que o justifique (Art. 7°, inciso I).

IV. Decisão da Autoridade Nacional: Por determinação da Autoridade Nacional de Proteção de Dados (ANPD).

V. Para cumprir obrigação legal: Quando necessário para o cumprimento de obrigação legal ou regulatória pelo controlador.

5.3.2. Formas de Eliminação (Art. 16):

O artigo 16 descreve as formas de eliminação dos dados:

I. Eliminação: Exclusão definitiva dos dados.

II. Anonimização: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

III. Bloqueio: Suspensão temporária de qualquer operação de tratamento, mediante guarda segura dos dados pessoais.

5.3.3. Procedimentos para a Eliminação:

A Administração Pública Municipal deve estabelecer procedimentos claros e seguros para a eliminação dos dados, considerando:

- Inventário de dados: Manter um inventário atualizado dos dados pessoais tratados, identificando a finalidade, a base legal e o prazo de conservação.
- Política de eliminação: Definir uma política de eliminação de dados, que especifique as responsabilidades, os procedimentos e os métodos de eliminação.
- Segurança da informação: Garantir a segurança dos dados durante o processo de eliminação, evitando acessos não autorizados e vazamentos.
- Documentação: Documentar todo o processo de eliminação, incluindo a data, a forma de eliminação e os responsáveis.
- Meios adequados: Utilizar meios adequados para a eliminação dos dados, considerando o tipo de dado e o meio de armazenamento. A simples exclusão de arquivos pode não ser suficiente em alguns casos, sendo necessária a utilização de técnicas específicas para garantir a eliminação completa.

- Dados em backups: Considerar a eliminação dos dados também em backups e cópias de segurança.
- Terceiros: Se os dados forem tratados por terceiros, garantir que eles também realizem a eliminação dos dados conforme a LGPD.

5.3.4. Exceções à Eliminação (Art. 17, §1°):

Mesmo nas hipóteses do Art. 17, a LGPD prevê exceções para a eliminação dos dados quando necessário para:

I. Cumprimento de obrigação legal ou regulatória pelo controlador: Por exemplo, guarda de documentos fiscais por prazo determinado por lei.
II. Estudo por órgão de pesquisa: Desde que garantida a anonimização dos dados sempre que possível.
III. Transferência a terceiro: Desde que respeitados os requisitos da LGPD.
IV. Uso exclusivo do controlador: Desde que garantido o sigilo e respeitados os direitos do titular.
V. Exercício regular de direitos em processo judicial, administrativo ou arbitral.

5.4. Anonimização

A anonimização, conforme o Art. 5°, inciso IX, da LGPD, é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Em essência, torna-se extremamente difícil identificar o titular dos dados, mesmo com o uso de informações adicionais ou cruzamento de bases de dados, entretanto, apesar do cenário de quase impossibilidade, é um processo que pode ser reversível.

5.4.1. Como a anonimização deve ser feita:

A anonimização envolve técnicas que removem ou modificam informações identificadoras, como:

- Supressão: Remoção completa de atributos identificadores, como nome, CPF, endereço, etc.
- Generalização: Substituição de valores específicos por categorias mais amplas. Exemplo: Substituir a idade exata por uma faixa etária (20-25 anos).
- Perturbação: Adição de ruído aos dados, alterando ligeiramente os valores sem comprometer a utilidade das informações. Exemplo: Arredondar valores numéricos.
- Pseudonimização seguida de anonimização: Inicialmente, os dados são pseudonimizados, substituindo identificadores diretos por pseudônimos. Em seguida, aplicam-se técnicas de anonimização aos dados pseudonimizados.

A escolha da técnica mais adequada depende do contexto e do tipo de dado. É importante garantir que a técnica escolhida torne a reidentificação praticamente impossível. A consulta a especialistas e a realização de testes são recomendadas para assegurar a eficácia da anonimização.

5.4.2. Quando a anonimização deve ser feita:

A anonimização deve ser considerada sempre que possível, especialmente quando os dados pessoais não são mais necessários para a finalidade original do tratamento. Algumas situações em que a anonimização é particularmente relevante:

- Pesquisas estatísticas: Permite a realização de estudos e análises sem comprometer a privacidade dos indivíduos.
- Desenvolvimento de novas tecnologias: Utilização de dados anonimizados para treinar algoritmos de inteligência artificial, por exemplo.
- Compartilhamento de dados com terceiros: Minimiza os riscos de privacidade ao compartilhar dados com outras organizações.
- Cumprimento de obrigação legal de eliminação (Art. 17): Quando a finalidade do tratamento for atingida ou o consentimento for retirado, a anonimização pode ser uma alternativa à eliminação completa dos dados, permitindo que sejam utilizados para outras finalidades.

5.4.3. Limitações da Anonimização:

Embora a anonimização seja uma técnica eficaz, ela não é infalível. Algumas limitações incluem:

- Reversibilidade: Em alguns casos, dados anonimizados podem ser revertidos por meio de técnicas avançadas de análise de dados ou combinação com outras informações.
- Dados Relacionados: A combinação de dados anonimizados com outras fontes de dados podem possibilitar a reidentificação.

- Condições de Contexto: Dependendo do contexto, a anonimização pode não ser suficiente para proteger a identidade de indivíduos, especialmente em pequenas amostras.

5.4.4. Benefícios e vantagens da anonimização:

Proteção da privacidade: Elimina o risco de identificação dos titulares dos dados, garantindo sua privacidade.

Conformidade com a LGPD: A anonimização é uma forma de cumprir as obrigações da LGPD em relação à eliminação de dados e à minimização da coleta.

Redução de riscos de segurança: Dados anonimizados não estão sujeitos às mesmas obrigações de segurança que os dados pessoais, reduzindo os riscos de vazamentos e multas.

Possibilidade de uso para outras finalidades: Dados anonimizados podem ser utilizados para pesquisas, desenvolvimento de tecnologias e outras finalidades que não seriam possíveis com dados pessoais.

Fomento à inovação: A disponibilidade de dados anonimizados pode estimular a inovação e o desenvolvimento de novos serviços públicos.

Transparência e confiança: A adoção da anonimização demonstra o compromisso da Administração Pública com a proteção da privacidade dos cidadãos, aumentando a transparência e a confiança.

5.5. Compartilhamento e Divulgação de Dados

O compartilhamento e a divulgação de dados na Administração Pública Municipal são regidos pela LGPD e devem observar requisitos específicos para garantir a proteção da privacidade dos cidadãos. A lei prevê diferentes cenários e bases legais para essas atividades.

O compartilhamento e a divulgação de dados devem ser realizados com cautela e respeito à privacidade dos cidadãos. A observância das regras da LGPD e da Lei de Acesso à Informação é essencial para garantir a transparência e evitar sanções. A consulta ao Encarregado (*DPO*) é fundamental para garantir a segurança jurídica dos procedimentos.

5.5.1. Compartilhamento de Dados:

O compartilhamento de dados ocorre quando a Administração Pública transfere dados pessoais a outro órgão ou entidade, pública ou privada. A LGPD estabelece regras e requisitos para o compartilhamento, visando a proteger os dados pessoais e garantir a transparência.

5.5.2. Bases legais para o compartilhamento (Art. 7°, incisos e alíneas):

I. Consentimento: O titular dos dados consente com o compartilhamento para finalidade específica.

II. Cumprimento de obrigação legal ou regulatória pelo controlador: Por exemplo, compartilhamento de dados com o Ministério Público para fins de investigação.

III. Execução de políticas públicas: Previstas em leis e regulamentos.

IV. Estudos em pesquisa em saúde pública: Desde que observados os requisitos da LGPD e outras normas específicas.

V. Exercício regular de direitos em processo judicial, administrativo ou arbitral.

VI. Proteção da vida ou da incolumidade física do titular ou de terceiros: Em situações de emergência.

VII. Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária: Compartilhamento de informações médicas entre profissionais de saúde.

VIII. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

IX. Proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

5.5.3. Requisitos para o compartilhamento:

Finalidade específica: O compartilhamento deve ter uma finalidade específica, informada ao titular dos dados.

Necessidade: Compartilhar apenas os dados estritamente necessários para a finalidade.

Segurança: Garantir a segurança dos dados compartilhados, implementando medidas de proteção adequadas.

Transparência: Informar ao titular sobre o compartilhamento, a finalidade e os destinatários dos dados.

Formalização: O compartilhamento deve ser formalizado por meio de instrumento jurídico que especifique as responsabilidades e as obrigações das partes envolvidas (Art. 26).

5.5.4. Divulgação de Dados:

A divulgação de dados ocorre quando a Administração Pública torna informações públicas, acessíveis a qualquer pessoa. A LGPD impõe restrições à divulgação de dados pessoais, permitindo apenas em casos específicos:

- Dados anonimizados (Art. 5°, inciso IX e Art. 16, inciso II): Dados que passaram por processo de anonimização, tornando impossível a identificação do titular.
- Informações públicas (Lei de Acesso à Informação - Lei n° 12.527/2011): Informações que devem ser divulgadas em atendimento à Lei de Acesso à Informação, desde que não violem a privacidade e a intimidade dos indivíduos. Nesse caso, é importante observar os segredos de justiça e as informações pessoais cuja divulgação possa colocar em risco a segurança do indivíduo ou de sua família (Art. 23).

6. MEDIDAS DE SEGURANÇA

A LGPD exige a implementação de medidas de segurança para proteger os dados pessoais sob a guarda da Administração Pública Municipal. Essas medidas devem ser proporcionais aos riscos envolvidos no tratamento dos dados e abrangem aspectos técnicos e administrativos. Aqui estão algumas das principais medidas de segurança que devem ser implantadas:

6.1. Medidas Técnicas

- Pseudonimização e Anonimização: Transformar os dados pessoais de forma que não possam ser atribuídos a um indivíduo sem o uso de informações adicionais, protegidas separadamente. A anonimização, mais rigorosa, torna a reidentificação impossível.
- Criptografia: Codificar os dados pessoais, tornando-os ilegíveis para pessoas não autorizadas. Utilizar algoritmos de criptografia robustos e chaves de segurança adequadas.
- Controle de Acesso: Implementar mecanismos para restringir o acesso aos dados pessoais apenas aos servidores que precisam deles para o exercício de suas funções. Utilizar senhas fortes, autenticação multifator e controle de permissões.
- *Firewall*: Utilizar *firewalls* para proteger a rede municipal contra acessos não autorizados e ataques externos. Configurar as regras do firewall para bloquear tráfego suspeito.

- Antivírus e *Antimalware*: Instalar e manter atualizados softwares antivírus e *antimalware* em todos os computadores e dispositivos da rede municipal.
- Segurança na Nuvem: Ao utilizar serviços de armazenamento em nuvem, garantir que o provedor ofereça medidas de segurança adequadas para a proteção dos dados pessoais. Verificar a conformidade do provedor com a LGPD.
- *Backups* e Recuperação de Dados: Realizar *backups* regulares dos dados pessoais, garantindo a disponibilidade e a integridade das informações em caso de incidentes. Testar os procedimentos de recuperação de dados periodicamente.
- Registro de Atividades (*Logs*): Manter registros das atividades realizadas nos sistemas que contêm dados pessoais, permitindo a auditoria e a identificação de acessos indevidos.

6.2. Medidas Administrativas

- Política de Segurança da Informação: Elaborar e implementar uma política de segurança da informação que defina as regras e procedimentos para o tratamento de dados pessoais.
- Treinamento dos Servidores: Capacitar os servidores públicos sobre as medidas de segurança e as melhores práticas para a proteção de dados.
- Gestão de Senhas: Implementar políticas de senhas fortes e procedimentos para a troca periódica de senhas.
- Gestão de Acessos: Controlar o acesso físico e lógico aos locais e sistemas que contêm dados pessoais.

- Inventário de Dados Pessoais: Manter um inventário atualizado dos dados pessoais coletados, armazenados e tratados pelo município.
- Avaliação de Riscos: Realizar avaliações de riscos para identificar as vulnerabilidades e as ameaças aos dados pessoais.
- Plano de Resposta a Incidentes: Elaborar um plano de resposta a incidentes de segurança que defina os procedimentos a serem adotados em caso de vazamento de dados ou outros incidentes.
- Contratos com Terceiros: Ao contratar empresas que tratam dados pessoais em nome do município, incluir cláusulas específicas sobre a proteção de dados nos contratos.

6.3. **Boas Práticas**

- Princípio da Minimização dos Dados: Coletar apenas os dados pessoais estritamente necessários para a finalidade específica.
- Princípio da Limitação da Finalidade: Utilizar os dados pessoais apenas para a finalidade informada ao titular.
- Privacidade desde a Concepção (*Privacy by Design*): Incorporar a proteção de dados desde a concepção de novos sistemas e processos.
- Segurança desde a Concepção (*Security by Design*): Implementar medidas de segurança desde o desenvolvimento de sistemas e aplicações.

7. PENALIDADES E SANÇÕES

As penalidades, sanções e multas pelo descumprimento da LGPD na Administração Pública Municipal são severas e visam garantir a proteção dos dados pessoais dos cidadãos. A aplicação dessas sanções considera a gravidade da infração, os danos causados e a boa-fé do infrator. Vamos analisar as legislações pertinentes:

O descumprimento da LGPD pode acarretar diversas penalidades, desde advertências até multas milionárias, suspensão de atividades e responsabilização civil. A gravidade das sanções varia de acordo com a natureza da infração e os danos causados. A implementação de um programa de governança em privacidade e proteção de dados, com a atuação do Encarregado (*DPO*), é crucial para mitigar os riscos e garantir a conformidade com a legislação.

As penalidades são aplicadas pela ANPD após processo administrativo que assegure o direito à ampla defesa e ao contraditório. A gradação da penalidade leva em consideração a boa-fé, a natureza, a gravidade e a duração da infração, os danos patrimoniais e morais causados, a condição econômica do infrator, a vantagem auferida ou pretendida, o grau de reincidência, a cooperação do infrator e a adoção de política de boas práticas e governança.

7.1. Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018)

- Art. 52: Define as sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados (ANPD):

I. Advertência: Com indicação de prazo para adoção de medidas corretivas.

II. Multa simples: De até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração. No caso de órgão público, a multa será aplicada de acordo com a legislação pertinente.

III. Multa diária: Limitada ao valor previsto no inciso II.

IV. Publicização da infração: Divulgação da infração após procedimento administrativo.

V. Bloqueio dos dados pessoais a que se refere a infração: Até a sua regularização.

VI. Eliminação dos dados pessoais a que se refere a infração: Apagar os dados pessoais tratados em desconformidade com a lei.

VII. Suspensão parcial do funcionamento da base de dados: Pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador.

VIII. Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados: A proibição será aplicada por período indeterminado, até a regularização da atividade de tratamento pelo controlador.

- Art. 53: A aplicação das sanções previstas no art. 52 levará em conta:

I. A gravidade e a natureza das infrações e dos direitos pessoais afetados;

II. A boa-fé do infrator;

III. A vantagem auferida ou pretendida pelo infrator;

IV. A condição econômica do infrator;

V. A reincidência;

VI. O grau do dano;

VII. A cooperação do infrator;

VIII. A adoção reiterada e demonstrada pelo infrator de mecanismos e procedimentos internos capazes de minimizar o dano;

IX. A natureza dos dados afetados.

- Art. 54: Dispõe sobre a aplicação de sanções em caso de descumprimento de decisões da ANPD.

7.2. Código Penal (Decreto-Lei n° 2.848/1940)

Em casos mais graves, como vazamento de dados pessoais com intenção criminosa, podem ser aplicadas as sanções previstas no Código Penal, como os crimes contra a inviolabilidade dos segredos:

- Art. 153: Violação de correspondência ou comunicação telegráfica, de dados ou sistema informático.
- Art. 154: Divulgação de segredo.

7.3. Responsabilidade Civil

Além das sanções administrativas e penais, a Administração Pública Municipal pode ser responsabilizada civilmente por danos causados pelo tratamento indevido de dados pessoais, tendo que indenizar os titulares dos dados pelos prejuízos sofridos.

8. VANTAGENS E BENEFÍCIOS DA LGPD NA ADMINISTRAÇÃO PÚBLICA MUNICIPAL

8.1. Para Administração Pública

- Melhoria da Governança e Gestão de Dados: A LGPD impulsiona a organização e sistematização dos dados pessoais sob a guarda do município. Isso leva a uma maior eficiência na gestão da informação, facilitando a tomada de decisões baseadas em dados confiáveis e atualizados. O mapeamento dos dados, exigido pela lei, permite identificar fluxos de informações, redundâncias e possíveis vulnerabilidades, otimizando processos e reduzindo custos.
- Aumento da Segurança da Informação: A implementação da LGPD exige a adoção de medidas de segurança para proteger os dados pessoais contra acessos não autorizados, vazamentos e outras ameaças. Isso fortalece a segurança da informação no município, protegendo não apenas os dados dos cidadãos, mas também informações estratégicas da própria administração.

- Redução de Riscos e Custos com Incidentes de Segurança: Ao implementar as medidas de segurança previstas na LGPD, o município reduz significativamente os riscos de incidentes de segurança, como vazamentos de dados. Consequentemente, diminui também os custos associados a esses incidentes, que podem incluir multas, indenizações e danos à reputação.
- Maior Transparência e Prestação de Contas: A LGPD promove a transparência no tratamento de dados pessoais, exigindo que o município informe aos cidadãos como seus dados são coletados, utilizados e protegidos. Isso fortalece a confiança da população na administração pública e contribui para uma maior prestação de contas.
- Melhoria da Qualidade dos Serviços Públicos: Com dados mais organizados, seguros e acessíveis, a administração pública pode oferecer serviços mais eficientes e personalizados aos cidadãos. A LGPD contribui para a modernização da gestão pública, impulsionando a transformação digital e a inovação.

8.2. **Para os Munícipes**

- Maior Controle sobre seus Dados Pessoais: A LGPD garante aos cidadãos o direito de saber quais dados pessoais o município possui sobre eles, como são utilizados e com quem são compartilhados. Também assegura o direito de corrigir informações incorretas, solicitar a portabilidade dos dados e, em certos casos, solicitar a eliminação dos dados.

- Maior Segurança e Privacidade: Com a implementação da LGPD, os cidadãos têm a garantia de que seus dados pessoais serão tratados com segurança e sigilo, protegendo sua privacidade e evitando o uso indevido de suas informações.
- Aumento da Confiança na Administração Pública: A transparência e o respeito à privacidade promovidos pela LGPD contribuem para o aumento da confiança dos cidadãos na administração pública, fortalecendo a relação entre o governo e a sociedade.
- Exercício da Cidadania: A LGPD empodera os cidadãos, dando-lhes maior controle sobre suas informações e permitindo que participem ativamente da proteção de seus dados pessoais.

Considerações Finais

Esta cartilha é um guia introdutório à LGPD. Recomenda-se a consulta à legislação completa e a participação em treinamentos específicos para aprofundar o conhecimento sobre o tema. A correta aplicação da LGPD é essencial para a proteção dos dados pessoais e para a construção de uma Administração Pública no Município de Itapevi mais transparente e ética.