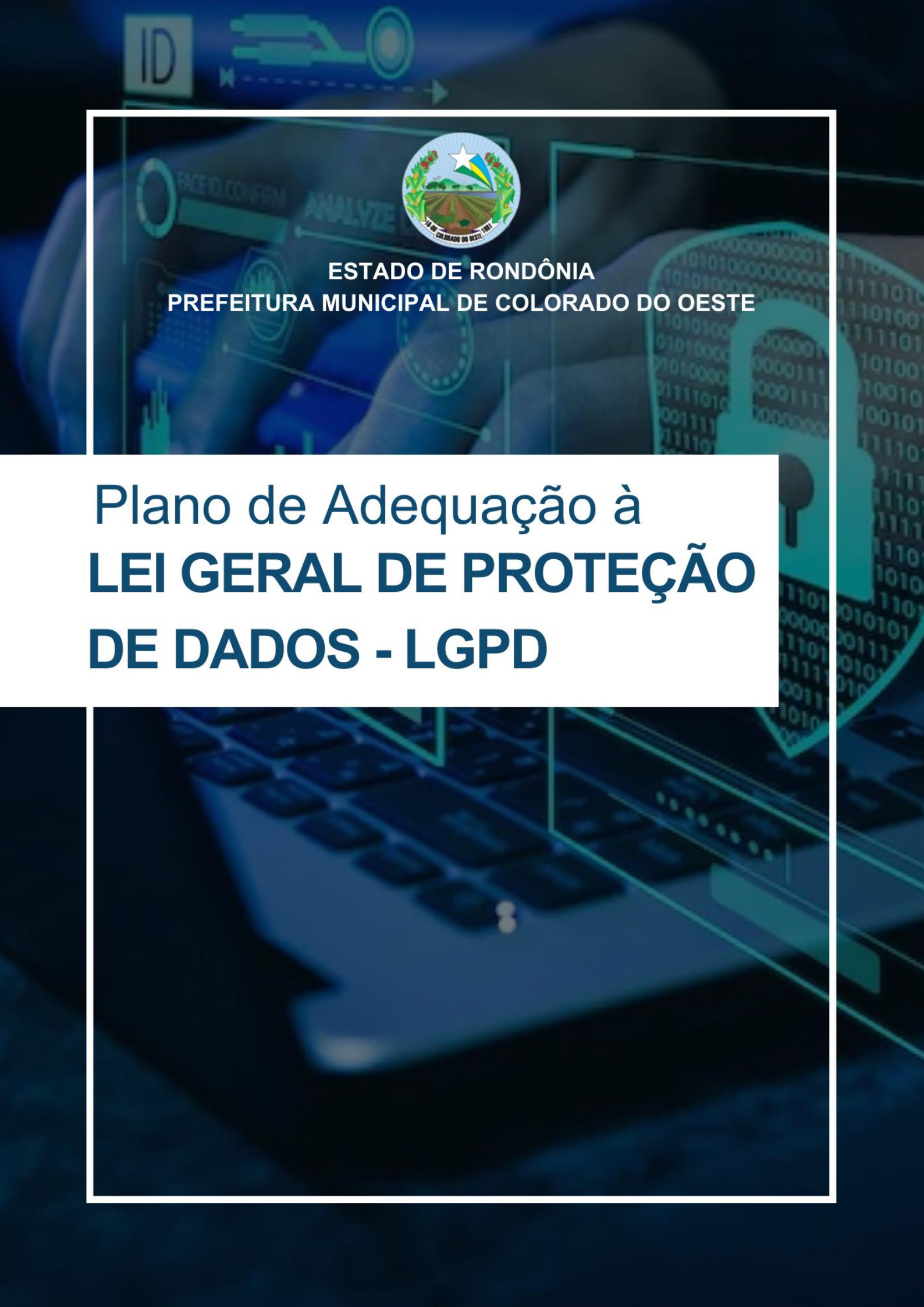


ESTADO DE RONDÔNIA
PREFEITURA MUNICIPAL DE COLORADO DO OESTE

Plano de Adequação à LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

PREFEITO MUNICIPAL

Prof. Ms. José Ribamar de Oliveira

VICE-PREFEITO MUNICIPAL

João Batista Pereira

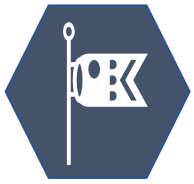
CONTROLADOR GERAL

Tertuliano Pereira Neto

EQUIPE TÉCNICA DE ELABORAÇÃO

Cleidiane Ester Timm – Controladora Interna

Iago de Souza Ladislau – Técnico em Informática



MISSÃO

Oferecer aos Coloradenses serviços públicos de qualidade e confiabilidade.

VISÃO

Realizar uma gestão que seja referência regional e estadual na prestação dos serviços públicos.

VALORES

Mudanças para Colorado avançar.
Transparência
Confiança
Comprometimento
Empreendedorismo
Responsabilidade social e ambiental.

SUMÁRIO

1. Introdução

A Lei Geral de Proteção de Dados (LGPD) – Lei n. 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica, de direito público ou privado, abrangendo inclusive o tratamento realizado nos meios digitais, e tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Conforme o art. 23 da LGPD, o tratamento de dados pessoais pela Administração Pública "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público". Ademais, deverá informar as hipóteses em que realiza o tratamento de tais dados, fornecendo informações claras e atualizadas sobre a previsão legal, finalidade, procedimentos e práticas utilizadas, assim como indicar um encarregado pelo tratamento desses dados.

Ressalta-se que podem ser titulares de dados pessoais quaisquer indivíduos, desde os próprios servidores até usuários dos serviços públicos, cuja privacidade deve ser preservada. Portanto, implementar a LGPD no âmbito da PMCO é uma atividade importante para a proteção dos dados pessoais de todas e todos.

Diante disso, a Prefeitura Municipal de Colorado do Oeste como parte ente da Administração Pública Direta, visando se adaptar às diretrizes e às exigências da LGPD, agindo com responsabilidade e transparência, apresenta o presente Plano de Adequação à LGPD. Este Plano tem por objetivo descrever o conjunto das principais ações voltadas para alcançar a conformidade com a LGPD. Para regulamentar a Lei no âmbito municipal, foi editado o Decreto Regulamentar n. 242, de 17 de julho de 2023.

2. Objetivos do Plano de Ação

2.1. Objetivos Gerais

- Implementar a Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD) no âmbito da Prefeitura Municipal de Colorado do Oeste;
- Implantar as diretrizes estratégicas e operacionais da LGPD nos processos da instituição;
- Conscientizar o órgão para garantir a proteção da privacidade de dados pessoais tratados na PMCO;
- Atender aos direitos dos titulares de dados.

2.2. Objetivos Específicos

- Conferir transparência sobre o uso dos dados pessoais pela PMCO;
- Instituir e implementar a política de privacidade de dados pessoais no âmbito da PMCO;
- Oferecer maior clareza à gestão sobre os ciclos de vida dos dados pessoais;
- Disseminar os conhecimentos necessários acerca do tema, conscientizando a todos os servidores da PMCO sobre a importância do cuidado ao realizar o tratamento de dados pessoais no órgão;
- Definir mecanismos de governança para monitoramento do tratamento de dados pessoais.

3. Método

Para execução dos trabalhos, a Prefeitura de Colorado do Oeste por intermédio do Comitê Gestor de Proteção de Dados - CGPD, adotará os seguintes métodos:

- Avaliação de problemas;
- Reuniões periódicas de *report*;
- Articulações com Secretarias responsáveis pelo tratamento de dados;
- Distribuição de tarefas;
- Orientação pela legislação.

4. Legislação base

Constituição da República Federativa do Brasil;

Lei n° 13.709/2018, Lei Geral de Proteção dos Dados – LGPD;

Lei n° 13.853/2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

Decreto Regulamentar n. 242, de 17 de julho de 2023, decreto da Prefeitura Municipal de Colorado do Oeste/RO.

5. Conceitos

Para adequação da PMCO à LGPD faz-se necessário adentrar em alguns aspectos dessa norma para que haja maior clareza sobre o melhor caminho a seguir. Nesse sentido é fundamental conhecer as hipóteses legais e buscar a aplicação dos princípios no decorrer de todo o processo de adequação, sendo eles:

5.1. Dado Pessoal

Dado pessoal é a informação relacionada à pessoa natural identificada ou identificável. Exemplo: CPF, RG, endereço, entre outros.

5.2. Dado Pessoal Sensível

Dado pessoal sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Tendo em vista que tais dados podem colocar o titular em situação de vulnerabilidade ou discriminação, o tratamento desse tipo de dado deve observar um cuidado maior que os outros, tendo a LGPD previsto algumas regras específicas para tanto.

5.3. Dado Anonimizado

Relativo a usuário que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento. A anonimização de dados deve seguir preceitos da segurança da informação, os quais estão sob responsabilidade, no âmbito da PMCO, da Coordenação de Tecnologia da Informação.

5.4. Banco de Dados

Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

5.5. Titular dos Dados Pessoais

Pessoa natural identificada ou identificável, independente da sua nacionalidade ou do local da sua residência. No âmbito da PMCO, os titulares podem ser cidadãos que utilizem os serviços da Prefeitura; ou o próprio público interno (servidores e colaboradores).

5.6. Controlador

É a quem compete as decisões referentes ao tratamento de dados pessoais. Por exemplo, o Município de Colorado do Oeste é o controlador dos dados tratados na realização das suas atividades legais e constitucionais.

5.7. Operador

É a pessoa a quem compete o tratamento de dados pessoais em nome e por ordem do Controlador. A título de exemplo, operadores são os fornecedores contratados pelo poder público que venham a tratar os dados do cidadão na execução de um contrato. É o caso da Pública Serviços Ltda, quando presta serviços ao Município.

5.8. Encarregado

É definido pela LGPD no seu artigo 5º, inciso VIII: "pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a **Autoridade Nacional de Proteção de Dados (ANPD)**". Além de servir como um canal de comunicação, a LGPD atribuiu outras funções ao Encarregado, como as de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

5.9. Agente de tratamento

O controlador e o operador.

5.10. Anonimização

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

5.11. Consentimento

Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

5.12. Bloqueio

Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

5.13. Eliminação

Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

5.14. Transferência internacional de dados

Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

5.15. Uso compartilhado de dados

Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

5.16. Relatório de impacto à proteção de dados pessoais

Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

5.17. Órgão de pesquisa

Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

5.18. Autoridade Nacional de Proteção de Dados – ANPD

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo o território nacional

5.19. Tratamentos de Dados Pessoais

Qualquer operação ou conjunto de operações realizada com dados pessoais ou conjunto de dados pessoais por meios automatizados ou não. Tais operações podem ser: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

5.20. Consentimento para Tratamentos dos Dados

O usuário deve permitir o tratamento de seus dados pessoais e essa permissão tem que ser livre, informada e inequívoca, por meio da qual o titular concorda com tal tratamento para uma finalidade determinada.

As definições trazidas no artigo 5° contribuem para a compreensão dos procedimentos de adequação, inclusive com dispositivos para harmonização com a Lei de Acesso à Informação (LAI), como por exemplo nas situações que oferecem a possibilidade ou implicam na necessidade de procedimentos de pseudoanonimização e anonimização de dados para evitar a exposição de pessoas envolvidas com a questão que precisa ser divulgada. É imprescindível que haja o equilíbrio entre a Proteção de Dados (como um direito individual) e a proteção da segurança pública (como um direito coletivo), para que se fortaleça o combate ao crime organizado, à fraude digital e ao terrorismo.

Como registrado anteriormente, a LGPD se caracteriza como um marco regulatório para o tratamento de dados pessoais. Além disso, traz um forte caráter de proteção a direitos individuais que estão expressos nos princípios estabelecidos no seu artigo 6° (conforme síntese abaixo) e nos demais artigos da referida lei.

Quadro 01: Direitos garantidos aos titulares de dados (Art. 6º)

Direitos dos Titulares de Dados que decorrem dos princípios	Princípio Correspondente
Direito ao tratamento subordinado aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.	Princípio da Finalidade
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.	Princípio da Adequação
Direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.	Princípio da Necessidade
Direito a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais.	Princípio do Livre Acesso
Direito a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento.	Princípio da qualidade dos dados
Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.	Princípio da Transparência
Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição perda, alteração, comunicação ou difusão.	Princípio da Segurança
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.	Princípio da Prevenção
Direito de não ser discriminado de forma ilícita ou abusiva	Princípio a não discriminação

Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais,	Princípio da responsabilização e prestação de contas

Fonte: Guia de Boas Práticas para Implementação na Administração Pública Federal (2020).

No capítulo II da LGPD estão elencados os requisitos para o tratamento dos dados pessoais, que pode ser realizado desde que tenha previsão em uma das hipóteses previstas no Art. 7°, uma vez que garantidas tais condições permitam a verificação por parte do Controlador e do Operador se o tratamento de dados que foi definido pela instituição é permitido.

O quadro abaixo traz uma síntese dessas hipóteses para tratamento de dados pessoais:

Quadro 02: Hipótese de tratamento de dados pessoais (Art.7°)

Hipótese de Tratamento
Mediante consentimento do titular
Para cumprimento de obrigação legal ou regulatória
Para execução de políticas públicas
Para realização de estudo e pesquisas
Para execução ou preparação de contrato
Para exercício de direitos em processo judicial, administrativo e arbitral
Para proteção da vida ou da incolumidade física do titular ou de terceiro
Para tutela da saúde do titular
Para atender interesses legítimos do controlador ou de terceiro
Para proteção do crédito
Para garantia da prevenção à fraude e à segurança do titular

Fonte: Guia de Boas Práticas para Implementação na Administração Pública Federal (2020).

A LGPD também dispõe de critérios para situações que pode haver a dispensa do consentimento do titular dos dados, conforme destacado no quadro abaixo:

Quadro 03: Hipóteses nas quais o tratamento de dados é permitido com dispensa da exigência do consentimento do titular

Hipóteses (Art.7º)	
Questões legais	Para o cumprimento de obrigação legal ou regulatória pelo controlador (Art. 7º, inciso II).
Políticas públicas	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, inciso III).
Pesquisas	Para a realização de estudos por órgão de pesquisa, garantida sempre que possível, a anonimização dos dados pessoais (Art. 7º, inciso IV).
Contratos	Quando necessário 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, inciso V).
Processo Judicial	Para o exercício regular de direitos em processo judicial, administrativo ou arbitral (Art. 7º, inciso VI).
Vida	Para a proteção da vida ou da incolumidade física do titular ou de terceiros (Art. 7º, inciso VII).
Saúde	Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (Art. 7º, inciso VIII).
Legítimo interesse	Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso que prevalecer direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (Art. 7º, inciso IX).
Crédito	Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (Art. 7º, inciso X).

No entanto, é necessário ponderar a respeito desse tipo de autorização listado no Quadro 03, pois deve-se manter a circulação de dados pessoais de forma restrita e só podem ser usados em consonância com a finalidade que ensejou a sua solicitação. Por

outro lado, a Lei de Acesso à Informação (Lei 12.527/2011) estabelece a possibilidade de divulgação quando houver interesse preponderante e irrestrito para fins de transparência, como em nos casos de contratos públicos firmados entre empresas e a administração pública. De qualquer forma, não temos dúvida que a ampla divulgação de dados pessoais pode gerar impactos negativos para os titulares e por essa razão merecem atenção redobrada.

6. Etapas do Plano de Adequação

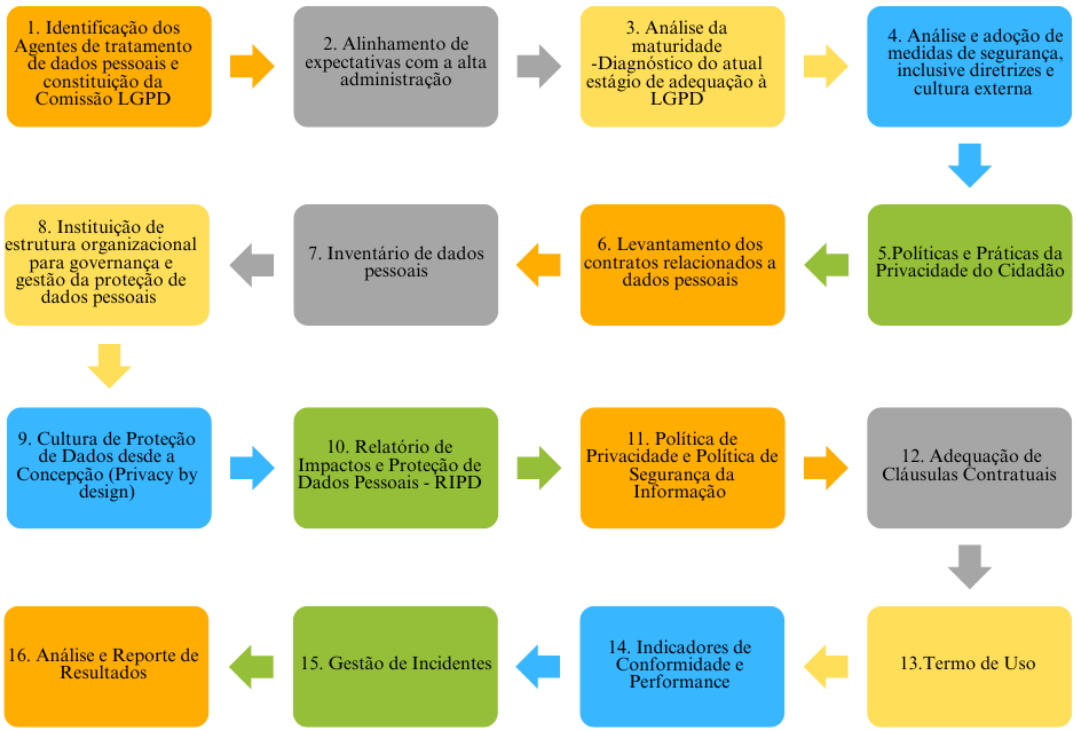
A adequação da Prefeitura Municipal de Colorado do Oeste à LGPD está diretamente condicionada a um esforço para transformação cultural da instituição e visa alcançar todas as dimensões, e precisa envolver algumas ações fundamentais ou desde a estratégica até a operacional, essa transformação envolve:

- ✓ Conscientização da dos usuários.
- ✓ Apoio da alta administração.
- ✓ Definição dos atores envolvidos.
- ✓ Capacitação/Treinamento especializado.
- ✓ Criação de uma Política Institucional de Proteção e Privacidade de Dados Pessoais.
- ✓ Constituição de grupo de trabalho para gestão de riscos e incidentes relacionados à LGPD.

Nesse contexto apresenta-se o fluxo (Figura 1) que traz uma síntese das ações para adequação à LGPD a seguir consta a descrição das etapas a serem seguidas, cuja representação visual na Figura 2.

FIGURA 1: FLUXO DAS AÇÕES PARA ADEQUAÇÃO DA PMCO À LGPD

FIGURA 2: ETAPAS DO PLANO DE ADEQUAÇÃO



6.1. Identificação dos agentes de tratamento de dados

Esta etapa consiste em identificar os agentes de tratamento de dados pessoais (controlador e operador) e o encarregado. A definição dos papéis serve para resguardar ambas as partes, os agentes públicos ou privados e os titulares de dados pessoais. Os agentes de tratamento de dados pessoais desempenham um importante papel no levantamento das informações necessárias para adequação da prefeitura à LGPD.

Controlador: é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. No âmbito da Administração Pública será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade que representa a instituição, a qual está imbuída de adotar as decisões acerca do tratamento de tais dados.

Operador: é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. São agentes públicos que exercem tal função, bem como pessoas jurídicas representante do Controlador, que exercem atividade de tratamento no âmbito de contrato ou instrumento congênere.

Encarregado: Pessoa indicada (natural ou jurídica) pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

6.2. Alinhamento de expectativas com a alta administração

Consiste na apresentação das expectativas da alta administração e das prioridades às ações mais urgentes que guiarão a cultura de proteção de dados na instituição.

6.3. Análise da maturidade - Diagnóstico do atual estágio de adequação à LGPD

Nessa etapa será analisado o nível de maturidade da instituição à LGPD com o objetivo de fornecer informações necessárias para um diagnóstico. Os resultados

apresentarão um índice de maturidade que possibilitará o direcionamento de esforços e a priorização das ações necessárias, visando a melhoria do tratamento e da proteção de dados.

6.4. Análise e adoção de medidas de segurança inclusive diretrizes e cultura externa

Nesta etapa deve ocorrer o planejamento com a análise de quais medidas de segurança podem ser adotadas (Art. 46 da LGPD). Cada medida deve acompanhar o objetivo que se espera alcançar com a aplicação da medida, para o aprimoramento de diretrizes e cultura de respeito e proteção de dados pessoais.

Quadro 04: medidas de segurança

MEDIDA DE SEGURANÇA	DESCRIÇÃO
Classificação da Informação	Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a instituição.
Compartilhamento, uso e proteção da informação	Assegurar a privacidade e proteção das informações de identificação pessoal, conforme requerido por legislação e regulamentação pertinente.
Continuidade das atividades	A proteção de dados deve ser contemplada nos sistemas de gestão da continuidade das atividades da instituição
Controle de acesso lógico	Limitar o acesso à informação e aos recursos de processamento da informação.
Controles criptográficos	Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.
Controles de coleta e preservação de evidências	A instituição deve definir e aplicar procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências para a proteção de dados pessoais.
Cópia de segurança	Cópias de segurança das informações, de softwares e das imagens do sistema devem ser efetuadas e testadas regularmente, conforme a política de segurança definida.

Desenvolvimento seguro	Garantir que a proteção de dados está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.
Gestão de mudanças	Mudanças na organização, nos processos de negócios, nos recursos de processamento da informação e nos sistemas que afetam a proteção de dados devem ser controladas.
Gestão de riscos	Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a instituição. Destinado a fornecer segurança razoável quanto à proteção dos dados pessoais e à realização de seus objetivos.
Organização de segurança	Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança dos dados dentro da organização.
Política de segurança	Prover orientação da direção e apoio para a segurança dos dados pessoais de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.
Proteção física e do ambiente	Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento e informações institucionais.
Registro de eventos e rastreabilidade	Registrar eventos e gerar evidências a fim de proporcionar rastreabilidade.
Segurança em redes	Assegurar a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.
Segurança nas operações	Garantir a operação segura e correta dos recursos de processamento da informação.
Tratamento e resposta a incidentes	Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais, incluindo a comunicação sobre fragilidades e eventos de segurança.

Fonte: ENAP/2020/ABNT/ISO 27002:2013; ISO/IEC 29151:2016.

Para cada medida de segurança deverão ser elencados controles a serem aplicados sobre os ativos organizacionais, que são bases de dados, documentos, equipamentos, locais físicos, sistemas e até mesmo pessoas que compõem uma instituição.

Sugere-se que seja criada uma planilha de controle na qual deve constar a descrição do controle em formato de pergunta que tem a finalidade de verificar se o controle está sendo

aplicado no ativo organizacional. Para tanto, propõe-se no Anexo 1 um quadro para controle das ações específicas de segurança que podem ser aplicadas sobre os ativos organizacionais.

6.5. Políticas e práticas para proteção da privacidade do cidadão

Nessa etapa são especificadas as políticas e práticas para proteger a privacidade do cidadão e garantir que o uso dos dados pessoais seja adequado, de acordo com a legislação. Para tanto, é necessário definir os papéis específicos dos servidores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação dessas informações. Outro ponto a se destacar nessa etapa são as ações educativas que devem ser ofertadas a servidores (incluindo terceirizados) que atuem ou tenham acesso a dados de usuários ou outras pessoas que tenham vínculo com a instituição.

6.6. Levantamento dos contratos relacionados a dados pessoais

Para as adequações contratuais (já existentes e futuras) deverão ser utilizadas as informações mapeadas no Inventário de dados. Para tanto é fundamental a existência de um Grupo de Trabalho para analisar os dados que já foram mapeados no inventário e se criar um Programa de Gerenciamento de Privacidade/PGP para proteger os direitos do cidadão. Sugere-se que sejam observados os aspectos listados no quadro 05.

Gerenciamento de Direitos Individuais	Consentimento e rastreamento de Preferência	Redução de responsabilidade por violação
1-Respeito aos direitos individuais de privacidade. 2-Respeito ao direito do titular acessar seus dados pessoais tratados na instituição. 3-Direito do titular solicitar atualização de seus dados. 4-Adoção de procedimentos de	1-Reunir o consentimento. 2-Rastrear solicitações de preferências tanto dos titulares de dados como dos agentes de tratamento.	1-Criptografia. 2-Anonimização de dados.

preparação para recebimento das demandas (incluindo reclamações), realização de triagem e respostas aos titulares dos dados (demandantes).		

Fonte: Guia de Elaboração de Programa de Governança em Privacidade, 2020 (adaptado).

6.7. Inventário de dados pessoais

Essa etapa consiste no mapeamento dos dados pessoais tratados na instituição que indicará em que grau a Prefeitura Municipal de Colorado atende o que está disposto na LGPD e quais controles ainda não foram observados. É uma ferramenta que identifica quais dados pessoais são tratados, onde ficam armazenados e que operações são realizadas com eles e a partir deles, devendo observar o previsto no Art. 37 da LGPD. Atualmente a ferramenta mais utilizada para mapear os dados de instituições públicas ou privadas é conhecida como Record Of Processing Activities/ROPA, que segue princípios General Data Protection Regulation-GDPR, que é regulamento adotado para a proteção de dados na Europa. Para Pinheiro (2018) consiste em criar uma matriz de tratamento de dados pessoais que será alimentada com as informações de quais são os tipos de tratamento de dados e para quais finalidades.

6.8. Instituição de estrutura organizacional para governança e gestão da proteção de dados pessoais

A execução do Plano de Adequação à LGPD, bem como a realização das atividades pertinentes às atribuições do Encarregado, deve ocorrer de forma estruturada e planejada. Sugere-se que tenha como base a Portaria da Anatel n°1197, de 25 de agosto de 2020, que estabelece as competências de um Escritório de Apoio a Proteção de Dados, que obedece a estrutura recomendada, embora num primeiro momento possa

ser exercido pela própria Comissão de Segurança da Informação e Avaliação de Processos Sigilosos.

6.9. Cultura de segurança e proteção de dados pessoais desde a concepção (privacy by design)

Um dos maiores desafios para o Plano de Adequação da PMCO à LGPD será uma mudança na cultura organizacional da instituição, envolvendo um processo de orientação e sensibilização de todos os envolvidos. Neste aspecto, algo a ser difundido é o conceito de privacidade desde a concepção de práticas, serviços, projetos, produtos e sistemas, persistindo em todo o ciclo em que haja dados pessoais sendo trabalhados, sobretudo naqueles que estejam presentes nas tecnologias da informação e comunicação.

6.10. Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais/RIPD é o documento de comprovação por meio do qual o Controlador pode apresentar o registro de todas as etapas de uma avaliação de riscos nas operações que envolvam essas informações, incluindo a coleta, tratamento, uso e compartilhamento. Para tanto, precisam estar estabelecidas e implementadas quais são medidas adotadas para mitigar os riscos que possam afetar os direitos fundamentais dos titulares, conforme está previsto no inciso XVII do art. 5°, combinado com o parágrafo único do Art. 38, da LGPD.

> Art. 5° Para fins desta Lei, considera-se:
> (...)
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
> (...)

> Art.38. A autoridade Nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O RIPD deverá ser produzido antes da instituição iniciar o tratamento das informações pessoais dos seus usuários e servidores. Deve ocorrer na fase inicial da implantação do Plano de Adequação (ENAP/2021), contemplando as várias ações que se inserem nas etapas que ora estão sendo descritas e que o esquema do trabalho em espiral consta no Anexo 1, que são “Etapas da fase de Elaboração do RIPD”, presente no “Guia de boas práticas sobre a LGPD”, produzido pelo Comitê Central de Governança de Dados.

6.10.1 Etapas da fase de elaboração do RIPD

1ª Etapa: Identificar os Agentes de Tratamento e o Encarregado

A primeira etapa na elaboração do Relatório de Impacto à Proteção de Dados Pessoais - RIPD, compreende a identificação dos agentes de tratamento de dados pessoais (Controlador e Operador) e o Encarregado, que ficarão responsáveis pelo levantamento das informações primordiais para a elaboração do RIPD.

O artigo 5° da LGPD, em seus incisos VI, VII e VIII trazem a definição desses atores conforme segue abaixo:

> Art.5° Para fins desta Lei, considera-se:
> VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
VIII - encarregado pessoa indicada pelo controlador e operador para atuar como canal de comunicação de Dados (ANDP).

2ª etapa: Identificar a necessidade de elaborar o Relatório

O Relatório de Impacto à Proteção de Dados Pessoais é o documento que serve de norteador para a adequação da PMCO à LGPD. Portanto, recomendamos sua elaboração. Nesse documento deverá constar informações de quais dados pessoais são coletados, tratados, usados, compartilhados e quais são as medidas adotadas para a mitigação de possíveis riscos. Além dos casos específicos previstos pela LGPD, o RIPD também poderá ser elaborado ou atualizado nas situações em que haja a possibilidade de ocorrência de impactos a privacidade dos dados pessoais, resultante de:

A - Uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados.

B - Rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art.12 §2°).

C - Tratamento de dado pessoal sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (LGPD, art. 5º, II).

D - Processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20).

E - Tratamento de dados pessoais de crianças e adolescentes (LGPD, art.14).

F - Tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art.42).

G - Tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art.4°, §3°).

H - Tratamento no interesse legítimo do controlador (LGPD, art. 10, §3º).

I - Alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operações do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados etc.

J - Reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Obs.: Quando houver a necessidade de elaboração de um RIPD, devem se esclarecer qual (ais) dos itens acima demonstram essa necessidade.

3º etapa: Descrever o tratamento

Nessa etapa são descritos os processos de tratamento de dados pessoais e dados pessoais sensíveis que podem gerar riscos às liberdades civis e aos direitos fundamentais, contempla a especificação da natureza, escopo, contexto e finalidade do tratamento.

O objetivo dessa descrição é reunir as informações que permitirão conhecer a conjuntura institucional referente aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos (ENAP/2020).

É importante destacar que a LGPD (Art. 5°, X), considera tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Se a instituição entender mais condizente com sua realidade de tratamento de dados pessoais, pode reunir a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD.

- **Natureza do tratamento:** representa como a instituição pretende tratar ou trata o dado pessoal;

- **Escopo do tratamento:** representa a abrangência do tratamento de dados;
- **Contexto do tratamento:** inclui fatores internos e externos que podem afetar as expectativas do titular.
- **Finalidade do Tratamento:** é a razão ou motivo pelo qual se pretende tratar os dados pessoais. A definição da finalidade é uma etapa importante, pois, justificará o tratamento e base para informar o titular dos dados.

  Ao detalhar a finalidade de tratamento de dados pessoais deve se considerar:

  A. Que indicam qual (is) o (os) resultado (s) pretendido (os) para os titulares dos dados pessoais, informando o quão importante são esses resultados.

  B. Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

4ª etapa: Identificar partes interessadas consultadas

Devem ser identificadas as partes interessadas relevantes internas e externas, consultadas a fim de obter opiniões legais técnicas ou administrativas sobre os dados pessoais que são objetos do tratamento. Nessa etapa, deve-se destacar:

A. Quais partes foram consultadas, como por exemplo, operador (LGPD, art. 5°, VII), encarregado (LGPD, art.5°, VIII), gestores, especialistas em segurança da informação, consultores jurídicos etc.

B. O que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também se devem observar os riscos de não conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).

Obs.: Na impossibilidade de registrar o que foi consultado, é necessário justificar o motivo de não ter realizado o registro.

5ª etapa: Descrever necessidade e proporcionalidade

Nessa etapa deve ser demonstrado que as operações realizadas sobre os dados pessoais se limitam ao mínimo necessário para o alcance de suas finalidades, com alcance dos dados adequados proporcionais e não excessivos em relação às finalidades do tratamento de dados (Art. 6°, III da LGPD).

Outro ponto a ser destacado é a fundamentação legal para o tratamento que se deseja realizar. Se o embasamento for o legítimo interesse8 do controlador (Art. 10, LGPD), deve por exemplo ser provado que:

A. O tratamento de dados pessoais é indispensável.
B. Inexistência de outra base legal possível de se utilizar para alcançar o mesmo propósito.
C. O processamento proposto de fato auxilia no propósito almejado.
D. Como será garantida a qualidade (exatidão, clareza, relevância e atualização dos dados e minimização dos dados).
E. Quais medidas são adotadas a fim de assegurar que o operador (Art. 5º, VII, LGPD), realize o tratamento de dados pessoais, conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (Art.5°, VI, LGPD).
F. Como estão implementadas as medidas que assegurem o direito de o titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
G. Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
H. Quais são as salvaguardas para as transferências internacionais de dados.

É necessário também criar os procedimentos para atender os direitos previstos no art. 18 da LGPD, que trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os seus dados pessoais. Além disso, é necessário estabelecer quem na instituição representa o controlador na coleta, tratamento e proteção de dados.

6ª etapa: Identificar e avaliar os riscos

O relatório deve ter uma seção que trata da identificação e avaliação de riscos na qual deverá tratar das ações necessárias para identificar e avaliar os riscos que podem comprometer a privacidade dos dados pessoais tratados pela instituição.

No art. 5°, XVII da LGPD está disposto o que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco".

O procedimento inicial é a identificação dos riscos que geram impacto potencial sobre o titular dos dados pessoais.

Para cada risco identificado, deve ser definida a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

É importante enfatizar que deve ser identificado qualquer tipo de risco que afete o tratamento de dados pessoais, independentemente de sua natureza (técnica, administrativa, de segurança da informação ou de privacidade).

7ª etapa: Identificar medidas para tratar os riscos

Nessa etapa devem ser reunidas as informações que se referem às medidas que serão adotadas para cada situação que podem ser de segurança, técnicas ou administrativas.

O art. 46 da LGPD determina que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Durante esse processo, a instituição pode decidir que alguns riscos são aceitáveis, até um risco de nível alto, em razão dos benefícios do processamento dos dados pessoais e dificuldades de mitigação. Se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.

No primeiro momento deve-se identificar em qual fase do ciclo de vida de dados pessoais o risco pode gerar algum tipo de impacto, com essa informação determina-se a medida a ser aplicada para o tratamento do risco.

A efetivação das medidas de segurança ocorre mediante a aplicação dos controles sobre os ativos organizacionais.

8ª etapa: Aprovar o relatório

Essa etapa compreende a formalização da aprovação do RIPD por meio da obtenção das assinaturas do responsável pela elaboração do RIPD e pelas autoridades que representam o controlador e operador. O responsável pela elaboração do relatório pode ser o próprio encarregado, ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar essa tarefa.

9ª etapa: Manter revisão

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados na instituição. As mudanças podem ser motivadas por alterações:

A. Significativas na finalidade do tratamento de dados pessoais que impacte no processo de como esses dados são tratados.
B. Expressivas na quantidade de dados pessoais coletados e no contexto do tratamento de dados resultantes de identificação de falta de segurança no uso de uma nova tecnologia, nova preocupação pública sobre o tipo de tratamento de dados realizado pela instituição ou vulnerabilidade de um grupo específico de titulares de dados pessoais.

A instituição deve manter a revisão do RIPD para demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações na conjuntura tecnológica, normativa, política e institucional.

6.11. Política de privacidade e de segurança da informação

Segundo a Instrução Normativa n°1 de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, nessa etapa ocorre a atualização das diretrizes internas de proteção de dados pessoais. Para tanto, é feita uma revisão para verificar se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessária a retenção de determinados dados tratados e se é necessário revisar alguns contratos. Também é necessário fazer uma busca se já existe uma Política de Privacidade na Instituição para que seja atualizada ou construída conforme o Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos.

A Política de Privacidade é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário.

A Política de Privacidade, que faz parte do Termo de Uso, origina-se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados e informarem como as atividades de tratamento de dados atendem os princípios dispostos no artigo 6° da LGPD.

A Política de Privacidade é um dever do controlador e um direito do usuário, portanto, deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares dos dados seja garantida de forma eficiente e como os princípios da: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

A Política de Privacidade deve contemplar os seguintes tópicos:

- Controlador;
- Operador;
- Encarregado;
- Quais dados são coletados;
- Qual o tratamento realizado e para qual finalidade;

- Compartilhamento de dados;
- Segurança dos dados;
- Uso de Cookies;
- Tratamento posterior dos dados para outras finalidades;
- Transferência internacional de dados.

Os direitos dos titulares precisam ser gerenciados e para início desse processo é necessário que as informações referentes às obrigações quanto ao fornecimento de informações aos titulares com relação ao tratamento dos dados pessoais, termo de uso e política de privacidade sejam bem explicadas para dirimir qualquer tipo de dúvida que possa surgir.

6.12. Adequação de cláusulas contratuais

Para adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados pelo Inventário realizado na etapa de Iniciação e Planejamento da Adequação da PMCO à LGPD é necessário revisar os documentos vigentes e os dados já coletados. No âmbito dos contratos administrativos, pode ser necessário que a Administração Pública revisite as cláusulas contratuais econômicas firmadas, mesmo após concluído o certame. Pode ser necessário incluir novas cláusulas, conforme os princípios da LGPD, preconizados no seu art. 6º.

6.13. Termo de uso

O Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele. Representa o compromisso do Controlador e Operador com a transparência ao titular de dados pessoais e comunica como as atividades de tratamento desses dados observam os princípios dispostos na LGPD.

Para assegurar aos cidadãos o amplo acesso às informações é fundamental que os termos devam ser regularmente atualizados a fim de refletir, de modo claro e preciso, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares, que comumente serão utilizados pela instituição no exercício de suas competências legais ou execução de políticas públicas com previsão legal. Os tópicos que devem constar no Termo de Uso são:

- Aceitação dos Termos e Políticas;
- Definições;
- Arcabouço Legal;
- Descrição do serviço;
- Direitos do usuário;
- Responsabilidade do usuário e da Administração Pública;
- Mudanças no Termo de Uso;
- Informações para contato e foro.

6.14. Indicadores de Conformidade e Performance

Os indicadores de Performance (Key Performance Indicator - KPI), incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no Plano de Adequação. Recomenda-se o uso dos seguintes indicadores:

A. Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais.
B. Resultados do Diagnóstico de Adequação à LGPD - índice de adequação.
C. Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados, número de serviços com dados pessoais do órgão *10010 .
D. Índice de serviços com termo de uso elaborado: quantidade de serviços com termo de uso elaborado/ quantidade de serviços do órgão *100.

E. Índice de serviços com RIPD elaborado: quantidade de serviços com RIPD elaborado/quantidade de serviços do órgão *100.
F. Índice de conscientização em segurança: quantidade de treinamentos realizados/quantidade de treinamentos previstos *100.
G. Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço/quantidade total de controles de segurança e privacidade identificados para o serviço *100.

6.15. Gestão de Incidentes

Deve ser criado um processo de Gestão de Incidentes, que registre os incidentes ou eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente e as medidas tomadas para mitigá-los para evitar as reincidências. Pode-se implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação e privacidade, de forma a reduzir o nível de risco ao qual a Solução de TIC e/ou órgão estão expostos, considerando os critérios de aceitabilidade de risco definidos pelo órgão.

6.16. Análise e Reporte de resultados

Para demonstrar o valor do Plano de Adequação para a alta administração é indicado que seja realizado um monitoramento que contenha a análise e reporte registro dos resultados. Dar publicidade a evolução das ações e resultados obtidos e a função da privacidade para o cidadão reforçam e fortalecem a cultura de privacidade dos dados.

Na etapa de monitoramento o Encarregado deve assumir a articulação desse processo exercendo a função de:

A. Gerenciamento do estabelecimento de métricas para auxiliar no acompanhamento das ações do Plano de Adequação à LGPD.

B. Divulgação dos resultados entre as diversas áreas da instituição - estabelecimento de uma estrutura de divulgação de resultados para a alta direção dos órgãos e entidades.

7. Referencial Teórico

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS - ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**, Brasília, ANPD, 2021.

BRASIL, **Constituição da República Federativa do Brasil**. Brasília: Senado Federal,1988.

BRASIL, Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 26 jul 2023.

BRASIL. Ministério da Economia. Comitê Central de Governança de Dados/CCGD. **Guia de Boas Práticas para Implementação na Administração Pública Federal**. Brasilia/DF, Abril/2020.

BRASIL. SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL. **Guia de Elaboração de Programa de Governança em Privacidade**. Ministério da Economia Outubro, 2020.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais – Comentários a Lei n°13709/18 – LGPD**. São Paulo: Ed. Saraiva Educação, 2018.

ANEXOS

ANEXO 1: CONTROLE DE AÇÕES DE MEDIDAS DE SEGURANÇA (SIM/NÃO)

	Existe e é executado um processo formal de Gestão de Mudanças na organização?	**É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?**	**Mudanças significativas são identificadas e registradas?**
Bases de Dados			
Documentos			
Equipamentos			
Locais			
Pessoas			
Sistemas			
Unidades Organizacionais			

Fonte: ENAP/2020 (adaptado)