Prefeitura Municipal de Maricá

Instituto de Ciência, Tecnologia e Inovação de Maricá

A Lei Geral de Proteção de Dados Pessoais (LGPD) com ênfase na gestão de contratos

Maricá, novembro de 2024

Presidente do ICTIM

Cláudio de Souza Gimenez

Presidente do Grupo de Trabalho

Laércio Aguiar da Rocha

Membros do Grupo

Bruno Augusto Ferreira de Barros

Fabrício Sousa Ferreira

Márcio Santarém Nogueira

Sumário

1. GLOSSÁRIO

A

Agentes de Tratamento: O **controlador** e o **operador** são os agentes responsáveis pelas operações de tratamento de dados pessoais. A escolha adequada desses agentes, considerando as exigências da LGPD, garante a segurança e privacidade dos dados.

Alta Administração: Compreende as autoridades que ocupam os cargos de mais alto escalão na hierarquia de uma instituição, como diretores, secretários e chefes de departamento.

Anonimização: Processo técnico pelo qual os dados são **irreversivelmente dissociados do titular**, tornando **impossível** a sua identificação. A anonimização é uma medida importante para proteger a privacidade dos indivíduos, especialmente em pesquisas e estudos que utilizam dados pessoais.

Autoridade Nacional de Proteção de Dados (ANPD): Órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. A ANPD tem um papel fundamental na proteção de dados pessoais no Brasil, atuando na regulamentação da lei, na orientação e fiscalização dos agentes de tratamento e na aplicação de sanções em caso de descumprimento da LGPD.

B

Banco de Dados: Conjunto estruturado de dados, organizado de forma a permitir a busca e recuperação de informações. Os bancos de dados que contêm dados pessoais devem ser protegidos por medidas de segurança adequadas para garantir a confidencialidade, a integridade e a disponibilidade das informações.

Bases Legais: Conjunto de justificativas legais que autorizam o tratamento de dados pessoais. As bases legais para o tratamento de dados pela Administração Pública estão previstas nos artigos 7º e 11 da LGPD. Algumas das bases legais mais relevantes para o ICTIM são: (i) **Consentimento**, (ii) **Cumprimento de obrigação legal ou regulatória**, (iii) **Execução de políticas públicas** e (iv) **Legítimo Interesse**.

C

Consentimento: Manifestação **livre**, **informada** e **inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para

uma finalidade **determinada**. Na Administração Pública, o consentimento tem aplicação limitada, mas ainda é relevante em algumas situações, como pesquisas de opinião.

Controlador: Pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O **ICTIM**, como órgão da administração pública, atua como controlador dos dados pessoais sob sua responsabilidade.

Cumprimento de Obrigação Legal ou Regulatória: Base legal que autoriza o tratamento de dados pessoais quando necessário para o cumprimento de uma obrigação legal ou regulatória pelo controlador. Essa base legal é fundamental para o ICTIM, pois muitas de suas atividades são determinadas por leis e regulamentos específicos que exigem o tratamento de dados pessoais.

D

Dados Pessoais: Qualquer informação relacionada a uma pessoa natural identificada ou identificável. A LGPD se aplica à proteção de todos os tipos de dados pessoais, independentemente do meio em que são armazenados ou processados.

Dados Pessoais Sensíveis: Categoria especial de dados pessoais que exigem maior proteção, como aqueles relacionados à *origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicato, saúde ou vida sexual*. O tratamento de dados sensíveis é **restrito** e exige **cuidados adicionais** para garantir a privacidade e a segurança dos titulares.

Direitos dos Titulares: Conjunto de direitos garantidos pela LGPD aos titulares de dados pessoais, como o direito de acesso, correção, eliminação, portabilidade e oposição ao tratamento de seus dados. O ICTIM tem a obrigação de garantir o exercício desses direitos pelos titulares de dados, implementando procedimentos e mecanismos para atender às suas solicitações.

Due diligence: Refere-se ao processo de análise e avaliação das práticas de proteção de dados pessoais de uma empresa ou organização. A LGPD estabelece diretrizes rigorosas sobre como os dados pessoais devem ser coletados, armazenados, tratados e compartilhados, e a due diligence é essencial para garantir a conformidade com esses regulamentos. Realizar a due diligence em conformidade com a LGPD é essencial para minimizar riscos legais, proteger a reputação do ICTIM e garantir a confiança dos titulares de

dados. Além disso, ajuda as organizações a se prepararem para auditorias e fiscalizações relacionadas à proteção de dados.

E

Eliminação de Dados Pessoais: Processo de exclusão definitiva dos dados pessoais, tornando-os irrecuperáveis. A eliminação dos dados pessoais deve ser realizada de forma segura e em conformidade com a LGPD.

Encarregado pelo Tratamento de Dados Pessoais (DPO – Data Protection Officer): Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. O DPO tem um papel fundamental na implementação da LGPD, orientando a instituição sobre a lei, promovendo a cultura de proteção de dados e atuando como ponto de contato para os titulares de dados e a ANPD.

Encarregado Setorial: No âmbito da Prefeitura, são pessoas indicadas pelos entes da Administração Direta, Autarquias, Fundações Públicas, Empresas Públicas e Sociedade de Economia Mista para atuarem como canal de comunicação entre os referidos entes e o Encarregado Geral da Prefeitura. No ICTIM, o Controlador, na figura do Presidente, designou os respectivos Diretores para serem os encarregados setoriais, que atuarão como um elo entre as demandas relacionadas a essas diretorias e o Encarregado Geral do ICTIM.

F

Finalidade: Objetivo específico, legítimo, explícito e informado ao titular para o qual os dados pessoais são tratados. A finalidade do tratamento deve ser determinada no momento da coleta dos dados e o uso dos dados para finalidades diferentes das originalmente informadas é vedado, a menos que haja uma nova base legal.

G

Governança em Privacidade: Conjunto de práticas, políticas e procedimentos implementados pelo controlador para garantir a conformidade com a LGPD e a proteção dos dados pessoais. A implementação de um programa de governança em privacidade abrangente é essencial para mitigar os riscos e promover uma cultura de proteção de dados.

I

Incidente de Segurança: Qualquer evento que comprometa a segurança dos dados pessoais, como acesso não autorizado, perda, alteração, comunicação ou difusão indevida. O ICTIM deve implementar medidas de segurança para prevenir e responder a incidentes de segurança, garantindo a proteção dos dados pessoais e notificando os titulares e a ANPD em caso de ocorrência.

Inventário de Dados Pessoais: Documento que contém a descrição detalhada de todos os dados pessoais tratados pelo controlador, incluindo a sua origem, finalidade do tratamento, base legal, medidas de segurança e informações de contato do controlador. O inventário de dados é um instrumento fundamental para a implementação da LGPD, permitindo ao controlador ter uma visão completa dos dados pessoais que trata e das suas responsabilidades.

L

Lei Geral de Proteção de Dados Pessoais (LGPD): Lei nº 13.709/2018, que dispõe sobre o tratamento de dados pessoais por pessoas físicas ou jurídicas de direito público ou privado, com o objetivo de proteger os direitos de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural. A LGPD introduz um novo paradigma para a proteção de dados pessoais no Brasil, com impactos significativos para o ICTIM e a Administração Pública em geral.

Legítimo Interesse: Base legal que autoriza o tratamento de dados pessoais quando necessário para atender aos interesses legítimos do controlador ou de terceiros, desde que não prevaleçam direitos e liberdades fundamentais do titular. A utilização do legítimo interesse deve ser justificada e documentada, demonstrando que o tratamento é necessário e proporcional aos interesses legítimos do controlador, sem violar os direitos dos titulares.

M

Medidas de Segurança: Conjunto de medidas técnicas e administrativas implementadas pelo controlador para proteger os dados pessoais contra acessos não autorizados, perda, alteração ou qualquer forma de tratamento inadequado. As medidas de segurança devem ser proporcionais aos riscos envolvidos no tratamento de dados e revisadas periodicamente para garantir a sua efetividade.

N

Necessidade: Princípio que estabelece que o tratamento de dados pessoais deve se limitar ao mínimo necessário para a realização de suas finalidades. O ICTIM deve coletar e tratar apenas os dados estritamente necessários para atingir a finalidade específica informada ao titular, evitando a coleta de informações excessivas ou irrelevantes.

O

Operador: Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador deve seguir as instruções do controlador e implementar medidas de segurança adequadas para proteger os dados pessoais.

P

Plano de Adequação: documento que define as diretrizes, procedimentos e medidas a serem adotados pelo ICTIM para garantir a conformidade com a LGPD. Ele deve ser elaborado de forma a abranger todos os aspectos do tratamento de dados pessoais, desde a coleta até a eliminação, e deve ser atualizado periodicamente

Política de Privacidade: Documento que descreve as práticas de tratamento de dados pessoais do controlador, informando aos titulares como seus dados são coletados, utilizados, armazenados e protegidos. A Política de Privacidade deve ser redigida em linguagem clara e acessível, e disponibilizada de forma transparente aos titulares de dados.

Portabilidade de Dados: Direito do titular de receber seus dados pessoais, em formato estruturado e interoperável, para transferi-los a outro fornecedor de serviço ou produto, mediante requisição expressa. A portabilidade de dados facilita a mudança de fornecedores pelos titulares, sem perda de seus dados.

Princípios da LGPD: Conjunto de princípios que devem nortear o tratamento de dados pessoais, como a finalidade, a adequação, a necessidade, a transparência, a segurança e a prevenção de danos. A observância dos princípios da LGPD é fundamental para garantir a proteção dos dados pessoais e a conformidade com a lei.

Privacy by Design: Traduzido como "Privacidade desde a Concepção" ou "Privacidade por Design", é um princípio que preconiza a integração da proteção de dados pessoais em todas as etapas do desenvolvimento de produtos, serviços e sistemas. Isso significa que a privacidade deve ser considerada como um elemento fundamental desde o início do projeto, e não como um complemento a ser adicionado posteriormente.

Privacy by Default: traduzido como "Privacidade por Padrão", determina que a proteção de dados seja a configuração padrão de qualquer sistema ou serviço. Isso significa que, por padrão, o sistema deve garantir o maior nível de privacidade possível, sem a necessidade de que o usuário realize configurações adicionais.

Pseudonimização: Processo técnico pelo qual os dados pessoais são substituídos por um identificador, dificultando a identificação do titular, mas permitindo a reversão mediante informações adicionais. A pseudonimização é uma medida de segurança que reduz os riscos à privacidade dos titulares, sem impedir a utilização dos dados para fins legítimos.

R

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): Documento elaborado pelo controlador para avaliar os riscos à privacidade decorrentes de um tratamento de dados pessoais e propor medidas de mitigação. A elaboração do RIPD é obrigatória em algumas situações, como em tratamentos de dados que envolvam alto risco aos direitos dos titulares. O controlador pode delegar a tarefa de elaboração do RIPD ao Encarregado de Proteção de Dados (DPO).

S

Sanções e Penalidades: Conjunto de medidas punitivas que podem ser aplicadas pela ANPD aos agentes de tratamento que descumprirem a LGPD. As sanções e penalidades variam de advertência à suspensão do tratamento de dados e podem gerar impactos financeiros e à reputação da instituição.

T

Termo de Consentimento: Documento que estabelece as regras e condições para a utilização de um serviço ou produto, incluindo o tratamento de dados pessoais. Os Termos de Consentimento devem ser redigidos em linguagem clara e acessível, informando aos titulares sobre os seus direitos e as responsabilidades do controlador.

Titular de Dados Pessoais: Pessoa natural a quem se referem os dados pessoais. O titular de dados pessoais é o centro da proteção da LGPD, tendo seus direitos e liberdades fundamentais protegidos pela lei.

Transparência: Princípio que garante ao titular o acesso a informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados pessoais. O ICTIM deve ser transparente em relação às suas

práticas de tratamento de dados, informando aos titulares como seus dados são utilizados, as bases legais para o tratamento, seus direitos e como exercê-los.

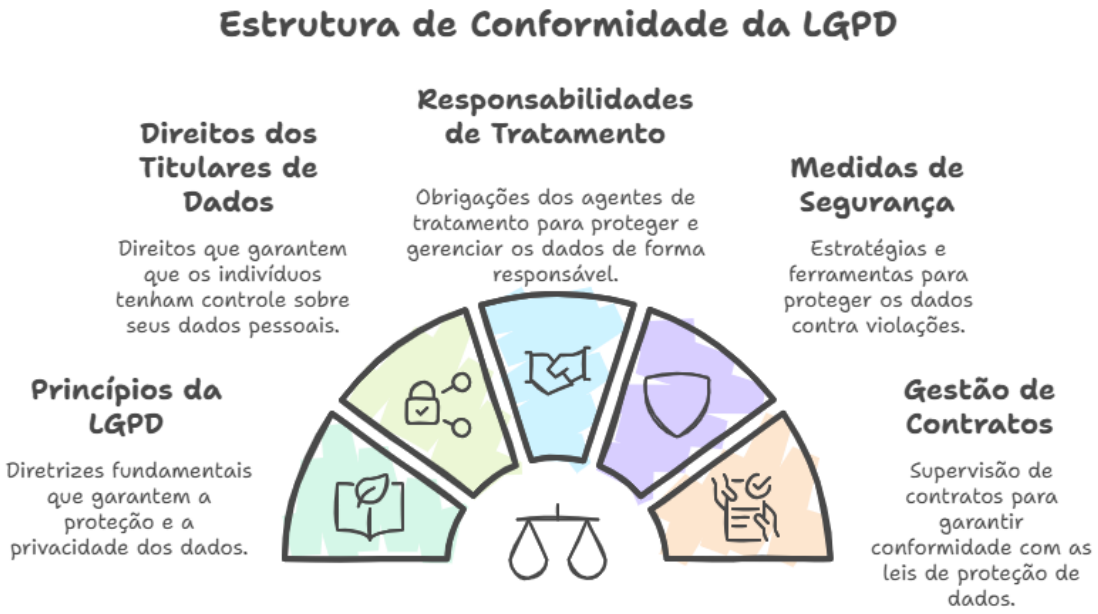
Tratamento de Dados Pessoais: Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. A LGPD regulamenta todas as fases do tratamento de dados pessoais, desde a coleta até a eliminação dos dados.

U

Uso Compartilhado de Dados: Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais entre órgãos e entidades públicos, ou entre estes e entes privados, para o cumprimento de suas competências legais ou para a execução de políticas públicas. O uso compartilhado de dados deve seguir regras específicas para garantir a segurança e a privacidade dos dados pessoais, observando os princípios da LGPD e a finalidade do tratamento.

2. PREMISSAS

Esta apostila aborda os principais aspectos da Lei Geral de Proteção de Dados Pessoais (LGPD), fornecendo aos servidores do ICTIM o conhecimento necessário para garantir a conformidade com a lei e proteger a privacidade dos cidadãos, especialmente no contexto da gestão e fiscalização de contratos. A apostila apresenta os princípios da LGPD, os direitos dos titulares de dados, as responsabilidades dos agentes de tratamento, as medidas de segurança, as boas práticas, exemplos práticos de aplicação da LGPD no ICTIM, um roteiro para implementação da LGPD e um checklist completo para auxiliar na adequação à lei. Aborda também a gestão de vulnerabilidades, um processo crucial para a segurança dos dados pessoais, detalhando as etapas e as ferramentas para a identificação, análise, tratamento e monitoramento de vulnerabilidades. A gestão e a fiscalização de contratos são parte fundamental da conformidade com a LGPD, demandando atenção especial dos servidores do ICTIM para garantir a proteção de dados pessoais em todas as etapas do ciclo de vida dos contratos.



A inclusão de informações sobre a **gestão e fiscalização de contratos no âmbito da LGPD** é essencial para que os servidores do ICTIM compreendam as suas responsabilidades e os procedimentos adequados para garantir a proteção de dados pessoais, tais quais:

- A importância de incluir cláusulas de proteção de dados em contratos com terceiros, especialmente com operadores que tratam dados pessoais em nome do ICTIM.
- A necessidade de realizar a due diligence dos fornecedores para garantir que eles estejam em conformidade com a LGPD e que possuam medidas de segurança adequadas para proteger os dados pessoais.
- A responsabilidade solidária entre controlador e operador em caso de violações à LGPD, o que reforça a importância da gestão e fiscalização de contratos.
- A necessidade de estabelecer um processo para a gestão de incidentes de segurança em relação aos contratos, incluindo a notificação aos titulares de dados afetados e à Autoridade Nacional de Proteção de Dados (ANPD).

Clique aqui para abrir a apostila de Gestão e Fiscalização de Contratos

3. INTRODUÇÃO À LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, tem como **objetivo principal proteger os direitos de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural**. Para isso, ela regulamenta o tratamento de dados pessoais por pessoas físicas ou jurídicas de direito público ou privado, inclusive nos meios digitais.

É crucial destacar que o Município de Maricá, por meio do Decreto nº 840, de 05 de abril de 2022, regulamentou a aplicação da LGPD em âmbito municipal. O decreto municipal estabelece diretrizes, competências, procedimentos e providências específicas a serem observadas por todos os órgãos da administração direta e indireta do Município, incluindo o ICTIM. O objetivo principal do decreto é garantir a proteção de dados pessoais em todas as esferas da administração pública municipal, promovendo a privacidade e a segurança dos cidadãos.

Considerando que o ICTIM lida com **dados pessoais sensíveis** e **não sensíveis**, a LGPD se torna essencial para garantir a segurança e privacidade dessas informações, evitando a exposição de dados dos cidadãos e usuários.

A importância da LGPD para o ICTIM se manifesta em diversos aspectos, como:

- **Estabelecimento de diretrizes claras para a coleta, armazenamento, uso e compartilhamento de dados pessoais:** A lei define as bases legais para o tratamento de dados, os direitos dos titulares dos dados e as obrigações do controlador (no caso,

o ICTIM). Isso garante que o ICTIM utilize os dados de forma transparente e ética, respeitando a privacidade dos indivíduos.

- **Proteção contra o uso indevido de dados:** A LGPD prevê sanções para o descumprimento da lei, incluindo multas e a proibição do exercício de atividades relacionadas ao tratamento de dados. Isso incentiva o ICTIM a adotar medidas de segurança e boas práticas para proteger os dados sob sua responsabilidade.

- **Fortalecimento da confiança do público e dos órgãos de controle:** A adequação à LGPD demonstra o compromisso do ICTIM com a proteção de dados e a privacidade dos cidadãos e usuários. Isso contribui para fortalecer a confiança do público e dos órgãos de controle na instituição e nos serviços prestados.

O ICTIM deve se atentar a alguns pontos específicos da LGPD:

- **Consentimento:** A lei exige que o ICTIM obtenha o consentimento do titular dos dados para realizar o tratamento, exceto em casos específicos. É importante que o consentimento seja livre, informado e inequívoco, ou seja, o titular deve ter clareza sobre como seus dados serão utilizados.

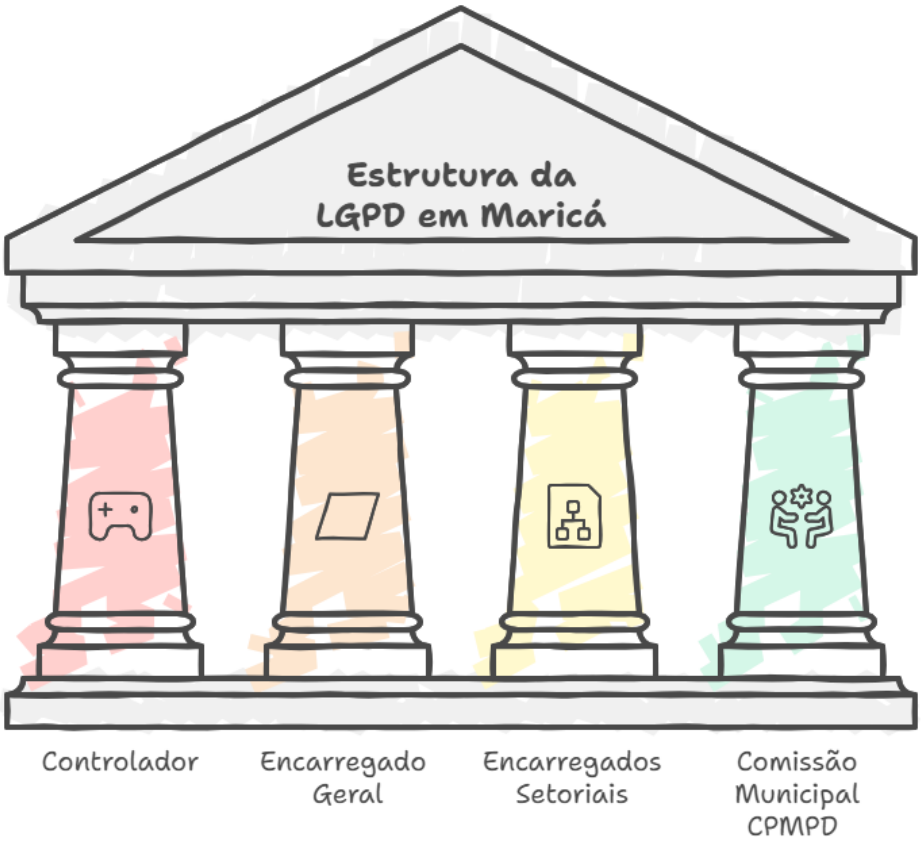
- **Finalidade:** O ICTIM deve coletar e utilizar os dados apenas para finalidades específicas, legítimas e informadas ao titular. O uso de dados para finalidades diferentes das originalmente informadas é vedado, a menos que haja uma nova base legal para o tratamento.

- **Necessidade:** A coleta e o tratamento de dados devem ser limitados ao mínimo necessário para atingir a finalidade pretendida. O ICTIM deve evitar coletar informações excessivas ou irrelevantes para a finalidade do tratamento.

- **Transparência:** O ICTIM deve ser transparente em relação às suas práticas de tratamento de dados, fornecendo aos titulares informações claras e acessíveis sobre como seus dados são utilizados. Isso inclui a publicação de uma política de privacidade detalhada e a disponibilização de um canal de comunicação para atender às solicitações dos titulares.

- **Segurança:** O ICTIM deve adotar medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados, perda, alteração ou qualquer forma de tratamento inadequado. As medidas de segurança devem ser proporcionais aos riscos envolvidos no tratamento.

Estrutura organizacional da LGPD em Maricá e a relação com o ICTIM



O Decreto nº 840, de 05 de abril de 2022, estabelece a estrutura organizacional para a aplicação da LGPD no município de Maricá, definindo os atores e suas responsabilidades na proteção de dados pessoais. A seguir, detalhamos essa estrutura e a relação do ICTIM com cada um dos atores:

a. Controlador

O Prefeito é o controlador dos dados pessoais, responsável por tomar as decisões referentes ao tratamento de dados em toda a Administração Municipal.

No ICTIM, o Presidente do Instituto é o controlador dos dados pessoais. Ele é o responsável por tomar as decisões referentes ao tratamento de dados no âmbito desta Autarquia, conforme Portaria nº 86, de 22 de outubro de 2024.

As suas responsabilidades incluem:

- Definir as finalidades e os meios para o tratamento de dados pessoais.

- Garantir que o tratamento de dados esteja em conformidade com a LGPD e o Decreto Municipal nº 840/2022.

- Nomear o Encarregado Geral de Proteção de Dados (DPO).

- Prover recursos para a implementação da LGPD.

É importante destacar que as decisões do Prefeito como Controlador impactam diretamente as atividades do ICTIM, que deve seguir as diretrizes e políticas estabelecidas para o tratamento de dados pessoais.

b. Encarregado Geral

O Encarregado Geral é a pessoa indicada pelo controlador, no caso, o Município de Maricá, para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Ele desempenha um papel fundamental na implementação e cumprimento da LGPD em âmbito municipal, com responsabilidades que abrangem desde a orientação dos servidores até a comunicação com a ANPD.

No município de Maricá, o Encarregado Geral é a Secretaria de Governo, representada por um servidor público designado para essa função.

E no caso do ICTIM, por ser um órgão da administração indireta, o Decreto Municipal nº 840/2022 o defina como Encarregado Setorial. No entanto, o Controlador (Presidente do ICTIM) designou um servidor público para ser o Encarregado Geral no âmbito do ICTIM, conforme Portaria nº 86, de 22 de outubro de 2024.

O Encarregado Geral do ICTIM se reporta diretamente ao Encarregado Geral (Secretaria de Governo), que tem a responsabilidade de supervisionar a implementação da LGPD em todo o Município. Essa estrutura hierárquica garante a uniformidade na aplicação da LGPD e facilita a comunicação entre os diferentes atores envolvidos na proteção de dados em Maricá.

Algumas de suas responsabilidades são:

- Elaborar o Plano de Adequação do ICTIM à LGPD, definindo as medidas a serem implementadas para garantir a conformidade com a lei.

- Treinar os servidores do ICTIM sobre a LGPD, os princípios da proteção de dados e as políticas internas.

- Fomentar a cultura de proteção de dados.

- Receber e analisar reclamações de titulares de dados, encaminhando-as ao Encarregado Geral.

- Manter o inventário de dados do ICTIM atualizado, documentando as atividades de tratamento de dados realizadas.

- Reportar ao Encarregado Geral sobre as atividades de proteção de dados do ICTIM, comunicando incidentes de segurança e garantindo a conformidade com as diretrizes estabelecidas.

- Comunicar à ANPD incidentes de segurança.

c. Encarregados Setoriais

Os Encarregados Setoriais são pessoas indicadas pelos entes da Administração Direta e Indireta do município, como as Secretarias Municipais, para atuarem como um elo entre esses entes e o Encarregado Geral. Eles auxiliam na implementação da LGPD em seus respectivos setores, repassando informações, promovendo treinamentos e colaborando na elaboração do Plano de Adequação.

Cada Secretaria Municipal deve designar um servidor para atuar como Encarregado Setorial.

No ICTIM, O Controlador, na figura do Presidente, designou os Diretores para serem os encarregados setoriais, que atuarão como um elo entre as demandas relacionadas a essas diretorias e o Encarregado Geral do ICTIM.

Algumas de suas responsabilidades são:

- Auxiliar o Encarregado Geral na elaboração do Plano de Adequação.

- Receber e analisar reclamações de titulares de dados, reportando ao Encarregado Geral.

- Manter o Encarregado Geral informado sobre as atividades de tratamento de dados ligados à sua área de atuação.

O Encarregado Setorial do ICTIM é responsável por garantir a conformidade com a LGPD dentro do instituto, reportando-se ao Encarregado Geral e seguindo as diretrizes estabelecidas.

d. Comissão Permanente Municipal de Proteção de Dados (CPMPD)

A CPMPD é um órgão colegiado formado por representantes de diferentes Secretarias Municipais, com a função de garantir a conformidade com a LGPD em âmbito municipal. A comissão atua de forma deliberativa e consultiva, analisando procedimentos, elaborando o Plano de Adequação, respondendo a consultas e auxiliando na implementação da LGPD.

A CPMPD é composta por seis servidores titulares e seus respectivos suplentes, representando as seguintes Secretarias:

- Secretaria de Assistência Social
- Secretaria de Educação
- Secretaria de Governo
- Secretaria de Planejamento, Orçamento e Fazenda / Serviços Integrados Municipal
- Secretaria de Planejamento, Orçamento e Fazenda / Subsecretaria de Governança e Gestão da Tecnologia e Sistemas de Informação (SSI)
- Secretaria de Saúde

A CPMPD define as diretrizes gerais para a proteção de dados no Município, que o ICTIM deve seguir. O Encarregado Geral do ICTIM pode consultar a CPMPD em caso de dúvidas sobre a aplicação da LGPD.

A gestão de contratos no contexto da LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) introduziu no Brasil um novo patamar de proteção de dados pessoais, impactando diretamente a forma como o ICTIM conduz a gestão e fiscalização de seus contratos. A LGPD aplica-se a todas as etapas do ciclo de vida de um contrato, desde a seleção de fornecedores até o término da relação contratual, e exige que a proteção de dados seja integrada em todas as fases.

A gestão e fiscalização de contratos assumem papel fundamental na conformidade com a LGPD, especialmente ao considerar a responsabilidade

solidária entre o ICTIM, como controlador de dados, e seus fornecedores e prestadores de serviços, que podem atuar como operadores de dados. Isso significa que o ICTIM pode ser responsabilizado por falhas na proteção de dados, mesmo que a responsabilidade direta seja do terceiro.

Clique aqui para abrir a apostila de Gestão e Fiscalização de Contratos

A importância da gestão de contratos para a conformidade com a LGPD

A gestão de contratos no contexto da LGPD vai além da simples inclusão de cláusulas de proteção de dados. É preciso haver uma **mudança de cultura dentro da instituição**, garantindo que a proteção de dados seja incorporada em todas as políticas, processos e procedimentos relacionados à gestão de contratos.

- **Planejamento contratual:** A proteção de dados deve ser considerada desde o planejamento das contratações, definindo os requisitos de proteção de dados que serão exigidos dos fornecedores e prestadores de serviços.

- **Seleção de fornecedores:** A conformidade com a LGPD deve ser um critério fundamental na escolha de fornecedores e prestadores de serviços, priorizando aqueles que demonstram compromisso com a proteção de dados e que possuem medidas de segurança adequadas.

- **Elaboração e revisão de contratos:** Os contratos devem conter cláusulas específicas que definam as responsabilidades do ICTIM e do fornecedor / prestador de serviços em relação à proteção de dados pessoais.

- **Due Diligence de fornecedores:** É fundamental realizar a due diligence dos fornecedores e prestadores de serviços para verificar sua conformidade com a LGPD, incluindo a análise de suas políticas de privacidade, medidas de segurança e procedimentos para resposta a incidentes.

- **Acompanhamento e fiscalização:** O ICTIM deve monitorar continuamente o cumprimento das obrigações de proteção de dados pelos fornecedores e prestadores de serviços, realizando auditorias periódicas e adotando medidas corretivas quando necessário.

Responsabilidades do ICTIM como Controlador de dados nos contratos com terceiros

O ICTIM, como controlador de dados, possui responsabilidades específicas em relação à proteção de dados pessoais nos contratos com terceiros, incluindo:

- **Definir a finalidade e os meios para o tratamento de dados pessoais:** O ICTIM deve estabelecer de forma clara e precisa as finalidades para as quais os dados pessoais serão tratados pelo fornecedor / prestador de serviços, bem como os meios que serão utilizados para o tratamento.

- **Garantir que o fornecedor / prestador de serviços atenda aos requisitos da LGPD:** O ICTIM deve se certificar de que o fornecedor / prestador de serviços possui as condições técnicas e organizacionais para garantir a segurança dos dados pessoais e cumprir com as demais obrigações previstas na LGPD.

- **Implementar medidas de segurança adequadas:** O ICTIM é responsável por implementar medidas de segurança adequadas para proteger os dados pessoais, mesmo que o tratamento seja realizado por um operador.

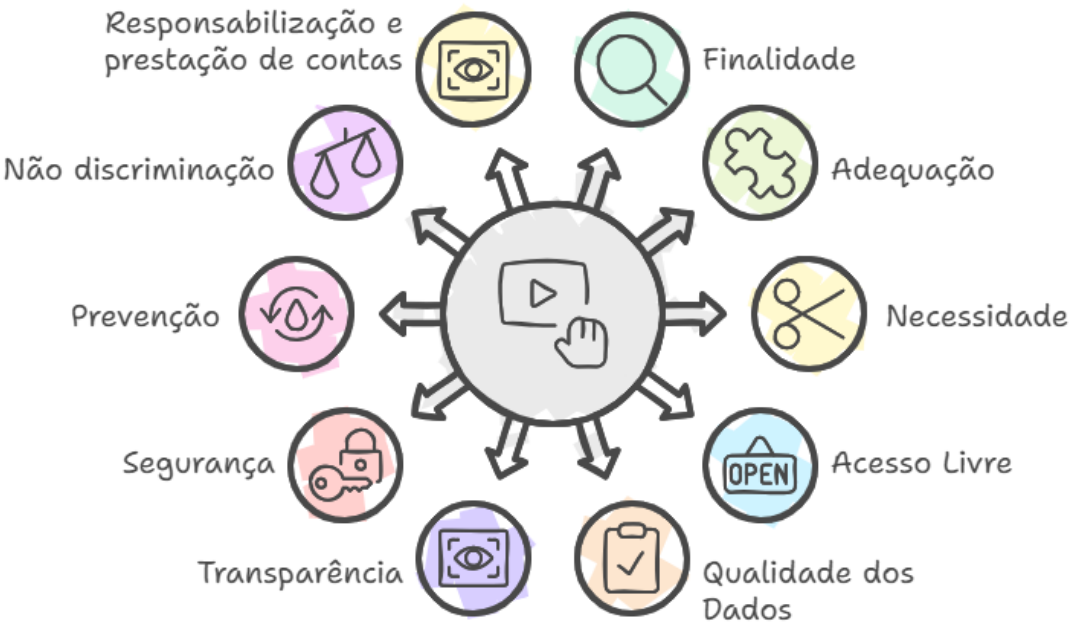
- **Responder a incidentes de segurança:** O ICTIM deve ter um plano de resposta a incidentes para lidar com eventuais violações

de dados pessoais, incluindo a notificação aos titulares de dados e à ANPD.

- **Supervisionar o tratamento de dados pelo fornecedor / prestador de serviços:** O ICTIM deve acompanhar o tratamento de dados realizado pelo fornecedor / prestador de serviços para garantir que as suas instruções estejam sendo seguidas e que a LGPD está sendo cumprida.

4. PRINCÍPIOS DA LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, define dez princípios fundamentais que devem nortear todas as atividades de tratamento de dados pessoais. Esses princípios, detalhados no Art. 6º da LGPD, visam garantir a proteção dos direitos de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. A seguir, uma breve explicação de cada um deles:



- **Finalidade:** A coleta e o tratamento de dados pelo ICTIM só podem ocorrer para finalidades legítimas, ou seja, previstas em lei ou respaldadas por outros fundamentos jurídicos; específicas, definidas de forma clara e precisa, delimitando o escopo do tratamento; explícitas, expressas de maneira clara e inequívoca, sem margem para dúvidas; e informadas ao titular dos dados, de forma que este tenha conhecimento prévio e inequívoco sobre a finalidade da coleta e do uso de seus dados.

O ICTIM deve garantir que o tratamento posterior dos dados seja compatível com a finalidade original, evitando o uso para finalidades distintas sem uma nova base legal. Vale ressaltar que a finalidade também deve ser pública, estando alinhada com as competências e atribuições legais do ICTIM, conforme previsto no Art. 23 da LGPD.

- **Adequação:** Este princípio complementa o princípio da finalidade, reforçando a necessidade de compatibilidade entre o tratamento dos dados e as finalidades informadas ao titular. O contexto em que o tratamento se insere é um fator crucial na análise da adequação.

  Exemplo: Coletar dados de contato para enviar comunicados sobre serviços prestados pelo ICTIM é considerado adequado. No entanto, utilizar esses mesmos dados para enviar publicidade de empresas parceiras, sem o consentimento explícito do titular, seria inadequado e violaria o princípio da adequação.

- **Necessidade:** O ICTIM deve se limitar a coletar e tratar apenas os dados estritamente necessários para atingir a finalidade específica informada ao titular. A coleta de dados excessivos ou irrelevantes, mesmo que com o consentimento do titular, é desaconselhada. A instituição deve analisar criteriosamente cada informação solicitada, justificando sua pertinência, proporcionalidade e necessidade em relação à finalidade do tratamento. O princípio da necessidade também se aplica a outras etapas do tratamento, como armazenamento e processamento de dados.

  Exemplo: Se o ICTIM coleta dados para um cadastro de usuários, informações como nome completo, CPF e data de nascimento podem ser consideradas necessárias. No entanto, solicitar dados como endereço completo, estado civil ou filiação partidária, sem uma justificativa plausível relacionada à finalidade do cadastro, configuraria violação ao princípio da necessidade.

- **Livre acesso:** Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

- **Qualidade dos dados:** Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

- **Transparência:** O ICTIM deve garantir a transparência em todas as suas práticas de tratamento de dados, fornecendo aos titulares informações claras, precisas, facilmente acessíveis e em linguagem simples. A instituição deve ser proativa na divulgação dessas informações, disponibilizando-as de forma ostensiva, preferencialmente em seu site institucional, sem a necessidade de solicitação prévia do titular. As informações devem abranger:

    - Finalidade específica do tratamento;
    - Forma e duração do tratamento;
    - Identificação e informações de contato do controlador;
    - Informações sobre o uso compartilhado de dados;
    - Responsabilidades dos agentes que realizarão o tratamento;
    - Direitos do titular.

    Além disso, a identidade e informações de contato do Encarregado pelo Tratamento de Dados Pessoais devem ser divulgadas publicamente. Uma boa prática é a criação de uma política de privacidade detalhada, publicada no site institucional do ICTIM, com linguagem clara e acessível, e a disponibilização de um canal de comunicação para atender às solicitações dos titulares.

- **Segurança:** O ICTIM deve adotar medidas de segurança técnicas e administrativas adequadas para proteger os dados pessoais sob sua responsabilidade. Essas medidas devem ser proporcionais aos riscos envolvidos no tratamento e devem ser implementadas desde a concepção do sistema até a sua execução. As medidas de segurança visam proteger os dados contra:

    - Acessos não autorizados;
    - Situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

    Exemplos de medidas de segurança:

    - Criptografia de dados;
    - Controle de acesso aos sistemas, com autenticação forte e autorização baseada em funções;

- Backups regulares e seguros;
- Políticas de segurança da informação;
- Treinamento dos colaboradores em boas práticas de segurança da informação e proteção de dados.

- **Prevenção:** A LGPD destaca a importância da prevenção de danos como um princípio norteador do tratamento de dados. Isso significa que o ICTIM deve adotar medidas proativas para evitar a ocorrência de incidentes de segurança que possam comprometer os dados pessoais sob sua guarda.

  Exemplos de medidas preventivas:

  - Realização de Análise de Impacto à Proteção de Dados (AIPD) para identificar e mitigar riscos à privacidade;
  - Implementação de processos de governança em proteção de dados;
  - Monitoramento constante dos sistemas e da infraestrutura de TI para identificar vulnerabilidades;
  - Atualização regular dos softwares e sistemas de segurança.

- **Não discriminação:** Impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

- **Responsabilização e prestação de contas:** O ICTIM deve ser capaz de demonstrar a adoção de medidas eficazes e em conformidade com a LGPD. Isso significa que a instituição precisa documentar suas práticas de tratamento de dados, implementar mecanismos de controle e auditoria, e estar pronta para prestar contas à Autoridade Nacional de Proteção de Dados (ANPD) sobre suas atividades.

  Exemplos de medidas de responsabilização e prestação de contas:

  - Manutenção de registros das operações de tratamento de dados;
  - Implementação de um programa de governança em proteção de dados;
  - Designação de um Encarregado pelo Tratamento de Dados Pessoais;

- Realização de auditorias internas e externas para avaliar a conformidade com a LGPD.

Em conclusão, a compreensão e a aplicação diligente desses princípios são essenciais para que o ICTIM trate os dados pessoais de forma ética, responsável e em conformidade com a LGPD. A implementação de um programa de governança em proteção de dados, com base nesses princípios, garante a proteção dos dados pessoais, a privacidade dos cidadãos e usuários e a confiança do público na instituição.

5. DIREITOS DOS TITULARES DE DADOS

A Lei Geral de Proteção de Dados Pessoais (LGPD) não apenas estabelece princípios para o tratamento de dados pessoais, mas também garante aos titulares uma série de direitos em relação aos seus dados. O Capítulo III da LGPD, especificamente o Art. 18, detalha esses direitos, com o objetivo de empoderar o indivíduo e assegurar o controle sobre suas informações pessoais. O ICTIM, como controlador de dados, tem a obrigação de garantir o exercício desses direitos, estabelecendo procedimentos claros, acessíveis e eficazes para atender às solicitações dos titulares.

A seguir, uma análise detalhada de cada um dos direitos dos titulares de dados, com foco na aplicação prática pelo ICTIM:

Confirmação da existência de tratamento

O titular dos dados tem o direito de obter do ICTIM a confirmação de que seus dados pessoais estão ou não sendo tratados pela instituição. Essa confirmação deve ser fornecida de forma simples e imediata, sem custos para o titular.

Exemplo:

Um cidadão pode solicitar ao ICTIM a confirmação de que a instituição possui seus dados cadastrados em seus sistemas, independentemente da finalidade do tratamento.

Acesso aos dados

Caso seus dados estejam sendo tratados pelo ICTIM, o titular tem o direito de acessá-los, obtendo uma cópia integral das informações armazenadas. O acesso abrange não apenas os dados em si, mas também informações sobre a forma como são tratados, incluindo a finalidade do tratamento, as bases legais que o sustentam, os agentes de tratamento envolvidos, e com quais entidades os dados são compartilhados.

O ICTIM deve fornecer os dados em formato legível e de fácil compreensão, permitindo ao titular analisar as informações e tomar decisões sobre seus dados.

Exemplo:

Um usuário de um serviço do ICTIM pode solicitar acesso aos seus dados cadastrais, bem como informações sobre como esses dados são utilizados pela instituição.

Correção de dados incompletos, inexatos ou desatualizados

O titular tem o direito de solicitar a correção de seus dados caso estejam incompletos, inexatos ou desatualizados. O ICTIM tem a obrigação de analisar a solicitação e, se procedente, realizar a correção dos dados de forma tempestiva, garantindo a qualidade e a confiabilidade das informações sob sua guarda.

Exemplo:

Um cidadão pode solicitar ao ICTIM a correção de seu endereço ou número de telefone, caso tenham sido alterados.

Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade

O titular tem o direito de solicitar a anonimização, o bloqueio ou a eliminação de seus dados caso se enquadrem nas seguintes situações:

- **Dados desnecessários:** Informações que não são mais relevantes para a finalidade original do tratamento, ou cuja coleta não se justifica.
- **Dados excessivos:** Informações coletadas em quantidade superior ao necessário para atingir a finalidade do tratamento.
- **Dados tratados em desconformidade:** Informações tratadas em violação à LGPD ou a outras normas aplicáveis.

A anonimização torna os dados irreversivelmente dissociados do titular, impossibilitando sua identificação. O bloqueio consiste na suspensão temporária do tratamento, impedindo o acesso aos dados, sem sua exclusão definitiva. A eliminação consiste na exclusão definitiva dos dados dos sistemas do ICTIM.

O ICTIM deve analisar a solicitação do titular e, se procedente, adotar a medida mais adequada, considerando os princípios da LGPD e as normas de gestão de documentos e arquivos.

Exemplo:

Um cidadão pode solicitar a eliminação de seus dados de um banco de dados do ICTIM, caso o tratamento tenha se encerrado ou se os dados não forem mais necessários para a finalidade original.

Portabilidade dos dados a outro fornecedor de serviço ou produto

O titular tem o direito de solicitar a portabilidade de seus dados a outro fornecedor de serviço ou produto, desde que o tratamento seja realizado com base em consentimento ou em contrato. A portabilidade consiste na transferência dos dados em formato interoperável, permitindo sua utilização por **outro controlador**.

O ICTIM, ao receber a solicitação, deve viabilizar a portabilidade dos dados, garantindo a segurança e a integridade das informações durante o processo.

Exemplo:

Um usuário de uma plataforma digital do ICTIM pode solicitar a portabilidade de seus dados para uma plataforma similar, de outro fornecedor.

Eliminação dos dados tratados com base no consentimento

O titular tem o direito de solicitar a eliminação de seus dados quando o tratamento tiver como base legal o seu consentimento, exceto nas hipóteses previstas no Art. 16 da LGPD, como:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Exemplo:

Um cidadão que consentiu com o uso de seus dados para receber informativos do ICTIM pode solicitar a eliminação desses dados, caso não deseje mais receber os comunicados.

Informação sobre as entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados

O titular tem o direito de obter do ICTIM informações sobre as entidades públicas e privadas com as quais seus dados foram compartilhados, incluindo a finalidade do compartilhamento. Essa medida garante a transparência sobre o fluxo dos dados e permite ao titular acompanhar o uso de suas informações por outras organizações.

Exemplo:

Um cidadão pode solicitar ao ICTIM informações sobre quais órgãos governamentais têm acesso aos seus dados, bem como a finalidade desse compartilhamento.

Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa

O titular tem o direito de ser informado sobre a possibilidade de não fornecer consentimento para o tratamento de seus dados, bem como sobre as consequências da negativa. O ICTIM deve esclarecer, de forma clara e objetiva, as implicações da recusa em consentir com o tratamento, sem exercer qualquer tipo de pressão ou coação sobre o titular.

Exemplo:

Ao solicitar o cadastro em um serviço do ICTIM, o cidadão deve ser informado sobre a possibilidade de recusar o fornecimento de seus dados e sobre as consequências dessa decisão, como a impossibilidade de utilizar o serviço.

Revogação do consentimento

O titular tem o direito de revogar o consentimento a qualquer momento, caso tenha autorizado o tratamento de seus dados com base nesta hipótese legal. A revogação deve ser facilitada pelo ICTIM, sem custos para o titular, e deve ter efeito imediato, interrompendo o tratamento dos dados.

Exemplo:

Um cidadão que consentiu com o uso de seus dados para receber informações sobre os projetos do ICTIM pode revogar o consentimento a qualquer momento, deixando de receber as mensagens.

Implementando os direitos dos titulares no ICTIM

A garantia dos direitos dos titulares de dados não é apenas uma obrigação legal para o ICTIM, mas também um elemento fundamental para construir uma relação de confiança com os cidadãos e usuários. Para assegurar o exercício efetivo desses direitos, o ICTIM deve adotar as seguintes medidas:

1. **Criar procedimentos claros e acessíveis:** O ICTIM deve desenvolver procedimentos internos detalhados, que orientem os colaboradores sobre como lidar com as solicitações dos titulares, garantindo a uniformidade e a eficiência no atendimento. Esses procedimentos devem ser documentados e disponibilizados aos colaboradores.

2. **Disponibilizar múltiplos canais de comunicação:** O ICTIM deve oferecer aos titulares diferentes formas de exercer seus direitos, como um formulário online em seu site institucional, um endereço de e-mail dedicado, ou um número de telefone exclusivo. É fundamental garantir a acessibilidade para todos os cidadãos, inclusive para pessoas com deficiência.

3. **Estabelecer prazos para resposta:** A LGPD prevê prazos para o atendimento das solicitações dos titulares. O ICTIM deve definir prazos internos ainda mais rigorosos, buscando responder às demandas com a maior agilidade possível.

4. **Treinar os colaboradores:** Todos os colaboradores do ICTIM que lidam com dados pessoais devem receber treinamento adequado sobre a LGPD e os direitos dos titulares. O treinamento garante que os colaboradores estejam aptos a atender as solicitações dos titulares de forma correta e eficiente.

5. **Monitorar e aprimorar os procedimentos:** O ICTIM deve monitorar constantemente a efetividade de seus procedimentos para garantir o atendimento

adequado aos direitos dos titulares. A partir da análise dos resultados, a instituição deve promover a melhoria contínua dos seus processos.

Ao implementar essas medidas, o ICTIM demonstra seu compromisso com a proteção de dados pessoais e a privacidade dos cidadãos e usuários, reforçando sua reputação como uma instituição confiável e ética. A garantia dos direitos dos titulares não é apenas uma questão de cumprimento legal, mas também um diferencial competitivo, que fortalece a imagem da instituição perante a sociedade.

6. BASES LEGAIS PARA O TRATAMENTO DE DADOS

A LGPD estabelece um conjunto de bases legais que autorizam o tratamento de dados pessoais. O tratamento somente é considerado lícito se fundamentado em, pelo menos, uma dessas bases, que visam a garantir a proteção dos direitos fundamentais dos titulares dos dados. As bases legais estão previstas nos artigos 7º, 11º e 23º da LGPD.

Todas as bases legais para tratamento de dados segundo a LGPD

- **Consentimento (art. 7º, I):** Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. O consentimento deve ser específico para cada finalidade e o titular deve ter a opção de aceitá-lo ou recusá-lo sem consequências negativas.

- **Cumprimento de obrigação legal ou regulatória (art. 7º, II):** O tratamento é necessário para o cumprimento de uma obrigação legal ou regulatória pelo controlador. Essa base legal se aplica quando a lei impõe ao controlador a obrigação de tratar dados pessoais.

- **Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (art. 7º, III):** O tratamento se justifica para a execução de políticas públicas, desde que previstas em lei ou regulamentos, ou respaldadas em instrumentos jurídicos.

- **Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (art. 7º, IV):** A LGPD permite o tratamento de dados para fins de pesquisa, desde que realizada por órgão de pesquisa e que a anonimização seja garantida sempre que possível.

- **Para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (art. 7º, V):** O tratamento é necessário para a execução de um contrato do qual o titular dos dados seja parte.

- **Para o exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, VI):** O tratamento se justifica para o exercício de direitos em processos judiciais, administrativos ou arbitrais.

- **Para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, VII):** A lei autoriza o tratamento de dados quando necessário para proteger a vida ou a integridade física do titular dos dados ou de terceiros.

- **Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 7º, VIII):** O tratamento é permitido para fins de tutela da saúde, em procedimentos realizados por profissionais e serviços de saúde, ou por autoridade sanitária.

- **Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 7º, IX):** O tratamento pode ser justificado pelo legítimo interesse do controlador ou de terceiros, desde que não prevaleçam direitos e liberdades do titular.

- **Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (art. 7º, X):** A lei prevê o tratamento de dados para proteção de crédito, observando a legislação específica sobre o tema.

Tratamento de dados sensíveis (art. 11)

O tratamento de **dados pessoais sensíveis**, como aqueles relacionados à origem racial ou étnica, convicção religiosa, opinião política, saúde ou vida sexual, somente poderá ocorrer em hipóteses específicas, como:

- **Havendo o consentimento específico e destacado do titular, para finalidades específicas (art. 11, I)**: É necessário o consentimento explícito do titular para o tratamento de seus dados sensíveis, sendo vedada a utilização de autorizações genéricas.

- **Sem fornecimento de consentimento pelo titular, nas hipóteses de**:
    - **Cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, II, a):** O tratamento é necessário para o cumprimento de uma obrigação imposta por lei ou regulamento.
    - **Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (art. 11, II, b):** É permitida a utilização de dados sensíveis para a execução de políticas públicas, desde que prevista em lei ou regulamento.

Bases legais mais relevantes para as atividades do ICTIM

1. **Consentimento:**

- **Definição**: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- **Aplicabilidade no ICTIM**: O consentimento pode ser utilizado para atividades como participação voluntária em pesquisas, com a opção de retirar o consentimento a qualquer momento, e recebimento de informativos ou comunicados, com a possibilidade de cancelar a assinatura.
- **Limitações no setor público**: A LGPD limita o uso do consentimento para tratamento de dados no setor público, especialmente quando o tratamento é necessário para o cumprimento de obrigações legais ou para a execução de políticas públicas.
- **Exigências da LGPD**: O consentimento deve ser:
    - **Livre:** O titular deve ter a opção de consentir ou não com o tratamento de seus dados, sem que haja consequências negativas em caso de recusa**.**
    - **Informado**: O titular deve receber informações claras e completas sobre as finalidades do tratamento, os tipos de dados coletados, os seus direitos e como exercê-los.
    - **Inequívoco:** O consentimento deve ser demonstrado por meio de uma ação afirmativa, que deixe clara a vontade do titular em relação ao tratamento de seus dados.

- **Específico:** O consentimento deve ser específico para cada finalidade do tratamento. Não é possível obter um consentimento genérico para diversas finalidades.
- **Destacado:** O consentimento deve ser apresentado de forma clara e destacada, de modo que o titular possa facilmente identificá-lo.

2. **Cumprimento de obrigação legal ou regulatória:**

- **Definição**: O tratamento é necessário para o cumprimento de uma obrigação legal ou regulatória pelo controlador.
- **Aplicabilidade no ICTIM**: Esta base legal se aplica a grande parte das atividades do ICTIM, visto que a instituição é regida por diversas leis e regulamentos, como a Lei nº 12.527/2011, Lei de Acesso à Informação (LAI) e a Lei nº 10.973/2004, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo.
- **Tipos de Normas**:
  - **Normas de Conduta:** Determinam como as pessoas devem se comportar em determinadas situações.

    Exemplo: leis que determinam a coleta de dados para fins específicos, como a emissão de documentos de identidade.
  - **Normas de Organização:** Definem a estrutura e o funcionamento de órgãos e entidades públicas.

    Exemplo: leis que definem as competências do ICTIM e exigem o tratamento de dados para o seu exercício.
- **Exemplos:**
  - Coleta de dados para fins de cadastro de servidores, conforme previsto em lei.
  - Compartilhamento de dados com órgãos de controle, em cumprimento a obrigações legais.
  - Divulgação de informações sobre a remuneração de servidores públicos, conforme previsto na Lei de Acesso à Informação (LAI).

3. **Execução de políticas públicas:**

- **Definição**: O tratamento é necessário para a execução de políticas públicas previstas em leis e regulamentos ou

respaldadas em contratos, convênios ou instrumentos congêneres.

- **Aplicabilidade no ICTIM**: O ICTIM realiza diversas atividades de pesquisa e desenvolvimento em áreas estratégicas para o Município de Maricá, que se enquadram nesta base legal. Essas atividades podem estar relacionadas a áreas como saúde, educação, desenvolvimento social e sustentável, tecnologia e inovação, meio ambiente, trabalho e renda.
- **Requisitos da LGPD:**
  - **Previsão em lei ou regulamento:** A política pública deve estar prevista em lei ou regulamento, ou respaldada em outros instrumentos jurídicos, como contratos, convênios ou acordos de cooperação.
  - **Finalidade pública:** O tratamento de dados deve ser necessário para a execução da política pública, visando ao atendimento do interesse público.
  - **Vinculação clara:** Deve haver uma vinculação clara entre o tratamento de dados e a execução da política pública, demonstrando a sua necessidade e adequação.
  - **Observância dos princípios da LGPD:** O tratamento de dados deve ser realizado em conformidade com os princípios da LGPD, como finalidade, adequação, necessidade, transparência e segurança.
- **Exemplos:**
  - Tratamento de dados para realização de estudos sobre a qualidade da água no município, em consonância com uma política pública de saneamento básico.
  - Compartilhamento de dados com outras instituições para implementação de um programa de desenvolvimento social, previsto em convênio.
  - Coleta de dados de saúde para fins de vigilância epidemiológica e controle de doenças, em conformidade com políticas públicas de saúde, como foi com a Pesquisa Sentinela Covid-19 Maricá, que foi realizada entre 2020 e 2022.

4. **Realização de estudos por órgão de pesquisa:**

- **Definição**: O tratamento é necessário para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
- **Aplicabilidade no ICTIM**: Esta base legal é fundamental para as atividades de pesquisa científica e tecnológica do ICTIM, especialmente em áreas como saúde pública, desenvolvimento de novas tecnologias e análise de dados socioeconômicos.
- **Requisitos da LGPD:**
    - **Órgão de pesquisa:** O tratamento deve ser realizado por um órgão ou entidade que tenha como finalidade a realização de pesquisas, como universidades, institutos de pesquisa e centros de desenvolvimento tecnológico.
    - **Finalidade de pesquisa:** O tratamento de dados deve ser necessário para a realização de estudos científicos, históricos, tecnológicos ou estatísticos.
    - **Anonimização:** A LGPD exige que os dados pessoais sejam anonimizados sempre que possível, de modo a proteger a identidade dos indivíduos.
    - **Medidas de segurança:** Nos casos em que a anonimização não for possível, devem ser implementadas medidas de segurança adicionais para proteger os dados pessoais.
- **Exemplos:**
    - Realização de pesquisas epidemiológicas com dados anonimizados de pacientes.
    - Desenvolvimento de modelos estatísticos para análise de indicadores socioeconômicos, com a garantia de que os dados individuais não sejam identificáveis.
    - Coleta de dados para pesquisas sobre a percepção da população em relação a políticas públicas, com a garantia de anonimato dos participantes.

É importante ressaltar que a escolha da base legal deve ser criteriosa e bem documentada, considerando as especificidades de cada atividade de tratamento de dados realizada pelo ICTIM. A documentação da base legal utilizada demonstra a conformidade com a LGPD e garante a proteção dos dados pessoais.

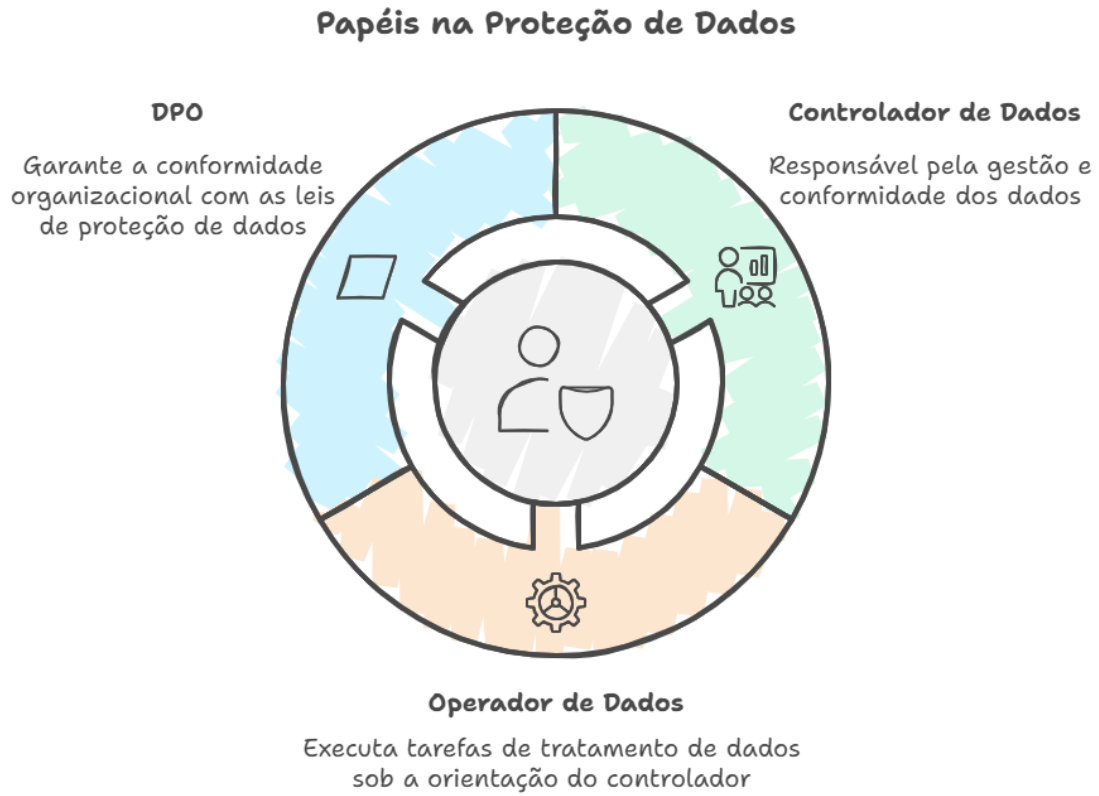
Boas práticas para a escolha da base legal: Plano de adequação

1. Realizar um mapeamento de todas as atividades de tratamento de dados realizadas pelo ICTIM, tanto internamente quanto externamente.
2. Analisar cuidadosamente as finalidades, os tipos de dados tratados e os riscos envolvidos em cada atividade.
3. Consultar a legislação e a jurisprudência para verificar as interpretações e as orientações sobre as bases legais.
4. Documentar a base legal escolhida para cada atividade de tratamento, justificando a sua adequação à LGPD.
5. Implementar medidas de segurança e governança para garantir a proteção dos dados pessoais.

A correta aplicação das bases legais é fundamental para o ICTIM garantir a conformidade com a LGPD, proteger os direitos dos titulares de dados e promover a confiança dos órgãos de controle e da sociedade em suas atividades.

7. AGENTES DE TRATAMENTO E O PAPEL DO DPO

A Lei Geral de Proteção de Dados Pessoais (LGPD) define claramente as responsabilidades dos agentes de tratamento de dados, o **controlador** e o **operador**, com o ***objetivo de garantir a proteção dos dados pessoais***. O texto fornecido destaca o caso do ICTIM, mas as responsabilidades se aplicam a qualquer organização que lida com dados pessoais.



Responsabilidades do Controlador

O Controlador, no caso o ICTIM, determina as finalidades e os meios de tratamento dos dados pessoais. Ele decide quais dados serão coletados, para que serão usados, como serão processados e por **quanto tempo serão armazenados (ver Portaria SMA nº 001/2024)**. Isso significa que o ICTIM tem a responsabilidade de:

- **Definir a base legal para o tratamento de dados**: O ICTIM deve identificar e documentar a justificativa legal para cada atividade de tratamento de dados. As bases legais mais comuns no contexto da administração pública são: (i) **cumprimento de obrigação legal ou regulatória, (ii) execução de políticas públicas e (iii) legítimo interesse,** em casos específicos e com a devida justificativa.

- **Implementar políticas de privacidade e segurança da informação**: O ICTIM deve elaborar e divulgar políticas claras e transparentes que informem aos **titulares dos dados** como seus

dados serão tratados e protegidos. Essas políticas devem ser revisadas e atualizadas periodicamente.

- **Nomear um Encarregado de Dados Pessoais**: O ICTIM deve designar um indivíduo ou equipe responsável por supervisionar a conformidade com a LGPD, atuar como ponto de contato entre o ICTIM, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Ação realizada por meio da Portaria nº 86, de 22 de outubro de 2024.

- **Obter consentimento, quando necessário**: Se o tratamento de dados pessoais pelo ICTIM se basear no consentimento, ele deve garantir que o consentimento seja livre, informado e inequívoco. O ICTIM também deve fornecer aos titulares dos dados a opção de revogar o consentimento a qualquer momento.

- **Garantir a segurança dos dados pessoais**: O ICTIM deve implementar medidas de **segurança técnicas e administrativas** apropriadas para *proteger os dados pessoais contra acesso não autorizado, perda, alteração ou divulgação*. Isso inclui medidas como **criptografia, controle de acesso, backups e treinamento de funcionários**.

- **Formalizar a relação com os operadores**: O ICTIM deve estabelecer contratos com seus operadores (fornecedores e prestadores de serviços) que definam claramente as responsabilidades de cada parte em relação à proteção de dados pessoais. Esses contratos devem garantir que o operador atenda aos requisitos da LGPD e às instruções do controlador.

- **Responder a incidentes de segurança**: O ICTIM deve ter um plano de resposta a incidentes de segurança para lidar com violações de dados pessoais. Esse plano deve incluir medidas para conter o incidente, investigar as causas, notificar a ANPD e os titulares dos dados afetados.

Responsabilidades do Operador

O operador, quando contratado pelo ICTIM, caso realize tratamento de dados pessoais em nome do controlador, não poderá usar os dados para qualquer outra finalidade além daquela determinada pelo controlador. As principais responsabilidades do operador incluem:

- **Seguir as instruções do controlador**: O operador deve realizar o tratamento de dados pessoais apenas de acordo com as instruções do ICTIM, garantindo que suas ações estejam

alinhadas com a base legal e as políticas de privacidade estabelecidas pelo controlador.

- **Implementar medidas de segurança**: O operador deve adotar medidas de segurança adequadas para proteger os dados pessoais contra acesso não autorizado, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Essas medidas devem ser proporcionais aos riscos envolvidos no tratamento dos dados.
- **Auxiliar o controlador no cumprimento da LGPD**: O operador deve cooperar com o ICTIM para garantir a conformidade com a LGPD, incluindo o fornecimento de informações relevantes sobre o tratamento de dados, a implementação de medidas de segurança e a resposta a incidentes de segurança.
- **Notificar o controlador sobre incidentes de segurança**: O operador deve notificar imediatamente o ICTIM sobre qualquer incidente de segurança que envolva os dados pessoais sob seu controle.
- **Manter registros das atividades de tratamento de dados**: O operador deve manter registros detalhados de todas as suas atividades de tratamento de dados pessoais, incluindo a finalidade do tratamento, a base legal, as categorias de dados processados e as medidas de segurança implementadas.

Responsabilidade solidária e contratos

A LGPD define que a responsabilidade em relação à proteção de dados pessoais é **solidária** entre o controlador e o operador. Isso significa que ambos podem ser responsabilizados por danos causados a titulares de dados em caso de violação à LGPD.

A formalização da relação entre o ICTIM e seus operadores por meio de contratos é crucial para delimitar as responsabilidades de cada parte e garantir a conformidade com a LGPD. Os contratos devem ser claros, detalhados e abordar os seguintes aspectos:

- Objeto e finalidade do tratamento de dados
- Base legal para o tratamento de dados
- Categorias de dados pessoais processados
- Obrigações e responsabilidades do controlador e do operador
- Medidas de segurança implementadas pelo operador

- Procedimentos para notificação e resposta a incidentes de segurança
- Duração do tratamento e procedimentos para eliminação dos dados

Em resumo, a LGPD define responsabilidades específicas para o controlador (ICTIM) e o operador, ambos com o dever de garantir a proteção dos dados pessoais. A formalização da relação entre as partes por meio de contratos detalhados é fundamental para delimitar responsabilidades, garantir a conformidade com a lei e proteger os direitos dos titulares dos dados.

Responsabilidades do Encarregado pelo Tratamento de Dados Pessoais (DPO)

O Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO), conforme definido na Lei Geral de Proteção de Dados Pessoais (LGPD), desempenha um papel crucial na garantia da conformidade de uma organização com a lei. Ele atua como um elo entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). As responsabilidades do DPO são abrangentes e exigem conhecimento técnico e jurídico da LGPD e das políticas internas da organização, tais quais:

- **Ponto de contato:** O DPO atua como o principal ponto de contato para titulares de dados que desejam exercer seus direitos em relação aos seus dados pessoais, como acesso, correção, portabilidade e exclusão. O DPO também deve receber e responder a solicitações da ANPD.
- **Orientação e supervisão:** O DPO é responsável por orientar os funcionários e contratados da organização sobre as práticas de proteção de dados e as obrigações da LGPD. Ele deve supervisionar a implementação e o cumprimento das políticas de privacidade e segurança da informação da organização.
- **Conscientização e treinamento:** O DPO deve promover a conscientização sobre a LGPD dentro da organização, conduzindo treinamentos e workshops para garantir que todos os funcionários estejam cientes de suas responsabilidades em relação à proteção de dados.
- **Elaboração e implementação de políticas:** O DPO desempenha um papel fundamental na elaboração e implementação das políticas de privacidade e segurança da informação, incluindo a política de privacidade, a política de segurança da informação, o plano de resposta a incidentes e os procedimentos para o exercício dos direitos dos titulares dos dados.

- **Mapeamento e gestão de dados:** O DPO deve auxiliar na identificação e mapeamento dos dados pessoais tratados pela organização, bem como na avaliação dos riscos associados a cada atividade de tratamento. Ele deve garantir que os dados pessoais sejam tratados de forma lícita, justa e transparente, em conformidade com os princípios da LGPD.
- **Análise de impacto à privacidade:** O DPO deve conduzir Análises de Impacto à Privacidade (RIPD) para avaliar os riscos à privacidade de novas tecnologias, sistemas ou processos que envolvam o tratamento de dados pessoais. O RIPD é um documento que identifica e avalia os riscos à privacidade e propõe medidas para mitigá-los.
- **Gerenciamento de incidentes de segurança:** O DPO deve supervisionar a gestão de incidentes de segurança que envolvam dados pessoais, incluindo a investigação, a notificação à ANPD e aos titulares de dados afetados e a implementação de medidas corretivas.
- **Comunicação com a ANPD:** O DPO é responsável por manter contato com a ANPD, respondendo a consultas, relatando incidentes de segurança e fornecendo informações sobre as atividades de tratamento de dados da organização.
- **Monitoramento e revisão:** O DPO deve monitorar continuamente a conformidade da organização com a LGPD, revisando as políticas e os procedimentos, avaliando a efetividade das medidas de segurança e propondo melhorias.

Requisitos de qualificação

O Encarregado pelo Tratamento de Dados Pessoais (DPO) precisa ter conhecimento técnico e jurídico sobre a LGPD, incluindo as melhores práticas de proteção de dados. A experiência em segurança da informação e privacidade também é crucial para que ele consiga desempenhar suas funções de forma eficiente. No contexto da administração pública, o DPO idealmente deve ser lotado em um órgão ou secretaria com expertise em tecnologia da informação.

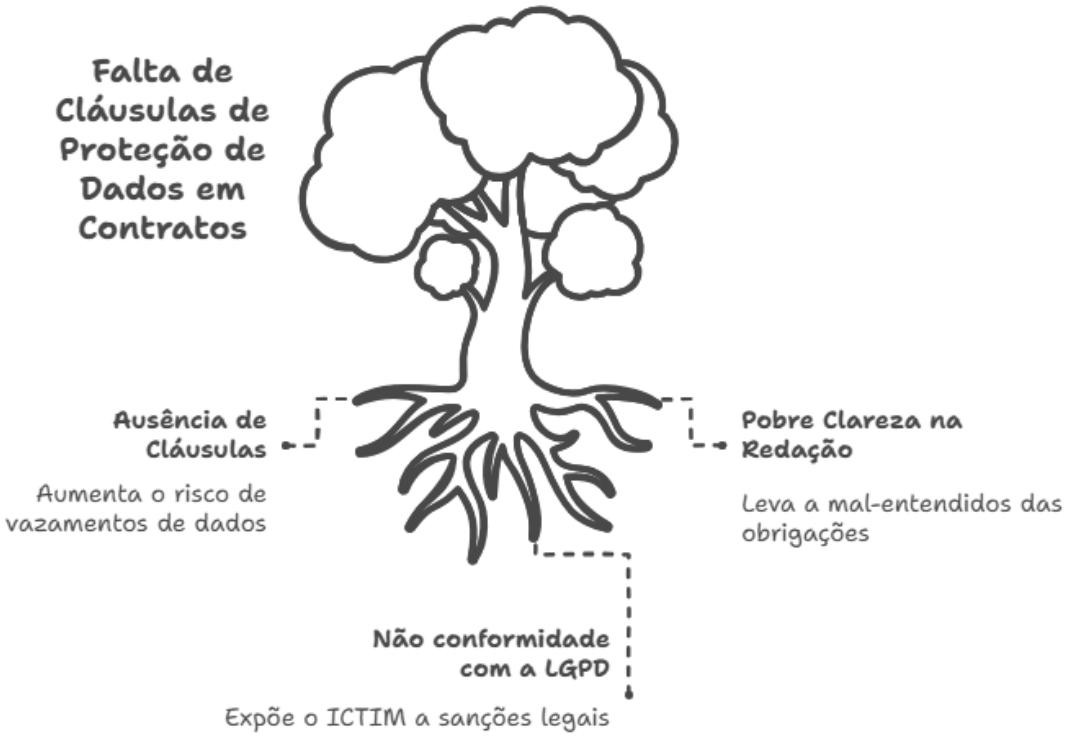
Importância da Independência e autonomia

O DPO deve ter autonomia para exercer suas funções sem interferências e pressões indevidas. Essa independência é fundamental para que ele possa atuar de forma imparcial e efetiva na proteção dos dados pessoais, garantindo a conformidade da instituição com a LGPD. O DPO deve ter acesso direto à alta administração para reportar suas atividades e recomendações, sem

intermediários. Isso garante que suas observações e alertas cheguem aos níveis mais altos de gestão, possibilitando ações corretivas e preventivas mais eficazes.

8. CLÁUSULAS DE PROTEÇÃO DE DADOS EM CONTRATOS

A inclusão de cláusulas específicas de proteção de dados em contratos com terceiros é essencial para garantir a conformidade do ICTIM com a LGPD. Essas cláusulas delimitam as responsabilidades do controlador (ICTIM) e do operador (fornecedor/prestador de serviço), definindo obrigações claras para a proteção dos dados pessoais durante todo o ciclo de vida do contrato. A ausência de tais cláusulas pode expor o ICTIM a riscos de vazamento de dados e às sanções previstas na LGPD.



É crucial que as cláusulas sejam redigidas de forma clara, concisa e abrangente, utilizando linguagem juridicamente precisa e acessível aos envolvidos. A seguir, detalhamos os aspectos que devem ser abordados nas cláusulas de proteção de dados:

Definição de termos e papéis

- **Controlador e Operador:** Definir claramente o papel do ICTIM como controlador e do fornecedor como operador de dados, estabelecendo os limites de responsabilidade de cada parte.

- **Dados pessoais:** Delimitar as categorias de dados pessoais que serão objeto do tratamento, especificando se são dados pessoais sensíveis ou não.
- **Finalidade do tratamento:** Indicar de forma precisa e detalhada as finalidades para as quais os dados pessoais serão tratados pelo operador, com base nas instruções do controlador.
- **Base legal:** Definir a base legal que autoriza o tratamento dos dados pessoais, justificando sua escolha e demonstrando a conformidade com a LGPD.

Obrigações do Operador

- **Confidencialidade:** Estabelecer a obrigação do operador de manter a confidencialidade dos dados pessoais, restringindo o acesso apenas aos funcionários autorizados e para as finalidades definidas no contrato.
- **Medidas de segurança:** Definir as medidas de segurança que o operador deve implementar para proteger os dados pessoais contra acessos não autorizados, perda, alteração ou qualquer forma de tratamento inadequado.
- **Subcontratação:** Regular a possibilidade de subcontratação de outros operadores pelo operador principal, exigindo que o ICTIM seja informado e que as mesmas obrigações de proteção de dados sejam aplicadas aos subcontratados.
- **Exercício dos direitos dos titulares:** Estabelecer procedimentos para que o operador auxilie o controlador no atendimento aos titulares de dados que desejam exercer seus direitos, como acesso, correção, exclusão e portabilidade dos dados.
- **Notificação de Incidentes de Segurança:** Definir a obrigação do operador de notificar o controlador imediatamente em caso de qualquer incidente de segurança que envolva os dados pessoais, fornecendo todas as informações relevantes para a investigação e a comunicação aos titulares e à ANPD.
- **Eliminação ou devolução dos dados:** Definir as condições para a eliminação ou devolução dos dados pessoais ao término do contrato, garantindo que os dados sejam apagados de forma segura e irreversível, ou devolvidos ao controlador.

Responsabilidades do Controlador

- **Instruções claras e precisas:** Fornecer ao operador instruções claras e precisas sobre o tratamento dos dados pessoais, definindo a finalidade, os meios e as medidas de segurança a serem adotadas.
- **Monitoramento e fiscalização:** Monitorar o cumprimento das obrigações do operador, realizando auditorias e solicitando relatórios periódicos sobre as medidas de segurança implementadas e os incidentes de segurança ocorridos.
- **Responsabilidade solidária:** Assumir a responsabilidade solidária com o operador em caso de descumprimento da LGPD, garantindo a reparação dos danos causados aos titulares de dados.

Disposições gerais

- **Jurisdição e legislação aplicável:** Definir a jurisdição e a legislação aplicável ao contrato, garantindo a aplicação da LGPD.
- **Alterações contratuais:** Prever a necessidade de revisão e atualização periódica das cláusulas de proteção de dados, para garantir a adequação às mudanças na legislação e às novas tecnologias.
- **Resolução de conflitos:** Definir os procedimentos para a resolução de conflitos entre as partes, priorizando a conciliação e a mediação.

Exemplos de cláusulas contratuais relativas à privacidade e proteção de dados pessoais em contratos administrativos

1. CLÁUSULA PRIMEIRA - DAS REGRAS APLICÁVEIS À PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

1.1. A CONTRATANTE se caracteriza por ser a controladora, a quem compete as decisões referentes ao tratamento de dados pessoais. A CONTRATADA se caracteriza como operadora, que realizará o tratamento de dados pessoais em nome da CONTRATANTE, seguindo as instruções fornecidas, observando as próprias instruções e normas sobre a matéria. (art. 5º, VI e VII, c/c art. 39, LGPD)

1.2. A CONTRATADA se compromete em seguir as normas relativas ao tratamento de dados pessoais, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD), regulamentações expedidas pela Autoridade Nacional de Proteção de Dados (ANPD) e pela Comissão Permanente Municipal de Proteção de Dados (CPMPD).

1.3. A CONTRATADA se compromete em seguir, no que couber, as orientações contidas nas normas ABNT NBR ISO/IEC 29151:2020 (código de prática para proteção de dados pessoais) e ABNT NBR ISO/IEC 27701:2019 (requisitos e fornecimento de diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação).

1.4. A CONTRATANTE indicará o encarregado pelo tratamento de dados pessoais, cujas informações para contato estarão disponíveis em seu site institucional https://ictim.com.br/lgpd/. (art. 23, III, e art. 41, LGPD)

1.5. A CONTRATADA deverá dar ciência à CONTRATANTE em caso de contrato com sub operador.

1.6. A CONTRATADA deve supervisionar os seus sub operadores e qualquer outra parte agindo em seu nome para que estes apenas realizem o tratamento de dados seguindo as instruções fornecidas por ela, assumindo responsabilidade integral por todos os atos e omissões do subcontratado, assim como pelos danos decorrentes, qualquer que seja sua natureza.

1.7. A CONTRATADA é responsável pela guarda de sigilo dos dados pessoais tratados ou por informações de cunho restrito ou confidencial que tenha acesso em decorrência da execução do contrato.

1.8. A CONTRATADA deve manter registro das operações de tratamento de dados pessoais que realizar. (art. 37, LGPD)

1.9. A CONTRATADA deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (caput, art. 46, LGPD)

1.10. A CONTRATADA é obrigada a reparar dano patrimonial, moral, individual ou coletivo que causar a outrem em razão do exercício de atividade de tratamento de dados pessoais, respondendo inclusive solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas da CONTRATANTE. (art. 42, LGPD)

1.11. A CONTRATADA, no âmbito de suas competências, deve formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (art. 50, LGPD)

1.12. A CONTRATADA deverá seguir as diretrizes do Programa de Governança em Privacidade, da Política de Privacidade, da Política de Segurança da

Informação e das regras de boas práticas da CONTRATANTE, que estão disponíveis no site institucional https://ictim.com.br/lgpd/.

1.13. A CONTRATADA se compromete em notificar/informar imediatamente à CONTRATANTE os casos de incidentes de segurança da informação que envolva o objeto deste contrato, podendo, a CONTRATANTE, acompanhar toda a fase de tratamento do incidente.

1.14. A CONTRATADA deve se atentar ao descarte seguro dos dados pessoais após o término de seu tratamento, autorizada a conservação nos termos da legislação vigente. (art. 15 e 16, LGPD)

1.15. A CONTRATADA se compromete em não compartilhar os dados pessoais com outras organizações ou pessoas sem autorização da CONTRATANTE, e nem a tratá-los de forma incompatível com as finalidades deste contrato. (art. 6º, I, LGPD)

1.16. A CONTRATANTE terá direito de monitorar, auditar, acompanhar e fiscalizar a conformidade da CONTRATADA, no que diz respeito à proteção de dados pessoais relativa à execução do contrato.

1.17. As PARTES darão conhecimento formal a seus empregados e colaboradores das obrigações e condições acordadas nesta cláusula. As diretrizes aqui estipuladas deverão ser aplicadas a toda e qualquer atividade que envolva a presente contratação.

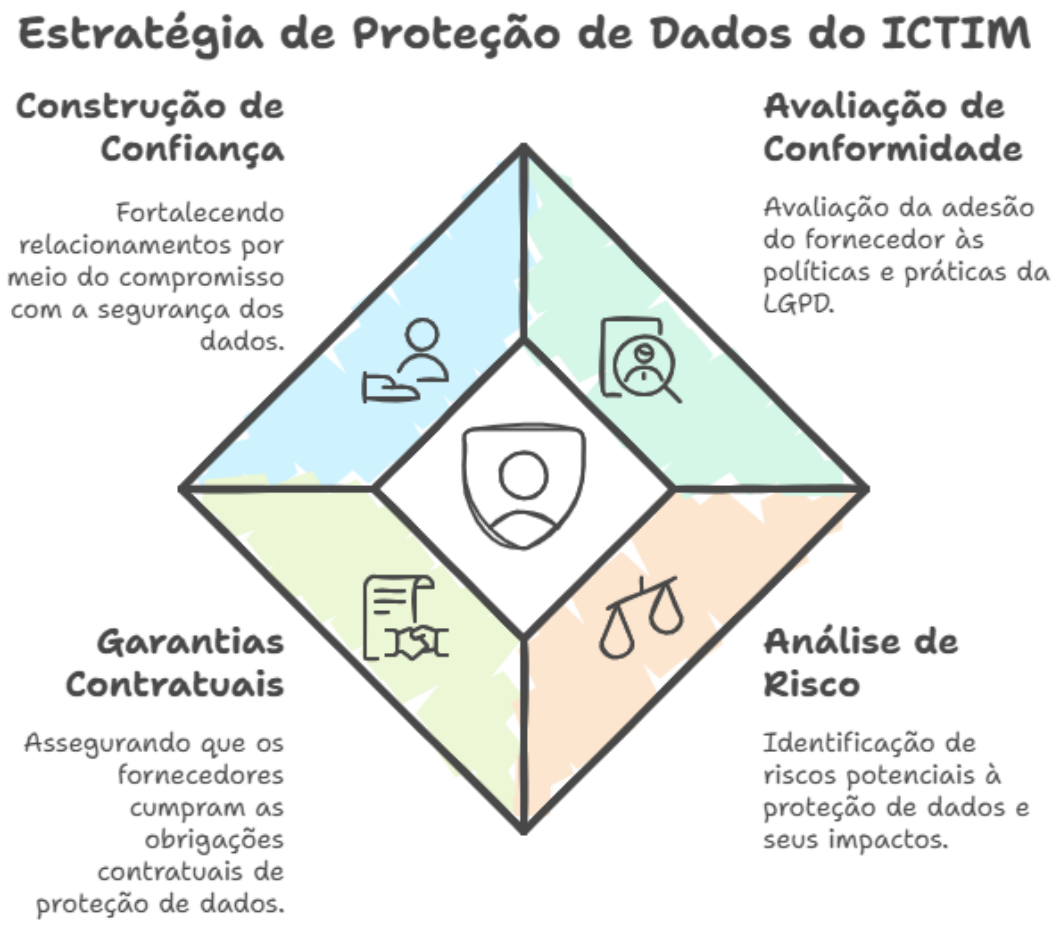
9. DUE DILIGENCE DE FORNECEDORES/PRESTADORES DE SERVIÇOS

A due diligence de fornecedores é uma etapa fundamental para garantir a conformidade com a LGPD e proteger os dados pessoais sob a responsabilidade do ICTIM. Trata-se de um processo de investigação e avaliação minuciosa dos fornecedores e prestadores de serviços que irão ter acesso a dados pessoais, com o objetivo de verificar se eles possuem as condições técnicas e organizacionais para garantir a segurança dos dados e cumprir com as demais obrigações previstas na LGPD.

A due diligence deve ser realizada antes da contratação do fornecedor, e deve ser atualizada periodicamente, para acompanhar as mudanças na legislação e nas práticas de proteção de dados do fornecedor e do prestador de serviço.

O principal objetivo da due diligence é mitigar os riscos relacionados à proteção de dados pessoais, assegurando que os fornecedores e prestadores de serviços do ICTIM estejam aptos a **tratar os dados de forma segura** e em conformidade com a LGPD.

A importância da due diligence reside na responsabilidade solidária entre o controlador (ICTIM) e o operador (fornecedor/prestador de serviço) estabelecida pela LGPD. Em caso de violação à LGPD por parte do fornecedor/prestador de serviço, o ICTIM também poderá ser responsabilizado, mesmo que a falha tenha ocorrido na operação do fornecedor/prestador de serviço.



A Due Diligence busca

- **Avaliar a conformidade do fornecedor/prestador de serviços com a LGPD:** Verificar se o fornecedor possui políticas de privacidade e segurança da informação adequadas à LGPD, se realiza o mapeamento de dados, se nomeou um Encarregado de Dados, se implementou medidas de segurança e se garante os direitos dos titulares.
- **Identificar e analisar os riscos relacionados à proteção de dados:** Avaliar a probabilidade e o impacto de potenciais incidentes de segurança, considerando a natureza dos dados

tratados, os sistemas e processos do fornecedor e as medidas de segurança implementadas.

- **Obter garantias de que o fornecedor/prestador de serviços irá cumprir com as obrigações contratuais:** Certificar-se de que o fornecedor/prestador de serviços possui as condições técnicas e organizacionais para cumprir com as cláusulas de proteção de dados estabelecidas no contrato.
- **Fortalecer a relação de confiança entre o ICTIM e seus fornecedores e prestadores de serviços:** Demonstrar o compromisso do ICTIM com a proteção de dados e fomentar uma cultura de segurança da informação em sua cadeia de fornecimento.

Etapas da Due Diligence de fornecedores e prestadores de serviços

O processo de due diligence de fornecedores pode variar de acordo com o tipo de serviço contratado, a sensibilidade dos dados tratados e o nível de risco envolvido. De forma geral, as seguintes etapas devem ser consideradas:

1. Planejamento e definição do escopo

- Definir os objetivos da due diligence, o escopo da avaliação e os critérios de análise.
- Identificar os fornecedores e prestadores de serviços que serão avaliados, priorizando aqueles que lidam com dados pessoais sensíveis ou que representam maior risco para a proteção de dados.

2. Coleta de informações

- Solicitar ao fornecedor/prestador de serviço documentação relevante, como políticas de privacidade e segurança da informação, relatórios de auditoria, certificações de segurança e contratos com subcontratados.
- Realizar questionários e entrevistas com os responsáveis pela proteção de dados no fornecedor/prestador de serviço, para aprofundar o entendimento de suas práticas e procedimentos.

3. Análise da documentação e das informações

- Verificar se as políticas e procedimentos do fornecedor/prestador de serviço estão em conformidade com a LGPD e com as melhores práticas de proteção de dados.

- Analisar as medidas de segurança implementadas pelo fornecedor/prestador de serviço, identificando potenciais vulnerabilidades e riscos.
- Avaliar a capacidade do fornecedor/prestador de serviço de responder a incidentes de segurança, verificando se ele possui um plano de resposta a incidentes e se realiza testes periódicos.

4. Elaboração de relatório e recomendações

- Documentar os resultados da due diligence em um relatório detalhado, incluindo as informações coletadas, as análises realizadas e as conclusões da avaliação.
- Elaborar recomendações para o ICTIM, indicando as medidas que devem ser adotadas para mitigar os riscos identificados, como a inclusão de cláusulas específicas no contrato, a exigência de certificações de segurança ou a realização de auditorias periódicas.

5. Acompanhamento e monitoramento

- Implementar as recomendações da due diligence, incorporando-as nas cláusulas contratuais e nos processos de gestão de fornecedores e prestadores de serviço.
- Realizar o acompanhamento periódico do fornecedor/prestador de serviço, verificando se ele continua cumprindo com as obrigações de proteção de dados.
- Atualizar a due diligence periodicamente, para garantir que ela continue relevante e eficaz.

Dicas para uma Due Diligence eficaz

- **Utilização de uma metodologia estruturada e documentada:** Isso garante que a due diligence seja completa e consistente, facilitando a análise dos resultados e o acompanhamento das ações corretivas.
- **Adaptação da due diligence às características do fornecedor/prestador de serviço:** Considere a natureza dos dados tratados, o tipo de serviço prestado e o nível de risco envolvido.
- **Comunique-se de forma clara e transparente com o fornecedor/prestador de serviço:** Explique os objetivos da due

diligence, os documentos que serão solicitados e as informações que serão avaliadas.

- **Envolvimento da equipe jurídica do ICTIM:** A assessoria jurídica é fundamental para a elaboração das cláusulas contratuais e para a interpretação da LGPD.
- **Mantenha a due diligence atualizada:** Acompanhe as mudanças na legislação e nas melhores práticas de proteção de dados, revisando e atualizando a due diligence periodicamente.

O Artigo 114, inciso V, do Decreto nº 840/2022 do município de Maricá, que regulamenta a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito municipal, determina a revisão e adequação dos contratos firmados pela administração pública à LGPD. Essa determinação visa garantir que os contratos celebrados pelo município, incluindo o ICTIM, estejam em consonância com as normas de proteção de dados e que as responsabilidades de cada parte, em relação ao tratamento de dados pessoais, estejam claramente definidas.

Benefícios da Due Diligence na Contratação de Fornecedores

- **Verificação da conformidade:** A due diligence permite analisar as políticas de privacidade, as medidas de segurança e os procedimentos de resposta a incidentes do fornecedor/prestador de serviço, garantindo que estejam adequados à LGPD.
- **Identificação de riscos:** A investigação possibilita identificar e analisar os riscos relacionados à proteção de dados, avaliando a probabilidade e o impacto de potenciais incidentes de segurança.
- **Fortalecimento da relação contratual:** A due diligence contribui para a elaboração de um contrato mais completo e seguro, incluindo cláusulas específicas de proteção de dados que definem as responsabilidades de cada parte.
- **Mitigação de responsabilidades:** Ao garantir a conformidade do fornecedor/prestador de serviço com a LGPD, o ICTIM minimiza os riscos de ser responsabilizado por falhas na proteção de dados.
- **Promoção da cultura de proteção de dados:** A due diligence demonstra o compromisso do ICTIM com a proteção de dados e incentiva seus fornecedores e prestadores de serviços a adotarem as melhores práticas de segurança da informação.

A revisão e adequação de contratos, em conjunto com a due diligence de fornecedores e prestadores de serviço, são etapas essenciais para o ICTIM garantir a conformidade com a LGPD e proteger os dados pessoais sob sua

responsabilidade. Ao adotar essas práticas, o ICTIM minimiza os riscos de incidentes de segurança, assegura o cumprimento da legislação e promove uma cultura de proteção de dados em sua cadeia de fornecedores.

10. A LGPD E O ICTIM: CONTEXTUALIZAÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) impacta diretamente as atividades do ICTIM, especialmente no contexto de projetos de pesquisa e inovação. É fundamental que o ICTIM compreenda e aplique corretamente os princípios da LGPD para garantir a proteção dos dados pessoais que coleta e processa.

Exemplos práticos de aplicação da LGPD no ICTIM

A aplicação da LGPD no ICTIM pode ser observada em diversos cenários, incluindo:

- **Projetos de pesquisa em saúde:** A coleta de dados pessoais sensíveis, como informações genéticas ou sobre condições de saúde, exige consentimento explícito dos participantes. O ICTIM deve informar os participantes sobre a finalidade da pesquisa, os tipos de dados coletados, as medidas de segurança adotadas e seus direitos como titulares de dados.
- **Banco de dados de pesquisadores:** A criação de um banco de dados para fomentar a colaboração em projetos de inovação requer transparência por parte do ICTIM. Os pesquisadores devem ser informados sobre a finalidade da coleta de dados, seus direitos como titulares e as medidas de segurança adotadas para proteger seus dados.
- **Plataforma online para compartilhamento de resultados de pesquisa:** A implementação de uma plataforma online exige medidas robustas de segurança, como criptografia e controle de acesso, para garantir a confidencialidade dos dados, especialmente aqueles protegidos por propriedade intelectual ou considerados sensíveis.

Desafios e áreas de atenção para o ICTIM

A aplicação da LGPD no contexto de pesquisa e inovação apresenta desafios específicos para o ICTIM, demandando atenção especial em algumas áreas:

- **Anonimização e Pseudonimização:** A anonimização, que remove completamente a identificação do titular dos dados, e a pseudonimização, que substitui informações identificáveis por

códigos ou outros meios, são técnicas importantes para proteger a privacidade dos indivíduos. No entanto, a aplicação dessas técnicas em conjuntos de dados complexos ou informações altamente identificáveis pode ser desafiadora, exigindo expertise técnica e cuidado na implementação.

Anonimização

A anonimização visa remover completamente a possibilidade de identificar o titular dos dados. Isso significa que os dados devem ser irreversivelmente dissociados do indivíduo, tornando a reidentificação impossível, mesmo com o uso de informações adicionais. O desafio reside em garantir a efetividade da anonimização, especialmente em conjuntos de dados complexos com alto poder de identificação.

Exemplo: Um estudo sobre doenças genéticas raras pode utilizar dados anonimizados de pacientes, removendo informações como nome, data de nascimento e endereço. No entanto, a combinação de informações genéticas específicas, histórico familiar e outras características clínicas pode levar à reidentificação do indivíduo, mesmo sem dados explicitamente identificadores.

Limites e riscos da anonimização:

- **Reidentificação por inferência:** A possibilidade de reidentificação por inferência é um risco significativo. A combinação de informações aparentemente inofensivas pode levar à identificação do indivíduo, especialmente com o uso de técnicas avançadas de análise de dados e a disponibilidade de grandes conjuntos de dados públicos.
- **Perda de utilidade dos dados:** A anonimização excessiva pode prejudicar a utilidade dos dados para pesquisa. A remoção de informações relevantes pode comprometer a qualidade da análise e a validade das conclusões do estudo.
- **Dificuldade de implementação:** A anonimização completa pode ser complexa e desafiadora do ponto de vista técnico, especialmente em conjuntos de dados com informações altamente sensíveis e interconectadas.

Pseudonimização

A pseudonimização substitui informações diretamente identificáveis por identificadores artificiais (pseudônimos), dificultando a identificação do titular sem o uso de informações adicionais mantidas separadamente pelo controlador. Essa técnica preserva a utilidade dos dados para pesquisa, ao mesmo tempo em que reduz os riscos à privacidade.

Exemplo: Um banco de dados de pesquisa pode substituir o nome dos participantes por códigos numéricos, mantendo a relação entre as informações coletadas. A chave para reidentificar os indivíduos é armazenada separadamente, com acesso restrito, e utilizada apenas em casos justificados.

Limites e riscos da pseudonimização:

- **Necessidade de gerenciamento adequado:** A pseudonimização exige o gerenciamento cuidadoso das chaves de reidentificação. Falhas na segurança ou no controle de acesso podem comprometer a privacidade dos indivíduos.

- **Possibilidade de reidentificação:** A reidentificação ainda é possível se as informações adicionais forem comprometidas ou se houver cruzamento com outras bases de dados.
- **Complexidade na implementação:** A implementação da pseudonimização exige expertise técnica para garantir a efetiva substituição dos identificadores e a proteção das informações adicionais.

Considerações importantes

A escolha entre anonimização e pseudonimização depende da natureza dos dados, da finalidade da pesquisa e dos riscos à privacidade envolvidos. A implementação dessas técnicas exige uma abordagem cuidadosa, considerando os desafios práticos e a necessidade de garantir a efetiva desidentificação dos dados em um ambiente tecnológico em constante evolução.

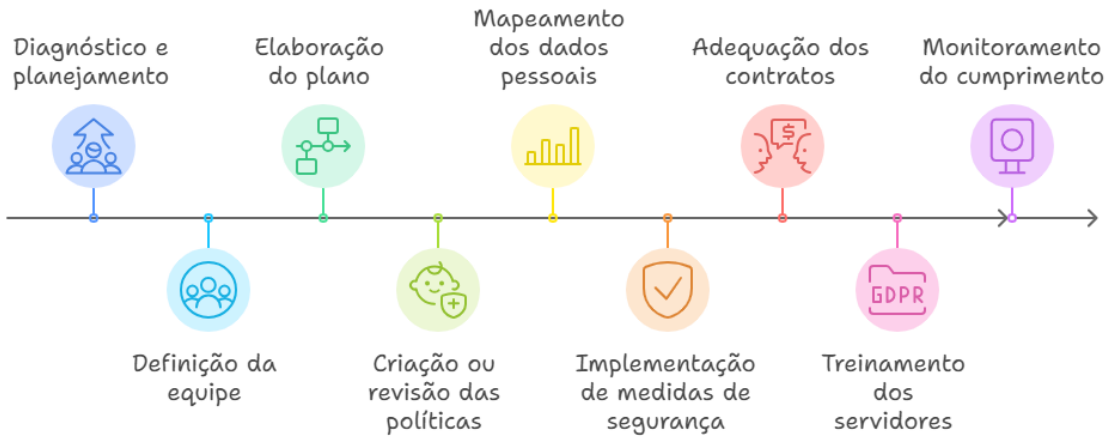
- **Tecnologia e inovação:** A rápida evolução tecnológica impõe ao ICTIM o desafio de se manter atualizado sobre as novas tecnologias e seus impactos na proteção de dados. O ICTIM deve adaptar continuamente suas medidas de segurança e práticas de governança, adotando soluções inovadoras para garantir a proteção dos dados pessoais em face de novas tecnologias e ameaças.
- **Cultura de proteção de dados:** É essencial promover uma cultura de proteção de dados entre os servidores do ICTIM. Isso envolve conscientização sobre a importância da LGPD, treinamento sobre boas práticas no tratamento de dados pessoais e a criação de mecanismos de responsabilização em caso de descumprimento das normas. A cultura de proteção de dados deve ser integrada aos processos e à rotina da instituição.

Aspectos práticos para implementação da LGPD no ICTIM

- **Fase 1: Diagnóstico e planejamento**
  - Realização de um diagnóstico da situação atual do ICTIM em relação à LGPD.
  - Definição da equipe responsável pela implementação da LGPD, conforme Portaria nº 86, de 22 de outubro de 2024.
  - Elaboração do plano de trabalho com prazos, metas e recursos.
- **Fase 2: Adequação**

- Criação ou revisão das políticas de privacidade e segurança da informação.
- Mapeamento dos dados pessoais tratados pelo ICTIM (inventário de dados).
- Implementação de medidas de segurança, técnicas e administrativas.
- Adequação dos contratos com operadores de dados.
- Treinamento dos servidores sobre a LGPD e as políticas internas.

- **Fase 3: Monitoramento e melhoria contínua**
  - Monitoramento do cumprimento da LGPD e das políticas internas.
  - Realização de auditorias periódicas para identificar riscos e oportunidades de melhoria.
  - Manter-se atualizado sobre as novas tecnologias e as melhores práticas em proteção de dados.



Checklists de conformidade

Checklists para auxiliar os servidores do ICTIM na verificação da conformidade com a LGPD em suas atividades, como:

- Checklist para coleta de dados pessoais.
- Checklist para tratamento de dados pessoais sensíveis.
- Checklist para compartilhamento de dados com terceiros.
- Checklist para transferência internacional de dados.

- Checklist para resposta a incidentes de segurança.

Documentos essenciais

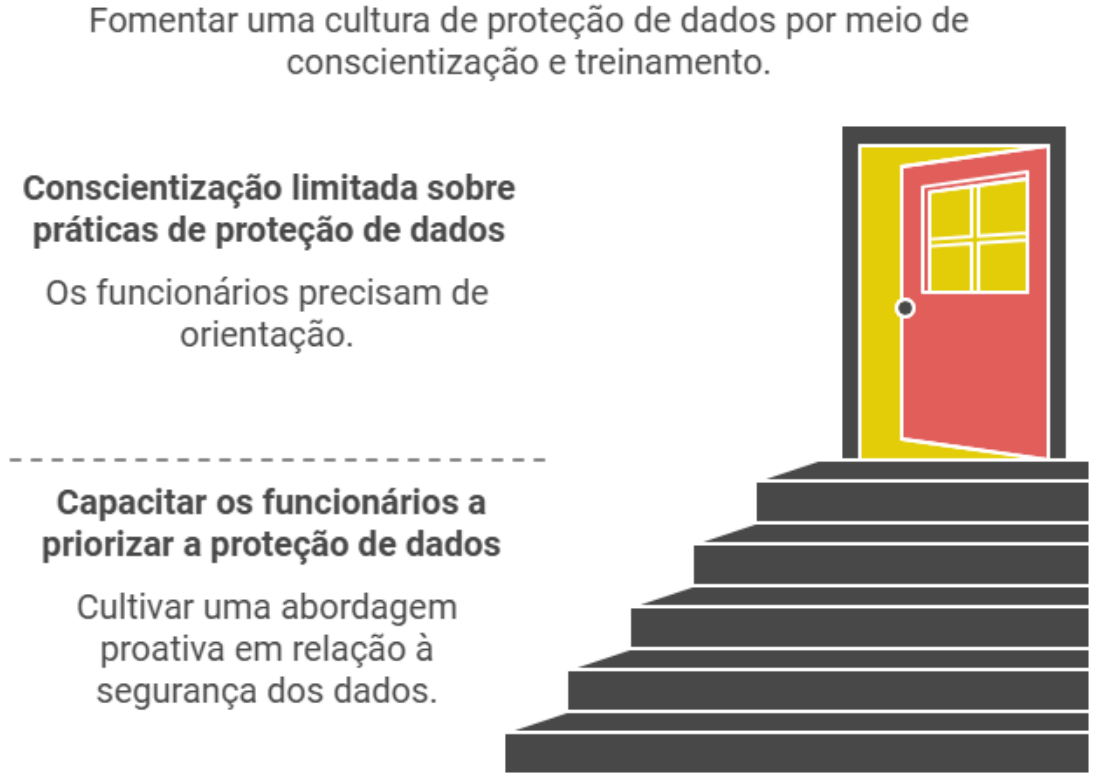
Documentos essenciais gerados a partir da implementação da LGPD no ICTIM:

- Política de Privacidade.
- Política de Segurança da Informação (PSI).
- Termo de Consentimento.
- Contrato com Operador de Dados.
- Plano de Resposta a Incidentes.
- Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Estratégias para promover a cultura de proteção de dados:

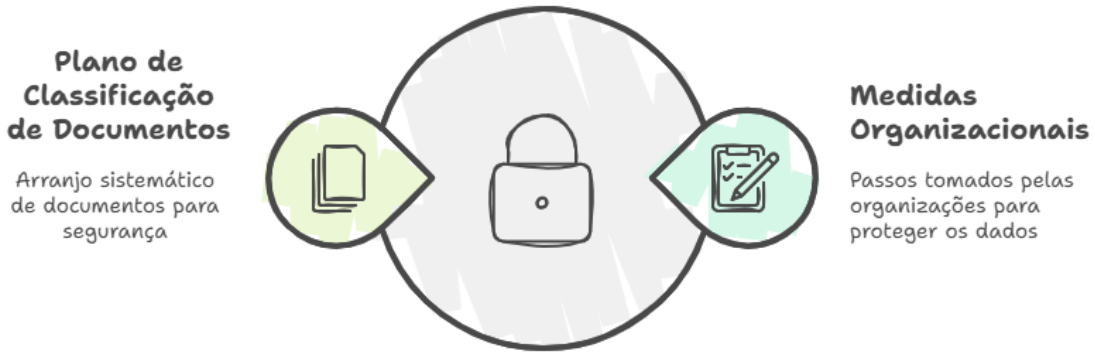
- **Comunicação interna:** Criação de campanhas de comunicação interna para conscientizar os servidores sobre a importância da proteção de dados.
- **Treinamentos periódicos:** Oferecer treinamentos periódicos sobre a LGPD, as políticas internas e as boas práticas.
- **Canais de denúncia:** Estabelecer canais de denúncia para que os servidores possam relatar violações à LGPD.
- **Reconhecimento:** Reconhecer os servidores que se destacarem na proteção de dados.

A implementação da LGPD no ICTIM é um processo contínuo que requer o comprometimento de todos os servidores, embora desafiadora, é crucial para garantir a proteção dos dados pessoais, a privacidade dos cidadãos e a confiança do público na instituição. As medidas de segurança e boas práticas são essenciais para mitigar os riscos e promover uma cultura de proteção de dados. É fundamental que o ICTIM adote uma postura proativa, invista em um programa de governança em privacidade robusto e se mantenha atualizado sobre as melhores práticas e evoluções na área de proteção de dados.



11. PLANO DE CLASSIFICAÇÃO DE DOCUMENTOS

A LGPD exige que as organizações, incluindo órgãos públicos, implementem medidas eficazes para a gestão e proteção dos dados pessoais que tratam. Uma dessas medidas é a elaboração e implementação de um Plano de Classificação de Documentos.



O Plano de Classificação de Documentos é um instrumento que define critérios para a organização e categorização dos documentos de acordo com a sua natureza, conteúdo e relevância, incluindo aqueles que contêm dados pessoais. Ele estabelece regras para a identificação, armazenamento, acesso,

compartilhamento, retenção e descarte de documentos, de forma a garantir a segurança, a confidencialidade e a disponibilidade das informações.

No contexto da LGPD, o Plano de Classificação de Documentos é fundamental para:

- **Identificar e classificar os dados pessoais**: Permite determinar quais documentos contêm dados pessoais e qual a sua sensibilidade (dados pessoais, dados pessoais sensíveis, etc.), facilitando a aplicação das medidas de segurança adequadas.

- **Organizar e controlar o acesso aos dados pessoais**: Facilita o controle de acesso aos documentos que contêm dados pessoais, restringindo o acesso apenas aos indivíduos autorizados, conforme os princípios da LGPD.

- **Definir prazos de retenção e descarte**: Permite estabelecer critérios para a guarda e descarte de documentos, garantindo que os dados pessoais sejam eliminados de forma segura e em conformidade com a lei após o término da sua finalidade.

- **Atender aos direitos dos titulares dos dados**: Facilita o atendimento aos direitos dos titulares dos dados, como o acesso, a correção, a portabilidade e a eliminação dos seus dados pessoais.

A Prefeitura Municipal de Maricá, por meio da Portaria SMA Nº 001, de 02 de janeiro de 2024, estabeleceu seu próprio Plano de Classificação e a Tabela de Temporalidade e Destinação de Documentos das Atividades-Meio do Poder Executivo Municipal. Este documento é um exemplo da aplicação prática da gestão de documentos no contexto da LGPD.

É importante ressaltar que o Plano de Classificação de Documentos deve ser revisado e atualizado periodicamente para garantir a sua adequação às necessidades da organização e às mudanças na legislação, incluindo a LGPD.

12. GESTÃO DE INCIDENTES DE SEGURANÇA EM CONTRATOS

A gestão de incidentes de segurança em contratos com terceiros é uma parte crucial da conformidade com a LGPD e da proteção dos dados pessoais sob a responsabilidade do ICTIM. Mesmo com medidas preventivas robustas, incidentes de segurança podem ocorrer, e é essencial estar preparado para responder de forma rápida e eficaz, minimizando os danos e cumprindo com as obrigações legais.

Definição de incidente de segurança

A LGPD define incidente de segurança como qualquer evento que comprometa a segurança dos dados pessoais, como acesso não autorizado, perda, alteração, comunicação ou difusão indevida. Em relação aos contratos com terceiros, os incidentes podem ter origem nas atividades do operador ou de seus subcontratados, e podem afetar os dados pessoais que o ICTIM, como controlador, lhes confiou.

Importância da gestão de incidentes em contratos

A gestão adequada de incidentes em contratos com terceiros é crucial para:

- **Conter os danos e minimizar os impactos do incidente:** A resposta rápida e eficaz pode evitar que o incidente se agrave, limitando o acesso não autorizado aos dados, recuperando dados perdidos e mitigando os riscos para os titulares de dados.
- **Cumprir com as obrigações de notificação da LGPD:** A LGPD exige que o controlador notifique a ANPD e os titulares de dados afetados em caso de incidentes de segurança que possam acarretar risco ou dano relevante. A falha na notificação pode resultar em sanções e penalidades para o ICTIM.
- **Preservar a reputação e a confiança do ICTIM:** A resposta transparente e responsável aos incidentes demonstra o compromisso do ICTIM com a proteção de dados e a privacidade dos titulares, minimizando os impactos negativos na reputação da instituição.

- **Aprimorar os processos e as medidas de segurança:** A análise do incidente permite identificar as causas e as falhas que o permitiram, possibilitando a implementação de medidas corretivas para evitar que incidentes semelhantes ocorram no futuro.

Etapas da gestão de incidentes em contratos

O processo de gestão de incidentes em contratos deve ser claro, objetivo e estar integrado ao plano geral de resposta a incidentes do ICTIM. As seguintes etapas devem ser consideradas:

1. Prevenção e Preparo

- **Cláusulas contratuais:** Incluir cláusulas específicas de gestão de incidentes nos contratos com terceiros, definindo as obrigações do operador em caso de incidente, como a notificação imediata ao ICTIM, a colaboração na investigação, a adoção de medidas de contenção e a comunicação aos titulares afetados.
- **Due Diligence de fornecedores e prestadores de serviços:** Avaliar a capacidade do fornecedor/prestador de serviço de responder a incidentes de segurança durante o processo de due diligence, verificando se ele possui um plano de resposta a incidentes, se realiza testes periódicos e se tem uma equipe capacitada para lidar com incidentes.

2. Identificação e notificação

- **Notificação pelo Operador:** O operador deve notificar o ICTIM imediatamente em caso de suspeita ou confirmação de um incidente de segurança que envolva dados pessoais sob sua responsabilidade.
- **Triagem do incidente:** O ICTIM deve avaliar a gravidade do incidente, classificando-o de acordo com o tipo de dado afetado, o número de titulares envolvidos, o potencial de dano e os riscos para a reputação da instituição.

3. Contenção e investigação

- **Conter o incidente:** Adotar medidas imediatas para conter o incidente, limitando o acesso não autorizado aos dados, isolando os sistemas afetados e mitigando os riscos de propagação do incidente.
- **Investigar o incidente:** Realizar uma investigação minuciosa para determinar as causas do incidente, a extensão dos dados

afetados, os responsáveis pelo incidente e as medidas que devem ser adotadas para remediar a situação.

4. Comunicação e notificação

- **Comunicar à ANPD:** Notificar a ANPD sobre o incidente de segurança, fornecendo as informações exigidas pela LGPD, como a descrição do incidente, os dados afetados, as medidas de contenção adotadas e as medidas que serão tomadas para remediar a situação.
- **Comunicar aos titulares afetados:** Notificar os titulares de dados afetados pelo incidente, informando-os sobre o ocorrido, os dados afetados, os riscos potenciais e as medidas que estão sendo tomadas para proteger seus direitos.

5. Remediação e aprimoramento

- **Implementar medidas corretivas:** Adotar as medidas necessárias para remediar o incidente, corrigindo as falhas de segurança, recuperando dados perdidos, implementando medidas de segurança adicionais e reforçando os processos de gestão de incidentes.
- **Revisar e aprimorar os processos:** Analisar o incidente para identificar as causas e as falhas que o permitiram, implementando medidas preventivas para evitar que incidentes semelhantes ocorram no futuro.

Comunicação eficaz e transparente

A comunicação transparente e eficaz é fundamental durante todo o processo de gestão de incidentes. O ICTIM deve manter o operador informado sobre o andamento da investigação, as medidas que estão sendo tomadas e as decisões que foram tomadas em relação ao incidente.

Da mesma forma, a comunicação com os titulares de dados afetados deve ser clara, objetiva e em linguagem acessível, informando-os sobre os seus direitos e as medidas que podem tomar para se proteger.

Documentação e registro

É essencial documentar todo o processo de gestão de incidentes, desde a notificação inicial pelo operador até a implementação das medidas corretivas. A documentação deve incluir:

- Registro do incidente, com data, hora, descrição do incidente, dados afetados, pessoas envolvidas e medidas tomadas.
- Relatórios de investigação, com a análise das causas do incidente, a identificação dos responsáveis e as recomendações para a remediação.
- Registros das comunicações com a ANPD, os titulares afetados e outras partes interessadas.

A documentação completa e organizada facilita a análise dos incidentes, a identificação de tendências e a implementação de medidas preventivas.

Recursos e ferramentas

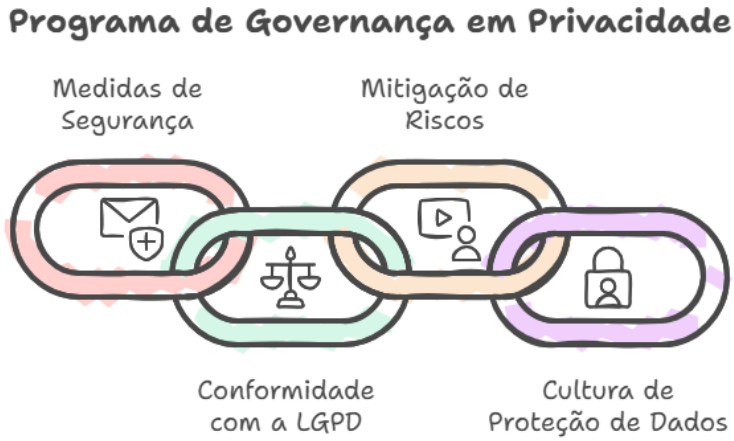
A gestão de incidentes em contratos com terceiros pode ser complexa e desafiadora, exigindo recursos e ferramentas adequadas. O ICTIM deve:

- **Definir responsabilidades:** Designar uma equipe ou um responsável pela gestão de incidentes em contratos, garantindo que ele tenha conhecimento da LGPD, das políticas internas e dos procedimentos de resposta a incidentes.
- **Implementar ferramentas de gestão de incidentes:** Utilizar ferramentas de software para registrar, rastrear, analisar e gerenciar incidentes de segurança, facilitando a comunicação, a colaboração e o acompanhamento das ações corretivas.
- **Realizar treinamentos:** Capacitar os servidores do ICTIM e os responsáveis pela proteção de dados nos fornecedores e prestadores de serviços sobre a gestão de incidentes, incluindo a identificação de incidentes, a notificação, a contenção, a investigação e a comunicação.

Ao implementar um processo estruturado e abrangente de gestão de incidentes de segurança em contratos, o ICTIM estará preparado para responder de forma eficaz aos incidentes, minimizando os danos, cumprindo com a LGPD e protegendo a privacidade dos titulares de dados.

13. MEDIDAS DE SEGURANÇA E BOAS PRÁTICAS

O ICTIM, como qualquer organização que lida com dados pessoais, precisa adotar medidas de segurança robustas para garantir a conformidade com a LGPD e proteger os direitos dos titulares dos dados. A implementação de um Programa de Governança em Privacidade abrangente é essencial para mitigar os riscos e promover uma cultura de proteção de dados na instituição.

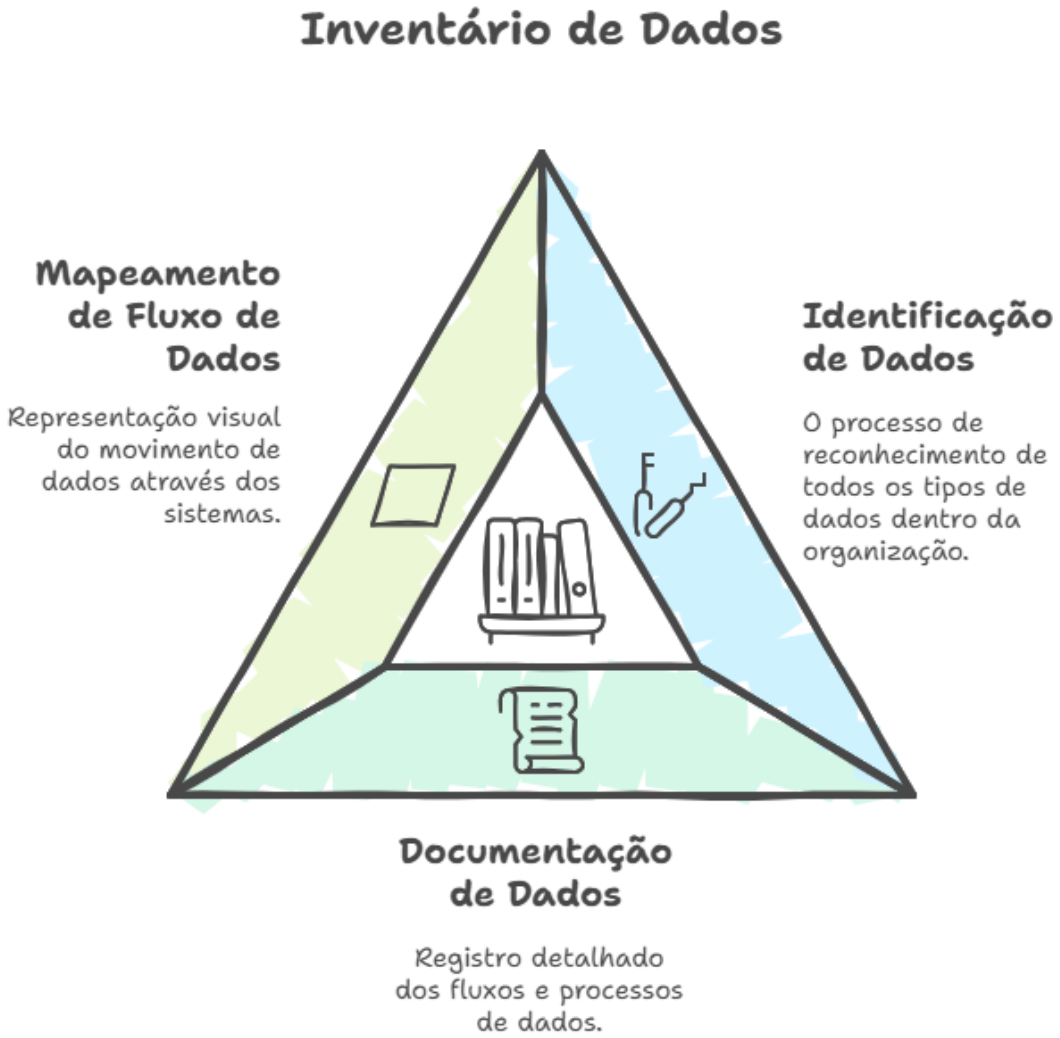


Inventário de dados

O inventário de dados, também conhecido como mapeamento de dados, é a base para um programa de governança em privacidade eficaz. Essa etapa crucial consiste em identificar todos os dados pessoais tratados pelo ICTIM, documentando detalhadamente cada fluxo de dados. As informações essenciais a serem registradas no inventário incluem:

- **Origem dos dados:** Como os dados pessoais foram coletados? (ex: formulários online, sistemas internos, etc.)
- **Categorias de dados:** Quais tipos de dados pessoais são tratados? (ex: nome, CPF, endereço, dados de saúde, etc.)
- **Finalidade do tratamento:** Para que os dados pessoais são utilizados? (ex: prestação de serviços, gestão de recursos humanos, etc.)
- **Base legal:** Qual a justificativa legal para o tratamento dos dados? (ex: consentimento, cumprimento de obrigação legal, etc.)
- **Prazos de armazenamento:** Por quanto tempo os dados pessoais serão armazenados?
- **Responsáveis pelo tratamento:** Quais setores e indivíduos dentro do ICTIM são responsáveis pelo tratamento dos dados?
- **Fluxos de dados:** Como os dados pessoais circulam dentro e fora do ICTIM? Quais sistemas e terceiros têm acesso aos dados?

Um inventário de dados completo permite ao ICTIM ter uma visão clara de como os dados pessoais são tratados, facilitando a identificação de riscos à privacidade e a implementação de medidas de segurança adequadas.



O ICTIM precisa elaborar e divulgar **políticas claras e transparentes** que informem aos titulares dos dados como seus dados pessoais serão tratados e protegidos.

Política de Privacidade

- Define os tipos de dados pessoais coletados, as finalidades do tratamento, as bases legais, os prazos de armazenamento e os direitos dos titulares.
- Esclarece como o ICTIM compartilha dados com terceiros, as medidas de segurança implementadas e os procedimentos para o exercício dos direitos dos titulares.
- Deve ser redigida em linguagem clara e acessível, disponibilizada em local de fácil acesso (ex: site do ICTIM).

Política de Segurança da Informação (PSI)

- Define as diretrizes e os procedimentos para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais tratados pelo ICTIM.
- Abrange medidas de segurança física (ex: controle de acesso às instalações) e lógica (ex: senhas, firewalls).
- Estabelece normas para o uso de dispositivos, softwares, redes e sistemas, definindo responsabilidades e procedimentos para lidar com incidentes de segurança.
- Deve ser revisada e atualizada periodicamente para acompanhar as mudanças tecnológicas e as novas ameaças.

Controle de acesso

O controle de acesso é fundamental para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais. O ICTIM deve implementar mecanismos de autenticação robustos para verificar a identidade dos usuários e restringir o acesso com base no princípio do menor privilégio, concedendo apenas o nível de acesso necessário para cada função. As medidas de controle de acesso incluem:

- **Senhas fortes:** Exigir o uso de senhas complexas, com combinação de letras maiúsculas e minúsculas, números e caracteres especiais.
- **Controle de acesso baseado em função:** Definir diferentes níveis de acesso para cada função, garantindo que os usuários só possam acessar os dados necessários para suas atividades.
- **Logs de acesso:** Registrar todas as tentativas de acesso aos sistemas e dados, permitindo a identificação de atividades suspeitas.
- **Gestão de Identidades e Acessos (IAM):** Soluções que centralizam o controle de acesso, simplificando a gestão de usuários e permissões.

Criptografia

A criptografia protege os dados pessoais transformando-os em um formato ilegível para pessoas não autorizadas. O ICTIM deve utilizar algoritmos criptográficos robustos para proteger os dados em repouso (armazenados em servidores e dispositivos) e em trânsito (transmitidos pela rede).

- **Criptografia de dados em repouso:** Proteger os dados armazenados em bancos de dados, arquivos e backups, utilizando criptografia de disco completo ou criptografia de arquivos seletivos.
- **Criptografia de dados em trânsito:** Proteger os dados transmitidos pela rede, utilizando protocolos de segurança como HTTPS, VPNs e TLS/SSL.

Backups

A realização de backups regulares é essencial para garantir a recuperação dos dados em caso de falha de hardware, ataque cibernético ou desastre natural. A norma para procedimentos de backup do ICTIM estabelece, dentre outras, o seguinte:

- A frequência dos backups, os dados a serem copiados e os procedimentos para a realização e a restauração dos backups.
- Armazenamento dos backups em local seguro, mantendo cópias em locais fisicamente separados dos sistemas principais, protegidos contra acesso não autorizado e desastres naturais.
- Realização de testes periódicos para garantir que os backups possam ser restaurados com sucesso em caso de necessidade.

Plano de Resposta a Incidentes

Apesar das medidas de segurança, incidentes de segurança podem ocorrer. O plano de resposta a incidentes define os procedimentos a serem seguidos em caso de violação de dados pessoais, com o objetivo de conter os danos, investigar as causas e garantir a comunicação transparente com os afetados. O plano deve:

- **Identificar os tipos de incidentes:** Definir os critérios para classificar os incidentes de segurança e determinar as ações a serem tomadas para cada tipo de incidente.
- **Estabelecer uma equipe de resposta:** Designar uma equipe responsável por coordenar as ações de resposta a incidentes.
- **Definir os procedimentos de contenção:** Descrever as medidas para isolar os sistemas afetados, impedir o acesso não autorizado e minimizar os danos.
- **Estabelecer os procedimentos de investigação:** Definir os métodos para coletar evidências, analisar as causas do incidente e identificar os responsáveis.

- **Definir os procedimentos de comunicação:** Estabelecer os protocolos para comunicar o incidente à ANPD, aos titulares de dados afetados e a outras partes interessadas, garantindo a transparência e a clareza das informações.

Treinamento dos Servidores

O fator humano é crucial para a segurança da informação. O ICTIM deve oferecer treinamentos regulares para seus servidores sobre a LGPD, as políticas internas e as boas práticas para a proteção de dados pessoais.

Os treinamentos devem abordar temas como:

- **Princípios da LGPD:** Conscientizar os servidores sobre os direitos dos titulares dos dados, os princípios da proteção de dados e as obrigações do ICTIM em relação à lei.
- **Políticas internas:** Apresentar as políticas de privacidade e segurança da informação, as normas de uso dos sistemas e os procedimentos para lidar com dados pessoais.
- **Boas práticas de segurança:** Ensinar os servidores a identificar e evitar ataques de phishing, criar senhas fortes, proteger dispositivos móveis, utilizar a internet com segurança e relatar incidentes de segurança.
- **Simulações de incidentes:** Realizar simulações para treinar os servidores a responder a diferentes tipos de incidentes de segurança.

Gestão de vulnerabilidades para a segurança de dados pessoais

A gestão de vulnerabilidades é um processo crucial para a proteção de dados pessoais, garantindo a confidencialidade, integridade e disponibilidade das informações. Em um ambiente tecnológico em constante evolução, com ameaças e riscos cada vez mais sofisticados, a identificação, análise, tratamento e monitoramento de vulnerabilidades são essenciais para evitar incidentes de segurança e proteger a privacidade dos cidadãos, sendo fundamental para:

- Proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
- Mitigar riscos à privacidade, incluindo a identificação e a correção de falhas de segurança em sistemas, softwares, hardwares e processos que envolvam o tratamento de dados pessoais.

- Garantir a conformidade com a LGPD, que exige a adoção de medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais.
- Preservar a confiança do público na instituição, demonstrando o compromisso com a proteção da privacidade dos cidadãos.

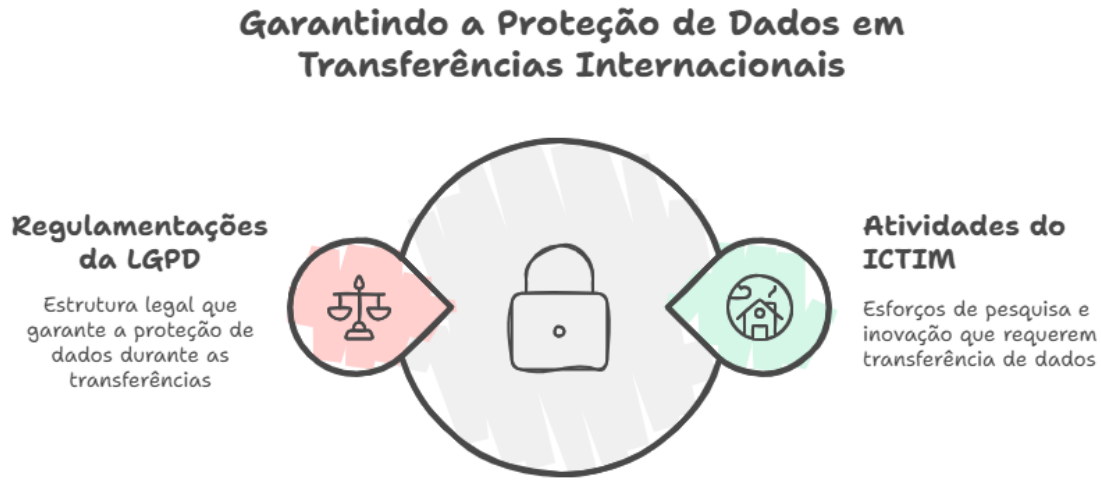
Etapas da Gestão de Vulnerabilidades

A gestão de vulnerabilidades é um processo cíclico que envolve as seguintes etapas:

1. **Identificação:** Consiste em identificar as vulnerabilidades existentes nos sistemas, softwares, hardwares e processos que envolvam o tratamento de dados pessoais. Essa etapa pode ser realizada por meio de varreduras automatizadas, testes de penetração, análises de código-fonte e auditorias de segurança.
2. **Análise:** Uma vez identificadas as vulnerabilidades, é necessário analisar a sua gravidade e o seu potencial de impacto para a segurança dos dados pessoais. Essa etapa envolve a classificação das vulnerabilidades de acordo com o seu nível de risco, utilizando critérios como a probabilidade de exploração, o impacto potencial e a complexidade da correção.
3. **Tratamento**: A etapa de tratamento consiste em corrigir as vulnerabilidades identificadas, implementando as medidas de segurança necessárias para proteger os dados pessoais. O tratamento pode envolver a atualização de softwares, a aplicação de patches de segurança, a reconfiguração de sistemas e a implementação de novas políticas e procedimentos de segurança.
4. **Monitoramento:** A gestão de vulnerabilidades é um processo contínuo que exige monitoramento constante para identificar novas vulnerabilidades e garantir que as medidas de segurança implementadas continuem eficazes. O monitoramento pode envolver a realização de varreduras periódicas, a análise de logs de segurança e o acompanhamento de alertas de segurança.

14. TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência internacional de dados, especialmente de dados pessoais, é um tema sensível e regulamentado pela LGPD no Brasil. O ICTIM, ao realizar pesquisas e atividades de inovação, pode se deparar com a necessidade de transferir dados para outros países ou organismos internacionais. No entanto, a LGPD impõe regras rigorosas para garantir a proteção dos dados pessoais mesmo quando transferidos para fora do território nacional.



Requisitos para transferência internacional de dados

A transferência internacional de dados pessoais somente é permitida em casos específicos, detalhados no Artigo 33 da LGPD. A lei busca garantir que os dados pessoais transferidos para outros países recebam um nível de proteção adequado, similar ao oferecido pela legislação brasileira.

As principais hipóteses que permitem a transferência internacional de dados pessoais são:

- **Países ou organismos internacionais com grau de proteção adequado:** A transferência é permitida para países ou organismos internacionais que ofereçam um nível de proteção de dados pessoais equivalente ao previsto na LGPD.
- **Garantias contratuais e mecanismos de proteção**: A transferência pode ocorrer se o controlador dos dados (no caso, o ICTIM) oferecer e comprovar garantias de cumprimento dos princípios, direitos do titular e regime de proteção da LGPD. Essas garantias podem ser demonstradas por meio de:
    - **Cláusulas contratuais específicas:** Acordos contratuais que estabeleçam obrigações específicas para a proteção dos dados transferidos.
    - **Cláusulas-padrão contratuais:** Modelos de cláusulas pré-aprovados pela ANPD, que garantem a proteção dos dados em transferências internacionais.
    - **Selos, certificados e códigos de conduta:** Reconhecimento formal de que a organização que recebe os dados atende a determinados requisitos de proteção de dados.

- **Outras hipóteses específicas:** A LGPD também prevê outras situações excepcionais que permitem a transferência internacional de dados, como:
    - **Cooperação jurídica internacional:** Transferências necessárias para a cooperação entre órgãos públicos de inteligência, investigação e persecução criminal, desde que em conformidade com acordos internacionais.
    - **Proteção da vida ou incolumidade física:** Transferências necessárias para proteger a vida ou a integridade física do titular dos dados ou de terceiros.
    - **Autorização da ANPD:** A transferência pode ser autorizada pela ANPD em casos específicos, mediante análise e aprovação prévia.
    - **Compromisso em acordo internacional:** Transferências previstas em acordos de cooperação internacional firmados pelo Brasil.
    - **Execução de política pública ou atribuição legal:** Transferências necessárias para a execução de políticas públicas ou cumprimento de obrigações legais, com a devida publicidade da operação.
    - **Consentimento específico e destacado:** O titular dos dados pode consentir, de forma livre, informada e inequívoca, com a transferência de seus dados para outro país, desde que a finalidade da transferência seja clara e destacada das demais finalidades do tratamento.

Avaliação da adequação do país ou organismo internacional

A LGPD exige que a transferência internacional de dados seja realizada apenas para países ou organismos internacionais que proporcionem um nível de proteção adequado aos dados pessoais. Para determinar a adequação, a ANPD pode realizar uma avaliação, considerando diversos fatores:

- **Legislação de proteção de dados:** A ANPD analisa as leis e regulamentações do país ou organismo internacional em relação à proteção de dados pessoais.
- **Natureza dos dados:** O tipo de dado pessoal a ser transferido é levado em consideração, sendo os dados sensíveis (como dados de saúde, origem racial, etc.) objeto de maior cuidado.

- **Princípios e direitos dos titulares:** A ANPD verifica se os princípios da LGPD, como finalidade, necessidade, transparência e segurança, são respeitados no país de destino, bem como se os direitos dos titulares de dados são garantidos.
- **Medidas de segurança:** A ANPD avalia as medidas de segurança adotadas pelo país ou organismo para proteger os dados pessoais contra acessos não autorizados e incidentes de segurança.
- **Garantias judiciais e institucionais:** A ANPD analisa se o país ou organismo possui mecanismos eficazes para garantir a proteção de dados pessoais, como a existência de uma autoridade de proteção de dados independente e a possibilidade de os titulares buscarem reparação judicial em caso de violações.

Papel do ICTIM e da ANPD

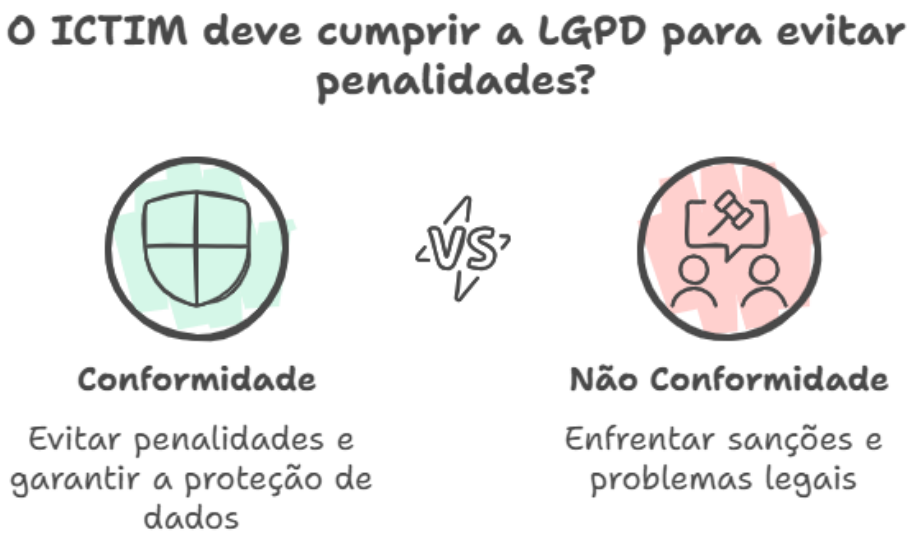
O ICTIM, como controlador dos dados, tem a responsabilidade de garantir a conformidade com a LGPD em todas as suas atividades de tratamento de dados, incluindo as transferências internacionais. É fundamental que o ICTIM:

- Realize o mapeamento de dados para identificar as transferências internacionais de dados pessoais.
- Avalie o nível de proteção oferecido pelo país ou organismo internacional, buscando informações junto à ANPD e consultando as decisões e pareceres da Autoridade sobre o tema.
- Implemente medidas de segurança e mecanismos de proteção adequados para garantir a proteção dos dados transferidos.
- Documente as transferências internacionais, mantendo registros das operações e das medidas de segurança adotadas.

Em caso de dúvidas sobre o nível de proteção oferecido por um país ou organismo internacional, o ICTIM pode requerer à ANPD uma avaliação formal, conforme previsto na LGPD. A ANPD, por sua vez, tem o papel de orientar, fiscalizar e aplicar sanções em caso de descumprimento da lei, atuando para garantir a proteção dos dados pessoais em transferências internacionais.

15. SANÇÕES E PENALIDADES

A LGPD estabelece um conjunto abrangente de regras e princípios para a proteção de dados pessoais, tanto no setor privado quanto no público. O descumprimento dessas normas pode acarretar sanções e penalidades significativas, incluindo para órgãos e entidades do poder público como o ICTIM.



Sanções e medidas disciplinares por descumprimento da LGPD no Município de Maricá

O Decreto Municipal nº 840/2022, que regulamenta a LGPD no Município de Maricá, estabelece em seu Artigo 27 a aplicação de medidas disciplinares aos servidores públicos municipais que descumprirem as normas de proteção de dados. O artigo prevê, ainda, a possibilidade de aplicação de sanções cíveis e penais, quando cabíveis.

> Art. 27. A não observância das normas e procedimentos constantes e/ou provenientes deste Decreto ensejará a aplicação das medidas disciplinares vigentes no Município de Maricá, além das cabíveis na esfera cível e penal, quando aplicáveis, bem como, as sanções e demais preceitos reparatórios na Lei Federal n. 13.709, de 2018.

Sanções e penalidades da LGPD

A Lei Federal nº 13.709/2018 (LGPD) prevê diversas sanções e penalidades para os casos de descumprimento da legislação, que variam de advertências a multas pesadas. É importante destacar que, embora o Decreto Municipal nº 840/2022 não determine a aplicação de multas para a administração pública municipal, as demais sanções previstas na LGPD podem ser aplicadas aos órgãos municipais e a seus servidores.

As sanções e penalidades aplicáveis a órgãos públicos como o ICTIM em caso de descumprimento da LGPD incluem:

- **Advertência com indicação de prazo para adoção de medidas corretivas:** É a primeira medida a ser aplicada pela Autoridade Nacional de Proteção de Dados (ANPD), alertando o órgão sobre a infração e estabelecendo um prazo para a regularização da situação.
- **Publicização da infração após confirmada a ocorrência:** A ANPD pode determinar a publicização da infração, tornando público o descumprimento da LGPD pelo ICTIM. Essa medida pode gerar grande repercussão negativa para a imagem da instituição.
- **Bloqueio dos dados pessoais até a regularização:** A ANPD pode determinar o bloqueio dos dados pessoais objeto da infração até que o ICTIM regularize a situação. Isso pode prejudicar a continuidade de serviços e atividades que dependam do tratamento dos dados bloqueados.
- **Eliminação dos dados pessoais relacionados à infração:** Em casos mais graves, a ANPD pode determinar a eliminação dos dados pessoais relacionados à infração, o que pode acarretar perda de informações importantes e dificuldades na prestação de serviços públicos.
- **Responsabilização do servidor público:** Além das sanções aplicáveis ao ICTIM como instituição, o servidor público responsável pela infração também pode ser responsabilizado administrativamente. As consequências para o servidor podem incluir advertência, suspensão, demissão, entre outras, dependendo da gravidade da falta.

A aplicação de qualquer uma dessas sanções pode ter um impacto significativo na reputação do ICTIM:

- **Perda de confiança dos cidadãos:** O descumprimento da LGPD pode levar à perda de confiança dos cidadãos na instituição, o que pode prejudicar a sua imagem e a sua capacidade de realizar suas atividades.
- **Dificuldade na obtenção de recursos:** A reputação negativa em relação à proteção de dados pode dificultar a obtenção de recursos financeiros e parcerias com outras instituições.
- **Aumento da fiscalização:** O ICTIM pode ser alvo de maior fiscalização por parte da ANPD e de outros órgãos de controle, o que pode resultar em maior burocracia e custos para a instituição.

Importância da conformidade com a LGPD

A conformidade com a LGPD no ICTIM é crucial para:

- Proteger os direitos fundamentais de liberdade e privacidade dos cidadãos e usuários.
- Preservar a reputação do ICTIM como uma instituição que preza pela ética e pela segurança da informação.
- Evitar a aplicação de sanções e penalidades, incluindo medidas disciplinares aos servidores.

A conscientização dos servidores sobre a importância da proteção de dados e as consequências do descumprimento da legislação é essencial para a construção de uma cultura de privacidade no ICTIM.

É importante ressaltar que, embora a **LGPD exclua a aplicação de multas simples ou diárias para órgãos públicos (Artigo 52, §3º)**, as penalidades previstas podem ter um impacto negativo considerável na reputação e na confiabilidade da instituição.

16. MODELOS DE TERMOS DE CONSENTIMENTO

MODELO ICTIM

Termo de Consentimento para Tratamento de Dados Pessoais

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

Introdução:

O Instituto de Ciência, Tecnologia e Inovação de Maricá (ICTIM), em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/18), solicita o seu consentimento para o tratamento de seus dados pessoais. Este formulário visa informá-lo sobre como seus dados serão coletados, utilizados, armazenados e protegidos pelo ICTIM.

1. Identificação do titular dos dados:

- Nome Completo:
- E-mail:

2. Dados coletados:

O ICTIM coletará os seguintes dados pessoais: (listar os dados específicos a serem coletados, por exemplo: nome, CPF, endereço, e-mail, telefone, dados de localização, etc.).

3. Finalidade do tratamento:

Seus dados pessoais serão utilizados para as seguintes finalidades: (especificar a finalidade do tratamento de forma clara e detalhada, por exemplo: participação em pesquisas, cadastro em eventos, recebimento de informativos, etc.).

4. Base legal para o tratamento:

A base legal para o tratamento de seus dados pessoais é o seu consentimento, conforme previsto no Art. 7º, I da LGPD. Você tem o direito de revogar este consentimento a qualquer momento, sem prejuízo para si.

5. Compartilhamento de dados:

Seus dados pessoais poderão ser compartilhados com: (especificar as entidades com as quais os dados poderão ser compartilhados e a finalidade do compartilhamento, por exemplo: instituições de pesquisa parceiras, órgãos governamentais, etc.). Asseguramos que o compartilhamento de dados será realizado apenas com base em lei ou com o seu consentimento específico.

6. Segurança dos dados:

O ICTIM se compromete a adotar medidas de segurança adequadas para proteger seus dados pessoais contra acesso não autorizado, uso indevido, alteração, divulgação ou destruição, em conformidade com o Art. 46 da LGPD. Essas medidas incluem: (listar as medidas de segurança implementadas pelo ICTIM, por exemplo: criptografia, controle de acesso, backups, etc.).

7. Retenção dos dados:

Seus dados pessoais serão armazenados pelo ICTIM pelo período necessário para cumprir com as finalidades descritas neste formulário e com as obrigações legais e regulatórias aplicáveis. Após esse período, seus dados serão eliminados de forma segura.

8. Direitos do titular dos dados:

A LGPD garante a você os seguintes direitos em relação aos seus dados pessoais:

- **Confirmação e acesso:** Confirmar a existência de tratamento de seus dados e solicitar acesso a eles.
- **Correção:** Solicitar a correção de dados incompletos, inexatos ou desatualizados.
- **Anonimização, bloqueio ou eliminação:** Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.

- **Portabilidade:** Solicitar a portabilidade de seus dados para outro fornecedor de serviço ou produto.
- **Eliminação:** Solicitar a eliminação de dados tratados com base no consentimento.
- **Informação:** Obter informações sobre as entidades com as quais seus dados foram compartilhados.
- **Oposição:** Opor-se ao tratamento de dados.
- **Revogação do consentimento:** Revogar o consentimento a qualquer momento.

Para exercer seus direitos, você pode entrar em contato com o Encarregado pelo Tratamento de Dados Pessoais do ICTIM por meio dos seguintes canais:

- E-mail: dpo@ictim.com.br

9. Consentimento:

Declaro que li e compreendi as informações contidas neste formulário e, por meio deste ato, **consinto** com o tratamento de meus dados pessoais pelo ICTIM para as finalidades aqui descritas.

Local e Data:

Assinatura do Titular dos Dados:

Observações:

- Este formulário de consentimento é específico para as atividades do ICTIM. Outras atividades que envolvam o tratamento de dados pessoais podem exigir formulários de consentimento específicos.
- O ICTIM se reserva o direito de atualizar este formulário de consentimento a qualquer momento, em conformidade com a legislação vigente.

MODELO PARA PROJETOS ESPECÍFICOS

Termo de Consentimento para Tratamento de Dados Pessoais

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

Eu, _____, declaro que estou ciente e concordo com o tratamento dos meus dados pessoais, fornecidos no questionário *[informar o tipo e o projeto vinculado]*, conforme descrito abaixo.

Finalidade do Tratamento:

Os dados pessoais fornecidos serão utilizados exclusivamente para a realização de uma pesquisa sobre *[informar a finalidade da pesquisa]*. Este procedimento está em conformidade com o Art. 6º, inciso I e II da Lei nº 13.709/2018, que estabelece a necessidade da finalidade específica e do consentimento do titular.

Necessidade do Tratamento:

Os dados solicitados, como nome completo, e-mail, idade, endereço, CEP, telefone, e informações sobre escolaridade, são essenciais para a coleta de informações que permitirão entender melhor *[detalhar a necessidade]*, em conformidade com o princípio da necessidade conforme o Art. 6º, inciso III da LGPD.

Período do Tratamento:

Os dados pessoais serão armazenados pelo período necessário para a consecução das finalidades mencionadas, não excedendo *[informar o tempo necessário para tratamento dos referidos dados pessoais]*, salvo indicação em contrário pelo titular ou pela necessidade de cumprimento de obrigações legais, conforme o Art. 15 da LGPD.

Confidencialidade e Segurança:

As informações coletadas serão tratadas de forma confidencial e não serão divulgadas, garantindo a proteção dos dados pessoais, conforme estabelecido pela Lei Geral de Proteção de Dados Pessoais (LGPD). Asseguramos que todas as medidas de segurança requeridas no Art. 46 da LGPD serão implementadas para proteção contra acessos não autorizados.

Direitos do Titular:

Estou ciente de que tenho o direito de acessar, corrigir e solicitar a exclusão ou anonimização dos meus dados pessoais a qualquer momento, bem como de revogar este consentimento, conforme previsto nos Art. 18 e Art. 8º, §5º da LGPD.

Ao assinar este termo, concordo com o tratamento dos meus dados pessoais para as finalidades supracitadas.

Data: ____/___/____

Assinatura: _____

Contatos para esclarecimento de dúvidas:

[Inserir informações de contato do projeto, como e-mail e telefone].

17. RECURSOS COMPLEMENTARES

Links úteis

A ANPD oferece uma variedade de recursos online que podem ser extremamente úteis:

- **Página inicial:** https://www.gov.br/anpd/pt-br - A página inicial da ANPD fornece acesso à legislação completa da LGPD (Lei nº 13.709/2018), notícias relevantes, informações sobre a estrutura da ANPD e seus membros, além de links para outras seções importantes do site.
- **Guias orientativos:** https://www.gov.br/anpd/pt-br/documentos-e-publicacoes - A seção de documentos e publicações da ANPD contém guias orientativos específicos sobre diversos temas relacionados à LGPD.
- **Fala.BR:** https://falabr.cgu.gov.br/ - A plataforma Fala.BR permite que cidadãos enviem sugestões, dúvidas e denúncias relacionadas à LGPD para a ANPD.
- **Guia para auxiliar a criação do Termo de Uso e Política de Privacidade:** https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_termo_uso_politica_privacidade.pdf
- **Guia de Resposta a Incidentes:** https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_resposta_incidentes.pdf
- **Guia de Gerenciamento de Vulnerabilidades e Modelo de Política de Gerenciamento de Vulnerabilidades:** https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_gerenciamento_vulnerabilidades.pdf

Sugestões de cursos online gratuitos

Diversas plataformas oferecem cursos online gratuitos sobre a LGPD, que podem auxiliar na capacitação dos servidores, alguns deles são:

- **LGPD: Como coordenar a atuação do município para a governança de dados aplicada:** Disponível na plataforma Escola Virtual.Gov.

https://www.escolavirtual.gov.br/curso/491

- **Praticando a LGPD:** Disponível na plataforma da Enap. https://suap.enap.gov.br/portaldoaluno/curso/1886
- **Fundamentos da Lei Geral de Proteção de Dados Pessoais:** Disponível na plataforma Escola Virtual Gov. https://www.escolavirtual.gov.br/curso/603
- **Lei Geral de Proteção de Dados Pessoais (LGPD):** Disponível na plataforma da EV | Fundação Bradesco. https://www.ev.org.br/cursos/lei-geral-de-protecao-de-dados-lgpd

Contatos de órgãos e entidades

- **ANPD:**
  - **Site:** https://www.gov.br/anpd/pt-br
  - **Telefone:** (61) 2025-8101
  - **E-mail:** protocolo@anpd.gov.br
- **Encarregado pelo Tratamento de Dados Pessoais do ICTIM:**
  - **Diretoria de Infraestrutura**
  - **E-mail:** dpo@ictim.com.br

18. REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação (LAI). Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 23/10/2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 23/10/2024.

BRASIL. Lei nº 14.133, de 1º de abril de 2021. Lei de Licitações e Contratos Administrativos. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 23/10/2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para o Poder Público. Brasília, DF: ANPD, 2023. Disponível em:

https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 23/10/2024.

MARICÁ. Decreto nº 840, de 5 de abril de 2022. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – no âmbito da Administração Municipal direta e indireta do Município de Maricá/RJ. Maricá, RJ: Prefeitura Municipal de Maricá, 2022. Disponível em: https://www.marica.rj.gov.br/wp-content/uploads/2022/08/JOM_1295_06-04-2022.pdf. Acesso em: 23/10/2024.

MARICÁ. Portaria SMA Nº 001, de 02 de janeiro de 2024. Estabelece o Plano de Classificação e a Tabela de Temporalidade e Destinação de Documentos das Atividades-Meio do Poder Executivo Municipal. Maricá, RJ: Prefeitura Municipal de Maricá, 2024. Disponível em: https://www.marica.rj.gov.br/wp-content/uploads/2024/01/JOM_1541_03-01-2024.pdf. Acesso em: 23/10/2024.