Plano de Adequação

Comissão Municipal de Proteção de Dados

Plano de Adequação 2022

Prefeitura Municipal de Mairiporã

Encarregado pelo Tratamento de Dados Pessoais

Alexandre Chimura sakemi

Comissão Municipal de Proteção de Dados

Data	Versão	Descrição	Autor
07/06/2022	1	Plano de Adequação à LGPD	

Sumário

Plano de adequação LGPD

1. Apresentação.

PMM- Prefeitura Municipal de Mairiporã;

O presente documento tem o propósito de demostrar a implantação na PMM da Leinº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais(LGPD) - alterada pela Lei nº 13.853, de 08 de julho de 2019.

2. Introdução.

A Lei Geral de Proteção de Dados (LGPD) entrou e vigor no dia 19 de setembro de 2020. Essa Lei "dispõe sobre o **tratamento de dados pessoais** (...) com o objetivo de proteger os direitos fundamentais de liberdade e **privacidade** e o livre desenvolvimento da personalidade da pessoa natural". Em síntese, garante à privacidade dos dados pessoais de todos os brasileiros. Portanto, implica diretamente em como a PMM**,** como um todo (e todos seus servidores)**,** trata os dados pessoais a que têm acesso. Dados pessoais são todas as informações referentes a pessoa, podendo ser o CPF, R.G, matrícula, endereço e os dados pessoais sensíveis que podem ser opção religiosa, orientação sexual, raça, renda e dados de saúde**,** por exemplo. A forma de tratamento destes dados pessoais, isto é, como os servidores da PMM recebem, armazenam e os distribuem, se não for realizado de acordo com a referida Lei, pode implicar em sanções a todos os envolvidos. Isso configurou uma verdadeira mudança de cultura sobre o tratamento de dados pessoais no Brasil de forma geral, e em particular na PMM. Além disso, deu enorme responsabilidade aos órgãos e instituições que optem por solicitar dados pessoais de seus usuários.

A LGPD define princípios (art. 6º) e condicionalidades (art. 7º) para o tratamento de dados pessoais. Isso é, todo o tratamento de dados pessoais realizado pela instituição deve, necessariamente, respeitar os dez princípios apresentados no art.6º da Lei[1], dentre os quais podemos destacar: identificar a finalidade para

[1] São eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e, responsabilização e prestação de contas.

qual há tratamento de cada dado pessoal, ou seja, deve haver um motivo específico para o tratamento daquele dado pessoal; e o livre acesso ao dono do dado pessoal a informações sobre como e porque ocorre o tratamento de seu dado pessoal. Além disso, todo tratamento de dado pessoal deve ser amparado em uma das hipóteses explicativas para intervenção de dados apresentados no art.7º, que no caso de nossa instituição**,** seria o inciso III, no qual diz: “pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos (...)”.

Outra exigência apresentada na LGPD, e que cabe estar nesta introdução pela grande importância ao longo de todo o documento, é a transparência do tratamento de dados pessoais que deve ser disponibilizada ao dono destes dados, chamado titular. São diversos os momentos no qual essa clareza é apresentada como um direito do titular, especialmente no art. 18. Assim, o titular tem o direito de saber como seus dados são tratados, em quais momentos, onde são arquivados, com quem são distribuídos, qual o tempo de guarda. Enfim, tudo sobre seus dados pessoais cedidos à instituição. E, além de ser respondida essas questões diretamente ao solicitante, também devem estar publicadas abertamente nas páginas da Instituição.

Depois de respeitar os princípios e condicionalidades para o tratamento de dados pessoais e respeitar todos os direitos do titular, a Lei trata com ênfase o tema de segurança e sigilo destes dados. Nesse caso, impõe como obrigação da instituição adotar medidas de segurança que impeçam o acesso indevido de terceiros. Estas medidas devem ser monitoradas, descritas e publicizadas, a fim de garantir sua efetividade.

Para trabalhar os quesitos que ressaltamos (princípios, condicionalidades, direitos do titular e segurança) e diversos outros apontado pela Lei, além de atender suas exigências, em 2 de Maio a Portaria 23.152/2022 designou o Encarregado de dados pessoais da PMM (DPO). Esta figura tem atribuição de atuar como canal de comunicação entre a PMM, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD). Em 6 de Abril o DECRETO Nº 9.484 constituiu a Comissão Municipal de Proteção de dados, com a participação de cinco servidores de diversos setores da PMM. Tal comissão**,** realiza reuniões quadrimestrais por oficio e quando forem provocados e já

produziu documentos informativos sobre a LGPD. Essa seria a estrutura de governança para a implantação da LGPD na PMM.

3. Objetivos do Plano de Adequação.

O objetivo geral deste documento é adequar a PMM aos requisitos da LGPD. De forma específica**,** isso significa realizar um conjunto de atividades que serão traduzidas em ações concretas a serem atingidas. As atividades são:

1- Identificar Controlador,Encarregado e apresentar estrutura de Governança**.**

2- Apresentar canal de comunicação e de denúncias para os titulares**.**

3- Capacitar e orientar servidores da PMM Atraves da Escola de Governo quanto a cultura de privacidade dados pessoais**.**

4- Mapear os dados pessoais utilizados na PMM – Inventário de Dados Pessoais (IDP)**.**

5- Verificar a adequação à lei do tratamento dos dados pessoais e seus riscos (analisar isso nos IDPs)**.**

6- Sistemas, base de dados e medidas de segurança**.**

7- Elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**.**

8- Elaborar termo de uso para aplicativos da PMM e anúncio de cookies nos sites da PMM**.**

9- Adequação de contratos e transferência internacional de dados**.** 10- Investigações internas e programas de auditoria e monitoramento**.**

3.1. Identificar Controlador, Encarregado e apresentar estrutura administrativa da LGPD na PMM.

O Controlador é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”. Portanto**,** é a figura central e de maior importância quanto à tomada de decisões sobre a LGPD na instituição. Além disso, não é uma opção a definição do Controlador, mas é imposta pela Lei, que em outras palavras, para nosso caso, diz que o Controlador é a PMM, representada pelos responsáveis de cada secretaria assim designados. A definição do Encarregado, por outro lado, é uma decisão discricionária**,** e sua figura é definida como: “pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção dos Dados (ANPD)”. O

artigo 41 da Lei detalha um pouco mais as atividades do Encarregado[2] e o Decreto da PMM designou o Encarregado de dados pessoais da PMM (DPO).

Entende-se como estrutura administrativa da LGPD na UFU as funções administrativas e estruturas administrativas que estão a cargo da tomada de decisão sobre o tema na instituição. Nesse sentido, além do Controlador e Encarregado, já citados, foi criada em 13 de novembro pela Portaria 971 do Reitor a Comissão de análise e implementação da LGPD, com a participação de nove servidores de diversos setores da UFU. Dessa forma, tem-se a estrutura responsável pela tomada de decisão e pela implantação da LGPD na UFU. Essa estrutura que irá definir orientações gerais e boas práticas a serem difundidas por toda a instituição, de forma que cada servidor entenda e aplique essa mudança de cultura que representa a LGPD. Esta estrutura também responde aos questionamentos e manifestações dos titulares de dados e da ANPD, são os que tem a responsabilização primeira no caso de falha de implantação da Lei,sem tirar a responsabilidade compartilhada de cada servidor que trata diretamente os dados pessoais.

3.1. Ações	Mar/21
Definir Encarregado	x
Criar Comissão de análise e implementação da LGPD	x

3.2. Apresentar canal de comunicação e de denúncias para os titulares

Foi criada página no site da PMM com divulgação da LGPD. Nesse espaço, são atendidas algumas obrigações legais, como informar canal de manifestação para titulares em caso de pedidos a instituição, que será por meio de correio eletrônico utilizado na PMM, além de apresentar informações doEncarregado, conforme art.41. Outrossim, neste espaço será reunido todo o material produzido pela Comissão. Portanto, é o espaço no qual o tema LGPD será publicizado pela instituição.O endereço é:

.

3.2. Ações	Maio/21
Criar página sobre LGPD na PMM	x

3.3. Capacitar e Orientar servidores quanto a cultura de privacidade de dados pessoais

Orientar pode significar indicar a direção correta com base em pontos referenciais. Estes pontos referenciais, quando falamos da LGPD, são as exigências práticas legais e às experiências exitosas socialmente reconhecidas. A atribuição desta orientação é do Encarregado e da Comissão**,** e é fundamental para comprovar as ações da instituição no sentido de obedecer estritamente a Lei.

As formas adotadas para essas ações podem ser diversas, mas as mais comuns observadas foram: comunicações oficiais para estrutura administrativa, como memorandos ; e divulgação de cartilhas no formato digital sobre o tema.Foi disponibilizado um curso pela Ecola de Governo com a participação de todos os responsaveis de cada secretaria para introduzir sobre o tema e pelo menos mais uma com certificação externa.

A capacitação segue no mesmo sentido apontado acima, isto é, prover caminhos positivos sobre o tema, porém, enquanto a orientação é emanada pela estrutura administrativa da LGPD**,** e deve ser seguida como instrução administrativa pelos servidores, a capacitação é uma decisão que cabe ao servidor, para que adquira conhecimentos mais detalhados e haja um reconhecimento institucional sobre esse esforço.

3.3. Ações	Jul/Ago21	Set/Out/21	fev/22	mar/22
Elaborar memorando mensais sobre o tema	x			
Divulgar cartillhas sobre o tema		x	x	x
Divulgar curso de capacitação sobre o tema que conte para progressão funcional			x	

[3] A Controladoria já elaborou um guia inicial. Além disso, pode ser encontrado em outras Instituições por exemplo:

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd

3.4. Mapear os dados pessoais utilizados na PMM – Inventário de Dados Pessoais (IDP)

O mapeamento dos dados pessoais pode ser entendido como rastrear, esquematizar, diagramar ou estruturar sua utilização na instituição. Isso significa ter a consciência, e o registro, desses processos**,** individualmente. Entender como o dado é coletado, o porquê de sua coleta, onde é armazenado, quais medidas de segurança o resguarda, quem o utiliza, com quem é compartilhado, enfim, todas ações que envolvem sua manipulação, do começo ao fim. Isso tudo, é uma forma de comprovar o entendimento sobre cada dado pessoal tratado, afinal a instituição deve ter um motivo evidente e um cuidado para solicitar informações de seus usuários ou de seus funcionários.

Esse tema é recorrente na LGPD, pois é constante a necessidade de comprovação da finalidade do tratamento, a forma de tratamento e comprovação de existência de tratamento. O art. 37 especifica isso quando diz que “o controlador e operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse”. De forma prática, e o que se tem difundido na administração pública, é que**,** para atingir essa ação é preciso fazer então um Inventário de Dados Pessoais (IDP), que “consiste em uma excelente forma de fazer um balanço do que o órgão e entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operação são realizadas com eles” (Brasil, 2020b).

Dessa forma, para ter o IDP completo da instituição, é preciso que cada processo que utilize dado pessoal faça seu IDP. O modelo de IDP adotado para essa tarefa foi baseado em modelo apresentado em curso da Guias operacionais para adequação à LGPD, que foi usado como referência e sofreu alterações por parte da Comissão para se adequar às necessidades da PMM.

Como forma de implantar essa estratégia que envolve todos os setores da PMM, pois todos terão que fazer seu IDP, sugere-se o seguinte caminho: 1- preenchimento do IDP em um setor piloto, que como sugestão fica a DTI, por

englobar diversos processos da instituição e por ter representante na Comissão. Essa experiência com piloto é importante para aprendizado da Comissão antes

da aplicação para toda a PMM; - Por fim, a validação e consolidação de todos os IDPs pela Comissão. Durante esse processo, cabe esclarecer o papel da Comissão e do Encarregado de acompanhamento e auxílio de qualquer setor que estiver com dúvida ou sugestão para o preenchimento do IDP. Ao final, a Comissão terá a palavra final para consolidar e validar todos os IDPs da instituição. Porém, será também fundamental seu acompanhamento e a ajuda aos envolvidos. Isso poderá ser feito por meio da disponibilização de canal de comunicação direto com os responsáveis pelos preenchimentos dos IDPs nos setores.

3.4. Ações	fev/22	mar/22	abr/22
IDP piloto no DTI	x		
Elaboração de memorando	x		
Apresentar Mapeamento para todas secretarias		x	
IDP de dois casos da graduação, PPGs e UAs		x	
Consolidação dos IDPs da graduação, PPGs e UAs		x	x
IDPs dos setores administrativos		x	x
Validação e consolidação de todos os IDPs pela Comissão			x

3.5. Verificar a adequação à lei do tratamento dos dados pessoais e seus riscos (analisar isso nos IDPs)

O Inventário de Dados Pessoais é o documento pelo qual cada setor irá informar como é feito seu tratamento dos dados pessoais. Com esse documento**,** será possível avaliar a conformidade com a LGPD, isto é, se a forma com que o setor manuseia os dados pessoais respeita as exigências da Lei. Os requisitos solicitados podem ser resumidos no art. 6º, já citado, que cita os princípios que devem ser seguidos para o tratamento de dados pessoais[6]. Assim, caberá à Comissão essa avaliação de cada IDP.Esse momento de avaliação de conformidade**,** também possibilita uma avaliação de riscos inicial sobre o tratamento de cada dado pessoal na instituição. A avaliação de riscos busca identificar situações ou vulnerabilidades que possam implicar em falhas em garantir privacidade, segurança e adequação à Lei do tratamento de dados pessoais. O "Guia de Avaliação de Riscos e de Privacidade", documento elaborado pela Secretaria de Governo Digital (SGD) doMinistério da Economia**,** com intuito de padronizar essa avaliação em esfera federal, apresenta uma lista com 14 riscos a serem considerados[8]. Ver anexo 2.O art. 46 da Lei é explícito ao afirmar medidas para mitigação de eventuais riscos: "os agentes de tratamento devem adotar medidas de segurança, técnicase 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". Assim, nesse momento, além de identificar possíveis riscos em cada IDP**,** cabe tambémapontar possíveis ações de combate a esses riscos. O "Guia de Avaliação de Riscos e de Privacidade" apresenta um conjunto de 113 medidas de segurançaa serem aplicadas nos órgãos como um todo, e que podem servir como referência de medidas a serem adotas pelos

setores responsáveis pelos IDPs. Ver anexo 3.

Após analisar os pontos de vulnerabilidades, cada setor com auxílio da Comissão deverá elaborar uma política de boas práticas frente aos pontos de vulnerabilidades**,** com a finalidade de informar sobre os riscos de uma conduta negligente. Ademais, trabalhar na elaboração de padrões de ética e de conduta para informar qual é o comportamento esperado do servidor em relação ao serviço que desempenha.

3.5. Ações	jun/22	julh/22	Ago/22
Validação e consolidação de todos os IDPs pela Comissão	x		
Comissão avaliar riscos em cada IDP recebido	x	x	
Comissão verificar medidas de segurança em cada IDP recebido	x	x	
Comissão construir junto com cada setor uma política de boas práticas			x

3.6. Sistemas, base de dados e medidas de segurança.

3.6. Ações	Ago/22	Set/22	Out/22
Elaboração de memorando	x		
Cada responsável por sistema ou base de dados responder questionário sobre medidas de segurança	x		X
Comissão validar essa análise de Privacidade e Segurança		x	
Comissão reunir com Comissão e apresentar desafios	x		

3.7. Elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é documento “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”. Nele, é descrito e publicizado todo o tratamento de dados (finalidade, descrição, identificação dos agentes, necessidade e etc), os riscos deste tratamento e as medidas de segurança adotadas. É similar ao IDP, porém com maior detalhamento e publicidade, isto é, deve ser divulgado amplamente. Além disso, o RIPD pode ser uma exigência legal da Autoridade Nacional de Proteção de Dados (ANPD), que a depender da situação pode exigir esse relatório para

averiguação dos processos na instituição (artigos 4º, 10, 32 e 38 da Lei).

Por não ser obrigatório, sua elaboração para todos os tratamentos de dados pessoais não é exigida, apenas quando provocado pela ANPD. Entretanto, é importante o mapeamento dessa ferramenta por parte da Comissão, que pode ser inquirida a qualquer momento. Dessa forma, é importante a Comissão elaborar o RIPD como aprendizado e para os casos mais importantes, quais sejam: o tratamento de dados pessoais de crianças e adolescentes e para os dados sensíveis.

3.7. Ações	mai/22	jun/22	jul/22	ago/22
Elaboração do RIPD para dados pessoais de crianças e adolescentes pelo setor responsável juntamente com a Comissão	x	x		
Elaboração do RIPD dos dados pessoais sensíveis pelo setor responsável juntamente com a Comissão			x	x

3.8. Elaborar termo de uso para aplicativos e política de privacidade para coleta de dados na PMM e anúncio de cookies nos sites da PMM.

O termo de uso e a política de privacidade são ferramentas apresentadas pela Secretaria de Governo Digital (SGD)[11] para atender à exigência de publicidade aos titulares dos tratamentos de seus dados pessoais. Esta exigência está no art. 23 da Lei: " que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos". Portanto, a Lei não cita sobre termo de uso e política de privacidade, diz apenas da necessidade da informação pública.

Segue abaixo o entendimento da SGD:

"**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. Já a **Política de Privacidade**, é um documento informativo, no 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.

Tanto o Termo de Uso quanto a Política de Privacidade originam-se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular dos mesmos**,** e informarem como as atividades de tratamento de dados atendem os princípios dispostos no artigo 6º da **Lei Geral de Proteção de Dados (LGPD)**. Portanto, os dois documentos constituem, ao mesmo tempo, um dever do controlador e um direito do titular.

O Termo deve apresentar informações claras e precisas em relação aos serviços oferecidos aos usuários pela aplicação e a forma de prestação deles, bem como os requisitos para acessá-los e os locais e formas para o usuário apresentar eventual manifestação sobre a prestação do serviço.

Em observância aos princípios da publicidade e da transparência**,** e a fim de garantir aos cidadãos amplo acesso às informações, os termos devem ser constantemente atualizados a fim de refletir, de modo claro e preciso, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos usuários, que somente poderão ser utilizados caso sejam necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos ou não sejam vedadas pela legislação".

Resumidamente, isso significa que, para publicizar os tratamentos de dados pessoais em casos de utilização de sistemas, é necessário elaborar o termo de uso e que tal termo seja anuído. Por outro lado, caso não envolva a utilização de sistema, apenas como forma de informar o titular da utilização de seus dados, faz-se então pertinente a política de privacidade. Portanto, há um entendimento que deve haver um termo de uso explícito em cada sistema utilizado pela PMM e**,** também uma política de privacidade explícita em toda coleta de dado pessoal na UFU, pois o titular deve ser informado sobre os procedimentos adotados com seus dados pessoais[12], e o melhor momento para tanto seria na coleta do dado pessoal do titular.

Outra informação que deve ser disponibilizada é sobre os cookies de navegação utilizadas nos sites da PMM. Essas ferramentas arquivam o histórico de navegação de cada usuário no site, o que se traduz em uma forma de tratamento de dado pessoal. O que se tem observado são alertas sobre cookies em diversos sites públicos e privados[13].

3.8. Ações	out/22	Nov/22	DEZ/22

Reunião com CTIC para expor a necessidade do termo de uso para os sistemas da UFU	x	x	
CTIC apresentar termos de uso para sistemas da UFU para validação da Comissão		x	
Comissão e CTIC avaliar a necessidade de elaborar política de cookies		x	
Comissão mapear os momentos de coletas de dados na UFU e verificar se apresentam política de privacidade		x	
Comissão elaborar uma política de privacidade para esses casos		x	x

3.9. Adequação de contratos e transferência internacional de dados O uso compartilhado de dados pessoais é uma previsão da LGPD. Ela disciplina como os órgãos públicos podem compartilhar seus dados com outros órgãos públicos ou com empresas privadas. O conceito é: "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". Para legalidade desse compartilhamento**,** os órgãos devem atender um conjunto de requisitos, alguns já tratados acima, e que podemos destacar: existir uma justificativa legal (uma finalidade) para esse compartilhamento, ser publicizado para o titular dos dados e o órgão ou empresa privada receptora desses dados comprovar medidas de segurança e privacidade. Tais exigências**,** impactam nos contratos da instituição com esses órgãos ou com empresas privadas, pois precisam refletir esses conceitos. Isto é, necessariamente é preciso estar no papel assinado entre as partes esses pontos de conformidade para que as empresas possam receber dados pessoais da PMM.

Especificamente sobre os contratos de TI, as exigências de conformidade são ainda mais amplas e demandam comprovação. Esses elementos são explorados no "Guia de boas práticas para especificação de requisitos de segurança da informação e privacidade em contratações de tecnologia da informação"[14].

Essas condicionalidades para compartilhamento de dados impactam também o caso de transferência internacional de dados, uma vez que não deixam de ser uma forma de transferência. Igualmente, este processo envolve um conjunto de

comprovações para os titulares de dados para que a instituição esteja resguardada.

3.9. Ações	mar/21	abr/21	mai/21
Comissão verificar nos IDPs se há compartilhamento de dados pessoais		x	x
Comissão consultar setor de contratos sobre contratos daUFU que compartilham dados pessoais	x		
Comissão consultar CTIC sobre contratos de TI e sua adequação a LGPD	x		
Comissão consultar DRII sobre transferência internacional de dados	x		
Comissão elaborar orientação sobre os riscos de compartilhamento não autorizados	x		

3.10. Investigações Internas e programas de auditoria e monitoramento As investigações internas deverão ser realizadas sempre que houver uma denúncia de irregularidade. Para isso, é necessário seguir uma lista de procedimentos na qual devem constar as hipóteses levantadas, o problema apresentado, os motivos para a instauração do processo, as pessoas envolvidase as testemunhas a serem entrevistadas. O ideal é que seja coletado o máximo de informações para um parecer justo e adequado.Procedimento para conduzir um processo de investigaçãoA investigação deve contar com atividades de inspeção, averiguação de registros e documentos e a análise detalhada de todas as informações recolhidas. Também**,** é importante que se observe o comportamento e as reações das partes, buscando entender todas asmotivações.

3.10.1. Rol de práticas recomendadas

- envolver a alta administração em todas as ações;
- discutir internamente entre os gestores e os responsáveis da investigação os procedimentos para uma auditoria;
- contar com o apoio técnico de outras áreas, como recursos humanos, tecnologia da informação, contabilidade, direito e finanças para a análise de informações específicas;
- conhecer todas as normas nacionais (como a Lei Anticorrupção) e

internacionais que se aplicarem, uma vez que pode haver questionamentos e envolvimento de órgãos fiscalizadores;

- repassar os fatos apurados aos meios responsáveis para providências necessárias, encaminhando todas as provas e documentos;
- preparar o setor de comunicação interna para comunicar os fatos dentro e fora da instituição, quando for o caso;
- tratar todas as informações com seriedade e profissionalismo, assegurando a confidencialidade durante todo o processo;
- criar mecanismos para evitar qualquer tipo de retaliação ao denunciante e às testemunhas;
- assegurar que o processo investigativo seja respeitado e que as medidas necessárias sejam tomadas, inclusive buscando evitar que o problema persista.

3.10.2. Realização de entrevistas

Durante uma entrevista é importante que se tenha imparcialidade e muito tato ao lidar com as pessoas, principalmente quando elas se encontram em situação frágil ou de desconforto. Se uma entrevista não for bem conduzida, ela pode levar a informações falsas ou parciais, que prejudicam o processo investigativo como um todo. A entrevista deve ser preparada com antecedência, ainda que o entrevistador seja experiente e conheça bem o assunto. O ideal é se despir de qualquer pré-julgamento, mesmo que haja indícios prévios. O planejamento é importante para entender quais são as testemunhas com maior relevância e como conversar com cada uma delas. Isso ajuda a entender qual a melhor abordagem, o que deve ser discutido e até mesmo para criar uma certa credibilidade com cada entrevistado, mesmo que imprevistos possam acontecer. É de fundamental importância**,** deixar os entrevistados à vontade, sendo claro e respeitoso com as pessoas. Também, é bom manter uma isenção sobre o assunto, não fazer perguntas tendenciosas ou que busquem orientar à resposta. Necessário se faz saber interromper o entrevistado**,** pois o tempo em um processo investigatório deve ser bem aproveitado**,** devendo o entrevistador não dar margem para

divagações fora de contexto. Deve-se juntar versões diferentes para uma mesma história a fim de criar uma narrativa mais condizente com os fatos a estratégia para essa questão, portanto, entrevistar uma pessoa por vez. O ideal é não realizar a entrevista sozinho, para que não passe algum detalhe despercebido, assim, enquanto uma pessoa toma nota, a outra entrevista.

3.10.3. Auditoria e monitoramento

Para realizar uma auditoria que seja eficaz**,** serão exigidos acessos às pastas, arquivos, vídeos, websites, que contenham dados pessoais/sensíveis, além da realização de testes de segurança, que simule invasões aos sistemas ou mesmo a possibilidade de alterar os arquivos contidos em pastas armazenadas em computadores locais.

Dessa maneira**,** é importante o envolvimento dos diretores e assessores acadêmicos de cada área nas operações para auxiliar os auditores e, especificar as restrições de acesso e procedimentos existentes em cada departamento.

É necessário apontar qual será o escopo**,** bem como as principais áreas que serão auditadas, se for o caso solicitar acompanhamento de um servidor da área de informática.

Após a auditoria**,** é essencial manter um monitoramento, com a finalidade de implementar novas medidas de proteção de forma preventiva e realizar procedimentos corretivos, criar relatórios regulares sobre o estado do setor, dentre outras tarefas.

3.10. Ações	set/22	out/22	nov/22	dez/22
Auditoria	x			
Monitoramento		x	x	x

Resumo Ações

3.1. Ações	nov/21	dez/21	jan/22	fev/22	mar/22	abr/22	mai/22	jun/21	jul/21	ago/21	set-dez/21
Definir Encarregado	x										
Criar Comissão de análise e implementação da LGPD	x										
3.2. Ações											
Criar página sobre LGPD na PMM		x									
3.3. Ações											
Elaborar ofícios circulares mensais sobre o tema		x		x	x	x	x	x	x	x	
Divulgar guias sobre o tema		x		x	x						
Divulgar curso de capacitação sobre o tema que conte para progressão funcional				x							
3.4. Ações											
IDP piloto na PMM				x							
Elaboração de Ofício Circular (com protocolo do processo)				x							
Apresentar Ofício para todas Unidades Administrativas e Acadêmicas					x						
IDP de dois casos da graduação, PPGs e UAs					x						
Consolidação dos IDPs da graduação, PPGs e UAs					x	x					
IDPs dos setores administrativos					x	x					
Validação e consolidação de todos os IDPs pela Comissão						x					
3.5. Ações											
Validação e consolidação de todos os IDPs pela Comissão						x					
Comissão avaliar riscos em cada IDP recebido						x	x				
Comissão verificar medidas de segurança em cada IDP recebido						x	x				
Comissão construir junto com cada setor uma política de boas práticas								x			
3.6. Ações											
Elaboração de Memorando					x						
Cada responsável por sistema ou base de dados responder questionário sobre medidas de segurança					x						
Comissão validar essa análise de Privacidade e Segurança						x					
Comissão reunir com Comissão e apresentar desafios					x						
3.7. Ações											

Elaboração do RIPD para dados pessoais de crianças e adolescentes pela setor reponsável juntamente com a Comissão							x	x			
Elaboração do RIPD dos dados pessoais sensíveis pelo setor responsável juntamente com a Comissão									x	x	
3.8. Ações											
Reunião com TI para expor a necessidade do termo de uso para os sistemas da PMM					x	x					
TI apresentar termos de uso para sistemas da PMM para validação da Comissão						x					
Comissão e TI avaliar a necessidade de elaborar política de cookies						x					
Comissão mapear os momentos de coletas de dados na PMM e verificar se apresentam política de privacidade						x					
Comissão elaborar uma política de privacidade para esses casos						x	x				
3.9. Ações											
Comissão verificar nos IDPs se há compartilhamento de dados pessoais						x	x				
Comissão consultar setor de contratos sobre contratos da PMM que compartilham dados pessoais					x						
Comissão consultar Licitação sobre contratos de TI e sua adequação a LGPD					x						
Comissão consultar sobre transferência internacional de dados					x						
Comissão elaborar orientação sobre os riscos de compartilhamento não autorizados					x						
3.10. Ações											
Auditoria											x
Monitoramento											x

Referências Bibliográficas
BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm .
Acesso em: 19 fev de 2021.

BRASIL. Ministério da Economia. Guia de Elaboração de Programa de Governança em Privacidade. Brasília, ME, 2020a. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf .

BRASIL. Ministério da Economia. Guia de Elaboração de Inventário de Dados Pessoais. Brasília, ME, 2020b. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca-de- dados/GuiaInventario.pdf

BRASIL. Ministério da Economia. Guia de Elaboração de Termo de Uso e Política de Privacidade para serviços públicos. Brasília, ME, 2020c. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaTermoUso.pdf

BRASIL. Ministério da Economia. Guia de Avaliação de Riscos de Segurança e Privacidade. Brasília, ME, 2020d. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de- avaliacao-de-riscos-de-seguranca-e-privacidade.pdf

BRASIL. Ministério da Economia. Guia de Avaliação de Riscos de Segurança e Privacidade. Brasília, ME, 2020d. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de- avaliacao-de-riscos-de-seguranca-e-privacidade.pdf

BRASIL. Ministério da Economia. Guia de Boas Práticas para Especificação de Requisitos de Segurança da Informação e Privacidade em Contratações de Tecnologia da Informação. Brasília, ME, 2020e. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de- dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. Guia de Boas
Práticas LGPD. Abril 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas- praticas-lei-geral-de-protecao-de-dados-lgpd . Acesso em: 19 fev de 2021.

Anexo 2

Lista de Riscos

ID	Riscos	Escopo do risco
1	Acesso não autorizado	Acesso indevido (permissões indevidas) a umambiente físico ou lógico.
2	Coleção excessiva	Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.
3	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais	Instituição não atende sua finalidade legal e compartilha os dados sem consentimento do titular dos dados pessoais (LGPD, art. 27).
		Garantia de atendimento dos direitos do titular, conforme descrito nos artigos 17 a 23 da LGPD.Art. 17. O titular dos dados pessoais tem direito a obter do controlador mediante requisição:I - confirmação da existência de tratamento;II - acesso aos dados; III - correção de dados incompletos, inexatos ou

4	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei
5	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.)	Dados de entrada que não são corretamente validados, operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado.
6	Informação insuficiente sobre a finalidade do tratamento	O tratamento de dados pessoais realizado de forma eletrônica ou documento em papel deve atender a uma finalidade e ser exposto de forma transparente e clara ao detentor dos dados pessoais.
7	Modificação não autorizada	Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada. Um processamento indevido pode gerar uma modificação não autorizada.

8	Perda	Perdas provocadas por ações intencionais de usuários oriundas de uma exclusão indevida ou devida e não comunicada, e provenientes de ações não intencionais como falhas em sistemas, sobrescrita de dados, falhas em hardware, entre outras.
9	Reidentificação de dados pseudonimizados	Dados pessoais podem ser reidentificados por cruzamento simples de dados pessoais (LGPD, art. 12 e 13).
10	Remoção não autorizada	Usuário não tem a permissão para retirar ou copiar dados pessoais para outro local.
11	Retenção prolongada de dados pessoais sem necessidade	O término da prestação de um serviço ou do prazo da retenção dos dados pessoais para fins legais deve culminar com aexclusão e/ou descarte seguro(a) dos dados pessoais.
12	Roubo	Dados roubados nas dependências interna do controlador/operador, falhas nos controles de segurança dos sistemas (a exemplo da ausência ou fraca criptografia, falha de sistema que permita escalação de privilégio ou tratamentos indevidos), entre outras.
13	Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)	Controlador de dados pessoais não obtém consentimento do titular para realizar um tratamentode dados pessoais sem embasamento legal.
14	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	A realização de operação de processamento de dados pessoais deve estar em conformidade com a LGPD. Qualquer operação de processamento que não atenda esserequisito pode produzir informações com vinculações ou associações indevidas.

SILVIO HIPOLITO:28743454828 Assinado de forma digital por SILVIO HIPOLITO:28743454828 Dados: 2023.02.13 16:05:41 -03'00'

Assinatura dos Membros da Comissão Municipal de Proteção de Dados

RENATO CEZAR CAVALLARI:••••••••• Assinado de forma digital por RENATO CEZAR CAVALLARI:••••••••••• Dados:••••••••••••••••••

Assinatura do Secretário da Comissão Municipal de Proteção de Dados

LUIZ YASSUHIRO AIACYDA AKIMURA:32016423803 Assinado de forma digital por LUIZ YASSUHIRO AIACYDA AKIMURA:32016423803 Dados: 2022.12.06 16:39:10 -03'00'

Assinatura do Presidente da Comissão Municipal de Proteção de Dados

ALEXANDRE CHIMURA SAKEMI:26855843824 Assinado de forma digital por ALEXANDRE CHIMURA SAKEMI:26855843824 Dados: 2022.12.06 16:40:53 -03'00'

Assinatura do Encarregador Municipal de Proteção de Dados (DPO)

gov.br Documento assinado digitalmente ALEXANDRE PIMENTEL LIRA Data: 15/02/2023 15:00:27-0300 Verifique em https://verificador.iti.br