PREFEITURA DE FLORIANÓPOLIS
CONTROLADORIA-GERAL

PLANO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

PROJETO PILOTO - 2023/2024

CONTROLADORIA-GERAL DO MUNICÍPIO (CGM)

Florianópolis/SC, 02 de agosto de 2023.

PLANO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

PROJETO PILOTO - 2023/2024

TOPÁZIO SILVEIRA NETO
Prefeito Municipal de Florianópolis

RONALDO BRITO FREIRE
Secretário Municipal Chefe de Gabinete

FABIO MURILO BOTELHO
Secretário Municipal de Governo

CARLOS EDUARDO DE SOUZA NEVES
Secretário Municipal da Casa Civil

RODRIGO DE BONA DA SILVA
Controlador-Geral do Município

EQUIPE TÉCNICA DE ELABORAÇÃO:

Controladoria-Geral do Município
Subcontroladoria-Geral da Transparência, Ouvidoria e Proteção de Dados

Rodrigo De Bona da Silva
Controlador-Geral do Município

Osvaldo Ricardo da Silva
Subcontrolador-Geral de Transparência, Ouvidoria e Proteção de Dados

Fernanda Almeida Marcon
Chefia de Departamento de Gestão e Proteção de Dados

Felipe Stefan Koerich Theis
Chefia de Departamento de Transparência e Acesso à Informação

Mauro Rodrigo da Costa
Chefia de Departamento de Ouvidoria-Geral

2023

PREFEITURA DE FLORIANÓPOLIS
CONTROLADORIA-GERAL

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
30/05/2023	1.0	Primeira versão do Plano de Adequação à LGPD	Equipe Técnica de Elaboração
02/08/2023	1.1	Primeira versão Revisada do Plano de Adequação à LGPD	Equipe Técnica e Gabinete CGM

PREFEITURA DE FLORIANÓPOLIS
CONTROLADORIA-GERAL

SUMÁRIO

1. APRESENTAÇÃO

Com vistas à proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade, a Lei Federal n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), primeira lei brasileira dedicada especialmente à regulação, em território nacional, do tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, entrou em vigor em setembro de 2020. Logo, a partir de então, a LGPD não constitui uma alternativa, mas impõe-se como uma obrigação a todos aqueles que tratam dados pessoais, inclusive o setor público.

De acordo com a referida lei, dados pessoais consistem nas informações relativas à identificação de pessoas naturais. São considerados sensíveis os dados pessoais referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual e dado genético ou biométrico, quando vinculado a uma pessoa natural.

Sendo assim, a LGPD assegura aos titulares dos dados, tais como estudantes, usuários do sistema de saúde, contribuintes, fornecedores e servidores públicos, um rol de direitos, como o acesso facilitado à finalidade, forma e duração do tratamento de seus dados pessoais, bem como a informações sobre o compartilhamento desses dados e a responsabilização dos agentes envolvidos, caso constatada alguma irregularidade.

Para assegurar esses direitos, torna-se obrigação das instituições indicar um ou mais **encarregados pelo tratamento de dados pessoais** (*Data Protection Officer* – DPO), figura que possui a função de atuar como canal de comunicação entre instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), assim como de adotar medidas de segurança que impeçam o vazamento de dados e seu acesso de forma indevida por terceiros. Para isso, o processo de tratamento de dados deve estar pautado nos princípios descritos no art. 6º da LGPD, com destaque para a necessidade, finalidade e adequação de sua realização, segurança, prevenção de danos, não discriminação, qualidade, responsabilidade, prestação de contas, livre acesso pelo titular e transparência.

No caso do setor público, o princípio da finalidade relaciona-se, sobretudo, com a execução de políticas públicas e com o cumprimento de obrigações legais ou regulatórias. Ainda que, eventualmente, seja dispensado o consentimento do titular para o tratamento dos dados pelo poder público, nas hipóteses legalmente definidas, tal dispensa não exime a administração pública de atender às demais obrigações da LGPD, em especial seus princípios gerais e a garantia dos direitos dos titulares.

A inobservância aos preceitos da LGPD pode ocasionar a aplicação de **penalidades administrativas, no âmbito regulatório da Autoridade Nacional de Proteção de Dados – ANPD, aos órgãos e entidades da administração pública** como, por exemplo, advertência, publicização da infração, bloqueio e até mesmo eliminação dos dados pessoais a que se refere a infração. Além das sanções administrativas a órgãos e entidades, estar em desconformidade com as normas de proteção de dados significa estar exposto a, no mínimo, outros três tipos de riscos: judicial (ações ajuizadas pelos titulares dos dados); financeiro (efeitos no âmbito interno); e reputacional (prejuízo à imagem).

Ademais, o agente público que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação, é obrigado a repará-lo, como também fica sujeito a processo administrativo disciplinar, conforme o caso.

Por outro lado, a adequação à LGPD pode representar uma oportunidade para que o Município adote medidas que geram: segurança para os gestores; transparência e confiança para os cidadãos e cidadãs titulares dos dados; otimização do fluxo de reputação/imagem e da gestão dos processos.

Destarte, a Controladoria-Geral do Município (CGM), como parte integrante da administração pública do Município de Florianópolis/SC e órgão central dos Sistemas de Controle Interno, Ouvidoria e Transparência Municipal, apresenta, por meio deste Plano de Ação, o **Programa Municipal de Adequação à Proteção de Dados Pessoais**, a ser instituído pelo Decreto Municipal que regulamenta a LGPD e dividido em 07 (sete) principais eixos, assim estruturados:

1. **Normatização;**
2. **Diagnóstico Inicial;**
3. **Capacitação e Sensibilização;**
4. **Instrumentalização;**
5. **Mapeamento de dados Pessoais;**
6. **Levantamento e Gestão de Riscos; e**
7. **Monitoramento.**

A publicação e ampla divulgação deste Plano, no *site* oficial da Prefeitura e da CGM e em outros meios oficiais, têm por objetivo descrever o conjunto das principais ações voltadas ao alcance da conformidade do Poder Executivo Municipal de Florianópolis com a LGPD, bem como conscientizar a todos os integrantes dos órgãos e entidades da administração direta e indireta do Município acerca de sua importância.

Cada órgão ou entidade municipal pode vir a desenvolver seu próprio Plano de Adequação, conforme suas peculiaridades, a partir do detalhamento do presente Plano a necessidades específicas, sob supervisão da CGM.

2. NORMATIZAÇÃO

A fim de iniciar o processo de adequação do Poder Executivo Municipal de Florianópolis à LGPD, foi proposto o **Decreto Municipal** de regulamentação da LGPD, que define conceitos, competências, a forma de atendimento às manifestações dos titulares de dados pessoais, de compartilhamento de dados, institui o **Programa Municipal de Adequação à Proteção de Dados Pessoais** e trata da disponibilização do Termo de Consentimento, Sigilo e Confidencialidade de Dados Pessoais e Sensíveis para servidores municipais.

Para além da edição de uma norma, a regulamentação, adequação, treinamento, monitoramento e efetiva implementação da LGPD em âmbito municipal consolida a institucionalização de uma **Política de Proteção de Dados Pessoais** para o Poder Executivo, o que envolve a elaboração de um documento que esclareça aos usuários dos serviços públicos os papéis e responsabilidades, a forma, os processos e procedimentos adotados no tratamento de seus dados pessoais, prazos de retenção de dados, informações de contato do encarregado, hipóteses de transferência e compartilhamento de dados com terceiros, medidas de privacidade empregadas, bem como busque atender aos princípios da transparência, do livre acesso e da prestação de contas previstos na lei.

Como toda política pública, a implementação da LGPD no Poder Executivo Municipal de Florianópolis ocorrerá a partir dos eixos pré-definidos, com etapas distribuídas temporalmente, dando ênfase aos sistemas e bases de dados que gerenciam os serviços públicos oferecidos aos usuários e centralizados na Carta de Serviços. Os serviços são, assim, elementos centrais na implementação da política, como pontos de coleta e tratamento de dados pessoais, devendo ser momentos cruciais de interação para registro de consentimento e informação sobre direitos dos titulares de dados.

Deve-se levar em conta, também, instrumentos como canais de ouvidoria e portais de transparência, revisão de processos de protocolo, atendimento, digitalização, adaptação de formulários físicos e virtuais, dentre outros.

Ademais, é necessário identificar as normativas internas impactadas pela LGPD no que tange a dados pessoais, privacidade e segurança da informação, por exemplo, a fim de providenciar adequação.

A partir da Política Municipal, cada órgão ou entidade poderá elaborar seu Plano de Acão específico, com apoio técnico da Controladoria-Geral do Município, que providenciará ainda orientação e qualificação aos profissionais que atuam com a temática. Todos os Planos de Proteção de Dados Pessoais serão disponibilizadas aos usuários nos *sites* da Prefeitura, da CGM e de cada secretaria, órgão ou entidade municipal, conforme o caso.

3. DIAGNÓSTICO INICIAL

CULTURA ORGANIZACIONAL

A adequação institucional à Lei Geral de Proteção de Dados Pessoais envolve uma mudança cultural em todos os níveis da administração pública municipal direta e indireta, seja o estratégico, o tático e gerencial ou o operacional, o que exige a sensibilização de todos os servidores quanto a essa dimensão da vida que demanda atenção nos tempos atuais: a **proteção de dados pessoais**.

É premente repensar velhos hábitos, e incorporar a necessidade de **resguardar a segurança da informação e a privacidade dos dados pessoais em todas as rotinas de trabalho da instituição**.

Nesse sentido, é essencial a realização de um **diagnóstico inicial** da cultura organizacional existente, com objetivo de conhecer e mensurar o nível de percepção dos servidores municipais em relação à LGPD, a fim de melhor identificar as necessidades, direcionar e aprimorar as ações de capacitação e conscientização dos agentes públicos sobre o assunto.

Tal avaliação deve ser considerada ponto de partida do Programa de Adequação à Proteção de Dados Pessoais, o que permitirá monitorar sua implementação e avanços ao longo do tempo. Será realizada com a máxima participação possível dos servidores de todas as áreas, por meio da aplicação de **questionário** conforme modelo do ANEXO I deste Plano[1].

ANÁLISE DO DIAGNÓSTICO

Com base nos resultados obtidos na fase de diagnóstico será possível dar continuidade ao processo de adequação à LGPD, sobretudo em atenção às principais necessidades de capacitação identificadas.

A **CGM prestará orientação e auxílio a todas as secretarias, órgãos e entidades públicas municipais** para que realizem, conforme as especificidades de cada ramo de atuação, a implementação das etapas do Programa, que serão aprofundadas a seguir, bem como a elaboração de Planos de Ação específicos.

[1] Adaptado do "Manual de Implementação da LGPD" da Controladoria-Geral do Estado do Paraná. Disponível em: < CGE publica guias para implantação da LGPD nos órgãos estaduais | Controladoria Geral do Estado do Paraná>.

4. CAPACITAÇÃO E SENSIBILIZAÇÃO

Tendo em vista a necessidade de conscientizar os agentes públicos municipais acerca da importância da segurança da informação e da privacidade dos dados pessoais dos titulares, sejam estes os próprios servidores ou, então, os cidadãos em geral, nos tratamentos envolvidos em suas diversas rotinas de trabalho, a CGM promoverá **cursos, palestras, treinamentos, divulgação de cartilhas,** dentre outras ações para propagar o conhecimento e desenvolver uma cultura organizacional alinhada à LGPD no âmbito do Poder Executivo Municipal de Florianópolis.

Para tanto, serão elaborados um **Plano de Capacitação** e um **Plano de Comunicação**, que poderão ser integrados aos planos anuais da CGM, com apoio da Escola de Governo e do Gabinete do Prefeito Municipal.

As ações poderão contar, ainda, com a participação e apoio de órgãos externos, entidades e universidades parceiras, da sociedade civil e de especialistas em temas relativos à proteção e governança de dados.

Dentre as principais temáticas e ações previstas para os anos de 2023 e 2024 encontram-se:

- Palestra de Introdução à Lei Geral de Proteção de Dados Pessoais – LGPD;
- Capacitação em parceria com a Polícia Civil de SC sobre Vazamento de Dados;
- Capacitação em parceria com a Polícia Civil de SC sobre Fraudes Digitais;
- Elaboração e Distribuição de Cartilha Ilustrada sobre Boas Práticas em Proteção de Dados Pessoais, a ser publicada no *site* oficial da CGM e distribuída digitalmente aos agentes públicos municipais;
- Reuniões Periódicas dos Encarregados de Dados Setoriais; e
- Envio de *E-mail* periodicamente com dicas rápidas e temas diversos relacionados à LGPD no setor público.

5. INSTRUMENTALIZAÇÃO

O processo de adequação à LGPD no âmbito do Poder Executivo Municipal de Florianópolis envolverá o desenvolvimento de metodologias, minutas-padrão, modelos de documentação e procedimentos necessários ao atendimento dos direitos dos titulares.

Alguns dos instrumentos para implementação das normas previstas pela Lei n. 13.709/2018 são:

- Inventário de Dados Pessoais (IDP);
- Termos de Uso;
- Termos de Consentimento;
- Termo de Compromisso, Sigilo e Confidencialidade;
- Relatório de Impacto à Proteção de Dados (RIPD);
- Plano de Contingência a Incidentes;
- Contratos, Acordos e Instrumentos Congêneres.

Os instrumentos e modelos serão desenvolvidos pela CGM com apoio técnico dos demais órgãos e entidades municipais, bem como por meio da Comissão Permanente de Gestão de Dados Pessoais, da Comissão Permanente de Dados Sensíveis e dos Grupos de Trabalho instituídos. Para tanto, previamente serão encaminhados aos setores responsáveis pelo tratamento de dados alguns formulários para alimentação, com o objetivo de dar uniformidade e celeridade às informações necessárias para a avaliação das Comissões e consequente adoção de providências.

Além disso, serão realizados estudos conjuntos entre a CGM, o Escritório de Desburocratização e Modernização da Secretaria Municipal de Governo, e a Superintendência de Governo Eletrônico do Gabinete do Prefeito, para implementação de soluções tecnológicas a baixo custo que permitam automatizar e gerenciar os consentimentos dos titulares e implementar outras atividades, tarefas e funcionalidades associadas à proteção de dados.

INVENTÁRIO DE DADOS PESSOAIS (IDP)

O Inventário de Dados Pessoais (IDP) consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição (art.

37 da LGPD), que envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade, tais como:

- atores envolvidos (agentes de tratamento e encarregado);
- finalidade (para qual fim o dado pessoal é coletado e tratado pela instituição);
- hipótese de tratamento e base legal (arts. 7° e 11 da LGPD);
- quais os dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 LGPD); e
- medidas de segurança adotadas.

Desta feita, a CGM recomenda que o IDP de cada órgão e entidade seja elaborado com base na **Planilha Eletrônica**[2] disponibilizada na versão mais atual do "Guia de Elaboração de Inventário de Dados Pessoais" do Governo Federal[3], com as devidas adaptações à realidade de cada área de atuação do Município. O referido Guia apresenta a estrutura do IDP, que é inspirado nos modelos propostos pelas autoridades de proteção de dados da França, Bélgica e Inglaterra.

A elaboração dos IDPs de cada secretaria e entidade municipal deve ocorrer sob a orientação e supervisão das Comissões Permanentes e as áreas de Desburocratização e Modernização e de Governo Eletrônico já mencionadas.

TERMOS DE USO

Termo de Uso ou **Contrato de Termo de Uso** é um **documento que estabelece as regras e condições de uso de determinado serviço**. Caso o Termo de Uso seja aceito pelo usuário, a utilização do serviço será vinculada às cláusulas dispostas nele.

O Termo de Uso origina-se da responsabilidade de os agentes de tratamento de dados serem transparentes no relacionamento com o titular de dados e informem como as atividades de tratamento de dados atendem aos princípios dispostos no artigo 6° da Lei Geral de Proteção

[2] Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx>

[3] Disponível em: <guia_inventario_dados_pessoais.pdf (www.gov.br)>

de Dados Pessoais (LGPD). Portanto, o documento constitui, ao mesmo tempo, um dever do controlador e um direito do titular.

Em se tratando da elaboração do Termo de Uso a ser adotado como modelo pelos órgãos e entidades municipais, a CGM recomenda a utilização da versão mais atual do "Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos" do Governo Federal[4], no qual constam os tópicos a serem inseridos no referido Termo, observadas também as etapas revisionais conjuntas com as Comissões Permanentes e as áreas de Desburocratização e Modernização e de Governo Eletrônico.

TERMOS DE CONSENTIMENTO

Uma das hipóteses que autorizam o tratamento de dados pessoais é o consentimento do titular dos dados, de acordo com o art. 7º, inciso I, da LGPD.

Nesses casos, o **consentimento para tratamento dos dados** deve ser formalizado via **documento que contenha todas as informações necessárias ao esclarecimento do titular, o que inclui a finalidade da coleta e tratamento de seus dados e eventual necessidade de compartilhamento**.

Conforme consta no "Guia de Boas Práticas" do Governo Federal[5], na hipótese de tratamento de dados com fundamento no livre consentimento, cada nova operação realizada com os dados pessoais deve ser objeto de nova requisição de consentimento, inclusive para o compartilhamento dos dados com outras entidades, de dentro ou fora da administração pública.

Uma das razões que justificam a importância de se firmar um termo é que **o ônus da prova do consentimento cabe ao controlador**, sendo proibido o tratamento de dados pessoais mediante vício de consentimento. Isso faz do consentimento uma etapa fundamental para o recebimento, tratamento e uso de dados, tornando o **gerenciamento dos consentimentos uma atividade estratégica, posto que passa a envolver riscos legais, financeiros e de imagem com impactos potencialmente imensos**.

Além disso, vale mencionar que **o titular dos dados tem liberdade para autorizar, negar ou revogar (reconsiderar) autorização anteriormente concedida para tratamento de seus dados pessoais.**

---

[4] Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_termo_uso_politica_privacidade.pdf>

[5] Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf >

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Termo que visa a proteção das informações confidenciais, dados pessoais e dados sensíveis de munícipes que utilizam o serviço público local, bem como de servidores públicos, disponibilizados pelo Município de Florianópolis, para bom e fiel desempenho das suas atividades de interesse público.

Por meio deste documento, o servidor público municipal compromete-se a realizar o tratamento e o compartilhamento de dados pessoais, sobretudo quando de caráter sensível, apenas conforme as finalidades públicas e específicas para as quais foram coletados, devidamente informadas aos seus titulares, e para a execução das atribuições que legalmente lhe competem no desempenho do cargo, emprego ou função pública que exerce, de modo a:

- manter sigilo e não utilizar as informações confidenciais a que tiver acesso em virtude de tratamento de dados pessoais, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;

- não efetuar nenhuma gravação, cópia ou *backup*, por qualquer meio ou forma, da documentação a que tiver acesso para fins diversos ao desempenho de suas atribuições legais;

- não repassar informações confidenciais a que tiver acesso a qualquer outra pessoa física ou jurídica fora do âmbito de suas atribuições legais;

- fazer uso adequado e necessário de informações contidas em sistemas informatizados e bancos de dados; e

- manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou informações confidenciais, devendo comunicar à Área de Proteção de Dados da Controladoria-Geral do Município, imediatamente, na hipótese de incidentes dessa natureza, o que não excluirá sua responsabilidade civil, administrativa e penal, conforme o caso.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD)

O inciso XVII, do artigo 5°, da Lei 13.709/2018, define o Relatório de Impacto à Proteção de Dados Pessoais - RIPDP como a “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”.

De acordo com o art. 38, parágrafo único da LGPD, o conteúdo mínimo do RIPDP abrange 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 deve ser revisto e atualizado anualmente ou quando houver mudança em processos ou sistemas que atinja o tratamento dos dados pessoais realizado pela instituição. A CGM recomenda que sejam observadas as orientações do Governo Federal[6] para elaboração de RIPD, com as devidas adaptações.

PLANO DE CONTINGÊNCIA OU RESPOSTA A INCIDENTES

A adequação à LGPD exige a adoção de medidas para prevenção e correção de **incidentes** que ocasionem o vazamento, a perda, a alteração, a divulgação ou o acesso não autorizado de dados pessoais sob a guarda do órgão ou entidade, a exemplo de ataques cibernéticos, aplicativos maliciosos (vírus), envio de correspondência eletrônica contendo dados pessoais a destinatário equivocado, uma violação das políticas e padrões de segurança do órgão, dentre outras situações.

No caso de incidentes, a Autoridade Nacional de Proteção de Dados deve ser comunicada em prazo razoável, nos termos do art. 48 da LGPD. Assim, o **Plano de Contingência** é um **documento que descreve as providências a serem adotadas quando da ocorrência de um Incidente de Segurança de Tecnologia da Informação, com a finalidade de reduzir possíveis danos e agilizar as medidas corretivas**.

O Plano deve abarcar: a definição de incidente para o órgão; os procedimentos a serem implementados caso ocorra um incidente; as ferramentas, tecnologias e recursos a serem utilizados nessas situações; os atores que fazem parte do processo, suas responsabilidades e atribuições.

[6] Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/apresentacoes/apresentacao_ripd.pdf>

ADEQUAÇÃO DE CONTRATOS, ACORDOS E INSTRUMENTOS CONGÊNERES

Tendo em vista que os instrumentos contratuais e outros semelhantes como convênios, acordos, termos de parceria, dentre outros, até então utilizados, não foram elaborados em atenção à LGPD, faz-se necessária sua revisão e adequação aos dispositivos atinentes à privacidade e proteção de dados pessoais.

Da mesma forma, deverão ser revisados todos os formulários utilizados em cada serviço prestado pelas diversas áreas da PMF, sejam físicos, em papel, ou digital, incluídos aqueles inseridos em sistemas informatizados. A revisão de formulários inclui a análise com relação à pertinência e necessidade de cada dado solicitado, à forma de coleta e armazenamento, à segurança da informação e aos avisos (*disclamers*), Termos e Condições que devem ser incluídos em cada um.

Para que este processo tenha êxito, é de <u>suma importância a participação ativa dos gestores e representantes de todas as áreas</u> que prestam serviços, que gerenciam dados e sistemas informatizados, tendo a CGM papel de facilitador e articulador, contribuindo para a consolidação da conformidade e para a padronização de procedimentos operacionais em âmbito municipal.

6. MAPEAMENTO DE DADOS PESSOAIS

Mapeamento de dados ou *data mapping* é uma atividade de catalogação de todo o fluxo de dados pessoais, que são objeto das operações de tratamento, ou seja, consiste em identificar, categorizar e registrar todo e qualquer processo de coleta, armazenamento e tratamento dos dados pessoais comuns, sensíveis e de crianças e adolescentes, em cada órgão e entidade do Município.

Em outras palavras, o mapeamento envolve identificar as tarefas e atividades que envolvam tratamento de dados pessoais em cada setor, de modo a rastrear todo o **ciclo de vida dos dados**[7], qual seja:

- Coleta;
- Retenção/Armazenamento;
- Processamento/Tratamento/Análise;
- Compartilhamento; e
- Descarte/Eliminação.

Com base nesse ciclo, propõe-se que o *data mapping* seja realizado a partir da seguinte trilha, a ser repetida por serviço e por área de cada órgão/entidade municipal:

1. IDENTIFICAÇÃO DO PROCESSO DE TRABALHO: por exemplo, processo de admissão de um novo servidor público; processo de matrícula de aluno em escola pública municipal; atendimento médico de paciente em Unidade Básica de Saúde; instauração de processo administrativo disciplinar; dentre outros;
2. MEIOS DE COLETA/ORIGEM DOS DADOS PESSOAIS: entradas e canais de captura dos dados (ex: *site*, aplicativos, estabelecimentos físicos, ligação telefônica...);
3. CATEGORIZAÇÃO DOS DADOS COLETADOS: conforme taxonomia de dados pessoais[8] prevista no ANEXO II deste Plano;
4. FINALIDADE DA COLETA DE DADOS: descrição da finalidade de acordo com o art. 6º, inciso I, da LGPD;

[7] Com base no "Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD)" do Governo Federal, disponível em < guia_lgpd.pdf — Governo Digital (www.gov.br)>.

[8] Taxonomia extraída do "Guia Orientativo sobre a Instrução Normativa CGM/SP N. 01/2022 para a Administração Pública do Município de São Paulo", disponível em: <GuiaOrientativosobreaInstrucaoNormativaCGM-SPnº01-2022paraaAdministracaoPublicadoMunicipiodeSaoPaulo_publicacao_26_01_2023.pdf (prefeitura.sp.gov.br)>

5. BASE LEGAL PARA O TRATAMENTO: conforme hipóteses previstas nos arts. 7º, 11 e 14 da LGPD;
6. MEIOS DE TRATAMENTO: meios empregados no tratamento dos dados (sistemas informatizados, documentos, locais de armazenamento, plataformas de *cloud*/nuvem, bancos de dados, etc.);
7. OPERADORES: agentes públicos que, na execução dos processos de trabalho, realizam o tratamento dos dados pessoais;
8. ENCARREGADO DE DADOS: pessoa física indicada pelo controlador cujas atribuições constam do art. 41, parágrafo 2º, da LGPD;
9. MEIOS DE COMPARTILHAMENTO DE DADOS: meios empregados no compartilhamento dos dados (sistemas informatizados, documentos...)
10. DESTINATÁRIOS DO COMPARTILHAMENTO DE DADOS: pessoas e unidades organizacionais destinatárias dos dados, inclusive internacionais, se for o caso;
11. MEIOS DE DESCARTE/ELIMINAÇÃO OU RETENÇÃO DOS DADOS
12. CONTROLES DE SEGURANÇA DA INFORMAÇÃO: meios empregados durante o processo de trabalho e o ciclo de vida dos dados pessoais para evitar incidentes, sejam ferramentas tecnológicas e/ou práticas organizacionais, por exemplo, criptografia, cópias de segurança (*backups*), autenticação em fatores múltiplos, *captcha* e algoritmo *hash.*

7. LEVANTAMENTO E GESTÃO DE RISCOS

Em seguida ao mapeamento dos processos de trabalho e dados pessoais coletados e mantidos pelo poder público, deve ser realizada a fase de gestão de riscos a fim de avaliar as lacunas de segurança da informação existentes, identificar os possíveis impactos negativos decorrentes de tais vulnerabilidades e planejar medidas e ferramentas corretivas e/ou mitigatórias.

O gerenciamento de riscos pode ocorrer por meio da metodologia denominada "Privacidade desde a Concepção" (*privacy by design*), isto é, pelo desenvolvimento de uma estrutura que incorpore a privacidade e a proteção de dados pessoais em todos os projetos e processos desenvolvidos pela instituição, desde seu desenho inicial, de modo **priorizar a prevenção do risco** e **não a remediação**[9].

Entretanto, em se tratando de serviços, processos e sistemas que já estão em funcionamento e não foram desenhados pensando na privacidade dos dados, o levantamento e avaliação dos riscos deve seguir uma metodologia objetiva, transparente e participativa. Com isso, se pode identificar um maior número de eventos e incidentes de risco, reconhecer melhor suas causas e consequências, permitindo avaliar controles e discutir propostas de medidas de mitigação mais precisas e eficientes.

Para tanto, a CGM propõe adaptar a **Metodologia de Gestão de Riscos** da Controladoria Geral da União (CGU), **pautada basicamente em *frameworks* internacionais e em normativos e referências nacionais de gestão de riscos e controles internos**, dos quais destacam-se: COSO Report (1992) e COSO-ERM - Enterprise Risk Management (2004), ABNT NBR ISO 31.000 (2009 e 2018) - Gestão de Riscos - Princípios e Diretrizes, ABNT NBR ISO 31010:2009 - GR - Técnicas para o processo de avaliação de riscos, Instrução Normativa Conjunta CGU/MP nº 01/2016, e Declaração de Posicionamento do IIA - Instituto dos Auditores Internos: As Três Linhas de Defesa [da Gestão] no Gerenciamento Eficaz de Riscos e Controles.

Por fim, importante esclarecer que é nesta fase de levantamento e gestão de riscos que devem ser elaborados os instrumentos referentes ao Relatório de Impacto à Proteção de Dados (RIPD) e ao Plano de Contingência a Incidentes, já apresentados anteriormente.

[9] Conforme "Guia de Boas Práticas na Aplicação da Lei Geral de Proteção de Proteção de Dados Pessoais nas Ouvidorias Públicas" da Rede Nacional de Ouvidorias, disponível em: < guia_lgpd.pdf — Governo Digital (www.gov.br)>.

8. MONITORAMENTO

O processo de adequação à LGPD é um trabalho contínuo. Após a implementação inicial em cada órgão e entidade municipal, é necessário o acompanhamento constante e a melhoria contínua de cada etapa e eixo de implementação do Programa Municipal de Adequação à Proteção de Dados Pessoais, com a aplicação de ajustes e medidas corretivas, quando necessário, e a capacitação e atualização periódica dos agentes públicos municipais no tema.

O monitoramento será mensalmente coordenado pela CGM, por meio da Subcontroladoria de Transparência, Ouvidoria e Proteção de Dados, com o apoio de Comissões Temáticas Permanentes – Comisão Gestora e Comissão de Dados Sensíveis – e, também, por Grupos de Trabalho em cada órgão ou entidade municipal, liderados pelos respectivos Encarregados pelo Tratamento dos Dados Pessoais.

Entende-se por Comissão Permanente de Gestão de Dados Pessoais a equipe de representantes da administração municipal designados para, sob coordenação da CGM e em matéria de proteção de dados pessoais: atuar como órgão consultivo e deliberativo; sugerir ao Controlador-Geral a edição de normas e diretrizes gerais; produzir manuais, cartilhas e documentos de apoio; direcionar e acompanhar as atividades de adequação em cada órgão e entidade municipal; e auxiliar na disseminação da cultura organizacional de privacidade e proteção aos dados pessoais.

A Comissão Permanente de Dados Sensíveis consistirá na equipe de representantes da administração municipal designados para, sob coordenação da Controladoria-Geral do Município, prestar suporte à Comissão Permanente de Gestão de Dados Pessoais no trabalho de orientação, execução, monitoramento e revisão periódica do Programa Municipal de Adequação à Proteção de Dados Pessoais, com foco nas peculiaridades inerentes ao tratamento de dados pessoais sensíveis, sobretudo quando referentes a crianças e adolescentes, dados de saúde, biométricos, convicções religiosas ou filosóficas, dentre outros.

Por sua vez, os Grupos de Trabalho serão compostos por representantes da administração municipal liderados pelos Encarregados pelo Tratamento dos Dados Pessoais e sob a orientação das comissões permanentes referidas acima, responsáveis por executar, em cada órgão ou entidade do Poder Executivo Municipal, o Programa de Adequação à Proteção de Dados Pessoais. Os Encarregados são as pessoas, em cada órgão/entidade, que atuarão como canal de comunicação entre o controlador (município), os titulares dos dados (cidadãos), e a Autoridade Nacional de proteção de Dados (ANPD).

9. PROJETO PILOTO

Propõe-se que o processo de adequação à LGPD seja iniciado por meio da implementação de cada uma de suas etapas em um Projeto Piloto, como estratégia de efetivação deste Plano, a ser realizado nas seguintes unidades institucionais:

1) no âmbito da própria CGM, órgão de menor porte;

2) no âmbito do Instituto de Previdência de Florianópolis, de menor porte; e

3) na Secretaria Municipal da Saúde (SMS), por meio da Diretora de Inteligência em Saúde, tendo em vista o grande porte e o volume de dados pessoais sensíveis e de alto risco tratados.

Para tanto, cada órgão-piloto poderá, mediante seu Grupo de Trabalho (GT), desenvolver um Plano de Ação de acordo com os eixos e etapas apresentados até aqui, com prazos e responsáveis definidos, aprovado pela autoridade máxima do órgão. Os pilotos serão monitorados semanalmente e os Planos reavaliados sempre que necessário.

Assim, pretende-se facilitar a identificação de eventuais pontos de correção e melhoria do presente Plano de Adequação para, progressivamente, aplicá-lo a todos os demais órgãos e entidades municipais.

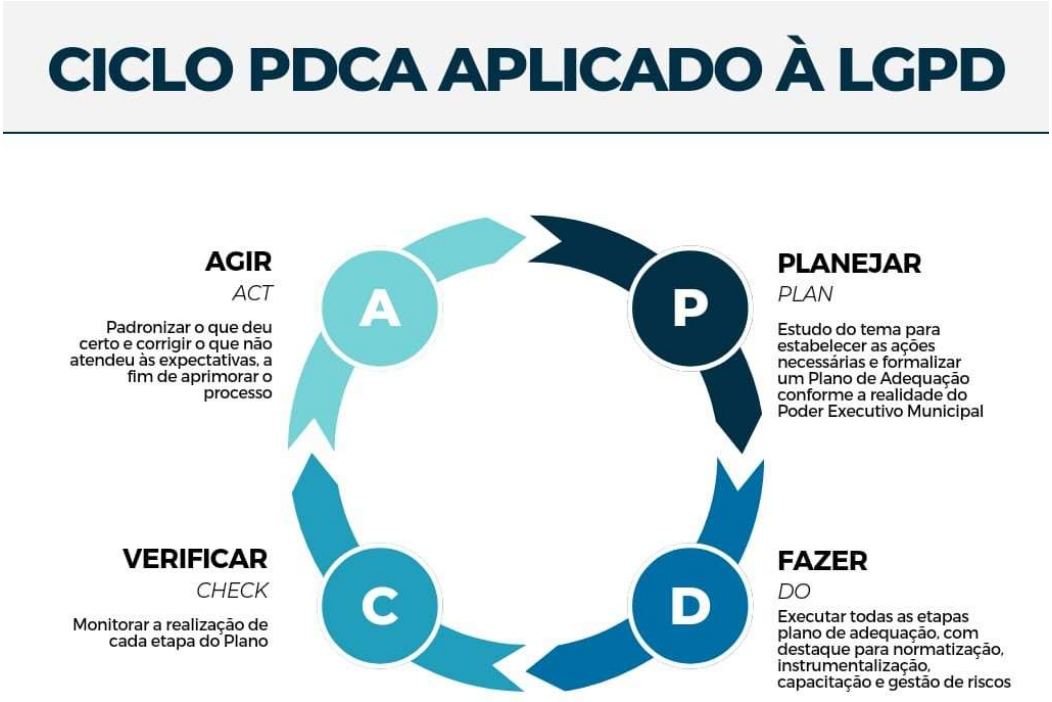
Vale ressaltar que a realização de Projetos Pilotos não impede a CGM de regulamentar, exarar orientações ou sanar eventuais dúvidas e, até mesmo, executar, simultaneamente, etapas deste Plano nos demais órgãos e entidades do Poder Executivo Municipal, conforme necessário.

10. REVISÃO E APRIMORAMENTO

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) entrou em vigor a partir de 2020, motivo pelo qual as instituições públicas e privadas ainda estão em fase de adequação a seus dispositivos.

Tendo em vista que ainda existem muitas discussões acerca da interpretação e implementação das normas referentes à proteção de dados pessoais, é necessário realizar a atualização periódica dos planos e políticas elaborados pelo Município.

Sendo assim, a implementação deste Plano será avaliada e revisada após o período do Projeto Piloto. Além disso, a Controladoria Geral do Município revisará os instrumentos desenvolvidos **anualmente** ou sempre que existirem alterações significativas no que tange à coleta, tratamento, guarda e compartilhamento de dados pessoais pelos órgãos e entidades municipais. Será aplicado o ciclo PDCA de melhoria contínua no processo de revisão do Plano visando a sua expansão, até a adequação de todos os órgãos e entidades municipais, conforme diagrama a seguir.



REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: Seção 1, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

GOVERNO FEDERAL. **Guia de Boas Práticas:** Lei Geral de Proteção de Dados (LGPD). 10 abr. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf.

GOVERNO FEDERAL. **Guia de Elaboração de Inventário de Dados Pessoais**: programa de privacidade e segurança da informação (ppsi). PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI). 2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_inventario_dados_pessoais.pdf.

GOVERNO FEDERAL. **Guia de Elaboração de Termo de Uso e Política de Privacidade**: guia de elaboração de termo de uso e política de privacidade. Guia de Elaboração de Termo de Uso e Política de Privacidade. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_termo_uso_politica_privacidade.pdf.

GOVERNO FEDERAL. **Oficina Dirigida**: relatório de impacto à proteção de dados pessoais - ripd. Relatório de Impacto à Proteção de Dados Pessoais - RIPD. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/apresentacoes/apresentacao_ripd.pdf.

PARANÁ (Estado). Controladoria Geral do Estado. **Manual de Implementação da LGPD da Controladoria-Geral do Estado do Paraná**. Disponível em: https://www.cge.pr.gov.br/Noticia/CGE-publica-guias-para-implantacao-da-LGPD-nos-orgaos-estaduais.

REDE NACIONAL DE OUVIDORIAS. **Guia de Boas Práticas na Aplicação da Lei Geral de Proteção de Proteção de Dados Pessoais nas Ouvidorias Públicas**. 2023. Disponível em: https://www.gov.br/ouvidorias/pt-br/ouvidorias/rede-de-ouvidorias/GuiadeBoasPraticasdaLGPD.pdf.

SÃO PAULO (município). Controladoria Geral do Município. **Guia Orientativo sobre a Instrução Normativa CGM/SP N. 01/2022 para a Administração Pública do Município de São Paulo.** 2022. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/GuiaOrientativosobreaInstrucaoNormativaCGM-SPn%C2%BA01-2022paraaAdministracaoPublicadoMunicipiodeSaoPaulo_publicacao_26_01_2023.pdf.

ANEXO I

MODELO DE QUESTIONÁRIO PARA DIAGNÓSTICO INICIAL - CULTURA ORGANIZACIONAL[10]

Este questionário procura identificar o conhecimento de todos os servidores municipais sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018. São 13 (treze) perguntas e não há identificação das pessoas respondentes.

*Obrigatório

1. Informe sua faixa etária:

- 18 a 29
- 30 a 59
- 60 a 69
- 70 ou mais.

2. Informe seu nível de escolaridade:

- Ensino Fundamental Incompleto
- Ensino Fundamental Completo
- Ensino Médio Incompleto
- Ensino Médio Completo
- Superior Incompleto
- Superior Completo
- Mestrado Ou Doutorado

3. Qual a sua secretaria de atuação?_____.

4. Você já participou de capacitação sobre a Lei Geral de Proteção de Dados dentro ou fora do órgão? *

- Palestra Seminário
- Curso (Presencial ou EaD) Leitura de textos e documentos
- Outro:
- Não possuo capacitação no assunto

[10] Extraído do "Manual de Implementação da LGPD" da Controladoria-Geral do Estado do Paraná. Disponível em: < CGE publica guias para implantação da LGPD nos órgãos estaduais | Controladoria Geral do Estado do Paraná>.

5. Você sabe o que são dados pessoais? *

- ○ Sim
- ○ Não

Se SIM, em sua opinião, o que são dados pessoais?*

_____

6. Em seu trabalho no órgão, você realiza alguma atividade que envolve dados pessoais? *

- ○ Sim
- ○ Não
- ○ Não sei

7. Por quais meios você trabalha com dados pessoais? *

- ○ Sistemas Informatizados
- ○ Planilhas Eletrônicas
- ○ Documentos Eletrônicos
- ○ Documentos Físicos
- ○ Outro:
- ○ Não sei dizer se trabalho com dados pessoais no dia a dia

8. Dos fluxos que fazem parte do seu trabalho no órgão, em quais você faz uso de dados pessoais? *

- ○ Cadastro de pessoas
- ○ Requisição de informações
- ○ Análise jurídica
- ○ Requerimentos diversos
- ○ Solicitação de cumprimento de decisões
- ○ Análise de processos administrativos
- ○ Outro:
- ○ Não sei informar

9. Por quais meios você recebe as solicitações para trabalhar com dados pessoais no órgão? *

- ○ E-mail
- ○ Físico
- ○ Telefone
- ○ Sistema informatizado
- ○ Outro:
- ○ Não sei responder

10. Há alguma orientação a respeito do tratamento dos dados pessoais que instruem as solicitações ou requerimentos? *

- Sim
- Não
- Não é necessária orientação, pois o uso da informação é institucional
- Outro:
- Não sei responder

11. Somente os dados pessoais estritamente necessários são acessados? *

- Sim
- Não
- Não sei informar

12. Dê uma nota, de 0 a 10, para o seu nível de conhecimento atual no tema de Proteção de Dados Pessoais:_____*

13. Deseja fazer alguma consideração sobre o assunto Proteção de Dados?

- Se sim, descreva: _____
- Não

ANEXO II – TAXONOMIA DE DADOS PESSOAIS[11]

i. Categorias ordinárias de dados pessoais:

1. Identificação pessoal:

a. Detalhes de identificação pessoal;

i. Dados de identificação pessoal atribuídos por instituições governamentais.

b. Dados de identificação eletrônica; e

c. Dados de localização eletrônica.

2. Corpo:

a. Detalhes biográficos;

b. Detalhes militares;

c. Descrição física; e

d. Detalhes imigratórios.

3. Mente:

a. Descrição psicológica.

4. Imagem:

a. Voz; e

b. Vídeo e imagem;

i. Dados de Vídeo e imagem enquanto relacionados à segurança pública;

5. Hábitos:

a. Detalhes sobre hábitos pessoais;

b. Detalhes sobre estilo de vida;

c. Detalhes sobre distinções;

d. Detalhes sobre bens e direitos enquanto relacionados aos hábitos pessoais;

e. Detalhes sobre viagens e deslocamentos;

f. Detalhes sobre denúncias, incidentes ou acidentes;

g. Detalhes sobre núcleos sociais; e

h. Detalhes sobre uso de mídias.

6. Lazer:

a. Detalhes sobre interesses de lazer.

7. Consumo:

a. Detalhes sobre bens e serviços enquanto relacionados a hábitos de consumo.

8. Finanças:

a. Detalhes de identificação financeira;

b. Detalhes sobre recursos financeiros;

c. Detalhes sobre dívidas e despesas;

d. Detalhes sobre situação financeira;

e. Detalhes sobre empréstimos, hipotecas e linhas de crédito;

f. Detalhes sobre assistência financeira;

---

[11] Taxonomia extraída do "Guia Orientativo sobre a Instrução Normativa CGM/SP N. 01/2022 para a Administração Pública do Município de São Paulo", disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/GuiaOrientativosobreaInstrucaoNormativaCGM-SPn%C2%BA01-2022paraaAdministracaoPublicadoMunicipiodeSaoPaulo_publicacao_26_01_2023.pdf

g. Detalhes de apólice de seguro;
h. Detalhes de plano de pensão;
i. Detalhes sore transações financeiras;
j. Detalhes sobre compensações financeiras;
k. Detalhes sobre atividades profissionais;
l. Detalhes sobre acordos e ajustes comerciais; e
m. Detalhes sobre autorizações enquanto relacionadas ao tratamento de dados financeiros.

9. Residência:
a. Detalhes residenciais.

10. Família:
a. Detalhes sobre relacionamentos atuais;
b. Detalhes sobre relacionamentos anteriores;
c. Detalhes sobre núcleo familiar.

11. Educação:
a. Dados acadêmicos;
b. Detalhes financeiro-acadêmicos;
c. Detalhes sobre qualificações e experiências acadêmico-profissionais.

12. Trabalho:
a. Detalhes sobre ocupações atuais;
b. Detalhes sobre processos de seleção;
c. Detalhes sobre rescisões;
d. Detalhes sobre ocupações anteriores;
e. Detalhes sobre avaliações de desempenho; e
f. Detalhes sobre disciplina e absenteísmo.

13. Filiações:
a. Detalhes sobre associações as quais é filiado o titular de dados pessoais.

14. Conflitos:
a. Detalhes sobre processos judiciais em curso;
b. Detalhes sobre decisões judiciais;
c. Detalhes sobre processos administrativos em curso; e
d. Detalhes sobre decisões administrativas.

i. Categorias especiais de dados pessoais:

1. Dados pessoais de crianças e adolescentes:
   a. Dados pessoais de crianças; e
   b. Dados pessoais de adolescentes.
2. Dados pessoais sensíveis:
   a. Origem racial ou étnica;
   b. Convicção religiosa;
   c. Filiação a organização de caráter religioso;
   d. Opinião política;
   e. Filiação a organização de caráter político;
   f. Filiação a sindicato;
   g. Filiação a organização de caráter filosófico;
   h. Saúde ou vida sexual;
   i. Genéticos; e
   j. Biométricos.