Manual de Adequação e Conformidade para o Tratamento de Dados Pessoais

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

Versão 1.0

Guarulhos, Setembro de 2021

MANUAL DE ADEQUAÇÃO E CONFORMIDADE PARA O TRATAMENTO DE DADOS PESSOAIS

Lei Geral de Proteção de Dados Pessoais -– LGPD

PREFEITURA DE GUARULHOS

Gustavo Henric Costa

Prefeito

Jesus Roque de Freitas

Vice-Prefeito

COMISSÃO DE ACESSO À INFORMAÇÃO

SECRETARIA DE GOVERNO

SECRETARIA DE JUSTIÇA

CONTROLADORIA GERAL DO MUNICÍPIO

SECRETARIA DE GESTÃO

SECRETARIA DE DIREITOS HUMANOS

CONTROLADORIA GERAL DO MUNICÍPIO

João Bruno Morato Macedo

Controlador Geral

Igor Said Mourad Naddi

Controlador Adjunto

DEPARTAMENTO DE TRANSPARÊNCIA E PROMOÇÃO DA INTEGRIDADE

Edson Ferreira Vale

Diretor do Departamento de Transparência e Promoção da Integridade

OUVIDORIA DO MUNICÍPIO

Ivo Shigueru Tomita

Ouvidor do Município

Renato Corte Lopes

Ouvidor Adjunto do Município

EQUIPE TÉCNICA DE ELABORAÇÃO DESTE MANUAL

Cecília Cristiane Frazão Martinez

Auxiliar Titular - CGM.04

Edson Ferreira Vale

Controlador de Dados - CGM.02

Ivo Shigueru Tomita

Operador Central - CGM.04

Jairo Costa dos Santos

Auxiliar Suplente - CGM.01

Renato Corte Lopes

Encarregado de Dados - CGM.04

Histórico de Versões

Data	Versão	Descrição	Autor
15/09/2021	1.0	Primeira Versão do Manual de Adequação e Conformidade para o Tratamento de Dados Pessoais	Equipe Técnica de Elaboração

PASSO A PASSO para a adequação e conformidade à LGPD no município de Guarulhos

SUMÁRIO

1

APRESENTAÇÃO

"Quem tem o conhecimento e sabe como utilizá-lo em seu benefício, tem o poder."
POLLONI (2000)

Com o veloz avanço tecnológico imposto ao mundo moderno nos últimos 50 anos, as organizações públicas e privadas tiveram que se adequar, estabelecendo políticas e procedimentos de segurança fundamentais para a gestão da segurança da informação e comunicações.

A segurança da informação evoluiu e não está apenas focada na confidencialidade da informação como anteriormente. Atende também os requisitos de assegurar disponibilidade, integridade, a autenticidade das informações. Todas as organizações estão em busca de comunicações seguras, dos sistemas seguros e de técnicas que permitam manipulação e armazenamento seguros das informações estratégicas.

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei Nacional nº 13.709, de 14 de agosto de 2018, estabeleceu as regras gerais para a proteção dos dados pessoais e da privacidade dos cidadãos, e foi regulamentada na Cidade de Guarulhos pelo Decreto Municipal nº 38.145, de 18 de junho de 2021.

Por essas normas, os agentes e servidores públicos devem conhecer e adotar as boas práticas de proteção e privacidade decorrentes de sua atividade funcional, preservando os direitos e garantias dos cidadãos em estrita conformidade com a lei.

A adequação dos órgãos e unidades em relação à LGPD requer uma transformação cultural inédita que alcançará os níveis estratégico, tático e operacional da instituição e deverá considerar a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço ou produto até sua execução (*Privacy by Design*), além de promover ações de conscientização de todo o corpo funcional no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Este trabalho visa à realização da análise das informações sob responsabilidade do Município de Guarulhos atualmente, com base nas orientações estabelecidas pela legislação vigente, pelas Normas NBR ISO/IEC 27001, 27002, 27005, 27705, 31000, e orientações disponibilizadas pela Controladoria Geral da União, identificar os equívocos de gestão hoje existentes no armazenamento e tratamento destes dados.

Como resultado, será apresentado um modelo para o correto tratamento dessas informações, tornando-as seguras, sem torná-las inacessíveis ou ineficazes, com respeito aos direitos legais dos titulares de dados, inclusive, nas hipóteses aplicáveis, o da respectiva exclusão dos seus dados, a qualquer tempo e obedecendo o seu desejo expresso e, cientificando-o das conseqüências desta solicitação.

A gestão da informação é fundamental para o desenvolvimento das organizações e, nesse contexto, o Tribunal de Contas da União – TCU, em suas auditorias com abordagem em segurança da informação, em órgãos da Administração Pública Federal - APF, tem determinado que se *inventarie os ativos de informação e estabeleça critérios para a classificação desses ativos* (Acórdão nº. 1.092/2007 do TCU). As auditorias realizadas pelo TCU objetivam avaliar se a gestão da segurança da informação está sendo efetivamente implementada e executada de modo a propiciar um ambiente seguro e disponível no qual as ameaças e vulnerabilidades sejam conhecidas e controladas.

Será com este foco que buscaremos implantar cada uma das normas delineadas pela LGPD, como um planejamento dinâmico e inicial, de modo que

as abordagens delineadas neste plano estarão abertas a processos colaborativos com os agentes de tratamento.

Assim, durante a execução deste, podem as etapas e ações serem conduzidas de modo adaptado ou aprimorado, uma vez que inexistem metodologias determinadas e as experiências de outras unidades administrativas ainda são escassas para balizar a atuação dos responsáveis e dificilmente serão suficientes para abarcar todas as peculiaridades técnicas de cada Secretaria, Coordenadoria, Órgãos do Terceiro Setor e empresas ao Município vinculadas contratualmente e demais situações previstas em Lei.

2

MELHORES PRÁTICAS ASSOCIADAS À PROTEÇÃO DE DADOS – Normas Internacionais (DDH + GDPR), Constituição Federal, Lei Nacional, Decreto Municipal, Portarias, entre outros documentos.

Pode parecer curioso e até mesmo irônico nos dias de hoje, mas o primeiro movimento ligado a privacidade tinha como lema o direito de "não ser perturbado"

Existem registros de que em 1980, dois advogados dos Estados Unidos, Samuel D. Warren e Louis Brandeis, escreveram o artigo "O Direito à Privacidade", que argumenta o "direito de ser deixado em paz", usando a frase como uma definição de privacidade.

2.1 A História da Privacidade de Dados

Apesar de estar constantemente ligado a escândalos, como vazamento de fotos íntimas ou a descoberta de algum caso extraconjugal, engana-se quem acredita que o assunto privacidade de dados se iniciou apenas com o uso em massa das mídias sociais. A História da Privacidade de Dados tem origens mais antigas do que muitos podem imaginar, precedendo a própria criação dos computadores.

A importância da privacidade retornou de forma mais relevante por volta de 1948, sendo largamente promovido como uma proteção contra a Europa no pós-guerra. Isso deve ser entendido como uma expressão do desejo de salvaguardar a vida familiar e pessoal de um indivíduo (conforme consagrado na Convenção Europeia de Direitos Humanos[1]).

Vários movimentos foram tomando forma a partir de então, uma vez que a conscientização sobre o poder dos computadores de processar e manipular dados sobre pessoas foram sendo ampliados dando origem a debates sobre o tema e a elaboração de diretrizes e leis:

Em 1979, surgem as primeiras leis gerais de proteção de dados, promulgadas em sete estados-membros da Europa (Áustria, Dinamarca, França, República Federal da Alemanha, Luxemburgo, Noruega e Suécia).

Em 1980, foram estabelecidas Diretrizes da Organização para Cooperação e Desenvolvimento Econômico (OCDE) sobre a proteção da privacidade e a Convenção do Conselho da Europa de 1980 sobre o processamento automático de dados pessoais

Em 1995, a União Européia (UE) avançou criando regras de proteção de Dados Chamados Diretiva 95/46/CE. Seu sistema abrangente de privacidade de informações, impactou muito além do Continente Europeu

[1] Artigo 12. Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Atenta à transferência de dados pessoais através das fronteiras internacionais, a UE procurou policiar o tratamento de dados nos países em desenvolvimento. Sua influência pode ser vista na Lei de Alteração de Privacidade da Austrália de 2000 – que foi modelada com base nos princípios europeus – e no acordo Safe Harbor de dados pessoais (2000) entre a UE e os Estados Unidos.

Em abril de 2016, o Parlamento Europeu adotou a GDPR, sigla para *General Data Protection Regulation*, ou em português "Regulamento Geral sobre a Proteção de Dados", para atualizar a diretiva de 1995.

Um fato interessante decorrente da promulgação da GPDR na União Européia, é que ela estabeleceu para seus estados membros, que eles somente poderão realizar comércio e/ou serviço (que incluam dados pessoais) com outros países cuja legislação seja minimamente equiparada com a deles.

Tal visão, em um Mundo de economia globalizada, impactou todos os países que tinham algum tipo de relação comercial com a UE, inclusive o Brasil.

2.2 E no Brasil?

Ainda que o Brasil tenha sido uma das Nações signatárias da Declaração Universal dos Direitos Humanos adotada pelas Nações Unidas em 10 de dezembro de 1948, somente com a Constituição Federal de 1988, normas verdadeiramente fortes foram estabelecidas no Brasil.

	**Em 1988, a Constituição Federal reconhece o direito à proteção de intimidade como um dos direitos fundamentais da pessoa humana (art. 5º, X e XII), com a previsão ao direito à intimidade, sigilo de correspondência e à vida privada, bem como, o direito ao acesso aos próprios dados através da criação do chamado remédio constitucional chamado "Habeas Data" (art. 5º, LXXII, "a"), para garantia ao direito acesso à informação.**
	**Em 1990, por meio da Lei nº 8.078/90, entrou em vigor o Código de Defesa do Consumidor – art. 6º, I, segurança e o direito à informação adequada e clara sobre os serviços prestados (art. 6º, III) .**
	**Em 2014, por meio da Lei nº 12.965/14, entrou em vigor o Marco Civil da Internet – art. 7º, VIII – direito a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais.** **O Marco Civil da Internet determina que o usuário terá garantido o direito à inviabilidade e ao sigilo das comunicações, ou seja, as empresas terão de desenvolver mecanismos para garantir, por exemplo, que os *e-mails* não sejam unidos pelos emissores e destinatários. E também garante a proteção a dados pessoais e registro de conexão.**
	**Em 2018, por meio da Lei 13.709/18, entrou em vigor a Lei Geral de Proteção de Dados Pessoais – LGPD - Seguindo a tendência internacional.**

	**Em 2019, o Senado Federal apresentou a PEC 17/2019, Proposta de Emenda à Constituição Federal, que visa alterar o inciso XII do art. 5º, bem como, acrescer o inciso "XXX – proteção e tratamento de dados pessoais", ao art. 22 – tudo com vistas a adaptação das Constituição aos tempos digitais.**

Curiosidades da LGPD pelo Mundo

Após a GDPR entrar em vigor em 2018, diversos países da América Latina, da Ásia e alguns estados dos EUA promulgaram legislações de privacidade de dados com o principal objetivo de manter e/ou impulsionar seu comércio de serviços envolvendo dados pessoais com a Europa.

Aqui é válido lembrar algumas diferenças básicas entre as legislações pelo Mundo. Nos Estados Unidos, por exemplo, cada estado possui uma legislação no tema e de forma geral o direito à privacidade é considerado um direito do consumidor. Muito diferente da Europa, onde o direito à privacidade é um direito humano proveniente da Convenção Européia dos Direitos Humanos em 1950, em Roma.

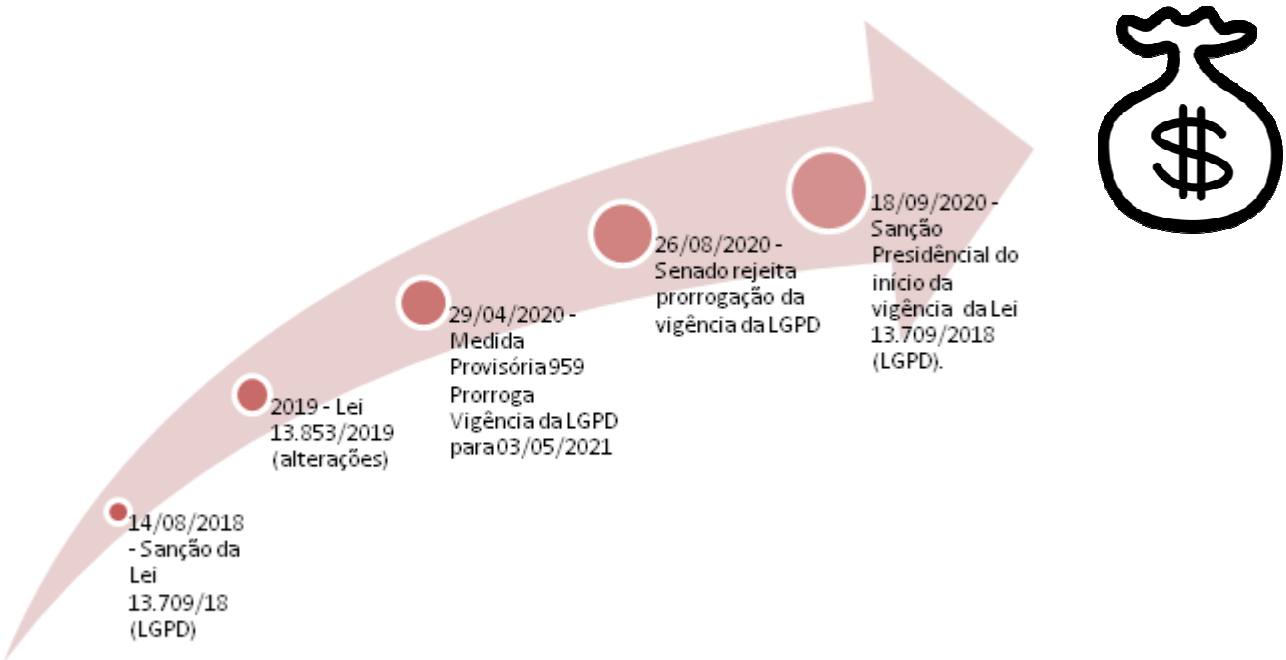
2.3 Brasil e sua LGPD

O Brasil seguiu o movimento global logo após a entrada em vigor da GDPR, ou seja, com a necessidade de manter suas relações comerciais com a União Europeia logo tratou de providenciar longo debate técnico para a

promulgação de uma legislação que atendesse tal foco lançando, então, a Lei Geral de Proteção de Dados Pessoais (LGPD) em 2018, com previsão de entrada em vigor em agosto de 2020.

A legislação brasileira foi considerada uma versão tropicalizada da GDPR, a LGPD é baseada na legislação europeia, e tem como objetivo aumentar a privacidade de dados pessoais iniciada de forma tímida pelo Marco Civil da Internet e assegurar o poder das entidades reguladoras para fiscalizar organizações.

Com a LGPD, os cidadãos brasileiros passam a possuir diversos direitos em relação aos seus dados pessoais e um maior controle sobre eles. No Brasil, assim como na Europa, a privacidade de dados passa a ser considerada um direito do cidadão e não um direito do consumidor apenas, como nos Estados Unidos.



A partir de 1º de agosto de 2021, a Autoridade Nacional de Proteção de Dados - ANPD poderá aplicar sanções administrativas em caso de infrações à LGPD. (Lei 14.010/20 - alterou o texto original da LGPD).

2.4 E no âmbito Municipal?

Quando avaliamos a História da Privacidade de Dados é possível perceber uma evolução significativa das legislações em privacidade de dados na medida em que as relações humanas por meio da internet se intensificaram.

Não há como se negar que informação sempre foi e será sinônimo de poder e caminhamos a passos largos para um mundo cada vez mais digital em que inteligências artificiais ajudam a traçar perfis de personalidade, eleitor, consumo e suas demandas e a empresas a faturar bilhões “vendendo soluções”, ou seja, vivemos em uma era conhecida como sociedade da informação, onde as empresas de dados superam a indústria petrolífera em valor de mercado.

Essa nova forma de sociedade representa desafios fundamentais à forma como percebemos e abordamos a privacidade, tanto como titular de dados como em nosso ambiente de trabalho onde estamos diante do desafio de dar aplicabilidade, o quanto antes, a uma legislação que deverá acrescentar procedimentos de segurança a nossa rotina já tão amarrada em burocracias regradas por determinações legais.

Como servidores do Município vemos de forma mais clara as mudanças legais a serem aplicadas internamente de forma bem tímida, porém, agora, o que antes parecia algo um tanto distante e pontual como os pedidos de acesso a informação, passará a ser necessariamente a uma rotina de trabalho a ser implantada em cada órgão da Administração seguindo as suas peculiaridades e competências legais, sob pena de a Municipalidade ser penalizada com multas.

A LGPD foi regulamentada no âmbito da Administração através do Decreto Municipal nº 38.145, de 18 de junho de 2021[2], com prazo bastante limitado para sua implementação e com adaptações à nossa realidade de grande órgão da Administração Pública e medidas fundamentais têm sido tomadas conforme destacamos abaixo:

---

2 **<https://www.guarulhos.sp.gov.br/06_prefeitura/leis/decretos_2019/36140decr.pdf>. Acesso em: 15 jul. 2021.**

	Designação de Gestores de Dados específicos e Encarregado nomeados pelo Sr. Prefeito em Portaria publicada no Diário Oficial.
	Capacitação inicial realizada através de cursos em EAD promovidos por órgãos parceiros com certificação em prontuário;
	Disponibilização de espaço junto ao site da Municipalidade onde são oferecidas informações de conteúdo vinculado a LGPD para consulta - https://www.guarulhos.sp.gov.br/lei-geral-de-protecao-de-dados
	Criação de Cartilha Introdutória, em formato digital no site https://www.guarulhos.sp.gov.br/sites/default/files/file/arquivos/CARTILHA%20-%20LGPD3.41.pdf
	Orientações Técnicas para diretrizes iniciais das áreas envolvidas publicadas em D.O. e também incluídas no Espaço Digital LGPD.
	Produção de documentos de suporte para a adequação e conformidade iniciais.

2.5 Da teoria à prática

Para que se entenda a grande importância da implementação desta Lei é preciso ter em mente que a informação é um dos principais ativos da Administração e como tal deve ser preservada em um ambiente seguro.

Aplicar a Segurança da Informação não é um modismo impulsionado por inúmeros escândalos de quebra de privacidade, mas a uma necessidade estabelecida por normas e padrões técnicos, pois a implantação de um conjunto de boas práticas em segurança da informação minimiza as chances de ocorrerem problemas de segurança e facilita a administração dos dados e dos recursos de forma segura.

Após auditorias realizadas, o Tribunal de Contas da União recomendou a conformidade e o desempenho dessas ações com base na norma ABNT NBR ISO/IEC 27002. De acordo com o Manual de Boas Práticas do TCU (2003) *"O objetivo dessas fiscalizações é contribuir para o aperfeiçoamento da gestão*

pública, para que a Tecnologia da Informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade".

Além da norma acima citada, outras normas técnicas são recomendadas pelo Controladoria Geral da União, vez que também serviram de orientação na construção do próprio texto da LGPD.

2.6 O Que é Segurança da Informação e Comunicação

Inicialmente, vemos o que a Norma ABNT NBR ISO/IEC 27002 no item 01. Introdução apresenta como definição para o assunto:

> "A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ver OECD Diretrizes para a Segurança de Sistemas de Informações e Redes)."

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

DADOS	INFORMAÇÃO	CONHECIMENTO
Simples observações sobre o estado do mundo	**Dados dotados de relevância e propósito**	**Informação valiosa da mente humana. Inclui reflexão, síntese, contexto**
Facilmente estruturado	**Requer unidade de análise**	**De difícil estruturação**
Facilmente obtido por máquinas	**Exige consenso em relação ao significado**	**De difícil captura em máquinas**
Frequentemente quantificado	**exige necessariamente mediação humana**	**Frequentemente tácito**

Facilmente transferível		**De difícil transferência**

A segurança da informação é obtida a partir da implementação de um conjunto de procedimentos de controle adequados, incluindo políticas, processos, capacitação de equipes, revisão de contratos, estruturas organizacionais e funções de software e hardware.

Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que a privacidade dos titulares seja protegida e os fins de interesse público de responsabilidade do Município sejam atendidos. “Convém *que isto seja feito em conjunto com outros processos de gestão do negócio*, ABNT NBR 27002.”

O Decreto Municipal nº 38.145, de 18 de junho de 2021, que regulamentou a LGPD no âmbito Guarulhense define segurança para os fins de ser aplicada nos órgãos e nas entidades da Administração Pública Municipal no seu artigo 3º, VII:

> VII - segurança: 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;

Veremos que existem várias normas que servem de orientação para proteger as informações, sistemas, recursos e serviços contra erros, manipulação não autorizada e desastres visando à redução do impacto e diminuir a probabilidade de incidentes de segurança durante todo ciclo de vida do dado dentro da gestão administrativa, ou seja, desde a coleta dos dados até a sua final eliminação.

2.7 Metodologias em segurança da informação

É certo, que o principal motivo pelo qual uma empresa investe em segurança é a obrigação no cumprimento de normas e regulamentações, já que, conforme observado no início deste trabalho, os interesses econômicos que envolvem as informações obtidas através do processamento de dados tem suplantado o respeito a privacidade do cidadão e o seu *"direito de ser deixado em paz*".

Já os Órgãos Públicos, em geral, devem também se alinhar às organizações e promover ações com as melhores práticas para proteção e controle da informação que estão sob seus cuidados, uma vez que, ao exercer suas políticas públicas muitas vezes acaba por ser detentor e, portanto, responsável pelo acesso e proteção a dados pessoais. Os padrões de boas práticas mais utilizados pelas áreas do governo e empresas e inclusive recomendadas pela Controladoria Geral da União são as normas ABNT NBR ISO/IEC 27002, 27001, 27005, 27705 e 31000, sendo que cada uma dessas práticas possui abordagem e escopo diferentes, como podemos verificar em apertada síntese a seguir.

2.8 Norma ABNT NBR ISO/IEC 27001:2013

A norma ABNT NBR ISO/IEC 27001:2013 é uma norma que possibilita às organizações a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), através do estabelecimento de uma política de segurança, controles e gerenciamento de riscos.

Inclui o ciclo PDCA (*Plan-Do-Check-Act* ou Planejar-Executar-Verificar-Agir) de melhorias e apresenta uma visão por processos. Segundo a Fundação Vanzolini (2008), o PDCA é um método de gestão que se caracteriza por um ciclo de ações que se repete continuamente de forma a incorporar alterações no ambiente. Seu emprego garante uma efetiva gestão da empresa.

Esta norma é bastante utilizada como referência em auditorias e serve como instrução normativa para toda administração pública. Seu objetivo fundamental é proteger as informações das organizações para que não caiam em mãos erradas ou se percam para sempre. A norma ABNT NBR ISO/IEC 27001

está dividida em 11 capítulos principais renomeados e reorganizados conforme segue:

1. Políticas de Segurança;

2. Organizando a Segurança da Informação;

3. Gerenciamento de ativos;

4. Segurança dos Recursos Humanos;

5. Segurança Física e Ambiental;

6. Gerenciamento das Comunicações e Operações;

7. Controle de Acessos;

8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;

9. Gerenciamento de Incidentes na Segurança da Informação;

10. Gerenciamento da Continuidade do Negócio;

11. Conformidade.

Nesta norma, o conceito de ativos foi ampliado para incluir pessoas e imagem/reputação da organização, além dos ativos de softwares, ativos físicos e serviços já existentes na versão de 2000.

2.9 Norma ABNT NBR ISO/IEC 27002:2013

A norma ABNT NBR ISO/IEC 27002:2013 é um manual de boas práticas de gestão de segurança da informação que tem como objetivo identificar os riscos e implantar medidas que de forma efetiva torne estes riscos gerenciáveis e minimizados.

A proteção de dados pessoais, segundo esta norma, ocorre a partir da implementação de uma série de controles como, por exemplo, a política de segurança, a classificação e controle dos ativos de informação, segurança física do ambiente, entre outros. A implantação desses controles não garante que a organização esteja 100% segura. O que se procura é reduzir os riscos a um nível aceitável pela organização.

Esta norma possui foco na gestão de informações estratégicas com padrão de segurança da informação, baseado em controles e contempla os seguintes aspectos de qualidade da informação:

- Confidencialidade: apenas pessoas autorizadas podem acessar as informações;
- Integridade: garantia que dados e sistemas estão corretos;
- Disponibilidade: usuários autorizados devem ter acesso às informações necessárias; e
- Confiabilidade: a imagem da instituição deve ser protegida.

As orientações contidas na norma são efetivas para o processo de segurança da informação na Administração e elenca os principais elementos desse processo que devem ser desenvolvidos e implantados.

Do material consultado pela equipe organizadora deste manual, vemos que muitos deles asseveram que mais importante para o órgão público do que buscar a **conformidade total** com esta ou aquela norma é conhecer a lista de recomendações e extrair o que puder ser útil para a realidade de cada órgão do Município. *"Serviço feito é melhor que serviço perfeito"*.

2.10 Norma ABNT NBR ISO/IEC 27005:2019

Esta Norma fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ABNT NBR ISO/IEC 27001.

Na ABNT NBR ISO/IEC 27005:2019, não há uma definição de método específico para gestão de risco, cabe à organização definir sua abordagem ao processo de gestão de riscos, levando em conta, por exemplo, o objetivo do seu SGSI, o contexto da gestão de riscos e o seu setor de atividade econômica. Ressaltando que há várias metodologias que podem ser utilizadas de acordo com a estrutura descrita nesta Norma para programar os requisitos de um SGSI adaptado à realidade.

As atividades do processo de gestão de riscos de segurança da informação, apresentadas na Seção 6, são detalhadas nas seguintes seções:

Seção 7 - definição do contexto;

Seção 8 - processo de avaliação de riscos;

Seção 9 - tratamento do risco de segurança da informação;

Seção 10 - aceitação do risco de segurança da informação;

Seção 11 - comunicação e consulta do risco de segurança da informação; e

Seção 12 - monitoramento e análise crítica de riscos de segurança da informação.

Os anexos desta norma apresentam ainda informações adicionais para as atividades de gestão de riscos de segurança da informação:

Anexo A - Definindo o escopo e os limites do processo de gestão de riscos de segurança da informação;

Anexo B - Identificação e valoração dos ativos e a avaliação do impacto são discutidas;

Anexo C - Exemplos de ameaças comuns;

Anexo D - Vulnerabilidades e métodos para avaliação de vulnerabilidades;

Anexo E - Exemplos de abordagens para o processo de avaliação de riscos de segurança da informação;

Anexo F - Restrições relativas à modificação do risco; e

Anexo G - Diferenças nas definições entre a NBR ISO/IEC 27005:2011 e a NBR ISO/IEC 27005:2019.

2.11 ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança – Requisitos e diretrizes

Esta norma especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Visa a aplicação de técnicas de segurança na gestão da privacidade da informação dentro do contexto da organização.

2.12 ABNT NBR ISO/IEC 31000:2018. Gestão de riscos – Diretrizes

A partir da edição desta Norma Internacional, na qual constam princípios e diretrizes para a gestão de riscos em geral em qualquer tipo de ambiente, todas as normas da família “27.000” deverão ser aplicadas em consonância com as normas da família “31.000” . A versão do ano de 2018 apresenta um guia mais claro e conciso, com o intuito de ajudar as organizações a usar os princípios de gerenciamento de risco para melhorar o planejamento e tomar melhores decisões.

2.13 Comparando as Normas de Segurança

Todas as normas apresentadas têm seu diferencial e sua importância na segurança das informações estratégicas. A norma ABNT ISO/IEC 27002 propõe a implantação de controle para garantir a segurança da informação enfatizando o que deve ser feito sem se preocupar com os processos ou tecnologias para atingir este objetivo. Para atingir o objetivo deve ser utilizada em conjunto com outras normas, como a ABNT ISO/IEC 27001.

A norma ABNT NBR ISO/IEC 27001 específica como implantar os controles da norma ABNT NBR ISO/IEC 27002 e para isso propõe um modelo de gestão SGSI.

Tabela 1 – Comparativo entre normas de segurança da informação

NORMA	ASPECTOS POSITIVOS	OBSERVAÇÕES
ABNT NBR-ISO/IEC 27001:2013	Implementa um sistema de gestão da segurança	Os itens são obrigatórios. É possível obter a certificação.
ABNT NBR-ISO/IEC 27002:2013	Tem o controle de segurança.	Os controles são recomendações. Não é possível obter certificação
ABNT NBR-ISO/IEC 27005:2011	Apresenta diretrizes de avaliação e gestão de risco.	Possibilita a escolha do método de avaliação que melhor atende o contexto individual.
ABNT NBR-ISO/IEC 27701:2019	Fornece diretrizes para a implementação, manutenção e melhoria contínua de um sistema de gestão de privacidade da informação (SGPI)	Define aplicabilidade nas organizações e indica responsáveis para as atividades de tratamento
ABNT NBR-ISO/IEC 31000:2018	São princípios e diretrizes para enfrentamento dos riscos pelas organizações em qualquer ambiente.	Utiliza-se de mecanismos de gerenciamento de risco que deverão ser observados toda vez que se utilizar das normas da família “27.000”.

2.14 A importância de realizar a Análise de Risco

A análise de risco é procedimento necessário atual das organizações abrangidas pela LGPD, previsto no art. 5º, XVII, pois é preciso saber qual o seu grau de exposição frente às ameaças capazes de comprometer a segurança dos dados pessoais e possíveis riscos. Para tanto, a LGPD prevê a elaboração do RIPD – Relatório de Impacto à Proteção de Dados Pessoais.

O objetivo da análise de risco por meio do RIPD é identificar e classificar todos os riscos inerentes à atividade da Administração, no que diz respeito a seus ativos de informação, demonstrando que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais as medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares destes dados.

Como é mais abrangente que uma análise de vulnerabilidade simplesmente, a análise de risco buscará, fundamentada em preceitos norteados pelas Normas Técnicas Internacionais por todas as possibilidades de exploração de vulnerabilidades lógicas (digitais) e físicas (equipamentos, arquivos e segurança interna).

Para analisar risco é necessário estudar os principais procedimentos dos departamentos, em cada unidade técnica dentro de sua competência, **avaliar as suas vulnerabilidades e classificar o risco destes processos**.

A análise de risco se divide em cinco partes de igual importância e deve ser implantada na totalidade, pois cada etapa isolada representa pouco e juntas estão alinhadas e apontam caminhos seguros em busca de um nível adequado de segurança para a Administração. São cinco etapas básicas que devemos aplicar:

- Identificação e classificação dos procedimentos internos que envolvem dados;

- Identificação e classificação dos dados segundo as orientações da LGPD;

- Análise de possíveis ameaças e prejuízos;

- Análise de vulnerabilidades;

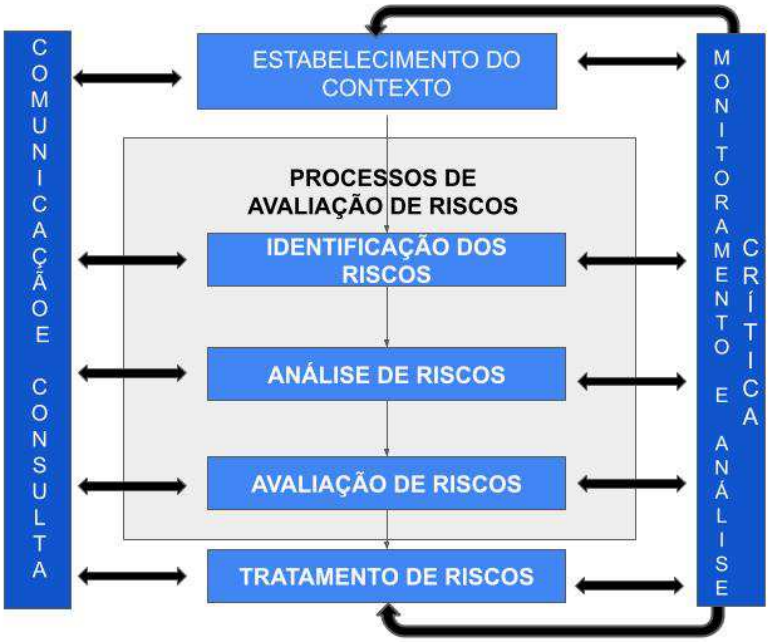
- Análise de Risco.

O resultado da análise de risco é um documento denominado RIPD (Relatório de Impacto à Proteção de Dados), em que a LGPD indica, em seu art.

38, parágrafo único[3], o seu conteúdo mínimo, onde se espera a demonstração, tanto para alta administração quanto aos órgãos de controle, de que todos os cuidados foram tomados, para que as atividades administrativas transcorram em segurança. Deve ser elaborada a relação dos ativos e indicado o seu valor e quais controles devem ser implementados estabelecendo os prazos.

Visão geral do processo de gestão de riscos de segurança da informação

Uma visão de alto nível do processo de gestão de riscos é especificado na ABNT NBR ISO 31000:2009 e apresentado conforme o gráfico a seguir:



A figura a seguir apresenta como esta Norma Internacional se aplica ao processo de gestão de riscos.

[3] **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 processo de gestão de riscos de segurança da informação consiste na definição do contexto (Seção 7), processo de avaliação de riscos (Seção 8), tratamento do risco (Seção 9), aceitação do risco (Seção 10), comunicação e consulta do risco (Seção 11) e monitoramento e análise crítica de riscos (Seção 12).

FIM DA PRIMEIRA OU DAS DEMAIS INTERAÇÕES

Como mostra a representação acima, o processo de gestão de riscos de segurança da informação pode ser iterativo para o processo de avaliação de riscos e/ou para as atividades de tratamento do risco. Um enfoque interativo na execução do processo de avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição. O enfoque interativo permite minimizar o tempo e o esforço despendidos na identificação de controles e, ainda assim, assegura que riscos de alto impacto ou de alta probabilidade possam ser adequadamente avaliados.

Ameaça x Vulnerabilidade x Valor do dado = RISCO

Antes de iniciarmos o procedimento de elaboração do RIPD importante se familiarizar com os seguintes conceitos:

Valor do dado: o dado não possui significado relevante, sendo assim ele não representa algo que tenha sentido em primeira análise, pois sozinho não permite gerar compreensão e consequentemente não possibilita fundamentar a tomada de decisão.

Uma vez que os dados sejam organizados e devidamente ordenados de forma a possibilitar a transmissão do significado e permita a compreensão em um contexto, temos a informação, que é um conjunto de dados de forma que o conhecimento possa ser fundamentado para a tomada de decisão que poderá gerar valor para o negócio.

Então, surge a necessidade de proteger os dados, em especial, os dados pessoais, visto que a consolidação pode transformar os dados em informação ao ponto de gerar valor.

Segurança da Informação é a proteção da informação de vários tipos de correção, componentes garantir a continuidade do negócio, minimizar os riscos que pode comprometê-lo, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software, que devem ser monitorados e continuamente melhorados, com o intuito de atender aos objetivos do negócio, mitigando os riscos e garantindo os preceitos de segurança da organização.

Ameaça: é todo e qualquer evento que possa explorar vulnerabilidades. Causa potencial de um incidente indesejado, que pode resultar em dano para os sistemas, pessoas ou a própria Administração.

Vulnerabilidade: é qualquer fraqueza que pode ser explorada para comprometer a segurança de sistemas ou informações. Fragilidade de um dado ou grupo de dados que pode ser explorada por uma ou mais ameaças.

As ameaças podem ser classificadas em:

- Ameaças intencionais.
- Ameaças da ação da natureza.

· Ameaças não intencionais.

São exemplos de ocorrência/evento:
· Erros humanos;
· Falhas de hardware;
· Falhas de software;
· Ações da natureza;
· Terrorismo
· Vandalismo, entre outras.

Para pensar

Ameaça* versus *Vulnerabilidade

Entende-se que a **ameaça** é o evento ou incidente, enquanto a vulnerabilidade é a fragilidade que será explorada para que a ameaça se torne concreta. As ameaças podem vir de diversas formas, como furto de equipamentos, mídias e documentos, escuta não autorizada, incêndio, inundação e radiação eletromagnética, até fenômenos climáticos como a perda de equipamentos em razão de descargas elétricas por um raio, por exemplo.

Risco: É a incerteza resultante da combinação da probabilidade de ocorrência de um evento e suas consequências. Uma pergunta “Qual o risco?” Levanta dúvidas a respeito da ocorrência de algo incerto ou inesperado. Em segurança da informação, esta incerteza reside nos aspectos tecnológicos implicados, nos benefícios e, principalmente, nas pessoas que em algum momento interagem com a tecnologia e se envolvem com os processos.

Riscos de segurança da informação: possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, assim prejudicando a organização.

Identificação de riscos: processo para localizar, listar e caracterizar elementos de risco. Por menor que seja a probabilidade de ocorrência de um risco, pode ser que ao existir, possa haver a exploração de uma vulnerabilidade, concretizando uma ameaça. Para se preparar para isso é necessário conhecer os riscos de todo o ambiente, através da realização de um processo formalizado de identificação de riscos (RIPD).

Impacto: mudança adversa no nível de design dos objetivos de negócios. Consequência avaliada dos resultados com a ocorrência de um evento em particular, em que conhecida vulnerabilidade foi explorada, uma ameaça ocorreu e o risco se concretizar. Qual foi o impacto deste evento para a

Administração? Quais as consequências geradas na vida do titular dos dados? Houve dano material ou imaterial? A Administração será responsabilizada? Haverá multas? Ações legais serão impetradas? Haverá danos de imagem?

Estimativa de riscos: processo utilizado para atribuir valores à probabilidade e consequências de um risco. A estimativa de riscos permite quantificar ou estimar de forma qualitativa um risco, permitindo às associações priorizar os riscos de acordo com os critérios incluídos.

Ações de modificação do risco: ações para impedir ou reduzir a possibilidade de ameaças ou consequências negativas, ou ambas, associadas a um risco.

Comunicação do risco: troca ou compartilhamento de informações sobre o risco entre os operadores de dados, o controlador e outras partes envolvidas, bem como os órgãos de controle.

Ação de evitar o risco: decisão de não se envolver ou agir de forma a mitigar uma situação de risco.

Retenção do risco: aceitação do ônus da perda ou do benefício do ganho associado a um risco determinado.

Compartilhamento do risco: compartilhamento com outra entidade ou pessoa física do ônus da perda ou do benefício do ganho associado a um risco.

Os produtos gerados da análise de risco são a planilha de identificação e classificação dos ativos, relatório executivo de riscos e um relatório técnico que lista as vulnerabilidades classificadas por grau de risco, descrição para correção e outras informações relacionadas, conforme preconiza o art. 5º, XVII da LGPD, o relatório deverá descrever *“medidas, salvaguardas e mecanismos de mitigação de risco“.*

Conforme orienta a Controladoria Geral da União em seu “Guia de Boas Práticas”, antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais comprometidos.

Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

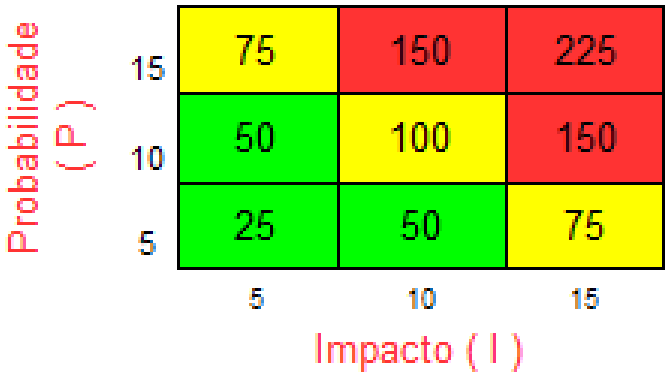
Como exemplo, a CGU se utiliza de parâmetros escalares que podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança.

Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

Parâmetros Escalares

CLASSIFICAÇÃO	VALOR
Baixo	**5**
Moderado	**10**
Alto	**15**

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.



Risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.

Considerando os princípios norteadores adotados pela Controladoria Geral da União, replicamos abaixo as orientações, exemplos lançados pelo órgão em seu guia orientativo.

As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela **Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016.**

Tendo em vista a seção 6 do modelo de **RIPD** constante do Anexo I, a identificação e avaliação de riscos envolve elencar os eventos de risco, a probabilidade, o impacto e o nível de risco.

A título de informação, é destacada a seguir uma tabela com lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais. O nível de probabilidade, impacto e nível de risco indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. Os doze primeiros itens representam riscos de privacidade obtidos da norma **ISO/IEC 29134:2017 seção 6.4.4**.

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

Tabela 5 Risco referente ao tratamento de dados pessoais

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P[1]	I[2]	NÍVEL DE RISCO (P X I)[3]
R01	Acesso não autorizado.	10	15	**150**
R02	Modificação não autorizada.	10	15	**150**
R03	Perda	5	15	**75**
R04	Roubo	5	15	**75**
R05	Remoção não autorizada.	5	15	**75**
R06	Coleção excessiva.	10	10	**100**
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	**150**

R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	**150**
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	**75**
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	10	15	**150**
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	**50**
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	**75**
R13	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.).	5	15	**75**
R14	Reidentificação de dados pseudonimizados.	5	15	**75**

Legenda: P – Probabilidade; I – Impacto.

1. Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

2. Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

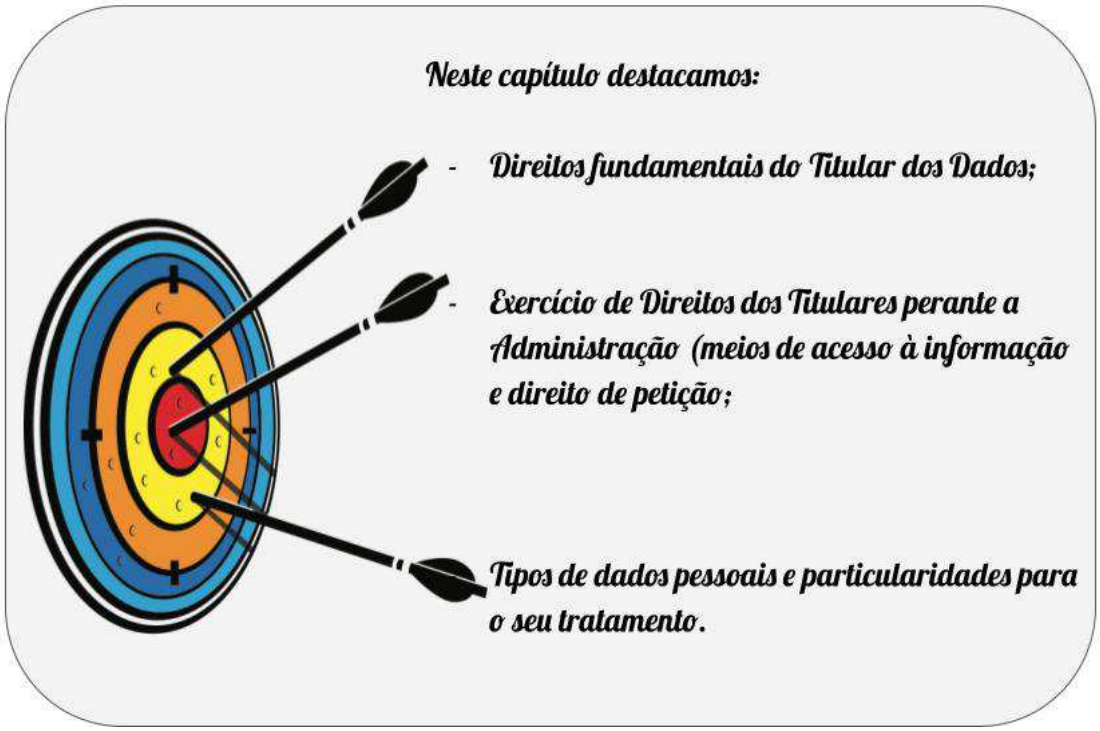
3. Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

Contextualizando:

Vamos à prática da LGPD?;)

3

GESTÃO DADOS PESSOAIS E A APLICABILIDADE DA LGPD EM NOSSA ROTINA



Como foi visto até este momento, o zelo pela segurança da informação no meio institucional público e privado não nasceu agora com a LGPD, foi um processo evolutivo, que foi sendo construído à medida que os dados foram sendo cada vez mais valorizados e os meios de sua obtenção cada vez mais maliciosos e invasivos graças aos meios tecnológicos cada vez mais eficazes, causando assim, prejuízos de toda sorte.

Neste manual, se pudéssemos dar uma característica principal para diferenciar a LGPD das demais normas de segurança da informação nacionais e internacionais vistas até o momento e ao longo da história, seria o foco na aplicabilidade a direitos fundamentais previstos na Constituição federal de 1988, principalmente, no respeito à liberdade e privacidade do cidadão em todas as suas formas, protegendo-a de todas os meios de possível exploração, inclusive,

com a criação de órgão fiscalizador especializado chamado Autoridade Nacional de Proteção de Dados (ANPD), com poderes de aplicar sanções aos infratores.

A Lei Geral de Proteção de Dados – LGPD, instituída pela Lei Nacional nº 13.709, de 14 de agosto de 2018, versa sobre o tratamento de dados pessoais. Como dado pessoal, considera-se, por esta lei, toda informação relacionada à pessoa natural identificada ou identificável, disposto em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Para o exercício das atividades inerentes a aplicabilidade da LGPD no âmbito de Guarulhos, cada servidor deverá estar sensibilizado quanto aos termos e responsabilidades que deverão incluir em sua rotina administrativa, quando envolver o tratamento de dados pessoais, ainda que não tenham sido solicitados pela Administração[4].

Como “tratamento de dados” a legislação define como toda e qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Tanto a Lei Nacional (LGPD) quanto o seu Decreto regulamentador de nº 38.145, de 18 de junho de 2021, deverão ser aplicados em sintonia com os demais regramentos municipais de caráter geral ou específicos de cada órgão técnico.

Em casos de dúvidas ou eventuais conflitos de normas não abarcados por este Manual, pelas Normas Técnicas e materiais disponibilizados durante o processo de implantação, a mesma deverá ser formalizada à Controladoria Geral do Município – CGM, que poderá contar com a colaboração da Procuradoria Geral do Município – PGM para a sua solução e possível inclusão em futuras orientações técnicas a serem disponibilizadas no portal eletrônico do Município https://www.guarulhos.sp.gov.br/lei-geral-de-protecao-de-dados.

[4] Um exemplo típico seria o oferecimento de uma denúncia em que o denunciante não tenha tido o cuidado de pedir o anonimato e ainda tenha fornecido informações que pudessem ser utilizadas pelo denunciado no momento da fiscalização para identificá-lo, causando deste modo problemas de ameaça à segurança e integridade do denunciante. Caberá aos servidores, em situação semelhante, tratar as informações oferecidas espontaneamente pelo titular dos dados, com a anonimização do denunciante e ocultação de todas as informações que possam identificar de onde partiu a denúncia objeto da fiscalização realizada pelo órgão público.

3.1 Responsabilidade quanto a gestão e proteção de dados

A princípio, qualquer servidor no exercício de suas atividades ao promover um tratamento de dados pessoais pode ser considerado um operador de dados. Contudo, para os fins de implantação e monitoramentos contínuos das políticas de proteção na gestão de dados, o Decreto Municipal nº 38.145/2021 regulamenta as seguintes funções que deverão existir em cada Unidade Administrativa e suas respectivas competências:

Controlador – servidor a quem competem as decisões referentes ao tratamento de dados pessoais em sua respectiva unidade;

Operador "Central" – servidor de referência que realiza o tratamento de dados pessoais em nome do controlador em sua respectiva unidade;

Encarregado de dados – pessoa indicada pelo controlador e operador como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); e

Auxiliar de proteção de dados (titular e suplente) – servidores que apoiam as atividades do controlador e operador em sua respectiva unidade.

O Capítulo IX da LGPD dispõe ainda sobre a criação de dois órgãos para atuar como de consulta e controle de âmbito Nacional:

Autoridade Nacional De Proteção De Dados (ANPD) - trata-se de órgão federal atrelado provisoriamente a Presidente da República a quem é assegurada autonomia técnica e decisória sobre a aplicação da LGPD, bem como, competências definidas consoante os incisos do art. 55-J.

Conselho Nacional De Proteção De Dados Pessoais e da Privacidade - trata-se de órgão colegiado que além de ser responsável por propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD, possui outras competências distribuídas pelos incisos do art. 58-B da LGPD.

Observação importante: tome nota.

Pelo art. 7º, §1º, do Decreto 38.145/21, a CAI deverá atuar como órgão deliberativo para apreciação e emissão de parecer prévio a respeito das diretrizes editadas pelo Encarregado de Tratamento de Dados, em parceria com o Controlador Geral do Município. Somente após parecer favorável da CAI as diretrizes emitidas deverão ser adotadas em toda Administração Direta do Município.

Obs.: A COMISSÃO DE ACESSO A INFORMAÇÃO - CAI, foi criada pelo Decreto Municipal n. 36.140/19, como órgão colegiado responsável pelos recursos ligados ao direito de acesso a informação.

3.2 Direitos fundamentais do Titular dos Dados

Cabe ao agente público, antes de iniciar alguma espécie de tratamento de dados pessoais, certificar-se previamente que a finalidade da operação esteja registrada de forma clara e explícita e os propósitos especificados e informados ao titular dos dados.

A princípio, pode parecer complexo mas, uma vez incorporado o sentido protetivo da LGPD frente ao cidadão no consciente coletivo administrativo, tudo passará a ser tão lógico, aceitável e perfeitamente exigível quanto era há mais de 10 anos a solicitação de documentos autenticados e com firma reconhecida.

Quando se trata do Poder Público, seus propósitos durante o tratamento devem estar vinculados à execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Tais políticas públicas, vale destacar, devem estar inseridas nas atribuições legais do órgão ou da entidade da administração pública que efetuar o referido tratamento, não sendo admissível desvios de finalidade ou compartilhamento de informações, sem autorização expressa do titular.

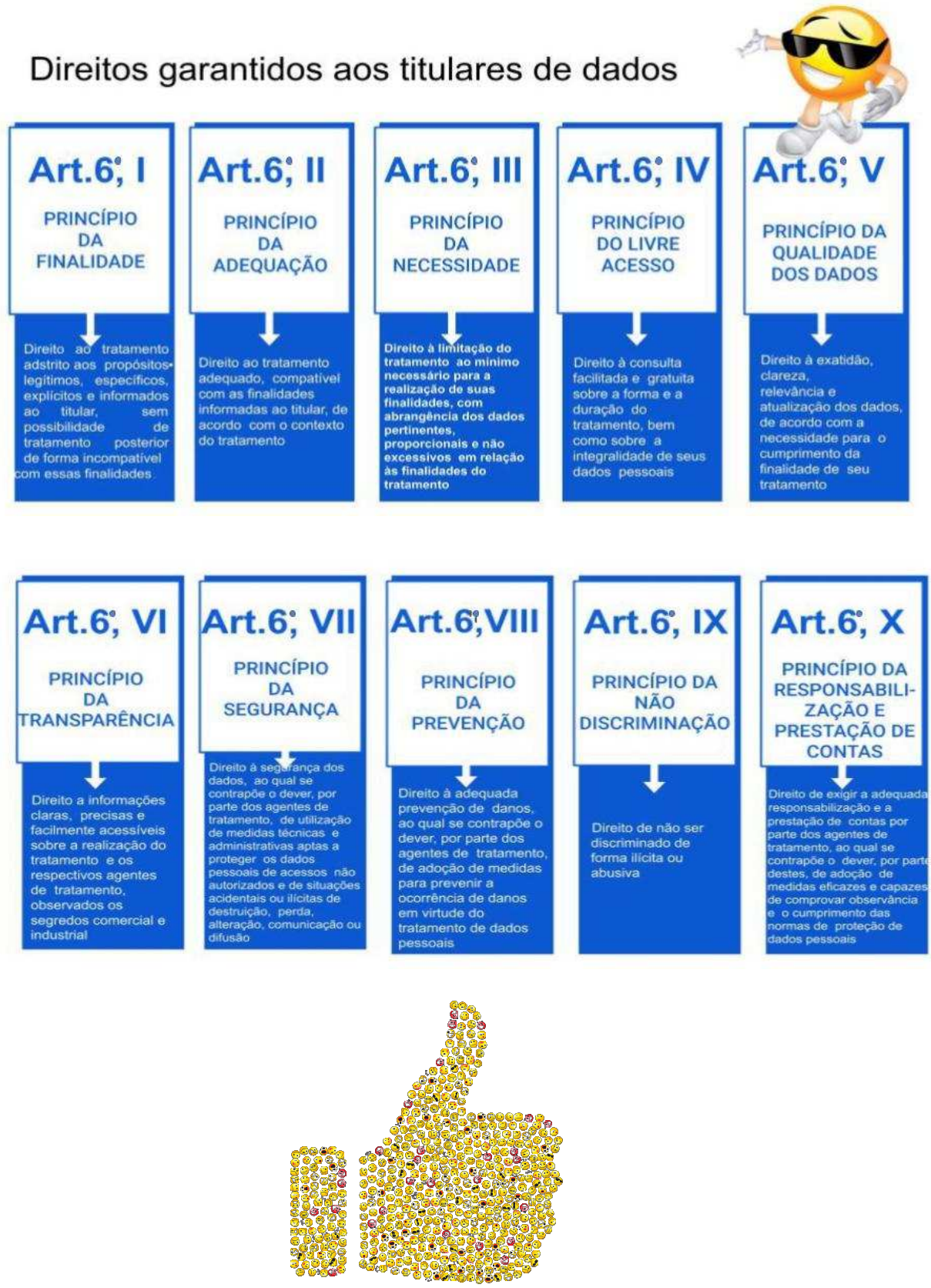
Há finalidades que dispensam o consentimento do titular e fazem parte da rotina de tratamento de dados no serviço público como cumprimento de obrigação legal ou regulatória pelo controlador, a exemplo das notificações de

natureza criminal e epidemiológicas. Nessas duas situações, o consentimento do titular de dados é dispensado.

Além disso, no tratamento feito pelo poder público, as regras previstas nos artigos 23 (procedimentos de atuação) e 30 (regulamentos da ANPD) da LGPD sempre devem ser seguidas de forma complementar.

A lei procura não abrir espaço para interpretações por parte da Administração Pública, sendo necessário conhecer as exceções para a análise da aplicabilidade no tratamento de dados pessoais em geral (art. 7º), bem como a correspondente base legal para o tratamento de dados pessoais sensíveis (art. 11), conforme as hipóteses a seguir:


Tratamento mediante consentimento do titular.
Tratamento para cumprimento de obrigação legal ou regulatória.
Tratamento para execução de Políticas Públicas
Tratamento para execução de Contratos e Procedimentos
Tratamento para a realização de estudos e pesquisas.
Tratamento para prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastros eletrônicos
Tratamento para o exercício de direitos em processo judicial, administrativo ou arbitral
Tratamento para proteção da vida ou da incolumidade física do titular ou de terceiro
Tratamento para proteção do crédito
Tratamento para atender aos interesses legítimos do controlador ou terceiro
Tratamento para tutela da saúde co titular.


Direitos garantidos aos titulares de dados
Art.6º, I
PRINCÍPIO DA FINALIDADE
Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades
Art.6º, II
PRINCÍPIO DA ADEQUAÇÃO
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento
Art.6º, III
PRINCÍPIO DA NECESSIDADE
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
Art.6º, IV
PRINCÍPIO DO LIVRE ACESSO
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais
Art.6º, V
PRINCÍPIO DA QUALIDADE DOS DADOS
Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento
Art.6º, VI
PRINCÍPIO DA TRANSPARÊNCIA
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
Art.6º, VII
PRINCÍPIO DA SEGURANÇA
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
Art.6º,VIII
PRINCÍPIO DA PREVENÇÃO
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
Art.6º, IX
PRINCÍPIO DA NÃO DISCRIMINAÇÃO
Direito de não ser discriminado de forma ilícita ou abusiva
Art.6º, X
PRINCÍPIO DA RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS
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 observância e o cumprimento das normas de proteção de dados pessoais

Além dos direitos dos titulares de dados que são decorrentes do art. 6º da LGPD, a Lei apresenta diretos específicos dos titulares de dados, que são destacados na tabela abaixo e decorrem dos próprios princípios vistos na tabela anterior.

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	REFERÊNCIA LEGISLATIVA (LGPD)
Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais	Arts. 7º, I, e 8º
Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei, mesmo para os casos de dispensa de exigência de consentimento	Art. 7º, § 6º
Direito à inversão do ônus da prova quanto ao consentimento	Art. 8º, § 2º
Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais	Art. 8º, § 4º
Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca	Art. 9º, § 1º
Direito de requerer a revogação do consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado	Art. 8º, § 5º
Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais	Arts. 7º, I, e 8º
Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei, mesmo para os casos de dispensa de exigência de consentimento	Art. 7º, § 6º
Direito à inversão do ônus da prova quanto ao consentimento	Art. 8º, § 2º
Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais	Art. 8º, § 4º
Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo	Art. 9º, § 1º

enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca	
Direito de requerer a revogação do consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado	Art. 8º, § 5º
Direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados, seja na finalidade, forma e duração do tratamento, alteração do controlador ou compartilhamento	Arts. 8º, § 6º e 9º, § 2º
Direito de acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de (entre outras): finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador; finalidade, responsabilidades dos agentes que realizarão o tratamento e direitos do titular, com menção explícita aos direitos contidos no art. 18.	Art. 9º
Direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações supervenientes no tratamento	Art. 8º, § 6º
Direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, ou, ainda, para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos	Art. 9º, § 3º
Direito de ser informado sobre a utilização dos dados pela administração pública para os fins autorizados pela lei e para a realização de estudos por órgão de pesquisa	Art. 7º, III e IV c/c art. 7º, § 1º
Direito de que o tratamento de dados pessoais cujo acesso é público esteja adstrito à finalidade, à boa-fé e ao interesse público que justificaram sua disponibilização	Art. 7º, § 3º
Direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento. No caso da	Art. 7º, § 5º

Administração Pública Federal (APF), em que o tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento	
Direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida quando o tratamento for baseado no legítimo interesse do controlador	Art. 10, § 1º
Direito à transparência do tratamento de dados baseado no legítimo interesse do controlador	Art. 10, § 2º
Direito à anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa	Art. 11, II, *c*
Direito de ter a devida publicidade em relação às hipóteses de dispensa de consentimento para: tratamento de dados sensíveis no cumprimento de obrigação legal ou regulatória pelo controlador; ou tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos	Art. 11, § 2º
Direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica (exceto nos casos de portabilidade de dados quando consentido pelo titular)	Art. 11, § 4º
Direito de que os dados pessoais sensíveis utilizados em estudos de saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas	Art. 13
Direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa sobre saúde pública	Art. 13, § 1º
Direito de não ter dados pessoais utilizados em pesquisa sobre saúde pública transferidos a terceiros	Art. 13, § 2º

pelo órgão de pesquisa	
Direito ao término do tratamento, quando verificado que: (i) a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) houve o fim do período de tratamento; (iii) houve comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no § 5º do art. 8º da Lei e resguardado o interesse público; ou (iv) por determinação da autoridade nacional, quando houver violação ao disposto na Lei	Art. 15
Direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação somente nas exceções legais	Art. 16

3.3 Exercício de Direitos dos Titulares perante a Administração (meios de acesso à informação e direito de petição)

Se com a Constituição Federal de 1988, um grande avanço em termos de direitos e garantias individuais foi alcançado, somente com o tempo foi possível ver os instrumentos do exercício destes direitos sendo regulamentados e exigidos para que sejam acessíveis aos interessados de forma simplificada e em todas as esferas do Poder Público.

O direito de acesso à informação e o direito de petição são dois exemplos concretos desta análise, uma vez que foram sendo regulamentados e aprofundados e hoje podemos identificar que sua aplicabilidade está muito mais acessível livre de custos a qualquer cidadão, conforme veremos a seguir.

3.3.1 Meios de acesso à informação em transparência passiva

Perante o poder público, os titulares de dados pessoais já possuíam a prerrogativa do exercício do direito de acesso simplificado a dados por meio dos mecanismos disciplinados desde pela Lei de Acesso à Informação - Lei 12.527/2011, a “LAI” já previa, em seu art. 31, procedimentos e diretrizes básicas para o tratamento de dados pessoais no âmbito público.

Entre eles, estão o tratamento transparente, a garantia expressa aos direitos de personalidade e o consentimento do titular para a disponibilização de suas informações àqueles que não possuíssem a necessidade de conhecê-la no

exercício de sua função pública e chegou a prever, inclusive, regulamentação específica para o tratamento de dados pessoais no âmbito público.

TOME NOTA: *É importante!*

- No âmbito de Guarulhos, a LAI foi regulamentada pelo Decreto n. 36.140/19, cujo texto deve ser conhecido pelos operadores de dados vez que nele há relevantes dispositivos sobre:

- Pedidos de acesso à informação;
- Procedimentos de acesso à informação;
- Recursos e prazos;
- Classificação de Informações quanto a graus e prazos de sigilo;
- Comissão de Acesso a Informação (CAI) e competências;
- Das informações pessoais;
- Das responsabilidades;
- Monitoramento e aplicação da Lei.

A Controladoria Geral da União reforça que a LGPD, *reconhecendo esse legado, no âmbito público, os prazos e procedimentos para o exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, citando (mas sem se ater exclusivamente) a Lei de Acesso à Informação, a Lei do Processo Administrativo e a Lei do Habeas data (essa última no âmbito judicial).*

Desta forma, submetem-se aos prazos e procedimentos já estabelecidos pela Lei nº 12.527/2011, regulamentado pelo Decreto Municipal n. 36.140/2019, em seu artigo 11, inclusive referente ao recebimento dos requerimentos junto ao Serviço e-SIC do Portal da Transparência do Município, http://portaltransparencia.guarulhos.sp.gov.br/acesso-a-informacao/acesso-%C3%A0-informa%C3%A7%C3%A3o – o exercício dos seguintes direitos expressamente previstos na Lei Geral de Proteção de Dados Pessoais:

🔒 - acesso à informação sobre a confirmação da existência de tratamento (art. 18, I);

🔒 - acesso aos dados pessoais de que é titular e que são objeto de tratamento pela Administração Pública Federal (art. 18, II);

 - acesso à informação sobre entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII);

 - nos casos em que o tratamento tiver origem no consentimento do titular ou em contrato, o acesso à cópia eletrônica integral de seus dados pessoais. Devem ser observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente inclusive em outras operações de tratamento (art. 19, § 3º); e

 - acesso às informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial (art. 20, § 1º).

3.3.2 Direito de petição e manifestação à administração pública de Guarulhos

Como vimos anteriormente, a LGPD cita expressamente a Lei n. 12.527/2011 (LAI) como referência não exclusiva para o exercício dos direitos dos titulares.

É de se lembrar que, ao mesmo tempo, ela aparta os procedimentos previstos daqueles a serem utilizados em face do poder público, ao mencionar que o exercício de tais direitos seria realizado por meio de legislação específica, concedendo liberdade ao titular de dados para eleger o meio ou veículo que melhor atender em primeira instância.

Como **a LGPD não estabelece a observância exclusiva do disposto na Lei de Acesso à Informação** e considerando a existência de procedimentos mais benéficos ao titular para o exercício de seus direitos no que se refere a esse último conjunto apresentado, o mecanismo mais célere estabelecido pelo **Código de Defesa dos Usuários de Serviços Públicos (Lei n° 13.460/2017[5])** pode ser escolhido para o recebimento de solicitações de providências e reclamações relativas ao tratamento de dados.

Além da vantagem em termos de prazo e procedimentos padronizados, com unidades de recebimento de petições e reclamações padronizadas e coordenadas, a Lei 13.460/2017, tem abrangência nacional, permitindo melhor coordenação entre instituições públicas na defesa dos direitos dos titulares de dados.

[5] https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/19141395/do1-2017-06-27-lei-no-13-460-de-26-de-junho-de-2017-19141216

TOME NOTA: *É importante!*

- No âmbito de Guarulhos, a Lei Nacional de Proteção e Defesa dos Direitos do Usuário dos Serviços Públicos - Lei Nacional nº 13460/2017, foi regulamentada pelo Decreto n. 35.382, de 6 de dezembro de 2018, cujo texto deve ser conhecido pelos operadores de dados vez que nele há relevantes dispositivos sobre:

- Estrutura, organização e funcionamento da Ouvidoria do Município;
- Procedimentos de acesso à Ouvidoria;
- Recursos e prazos;
- Classificação de manifestações de Ouvidoria (reclamações, denúncias, elogios, sugestões e INFORMAÇÕES ;
- Cartas de Serviços ao Usuário;
- Relatórios de atividade;
- Monitoramento e aplicação da Lei.

O titular do dado tem o direito, mediante requerimento expresso ou de representante legalmente constituído, sem custos, nos prazos e nos termos previstos em regulamento, de requisitar manifestação conclusiva do controlador ou agente responsável pelo tratamento sobre os seguintes itens:

- **correção de dados incompletos, inexatos ou desatualizados (art. 18, III);**
- **anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV);**
- **eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD (art. 18, VI); e**
- **revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20).**

Obedecendo o princípio da eficiência, a resposta ao titular deve ser providenciada de imediato sempre que possível e em formato simplificado; ou por declaração clara e completa, fornecida no prazo previsto em Lei e que indique: origem dos dados pessoais, a inexistência de registro, critérios utilizados, finalidade do tratamento.

O titular do dado tem a faculdade de optar por resposta por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

A petição deve ser respondida com agilidade, clareza e completude, sob pena de o titular dos dados ter a prerrogativa de representar contra o responsável na ANPD, organismos de defesa do consumidor ou ajuizar pretensão com tal causa de pedir.

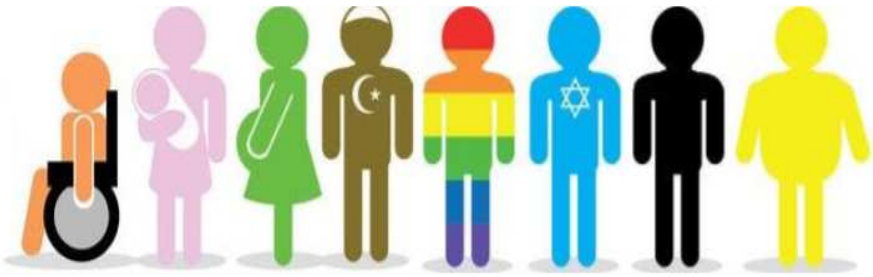
Na impossibilidade de atendimento imediato do requerimento do titular do dado pessoal, o controlador poderá comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

3.4 Tipos de dados pessoais e particularidades para o seu tratamento

Conforme vimos quando estudamos as Normas Internacionais de Segurança da Informação, seu foco está em implementar medidas protetivas para a para todo tipo de informação que possua de alguma forma valor agregado ou agregável para uma instituição.

O conceito de dado pessoal trazido pela Lei 12.527/2011 (Lei de Acesso à Informação - LAI), foi uma evolução sobre o conceito anterior, quando passou a olhar o titular de dados e as consequências que a falta de privacidade inconsequente traz sobre a vida de cada ser humano.

Tal enfoque foi mantido pela LGPD e evoluiu ainda mais ao aprofundar-se no conceito sobre os casos considerados **“informação sensível”**, ou seja: **“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”** (Art. 5º, II).



Diferentemente da LAI, no entanto, os direitos e salvaguardas sobre dados pessoais da LGPD incidem sobre todos os tipos de dados pessoais, observadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação, ou seja, a tutela da lei se estende não mais apenas aos dados pessoais sensíveis ou diretamente relacionados aos direitos de personalidade, mas, em maior ou menor medida, a todos os dados pessoais.

Conforme preconiza a Controladoria Geral da União: ***t****odos os tipos de atributos constituem informações pessoais, pois são relativos a titular pessoa física identificado ou identificável.*

Atributos genéticos e biométricos, por definição legal, constituem dados pessoais sensíveis.

Atributos biográficos, em conjunto com dados como números de cadastro tais como CPF, CNPJ, NIS, PIS, PASEP e Título de Eleitor são o que se denomina de dados cadastrais, que são, à luz da LGPD, dados pessoais. Isso porque, se qualquer dado, inclusive o cadastral, trouxer informação relacionada a pessoa natural identificada ou identificável, será considerado um dado pessoal.

Para maiores detalhes, favor checar o quadro "Por que informações como CPF e endereço são dados pessoais?".

Por sua vez, a depender do seu conteúdo, atributos biográficos poderão ou não ser considerados sensíveis. Nos termos da Lei, serão considerados sensíveis aqueles atributos biográficos que digam *respeito à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.*

Assim, em regra, o tratamento de atributos biométricos e genéticos se dará com base no regime de tratamento de dados pessoais sensíveis; já o tratamento de atributos biográficos será feito de acordo com o seu conteúdo, o qual definirá a tipologia do dado à luz da LGPD."

"Por que informações como CPF e endereço são dados pessoais?".

Conforme a LGPD, art. 5º, I, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. Este conceito é composto por quatro elementos:		
Elemento do dado pessoal	**Informação**	Pode ter natureza objetiva (ex. idade) ou subjetiva (ex. o devedor X é confiável).
	Relacionada a	Um dado pode ser considerado relacionado a um indivíduo se ele diz respeito a um dos seguintes critérios; I - se relaciona a um conteúdo sobre o indivíduo; II - tem finalidade de avaliar um indivíduo ou se comportamento; ou III - tem um impacto sobre interesses ou direitos do indivíduo
	Pessoa Natural	Para ser pessoa, a informação deve estar relacionada a um indivíduo humano
	**Identificada ou Identificável**	"**Identificada**" significa que a ligação ao indivíduo é feita de forma direta, ou como pelo tratamento de seu nome completo ou sua foto. Como "identificável", a ligação é indireta, é um processo de cruzamento de dados pode ser necessário para a identificação. Isto contudo não elimina a caracterização do dado como dado pessoal. é o caso de identificadores como o RG, o CPF o endereço e o telefone de uma pessoa natural.

A regra geral, como já foi abordado anteriormente, é a de que todo dado pessoal somente poderá ser tratado mediante o consentimento inequívoco do seu titular e para finalidade específica por ele conhecida e aceita, contudo, **em se tratando de Administração Pública, os arts. 6º, 7º, 9º, 11 e 26, prevêem a prerrogativa de tratamento de dados pessoais sem o consentimento do titular, desde que seja para a execução de políticas públicas**, devidamente estabelecidas em lei ou para o cumprimento de obrigação legal ou regulatória pelo controlador.

As unidades administrativas que porventura possuam dados sensíveis em sua base de dados, como parte de sua rotina de competências (por exemplo, educação, saúde, direitos humanos etc.) deverão manter suas rotinas desde que incluam novos procedimentos, como a coleta do consentimento explícito e para finalidade definida dos respectivos titulares dos dados. Como já citado

anteriormente, consentimentos podem ser revogados pelo titular, a qualquer tempo e sem necessidade de motivação expressa.

Dados relativos à saúde, bem como pertencentes a crianças e adolescentes, são considerados sempre sensíveis e dependem de autorização expressa dos seus titulares ou responsáveis legais para seu tratamento.

Importante ressaltar que, excepcionalmente, sem o consentimento do titular, a LGPD permite o tratamento de dados sensíveis quando a referida providência for indispensável à garantia de outros direitos fundamentais igualmente protegidos. São situações elencadas pela lei e deverão ser objeto de estudo mais aprofundado posteriormente.

4
DO TRATAMENTO DE DADOS PESSOAIS

Para o tratamento de dados pessoais será importantíssimo identificar dentro da rotina de cada unidade técnica administrativa, como se dá o fluxo de dados dentro da repartição a partir de sua coleta, nos termos do que prevê o art. 7º, I, do Decreto n. 38.145/2021:

1 - quais são estes dados;

2 - onde estão armazenados estes dados;

3 - por que foram coletados;

4 - como são tratados;

5 - quando são tratados;

6 - por quem são tratados; e

7 - qual o valor destes dados em caso de quebra de privacidade.

O Decreto Municipal nº 38.145/2021, ainda, regulamenta as seguintes funções de agentes de tratamento de dados que deverão existir em cada Unidade Administrativa e suas respectivas competências:

Controlador – servidor a quem competem as decisões referentes ao tratamento de dados pessoais em sua respectiva unidade;

Operador "Central" – servidor de referência que realiza o tratamento de dados pessoais em nome do controlador em sua respectiva unidade;

Encarregado de dados – pessoa indicada pelo controlador e operador como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); e

Auxiliar de proteção de dados (titular e suplente) – servidores que apoiam as atividades do controlador e operador em sua respectiva unidade.

Importante observar que sempre haverá locais em que o tratamento de dados será constante (ambulatórios, escolas, RH, CRAS etc.), enquanto em outros poderão ser esporádicos a depender até de circunstâncias alheias à vontade do servidor, como por exemplo, uma mensagem eletrônica em que o Munícipe ao se manifestar se excede desnecessariamente no fornecimento de dados pessoais (solicitações de serviço e denúncias).

Independentemente da frequência e forma a que o servidor estará exposto a dados pessoais alheios, caberá a este profissional fazer o levantamento destas situações em sintonia com os Controladores de suas unidades, observar as hipóteses de tratamento e a forma como deverá executá-los com vistas a preservação do titular, adequando-se ao cumprimento da LGPD através de um plano de ação a ser elaborado pelos agentes de tratamento, respeitando as particularidades de cada unidade técnica e administrativa.

4.1 Das hipóteses de tratamento de dados pessoais

O tratamento de dados pessoais deverá ser realizado pela administração pública nos termos do que determina art. 23 da LGPD, unicamente 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, desde que as hipóteses de tratamento sejam informadas ao titular desde que enquadrado em uma das hipóteses elencadas na Lei.

Referidas hipóteses podem ser compreendidas como condições necessárias para verificar se o tratamento de dados pelo controlador ou operador é permitido. As hipóteses de tratamento de dados pessoais são listadas no art. 7º da LGPD, enquanto no art. 11, que aborda as hipóteses autorizativas para o tratamento de informações pessoais sensíveis.

Segundo a LGPD, os dados pessoais sensíveis de pessoas naturais são aqueles **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** (art. 5º, II). São dados cujo tratamento pode ensejar a discriminação do seu titular, e por isso, são sujeitos a proteção mais rígida[6].

Cabe destacar que a lei autoriza o tratamento de dados sensíveis apenas em **situações indispensáveis**. Isso traz para o controlador o ônus da prova da alegada indispensabilidade.

A tabela a seguir elenca resumidamente as hipóteses de tratamento autorizadas pela LGPD, informando, em cada caso, a base legal referente ao tratamento de dados pessoais em geral (art. 7º), bem como a correspondente base legal para o tratamento de dados pessoais sensíveis (art. 11).

[6] É necessário que os órgãos e entidades da Municipalidade conheçam as hipóteses para:

- Analisar os casos de tratamento de dados pessoais já realizados, objetivando verificar se há hipótese legal que os autorize; e

- Avaliar previamente cada novo caso de tratamento que pretenda realizar, identificando as hipóteses legais autorizativas aplicáveis.

Identificação de Hipóteses de Tratamento pela LGPD			
HIPÓTESE DE TRATAMENTO	O QUE PRECISAMOS NOS ATENTAR E RESPONDER POSITIVAMENTE.	DISPOSITIVO LEGAL	
		TRATAMENTO DE DADOS PESSOAIS	TRATAMENTO DE DADOS SENSÍVEIS
Hipótese 1: Mediante consentimento do titular. Essa é uma hipótese em que o titular tem chance real de escolha sobre o tratamento de seus dados. Trata-se de hipótese possível quando as demais do art. 7º forem descartadas.	1. Serão viáveis a coleta e o armazenamento da opção de consentimento do titular de modo a poder comprovar posteriormente a sua expressa manifestação de vontade? 2. Se o consentimento se der de forma escrita, será garantido que a opção pelo consentimento conste de cláusula destacada das demais, em que o titular seja instado a escolher livremente pela anuência ou não ao consentimento solicitado? 3. O consentimento será solicitado para cada uma das finalidades de tratamento, e será informado ao titular que tipo de tratamento será realizado, antes que este opte pelo consentimento? 4. Será dada ao titular a opção de revogação do consentimento, a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado? 5. No caso de tratamento de dados de crianças e adolescentes, será solicitado o consentimento específico por pelo menos um dos pais ou pelo responsável legal? 6. No caso do tratamento de dados pessoais sensíveis, será registrada a manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento? Observações: a) É vedado o tratamento de dados pessoais mediante vício de consentimento. b) O consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. c) Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o titular deverá ser informado previamente sobre as mudanças de finalidade, podendo revogar o consentimento, caso discorde das alterações. d) As autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.	LGPD, art. 7º, I	LGPD, art. 11, I

Hipótese 2: Para o cumprimento de obrigação legal ou regulatória. Essa hipótese é aplicável quando é necessário processar dados pessoais para o cumprimento de obrigações legais ou regulatórias específicas. Não se enquadram nessa hipótese as obrigações estabelecidas por contrato.	1. É possível identificar a obrigação legal ou regulatória específica que requer o processamento do dado? 2. É possível identificar a competência legal do órgão que dará cumprimento à obrigação legal ou regulatória? 3. O titular do dado será informado sobre a norma que determina a obrigação legal ou regulatória que exige o tratamento do dado? 4. Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei? As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.	LGPD, art. 7º, II	LGPD, art. 11, II, “a”
Hipótese 3: Para a execução de políticas públicas. Essa hipótese é aplicável 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. Trata-se de uma hipótese que dispensa o consentimento do titular e que deve ser realizada por controladores que sejam pessoas jurídicas de direito público.	1. O controlador é pessoa jurídica de direito público? 2. Não sendo pessoa jurídica de direito público, o controlador é empresa pública ou sociedade de economia mista que realizará o tratamento de dados para execução de políticas públicas, e não para atividades inerentes ao regime de concorrência? 3. O tratamento do dado será realizado para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres? 4. É possível identificar claramente a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento de dados pessoais? 5. É possível identificar a competência legal que autoriza o órgão à execução da política pública? 6. O titular do dado será informado sobre a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento do dado? 7. Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei, inclusive quando da necessidade de compartilhamento de dados? 8. Será indicado um encarregado (Art. 5º, inciso VIII) para garantir a comunicação do órgão ou entidade pública com o titular do dado e com a Autoridade Nacional de Proteção de Dados, que verificará a observância das instruções e normas sobre a política pública em questão? Segundo o Art. 23 da LGPD, os órgãos e entidades públicas deverão realizar o tratamento de dados apenas para o atendimento de sua finalidade pública, no interesse público e com o objetivo de executar as competências ou atribuições legais do serviço público. Nesse contexto, não havendo uma delimitação inequívoca das atribuições legais que poderiam ser diretamente relacionadas à execução de políticas públicas, cabe aos órgãos e entidades analisar, no caso concreto, a possibilidade de enquadrar o tratamento do dado na hipótese prevista no Art. 7º, inciso III, combinada com o disposto no Art. 23.	LGPD, art. 7º, inciso III	LGPD, art. 11, II, “b”

Hipótese 4: Para a realização de estudos e pesquisas. Essa hipótese é aplicável para o tratamento de dados para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.	1. O controlador ou operador é órgão de pesquisa? 2. Os dados pessoais serão utilizados dentro do órgão estritamente para a finalidade estabelecida para o estudo ou pesquisa? 3. Em se tratando de estudos em saúde pública, os dados serão mantidos em ambiente seguro e controlado, e será garantida, sempre que viável, a anonimização ou pseudonimização dos dados? 4. O órgão de pesquisa garante que não serão revelados dados pessoais em caso de divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa realizada? 5. O órgão de pesquisa que tiver acesso aos dados pessoais assume a responsabilidade pela segurança da informação e se compromete a não transferir os dados a terceiros em circunstância alguma? Especificamente no que tange à realização de estudos em saúde pública, o art. 13 da Lei possibilita que os órgãos tenham acesso a bases de dados pessoais, inclusive os atributos sensíveis, que serão tratados exclusivamente dentro do referido órgão e estritamente para a finalidade de realização de estudos e pesquisas. Nessa hipótese, o órgão ou entidade deverá garantir que os dados sejam mantidos em ambiente controlado e seguro, e que, sempre que possível, sejam anonimizados ou pseudonimizados.	LGPD, art. 7º, inciso IV	LGPD, art. 11, II, “c”
Hipótese 5: Para a execução ou preparação de contrato. Essa hipótese é aplicável para o tratamento de dados necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular. As hipóteses de tratamento de dados estarão previstas no contrato. O consentimento é fornecido no ato de formalização do termo ou decorrente do mesmo.	1. O tratamento de dados pessoais se faz necessário para a consecução dos termos do contrato ou para a realização de procedimentos preliminares relacionados ao contrato?	LGPD, art. 7º, inciso V	Não se aplica

Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral. Essa hipótese é aplicável para o tratamento de dados necessário ao exercício regular de direitos do titular em processo judicial, administrativo ou arbitral, por quaisquer das partes envolvidas.	1. O tratamento de dados pessoais se faz necessário para o exercício de direitos do titular em processo judicial, administrativo ou arbitral? 2. O titular do dado será informado com destaque quando essa hipótese de tratamento for aplicada?	LGPD, art. 7º, inciso VI	LGPD, art. 11, II, “d”
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro. Essa hipótese é aplicável para o tratamento de dados para a proteção da vida ou da incolumidade física do titular ou de terceiros.	1. O tratamento de dados pessoais se faz necessário para proteger a vida ou a incolumidade física do titular ou de terceiros? 2. O titular está impossibilitado de oferecer o consentimento para o tratamento do dado pessoal?	LGPD, art. 7º, inciso VII	LGPD, art. 11, II, “e”
Hipótese 8: Para a tutela da saúde do titular. Essa hipótese é aplicável para o tratamento de dados para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.	1. O tratamento de dados pessoais será realizado por profissional de saúde, serviço de saúde ou autoridade sanitária? 2. O tratamento de dados pessoais se faz necessário para a tutela da saúde do titular?	LGPD, art. 7º, inciso VIII	LGPD, art. 11, II, “f”

Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro. Essa hipótese é aplicável para o tratamento de dados quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.	1. Foi identificado interesse legítimo do controlador, considerado a partir de situações concretas, que respeite as legítimas expectativas do titular em relação ao tratamento de seus dados? 2. O controlador se responsabiliza por garantir a proteção do exercício regular dos direitos do titular ou a prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular? 3. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada? 4. Serão adotadas medidas para garantir a transparência do tratamento de dados baseado no legítimo interesse do controlador? Órgãos e entidades públicas não devem recorrer a essa hipótese se o tratamento de dados ocorre para a consecução de políticas públicas ou de suas próprias competências legais. No entanto, em caso de finalidade diversa, essa opção poderá ser aplicável.	LGPD, art. 7º, inciso IX	Não se aplica
Hipótese 10: Para proteção do crédito. Essa hipótese é aplicável para o tratamento de dados para proteção do crédito do titular.	1. Foi identificada necessidade de tratamento de dados pessoais para a proteção do crédito do titular? 2. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?	LGPD, art. 7º, inciso X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular. Essa hipótese é aplicável para o tratamento de dados pessoais sensíveis para assegurar a identificação e autenticação do titular para a autenticação de cadastro em sistemas eletrônicos, visando à prevenção de fraudes e à garantia da segurança do titular.	Para enquadramento nessa hipótese, deve-se avaliar se não há outro meio para a identificação do titular sem a necessidade do tratamento de dados sensíveis. Esta hipótese refere-se, por exemplo, à possibilidade de uso de biometria para identificação e autenticação em sistemas eletrônicos. Destaca-se que essa hipótese não pode ser utilizada no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.	Não se aplica	LGPD, art. 11, II, “g”

O importante é avaliar caso a caso e documentar a(s) hipótese(s) aplicável(is), uma vez que o titular deverá conhecer a hipótese legal que autoriza o processamento de seus dados pessoais.

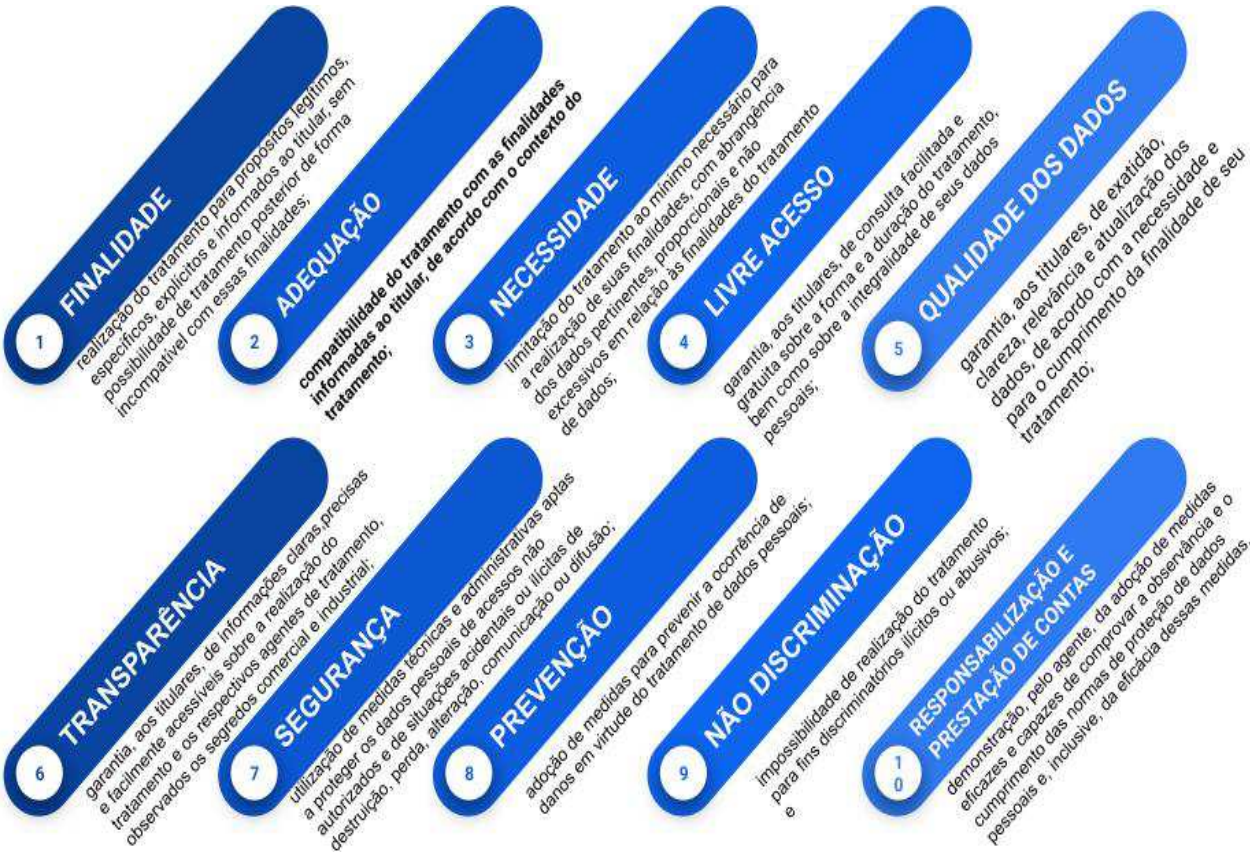
Além disso, o princípio da responsabilização e prestação de contas requer que o órgão ou entidade que realiza o tratamento de dados pessoais possa demonstrar que está plenamente aderente à LGPD, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto à sua eficácia.

Por essa razão, cabe ao órgão ou entidade pública avaliar bem a hipótese de tratamento aplicável, pois mudanças posteriores podem abalar a confiança do titular quanto aos interesses legítimos da instituição no uso de seus dados, além de comprometer os requisitos de transparência, responsabilização e prestação de contas.

4.2 Dos princípios aplicáveis ao tratamento de dados pessoais pela LGPD

Além das hipóteses legais de tratamento, há ainda que se observar se a administração, ao realizar este trabalho, agiu com boa-fé e respeitou os princípios fundamentais específicos contidos no artigo 5º da LGPD.

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

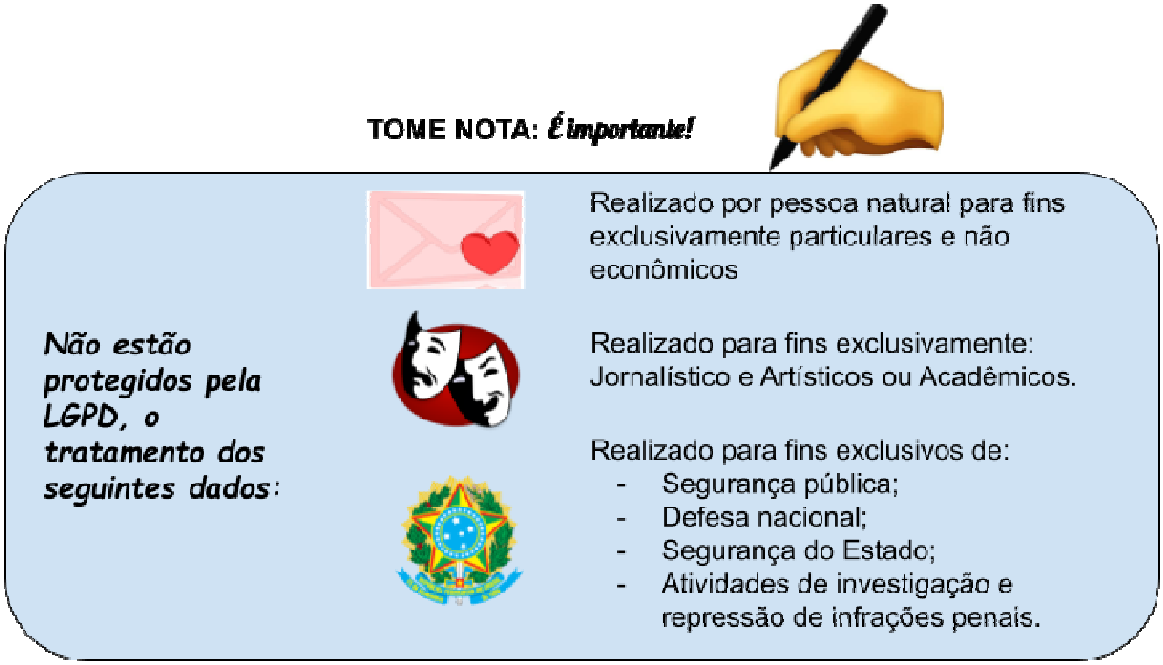


Não basta, portanto, o enquadramento em uma ou algumas das hipóteses legais autorizativas para se iniciar o tratamento de dados pessoais. É fundamental garantir que **TODOS** os princípios listados acima sejam respeitados.

No processo de adequação à LGPD, é recomendável a elaboração de listas de checagem que destacam questões fundamentais a serem verificadas para garantir a conformidade do tratamento de dados pessoais às disposições da lei, e poderão ser utilizadas tanto no início de novos tratamentos (*Privacy by Design*[7]*),* quanto na avaliação da conformidade de tratamentos iniciados antes da vigência da LGPD, ou seja, a prevenção a ocorrências de riscos de vazamento deverá ser constante.

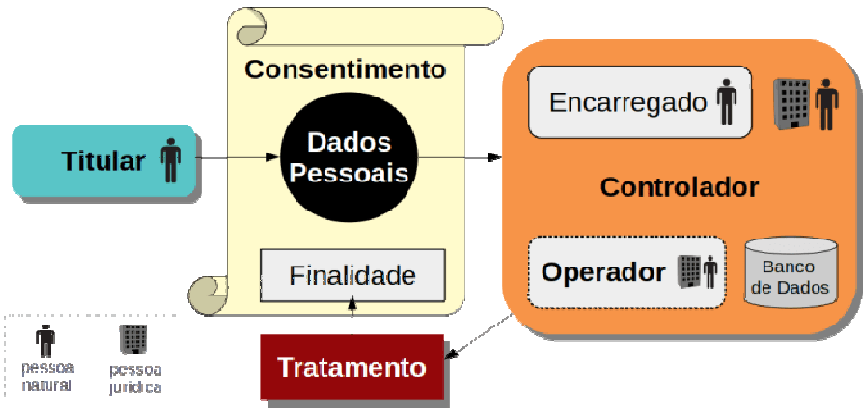
[7] **Privacy by Design** é uma estrutura de trabalho que tem como proposta central incorporar a privacidade e a proteção de dados pessoais em todos os projetos desenvolvidos por uma organização, desde a sua concepção.

4.3 Situações de tratamento não abarcados pela LGPD



4.4 Coleta de dados pessoais

A coleta é uma das operações de tratamento referenciadas pelo art. 5º, X, da LGPD. Considerando que o tratamento de dados pode ser representado por um ciclo de vida, essa operação representa a etapa inicial responsável por obter os dados pessoais do cidadão (titular dos dados). A representação do tratamento de dados pessoais como ciclo de vida é tratada no capítulo adiante deste documento.



Tendo em vista que a coleta é a operação inicial de tratamento dos dados pessoais, a realização de tal operação pela Municipalidade somente deve ser realizada mediante o atendimento das hipóteses de tratamento, das medidas de segurança, dos princípios expressos pela LGPD, dos direitos do titular e demais regras dispostas pela legislação.

Será no momento da coleta de dados que o consentimento do titular deverá ser recolhido em documento que esclareça a sua necessidade, finalidade e eventual possibilidade de compartilhamento, se o caso. Para fins ilustrativos, apresentaremos junto aos anexos, modelos genéricos de consentimos a serem adaptados à realidade de cada Unidade.

Todo o conteúdo deste documento visa justamente orientar as instituições para os cuidados que elas devem ter ao coletar e tratar os dados pessoais dos cidadãos de forma a assegurar a privacidade dos titulares de dados.

A incorporação da privacidade como padrão para o tratamento dos dados pessoais, indicando a limitação da coleta como uma das práticas preventivas a serem adotadas, reduz a possibilidade de vazamentos de dados e suas consequências.

4.5 Anonimização e pseudonimização

Segundo a LGPD, dado anonimizado é o dado que, considerados os meios técnicos razoáveis no momento do tratamento, perde a possibilidade de associação, direta ou indireta, a um indivíduo.

A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização, a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta. A partir do momento em que o dado é considerado anonimizado, e não permite mais qualquer identificação do seu titular, esse dado sai do escopo da legislação, por não mais se tratar de um dado pessoal, conforme previsto no art. 12 da LGPD.

É importante ressaltar, ainda que o dado seja considerado anonimizado pelo controlador, uma vez observada a possibilidade de reversão do processo que obteve a anonimização, permitindo a reidentificação do titular de dados, não se está diante de um dado verdadeiramente anonimizado, mas de um dado potencialmente pseudonimizado.

Pseudonimização é a técnica de tratar dados pessoais de uma forma em que os dados somente possam ser atribuídos a um titular de dados mediante a utilização de informações adicionais, não disponíveis a todos, desde que essas informações sejam mantidas em ambiente separado, controlado e seguro.

A título ilustrativo, criptografia é um método de pseudonimização, quando os dados somente podem ser atribuídos a um titular mediante o conhecimento da chave criptográfica. Sem conhecer a chave, os dados são ininteligíveis.

De acordo com a legislação em vigor, esses processos devem ser utilizados, sempre que possível, por meio da aplicação de meios técnicos razoáveis e disponíveis, na ocasião do tratamento dos dados.

A seguir, algumas recomendações para subsidiar a escolha da técnica a ser utilizada:

 Elencar os principais processos de trabalho que realizam tratamento de dados pessoais para a realização de estudos, especialmente em órgão de pesquisa, conforme Art. 7º, IV.

 Identificar os dados pessoais a que se referem os processos de trabalho listados, que não podem ter os titulares relacionados.

 Analisar o ciclo de vida de tratamento do dado a fim de mitigar riscos de violação de dados que não são mais de uso corrente. E, ainda, propor arquivamento ou eliminação dos dados, visto que a gestão de dados desnecessários no ambiente de produção causa aumento não apenas do quantitativo de dados a serem geridos, como também a manutenção do custo operacional relacionado a este processo (em atividades como armazenamento e gestão da segurança).

 Avaliar o risco de identificação do titular dos dados listados. Deve-se levar em consideração que, quanto maior o uso de tecnologias de análise de dados, quanto maior o volume de dados processados e quanto mais significativos forem estes dados, maior será o risco de violação.

 Quando houver a obrigatoriedade de proteção de dados pessoais, sem a necessidade de guarda dos dados que associam estes aos titulares, pode-se optar pelo processo de **anonimização**, sem prejuízo de atividades do órgão ou entidade. Caso contrário, pode-se optar pela técnica de pseudonimização.

 Definir um plano de comunicação para incidentes de violação de dados. O objetivo é propiciar maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo

cumprimento das atividades.

Documentar violações atestadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente.

Promover a conscientização contínua acerca da importância da proteção de dados no órgão ou entidade.

Cabe destacar que a pseudonimização, como técnica utilizada para proteção de dados pessoais, pode ser utilizada, por exemplo, para preservação da identidade do denunciante, conforme previsto no § 7º do art. 10 da Lei nº 13.460, de 2017.

A Ouvidoria do Município, responsável pelo tratamento de denúncias recebidas da população de diversas maneiras, providenciará a **pseudonimização dos dados do denunciante, garantido o sigilo ou anonimato conforme a sua vontade,** para o posterior envio aos órgãos de apuração competentes.

A pseudonimização também pode ser utilizada para proteger a identidade do usuário de serviço público ou autor de manifestação (independentemente do tipo), conforme previsão do art. 2º do Decreto Municipal nº 35.382/2018, que regulamenta a Lei Nacional supra.

Resumindo graficamente os dois itens anteriores:

4.6 Publicidade

O inciso I do art. 23 da LGPD impõe às pessoas jurídicas de direito público obrigações de transparência ativa, isto é, de **publicar informações sobre os tratamentos de dados pessoais por elas realizados em seus sítios eletrônicos de forma clara e atualizada, detalhando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desses tratamentos.**

Tal medida implica em uma reformulação de cada sítio eletrônico para a implementação destas informações relativas ao tratamento de dados pessoais, principalmente, quando for parte necessária ao exercício de sua competência legal.

Também deve ser dada **publicidade aos tratamentos de dados pessoais sensíveis** em que seja dispensado o consentimento do titular, seja para cumprimento de obrigação legal ou regulatória, seja para tratamento compartilhado de dados necessários para a execução de políticas públicas previstas em leis ou regulamentos, conforme prevê o §2º, do art. 11, da LGPD.

Outra informação a ser publicizada é a identidade e informações de contato do encarregado, por força do art. 41, §1º, da LGPD.

Quando o tratamento de dados pessoais envolver a obrigação legal de difusão destes em transparência ativa, estes devem ser publicados em formato interoperável e estruturado para o uso compartilhado, em cumprimento ao disposto no art. 25 da LGPD e como já previa o art. 8º, §3 da Lei nº 12.527/2011, a Lei de Acesso à Informação.

Quanto à localização da publicação das informações sobre o tratamento de dados pessoais, sensíveis ou não, sugere-se que, além dos itens especificados para serem publicados em seção específica denominada “Acesso à Informação” dos sítios eletrônicos dos órgãos da Municipalidade, há ainda a possibilidade de consulta às informações de transparência pelo e-SIC no http://portaltransparencia.guarulhos.sp.gov.br/.

A Controladoria Geral da União sugere como texto de introdução: “*Nesta seção, são divulgadas informações sobre o tratamento de dados pessoais realizado pelo(a) [nome do órgão ou entidade], compreendendo a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desse tratamento, em cumprimento ao disposto no inciso I do art. 23 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)”.*

Em seguida, devem ser publicadas as seguintes informações sobre o encarregado: DADOS DO ENCARREGADO (art. 41 da LGPD):

I. Nome e cargo do encarregado indicado pelo controlador;

II. Localização;

III. Horário de atendimento;

IV. Telefone e *e-mail* específico para orientação e esclarecimento de dúvidas.

Neste item, deve ser publicado, ainda, *banner* para a Ouvidoria do Município, que será o canal para endereçamento de petições e reclamações do titular de dados, previstas nos artigos 18 e 20 da LGPD, enquanto não houver um local específico para este fim elaborado pelo Departamento de Informática de Telecomunicações, no portão do Município.

A seguir, devem ser publicadas nessa seção versões resumidas dos Relatórios de Impacto à Proteção de Dados Pessoais - RIPD (ver seção 4.7 deste documento). Os relatórios devem contemplar o fornecimento das informações sobre previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dos tratamentos de dados pessoais adotados para cada Unidade Técnica.

Além de divulgação na seção de “Acesso à Informação” na página eletrônica do órgão, a informação sobre o tratamento de dados pessoais e a finalidade devem ser informadas na descrição do serviço na Carta de Serviços em vigor. Na descrição do serviço é importante também destacar quais são os dados pessoais utilizados pelo órgão e a base legal ou a política pública que respalda a obtenção de tais dados.

4.7 Relatório de Impacto à Proteção de Dados

4.7.1 O que é o Relatório de Impacto à Proteção de Dados Pessoais

O **Relatório de Impacto à Proteção dos Dados Pessoais (RIPD)** representa documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

Segundo o inciso XVII do art. 5º da LGPD, o RIPD é a documentação que deve ser mantida pelo **Controlador** dos dados pessoais.

> Art. 5º Para os 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;

Enquanto o art. 5º, XVII, define o que é um **RIPD**, o seu conteúdo mínimo é indicado pelo parágrafo único do art. 38, grifado abaixo.

> **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.

As próximas seções descrevem o processo de elaboração do RIPD, cujo modelo completo encontra-se em nossos anexos ao final deste manual.

O formulário de **RIPD** apresentado neste manual é apenas instrumento de orientação e constitui uma sugestão para auxiliar os órgãos da municipalidade a realizar a documentação da avaliação de impacto sobre dados pessoais sob seus cuidados.

Dessa forma, e caso seja considerado pertinente pelos órgãos, as seções e o conteúdo do modelo devem ser adaptados para se adequar a cada contexto particular.

4.7.2 Como elaborar o RIPD

O Relatório de Impacto a Proteção de Dados – RIPD deve ser elaborado **antes** de a unidade administrativa iniciar o tratamento de dados pessoais, preferencialmente na fase inicial do programa ou projeto que tem o propósito de usar esses dados para o fim de adequação à LGPD e diagnosticar possíveis fragilidades nas rotinas de tratamento de dados de cada unidade administrativa.

A elaboração do RIPD contempla as oito etapas destacadas pela figura a seguir.

1ª ETAPA (Preparação/nomeação de agentes de dados);

Nesta primeira etapa são designados os agentes de tratamento (controladores e operadores de dados) de cada Secretaria/Coordenadoria e Controladoria Geral do Município, bem como o encarregado segundo os termos e com as funções delimitadas pelo Decreto Municipal nº 38.145/21.

Estes servidores[8] serão nomeados através de Portaria do Sr. Prefeito e passarão por processo de sensibilização e capacitação sobre a Lei Geral de Proteção de Dados e as providências que deverão ser levadas a efeito para a elaboração do seu RIPD e o respectivo Plano de Adequação.

Nesta etapa está inclusa as seguintes providências que estão sendo levadas a efeito de forma concomitante:

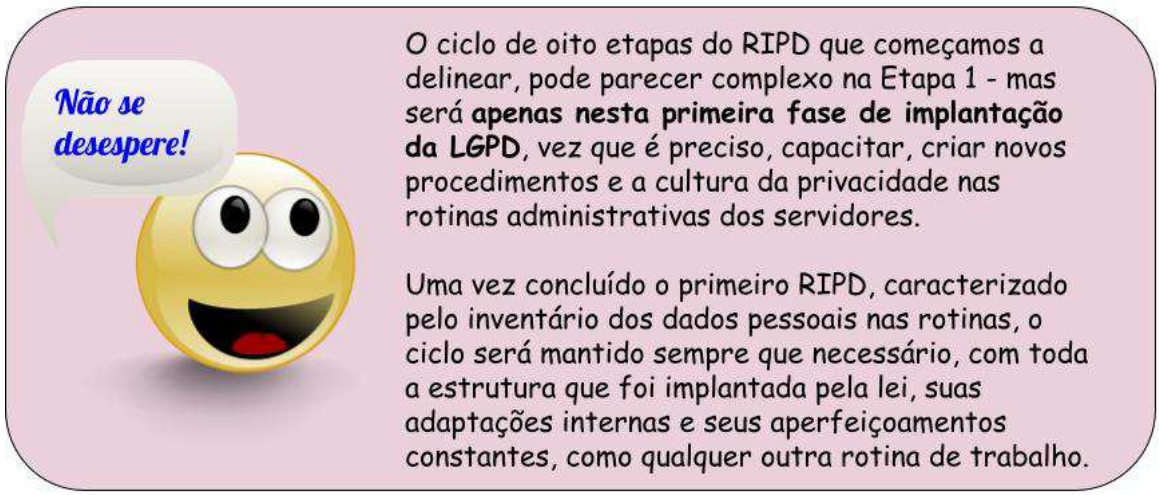
- criação dos canais de solução de dúvidas,

[8] A princípio, é essencial a capacitação dos agentes de tratamento nomeados pelo Prefeito, contudo, com a implantação das boas práticas de privacidade na rotina administrativa, implicará na conscientização de todo o quadro de servidores. (Nota dos autores).

- fornecimento de Plataforma EAD (MOODLE) para capacitação, divulgação de materiais, modelos de documentos e cursos em parceria com a ESAP;

- adaptação do site municipal pelo Departamento de Informática e Telecomunicações para atendimento às demandas dos servidores e munícipes para aplicação da LGPD, bem como, para diagnósticos relacionados procedimentos de segurança digital nos termos das Normas Técnicas adotadas pela LGPD;

- criação de documentos e Políticas Públicas associadas à Boas Práticas associadas à Privacidade e Proteção de Dados.



2ª ETAPA (Identificar a necessidade de elaborar o Relatório);

Preliminarmente e independentemente da fase de inventário que estamos dando início é fundamental conhecer os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado. São eles:

• Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);

• Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e

• A qualquer momento sob determinação da ANPD (art. 38).

Quando for necessária a elaboração do **RIPD**, o órgão deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do **RIPD**.

A elaboração de um único **RIPD** para todas as operações de tratamento de dados pessoais ou de um **RIPD** para cada projeto, sistema, ou serviço deve ser avaliada por cada Secretaria/Coordenadoria de acordo com os processos internos de trabalho. Assim, um órgão que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um **RIPD** único. Já outro que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único **RIPD** não seja a opção mais indicada, optando por elaborar RIPDs por partes (departamentos, procuradorias, divisões, escolas, UBSs, CRAS, Regionais etc.) por ser mais adequado à sua realidade.

Além dos casos específicos previstos pela LGPD no início desta abordagem relativas à elaboração do RIPD, é indicada a elaboração ou atualização do **Relatório de Impacto** sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

• uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;

• 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 § 2º);

• tratamento de 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” (LGPD, art. 5º, II);

• 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);

• tratamento de dados pessoais de crianças e adolescentes

(LGPD, art. 14);

• 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);

• 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. 4º, § 3º);

• tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);

• alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e

• reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Em síntese, nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o **RIPD** ser elaborado ou atualizado pela instituição.

3ª ETAPA - Descrever o tratamento.

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, escopo, contexto e finalidade** do tratamento.

Lembrando que a LGPD (art. 5º, 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*.

O objetivo principal desta descrição é fornecer cenário organizacional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

Caso a unidade que estiver fazendo a avaliação considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.

- Natureza do tratamento

A **natureza** representa como a instituição pretende tratar ou trata o dado pessoal. Importante descrever, por exemplo:

• como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;

• fonte de dados (ex: titular de dados, planilha eletrônica, arquivo extensão .xml, formulário em papel etc.) utilizada para coleta dos dados pessoais;

• com quais órgãos, entidades ou empresas os dados pessoais serão compartilhados;

• quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;

• se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e

• medidas de segurança atualmente adotadas.

Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.

- Escopo do tratamento

O **escopo** representa a abrangência do tratamento de dados.

Nesse sentido, considerar destacar:

• as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis.

• o volume dos dados pessoais a serem coletados e tratados;

• a extensão e frequência em que os dados são tratados;

• o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;

• o número de titulares de dados afetados pelo tratamento; e

• a abrangência da área geográfica do tratamento.

O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.

- Contexto do tratamento

Nesta etapa, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.

O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

• natureza do relacionamento da organização com os indivíduos;

• nível ou método de controle que os indivíduos exercem sobre os dados pessoais;

• destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;

• destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais, ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;

• destaque de qualquer experiência anterior com esse tipo de tratamento de dados;

• destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

- Finalidade do tratamento

A **finalidade** é a razão ou motivo pelo qual se deseja tratar os dados pessoais. **É importantíssimo estabelecer claramente a finalidade**, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.

Nesta etapa, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os exemplos de finalidades elencadas abaixo, embasados nos artigos 7º e 11 da LGPD, no que for aplicável:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- execução de políticas públicas;
- alguma espécie de estudo realizado por órgão de pesquisa;
- execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiro;
- tutela da saúde;
- atender aos interesses legítimos do controlador ou de terceiro;
- proteção do crédito; e
- garantia da prevenção à fraude e à segurança do titular.

Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos.

Ao detalhar a **finalidade** do tratamento dos dados pessoais, é importante:

• Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.

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

Neste momento, deve-se atentar para o caso de a **finalidade** ser para atender o legítimo interesse do controlador, assim, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas,

consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD[9].

Cumpre ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela tem relacionamento.

4ª ETAPA - Identificar partes interessadas consultadas.

Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Nessa etapa, é importante identificar:

Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizar a

[9] Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

segurança da informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.

5ª ETAPA - Descrever necessidade e proporcionalidade.

Descrever como o órgão avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o 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 de dados (LGPD, art. 6º, III).

- **A fundamentação legal para o tratamento dos dados pessoais.**
- **Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:**
  - **esse tratamento de dados pessoais é indispensável;**
  - **não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e**
  - **esse processamento de fato auxilia no propósito almejado.**
- **Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.**
- **Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).**
- **Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.**
- **Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.**
- **Quais são as salvaguardas para as transferências internacionais de dados.**

O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.

6ª ETAPA (Identificar e avaliar os riscos)

Conforme orientação contida no art. 5º, XVII, da LGPD, o Relatório de Impacto deve descrever

“medidas, salvaguardas e mecanismos de mitigação de risco“.

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.

Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Para tal, nos reportamos ao item **“2.7 A importância de realizar a Análise de Risco”** do presente Manual onde são explicitados os mecanismos de aferição de risco através de parâmetros escalares bem com referências diretas às Normas NBR ISO 27.001, 27.002, 27005 e 31.000.

7ª ETAPA (Identificar medidas para tratar os riscos)

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 (LGPD, art. 46).

Nesta fase, se forem necessárias avaliações técnicas referentes a segurança digital, é recomendável solicitar parecer do Departamento de Informática e Telecomunicações.

Importante reforçar que as medidas para tratar os riscos podem ser: de segurança, técnicas ou administrativas e deverão estar descritas no RIPD.

A coluna “Medida(s)” pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento de cada risco identificado na etapa “Identificar e avaliar riscos”.

A Municipalidade nem sempre conseguirá eliminar todos os riscos, mesmo porque a sofisticação dos “mal intencionados” é sempre cada vez maior.

Nesse sentido, a Controladoria Geral da União orienta o Poder Público que: uma vez identificado um risco de difícil eliminação ou mitigação, pode-se sopesar e decidir que alguns riscos são aceitáveis - até um risco de nível alto – devido aos benefícios do processamento dos dados pessoais para o interesse público e as respectivas dificuldades de mitigação. **No entanto a CGU recomenda, “*se houver um risco residual de nível alto, é***

recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais"[10].

A seguir, são apresentados exemplos de medidas para lidar com os riscos a fim de demonstrar o preenchimento da tabela constante da seção 7 do **RIPD**, que consta no Anexo I.

Tabela 6 Exemplos de medidas para lidar com os riscos

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO[1]	RISCO RESIDUAL 2			MEDIDA(S) APROVADA(S)[3]
			P	I	(P X I)	
R01 Acesso não autorizado.	1. Controle de acesso Lógico.	Reduzir	5	10	**50**	Sim
	2. Desenvolvimento seguro.					
	3. Segurança em Redes.					

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6 do RIPD.

1. Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.
2. Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.
3. Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

Neste momento, e a critério do responsável pela elaboração do RIPD, a coluna "Medida(s)" também pode ser preenchida de forma mais detalhada, indicando os principais aspectos da medida de segurança ou controles de segurança adotados para tratar o risco. Esse procedimento propicia mais visibilidade em relação ao tratamento do risco.

8ª ETAPA - Aprovar o Relatório

Nesta Etapa, já deverão estar formalizados para aprovação em processo administrativo físico e em formato digital seguro, o (s) RIPD(s) de

[10] Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD) - p.41.

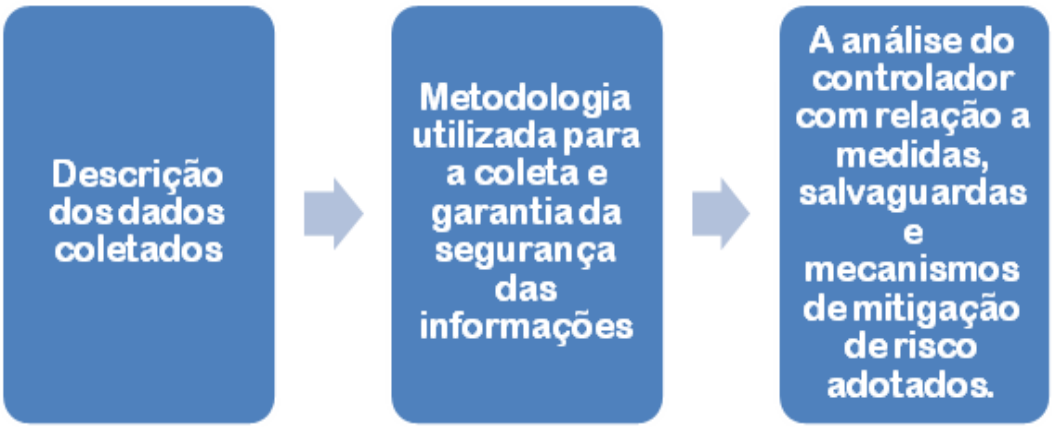
cada Secretaria/Coordenadoria e Controladoria Geral do Município. A referida documentação deverá estar assinada pelo Controlador e Operador Central, bem como, pelas autoridades titulares das respectivas Pastas e, posteriormente, o Encarregado.

O processo deve ser encaminhado para Controladoria Geral do Município - CGM, regularmente, para que o Encarregado acompanhe a aplicação da norma e expeça diretrizes de adequação à LGPD, quando necessário.

Cada órgão deverá manter seus respectivos relatórios seguros e organizados de forma que possam ser revistos para acompanhamento das medidas propostas e atualização periódica e, a qualquer tempo, em caso de incidentes, encaminhamento à ANPD, quando solicitado, ou a qualquer outro órgão de controle externo ou interno.

Salienta-se ainda que, conforme previsto no inciso I do art. 23 da LGPD, cada órgão deverá dar publicidade em suas respectivas páginas eletrônicas a uma versão resumida dos Relatórios de Impacto à Proteção de Dados Pessoais.

Resumidamente, o RIPD deverá conter os elementos abaixo:



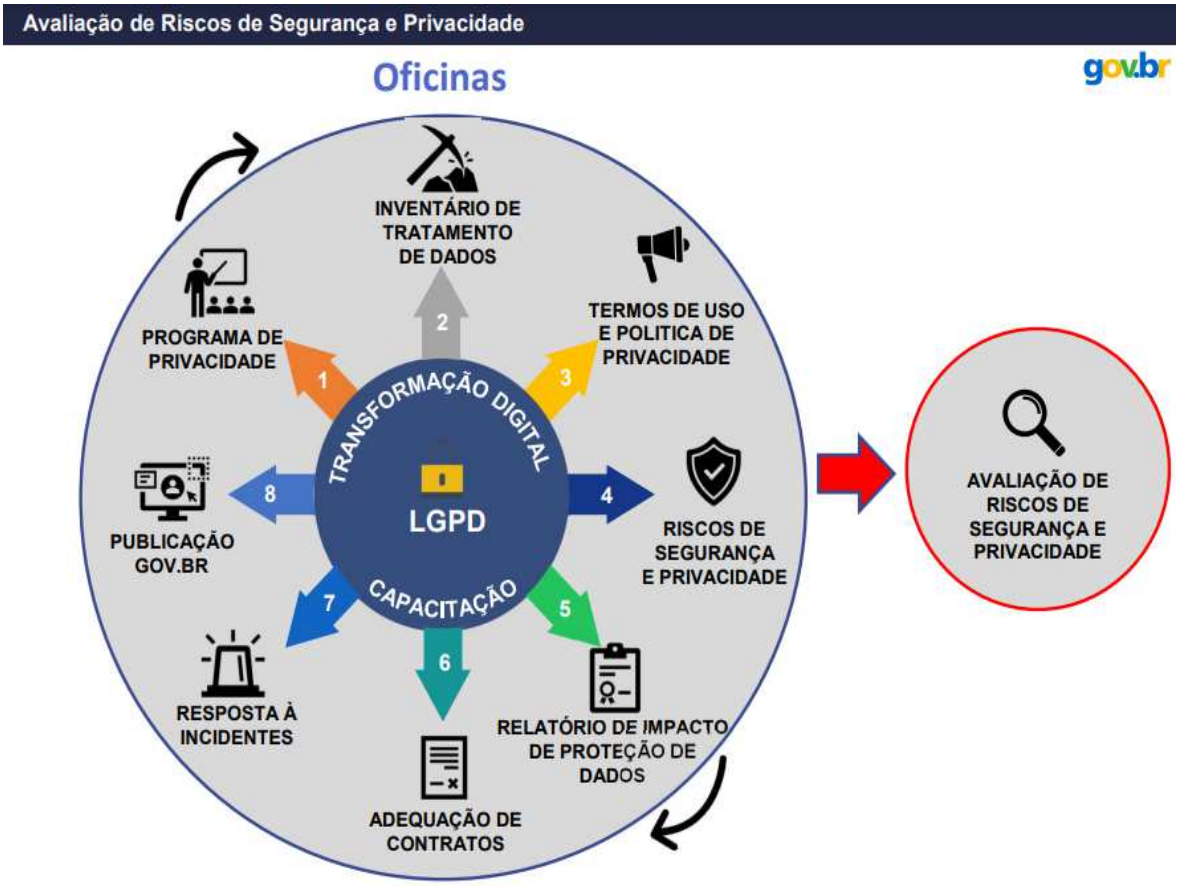
9ª ETAPA - Manter Revisão

O **RIPD** deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela unidade técnica da Municipalidade.

Cumpre destacar que as orientações referentes à identificação da necessidade de elaborar ou atualizar o **RIPD** constantes do item 4.7.2. 2ª

Etapa, deste documento contribuem para a identificação de casos em que o **Relatório de Impacto** deve ser atualizado.

Cada unidade da Municipalidade deve manter revisão do **RIPD** a fim de demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.



4.8 Término do Tratamento de Dados Pessoais

Independentemente, da abordagem deste assunto que faremos no capítulo seguinte, é relevante observar alguns cuidados pontuais quando o assunto é término do tratamento de dados pessoais.

Conforme expresso na LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses:

(i) exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade;

(ii) fim do período de tratamento;

(iii) revogação do consentimento ou a pedido do titular, resguardado o interesse público;

(iv) determinação da autoridade nacional em face de violação do disposto na Lei.

Na incidência de qualquer uma das hipóteses acima, a Lei determina que os dados sejam eliminados, a não ser nos casos em que:

(i) remanesça o cumprimento de obrigação legal ou regulatória pelo controlador;

(ii) sejam necessários para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados;

(iii) ocorra a transferência a terceiro, desde que respeitados os requisitos de tratamento dispostos em Lei; e

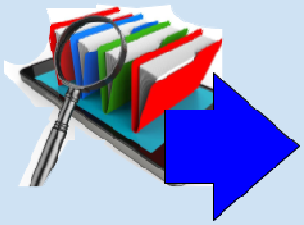
(iv) seja utilizado exclusivamente pelo controlador, vedado seu acesso por terceiro, e desde que anonimizados.

No âmbito da Administração Pública Municipal, é importante que este dispositivo seja harmonizado com a legislação municipal, que deve ser considerada conjuntamente na realização das operações com os dados pessoais contidos em meio físico ou digital, abrangendo documentos arquivados, ainda que estes sejam mantidos em sistemas informatizados e bases de dados. Nesse sentido, deve ser observada a aplicabilidade da Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011), sua regulamentação no âmbito local[11] e todas as normas municipais de gestão documental[12], ou seja, a interpretação da gestão dos dados deverá ser realizada sempre de forma ampla e sistêmica.

[11] DECRETO n. 36.140, de 15 de agosto de 2019. Regulamenta no âmbito do Poder Executivo Municipal a Lei Federal nº 12.527, de 18 de novembro de 2011, estabelecendo procedimentos e outras providências correlatas para garantir o direito de acesso à informação, conforme especifica. Disponível em: https://www.guarulhos.sp.gov.br/06_prefeitura/leis/decretos_2019/36140decr.pdf

[12]DECRETO n. 25.624, de 17 de julho de 2008. Dispõe sobre a Gestão de Documentos, os Planos de Classificação e a Tabela de Temporalidade de Documentos e define normas para avaliação, guarda e destinação de documentos de arquivo. Disponível em: https://www.guarulhos.sp.gov.br/06_prefeitura/leis/decretos_2008/25624decr.pdf

OBS: Tanto os Planos de Classificação de Documentos quanto as Tabelas de Temporalidade de Documentos de Arquivo serão divulgados por meio de Portaria expedida pela Secretaria de Gestão.”



A eliminação de documentos arquivísticos deve ser conduzida pelas respectivas Comissões de Avaliação de Documentos (CAD) dos órgãos e entidades da Administração Municipal, consoante orientações contidas no Decreto Municipal n. 25.624/2008.

Além dos cuidados preconizados pela LGPD, é imprescindível a utilização dos instrumentos técnicos de gestão de documentos, Tabelas de Temporalidade e Destinação de Documentos de Arquivo, em harmonia ainda, quando for o caso, com a classificação das informações quanto ao grau e prazos de sigilo previstos pela Lei de Acesso à Informação (Lei nº 12527/11), regulamentada pelo Decreto Municipal 36.140/2019.

5

O Ciclo de Vida dos Dados Pessoais

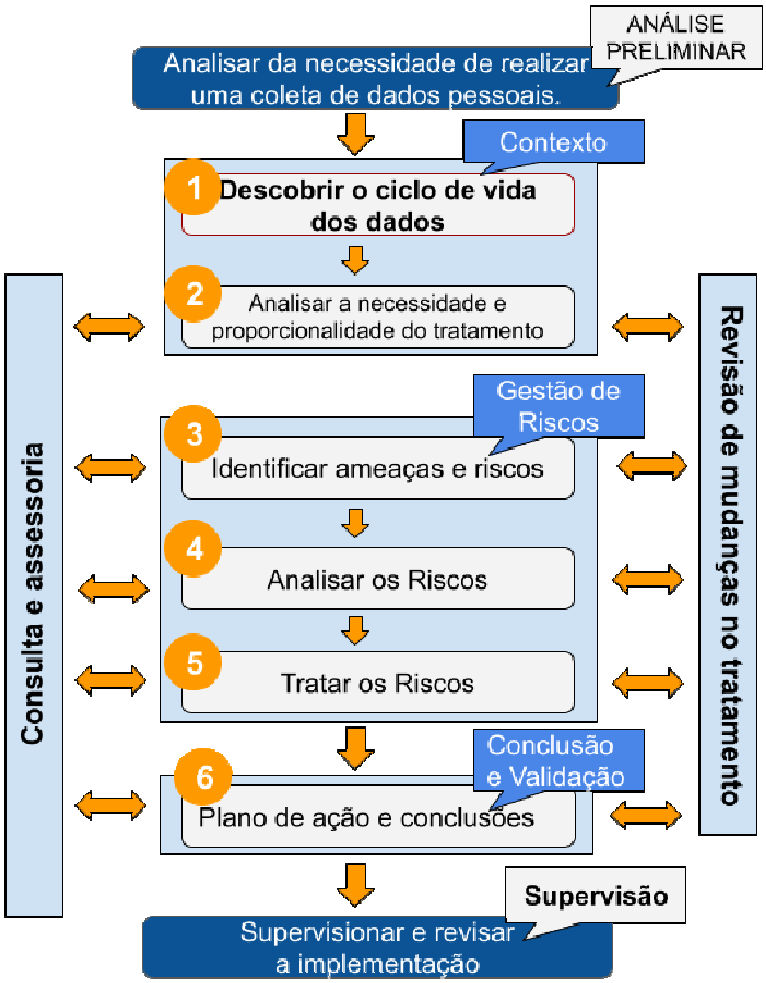
Estivemos dissertando, até o momento, sobre o histórico da LGPD, normas internacionais de segurança, noções sobre o que são dados e informações pessoais e algumas de suas peculiaridades, direitos dos titulares de dados, deveres e princípios a serem adotados pelo gestor de dados e formas de elaboração de relatórios.

Todas estas informações são extremamente importantes, mas serão de pouca ou nenhuma utilidade se os agentes de tratamento não conhecerem o ciclo de vida dos dados dentro da prática administrativa do órgão que representam para que, somente então, possam estudar e implementar estratégias eficazes de segurança da informação no contexto Municipal.

O dado pessoal é coletado para atender a uma finalidade específica pela Administração dentro de um contexto e pode, por exemplo, ser eliminado a pedido do titular dos dados[13] (LGPD, art. 18, IV), ao cumprimento de uma sanção aplicada pela Autoridade Nacional de Proteção de Dados (LGPD, art. 52, VI) ou ao término de seu tratamento (LGPD, art. 16). Dessa forma, percebemos a configuração de um ciclo que se inicia com a coleta e que determina a "vida" (existência) do dado pessoal durante um período de tempo, de acordo com certos critérios de eliminação.

[13] Ressalte-se que no caso de cumprimento de obrigação legal, como ocorre com a administração pública na maior parte dos casos, é autorizada a conservação do dado (LGPD, art. 16, I). Isso significa que, da mesma forma que o titular dos dados não precisa consentir o tratamento dos dados pessoais pela administração pública em casos determinados, também não é possível ao titular do dado solicitar a eliminação.

É fundamental destacar mais uma vez que a LGPD considera como tratamento todas as operações realizadas com dados pessoais. Assim, a LGPD não adota qualquer tipo de segregação, considerando como tratamento, por exemplo, tanto a coleta quanto o armazenamento de dados pessoais, mesmo essas operações tratando de propósitos diferentes.



Como é possível visualizar no esquema acima, somente a partir do conhecimento do ciclo de vida do dado pessoal todas as demais etapas poderão ser implementadas para segurança da informação.

Para orientar a prática do tratamento e apresentar os ativos institucionais envolvidos, divide-se o ciclo de vida do tratamento dos dados pessoais em cinco fases: coleta, retenção, processamento, compartilhamento e eliminação.

Nesta seção, abordaremos o que é cada fase do ciclo de vida, a relação das fases do ciclo com as operações de tratamento da LGPD, os tipos de ativos organizacionais e o relacionamento desses ativos com as fases do ciclo de tratamento, destacando as ações a serem executadas em tais fases.

5.1 FASES DO CICLO DE VIDA

Para implementar o correto tratamento dos dados pessoais e as medidas correlatas, o órgão precisa conhecer os dados pessoais que gerencia e quais processos, projetos, serviços e ativos perpassam o ciclo de vida do tratamento dos dados pessoais.

A LGPD considera como tratamento toda operação realizada com os 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.

Para além da legislação de proteção de dados pessoais, reforçamos, mais uma vez, o que já foi abordado no item 4.8, ou seja, **a aplicação da LGPD é SISTÊMICA.** Sempre será preciso observar a legislação de gestão de documentos, que deve ser considerada conjuntamente na realização das operações com os dados pessoais contidos em documentos arquivísticos[14], ainda que estes sejam mantidos em sistemas informatizados e bases de dados. Do mesmo modo, vale lembrar, a Lei de Acesso à Informação - LAI (Lei nº 12.527, de 18 de novembro de 2018) e o seu regulamento (Decreto Municipal n. 36.140/2019) igualmente apresentam regras específicas para o acesso a documentos que, embora apresentem dados pessoais, possuem valor permanente e foram recolhidos a instituições arquivísticas públicas. Resumindo: a LGPD e a LAI também devem, portanto, ser interpretadas sistematicamente.

Nesse cenário, o ciclo de vida do tratamento tem início com a coleta do dado e se encerra com a eliminação ou descarte. Cada fase do ciclo de vida tem correspondência com operações de tratamento definidas na LGPD.

A fase coleta/geração, refere-se à coleta, produção e recepção de dados pessoais independente do meio utilizado (documento em papel,

[14] Documento Arquivístico: documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência. (CTDE, 2016, p. 20). Ex. Histórico escolar.

documento eletrônico, sistema de informação etc.).

A retenção/armazenagem corresponde ao arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc.).

A utilização/processamento é qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação e extração e modificação de dados pessoais retidos pelo controlador.

O compartilhamento, por sua vez, envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhado de dados pessoais.

O arquivamento envolve qualquer operação que visa a guarda, conservação e possibilidade de recuperação de dados, seja para cumprimento de determinação legal (Ex. Históricos escolares, dados fiscais, etc.), seja por questões de segurança e auditabilidade interna.

Por fim, a eliminação/exclusão é qualquer operação que visa excluir um dado ou conjunto de dados pessoais armazenados em banco de dados, em virtude do tratamento da LGPD. Quando se tratar da eliminação de documentos arquivísticos, devem ser levadas em consideração as recomendações constantes da seção 4.8 - Término do Tratamento de Dados Pessoais deste manual.

Para ser um servidor "antenado", **olha a dica:**

- Cada unidade da Administração Municipal deve ter uma comissão permanente chamada CAD - Comissão de Avaliação de Documentos, com atribuições delegadas pelo Decreto nº 25624/2008, procure saber quem são estes colegas e como está sendo realizada a eliminação de documentos em seu local de trabalho, solicitando, ainda, a aplicação das Tabelas de Temporalidade de Documentos, convide-os a colaborar com o RIPD.

- Em caso da CAD não estar atualizada com o quadro atual de servidores ou atuante, procure informações de como proceder junto a chefia superior e/ou junto à Secretaria de Gestão.

Conforme descrito no art. 5º, X, da LGPD, qualquer "acesso" é uma operação de tratamento de dados presente em todas as fases do ciclo de vida dos dados pessoais, pois de alguma forma temos que realizar acesso ao dado pessoal para viabilizar sua coleta, retenção, processamento, compartilhamento ou eliminação.

Conforme orienta a CGU, as operações de tratamento de dados pessoais se cruzam com os procedimentos e operações da gestão de documentos, nas diversas fases do ciclo de vida do documento. Quando os dados pessoais integrarem documentos arquivísticos, os procedimentos e operações da gestão de documentos também precisam ser efetivados conjuntamente, como por exemplo, produção, recebimento, tramitação, arquivamento, classificação, indexação, atribuição de restrição de acesso, avaliação, transferência, acesso e eliminação.

Seja cauteloso, como vimos até o momento, em qualquer uma das etapas pode haver falhas na aplicação da LGPD, portanto, ***fica a dica:*** *é importante não apenas conhecer a Lei, mas criar mecanismos de prevenção e, acima de tudo, compartilhar conhecimento e responsabilidade com a equipe de servidores que terão qualquer tipo de acesso a dados pessoais.*

Alguns desses procedimentos e operações da gestão de documentos, apesar de serem referidos pelo mesmo termo, tem entendimento distinto daquele utilizado no contexto do tratamento de dados pessoais, e cada um deve ser entendido e realizado em conformidade com seu contexto.

No contexto da gestão de documentos, o ciclo de vida dos documentos de arquivo compreende três fases, a saber: produção, utilização e destinação final (eliminação ou guarda permanente). Em cada uma dessas fases são realizados os procedimentos e operações de gestão de documentos, conforme figura e quadro a seguir.

Produção: operações referentes à elaboração de documentos em razão da execução das atividades de um órgão ou entidade.

Utilização (uso e manutenção): operações referentes ao fluxo percorrido pelos documentos para o cumprimento de sua função administrativa, assim como de sua guarda, após cessar o seu trâmite.

Destinação final: operações referentes ao ato de decidir quais documentos devem ser eliminados (mediante autorização, conforme legislação vigente), bem como quais documentos devem ser mantidos por razões administrativas, legais ou fiscais. Para tal, envolve as atividades de análise, seleção e fixação de prazos de guarda dos documentos.

Relacionamento das fases do ciclo de vida dos documentos de arquivo X procedimentos e operações de gestão de documentos.

DOCUMENTOS DE ARQUIVO	
DOCUMENTOS DE ARQUIVO FASE DO CICLO DE VIDA DOS DOCUMENTOS DE ARQUIVO	**OPERAÇÕES DE TRATAMENTO NA GESTÃO DE DOCUMENTOS (INDEPENDENTEMENTE DO SUPORTE MATERIAL E DA ENTIDADE PRODUTORA) – LEI Nº 8.159/1991 E NORMA ABNT NBR ISO 15489:2018**
Produção	Elaboração, recebimento, registro, classificação, indexação e atribuição de restrição de acesso
Utilização(uso e manutenção)	Tramitação, controle, arquivamento, transferência para guarda intermediária, acesso e empréstimo.
Destinação final	Avaliação, seleção, eliminação e recolhimento para guarda permanente.

5.2 ATIVOS ORGANIZACIONAIS

A unidade administrativa onde você trabalha possui um manual de procedimentos internos? Se não houver, a necessidade de implementação da

LGPD será uma ótima oportunidade de se pensar em estruturar um manual já adaptado a boas práticas de administração e segurança, por outro lado, a existência de um manual de procedimentos poderá facilitar muito no processo de compreensão do ciclo de vida dos dados pessoais em sua unidade, identificando os ativos organizacionais dos processos internos e assim realizar o respectivo relatório (RIPD).

Por definição, ativos organizacionais são todos os componentes que atuam na elaboração e processamento de um projeto e são capazes de influenciar o seu resultado, deste modo, é importante identificar quais ativos organizacionais estão envolvidos em cada fase do ciclo de vida do tratamento dos dados pessoais, pois são variáveis a serem consideradas no momento da análise de riscos.

Os **principais ativos** são: **bases de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais**. A figura **a seguir** apresenta os principais ativos envolvidos no ciclo de vida do tratamento dos dados.

A seguir, são apresentadas definições para os ativos envolvidos no ciclo de vida do tratamento dos dados pessoais.

Base de dados: é uma coleção de dados logicamente relacionados, com algum significado. Uma base de dados é projetada, construída e preenchida (instanciada) com dados para um propósito específico.

Documento: unidade de registro de informações, qualquer que seja o suporte e formato (Arquivo Nacional, 2005).

Equipamento: objeto ou conjunto de objetos necessário para o exercício de uma atividade ou de uma função.

Local físico: determinação do lugar no qual pode residir de forma definitiva ou temporária uma informação de identificação pessoal. Por exemplo, uma sala, um arquivo, um prédio, uma mesa, etc.

Pessoa: qualquer indivíduo que executa ou participa de alguma 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.

Sistema: qualquer aplicação, software ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais: coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais.

Unidade organizacional: órgãos e entidades da Administração Pública.

5.3 RELACIONAMENTO DO CICLO VIDA DO TRATAMENTO DOS DADOS PESSOAIS COM ATIVOS ORGANIZACIONAIS

Para cada fase do ciclo de tratamento de dados é importante identificar os ativos organizacionais que estarão envolvidos.

Na fase de **Coleta** deve-se identificar os ativos envolvidos na coleta de dados pessoais. Esses dados podem entrar na organização por algum **documento**, algum **sistema** hospedado em algum **equipamento** localizado em **local físico** do órgão público. Podem ser coletados pela prestação de algum serviço externo ou serviço prestado pelo próprio órgão público por meio de alguma de suas **unidades organizacionais**.

Na fase de **Retenção**, deve-se avaliar os ativos utilizados para armazenar os dados pessoais. Esses dados podem estar armazenados em **bases de dados, documentos, equipamentos ou sistemas**. É preciso considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados, bem como os **locais físicos** onde estão localizados os ativos que armazenam esses dados. Se o armazenamento for em “nuvem”, por exemplo, é necessário considerar o serviço de armazenamento contratado e/ou utilizado.

A fase de **Processamento** segue a mesma linha de raciocínio das anteriores. Identifica-se os ativos onde são realizados os tratamentos dos dados. O tratamento pode ser realizado em **documento**, pode ser feito por um **sistema** interno ou contratado pelo órgão. É preciso identificar as **pessoas** (papéis organizacionais), **unidades** organizacionais **e equipamentos** envolvidos nesse tratamento. Onde estão **localizadas fisicamente** essas unidades organizacionais e os equipamentos envolvidos no tratamento também são importantes.

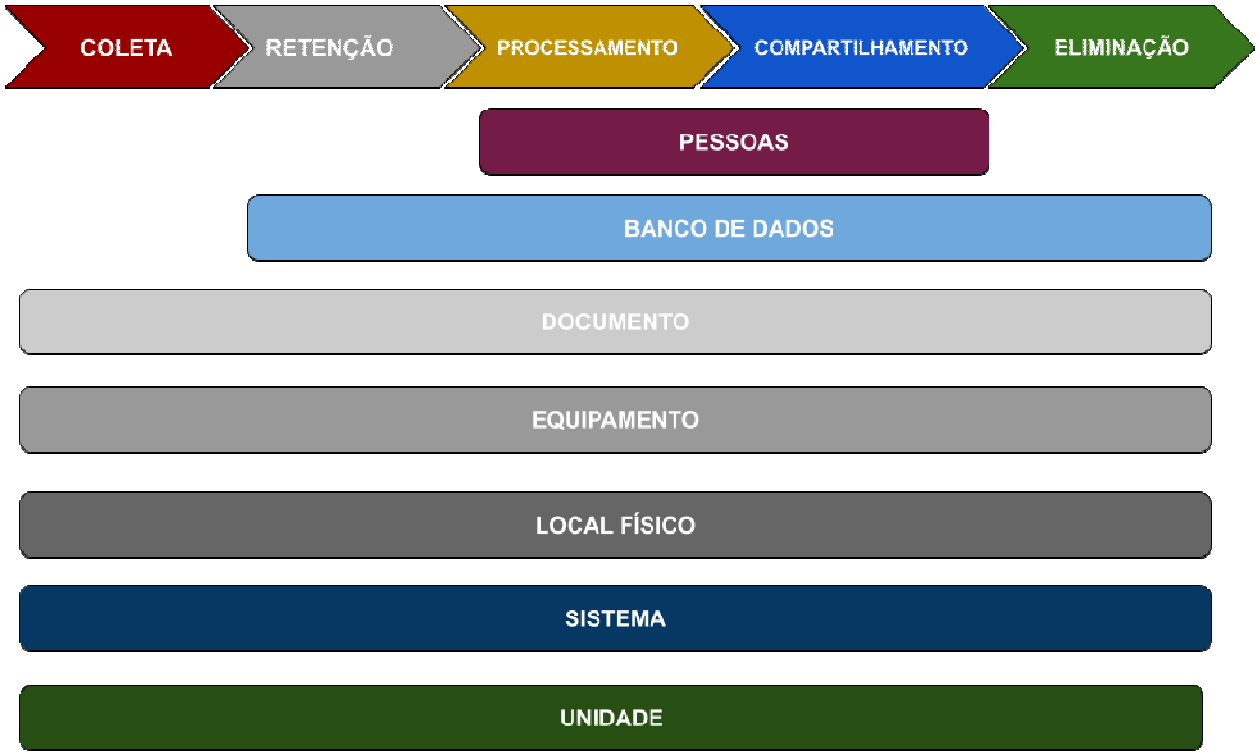
Na fase de **Compartilhamento** é preciso mapear os ativos envolvidos na distribuição ou divulgação dos dados pessoais para dentro e para fora do órgão público. Quais **sistemas** são usados para transmitir, exibir ou divulgar dados pessoais? Quais **pessoas** são destinatárias dessas informações? Quais **unidades organizacionais**, quais e**quipamentos** são usados para tal?

No que se refere à fase de **Eliminação**, deve-se avaliar os ativos que armazenam os dados pessoais que possam ser objeto de: solicitação de eliminação de dados a pedido do titular dos dados pessoais; ou descarte nos casos necessários ao negócio da instituição. Os dados pessoais a serem eliminados podem estar armazenados em ativos relacionados com **bases de dados, documentos, equipamentos ou sistemas**. É necessário considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados que possam ser objeto de eliminação ou descarte, bem como os **locais físicos** onde estão localizados os ativos que contenham dados a serem eliminados ou descartados. Se a eliminação do dado pessoal ou descarte do ativo tiver relação com solução em “nuvem”, por exemplo, é preciso considerar o serviço de armazenamento contratado ou utilizado

Quando os dados pessoais estiverem contidos em documentos arquivísticos, qualquer que seja o suporte ou formato, esses dados poderão ser tratados no contexto da LGPD, mas os documentos arquivísticos propriamente ditos, deverão seguir os procedimentos definidos pela legislação aplicável ao contexto da gestão destes documentos, conforme já foi objeto de análise anteriormente.

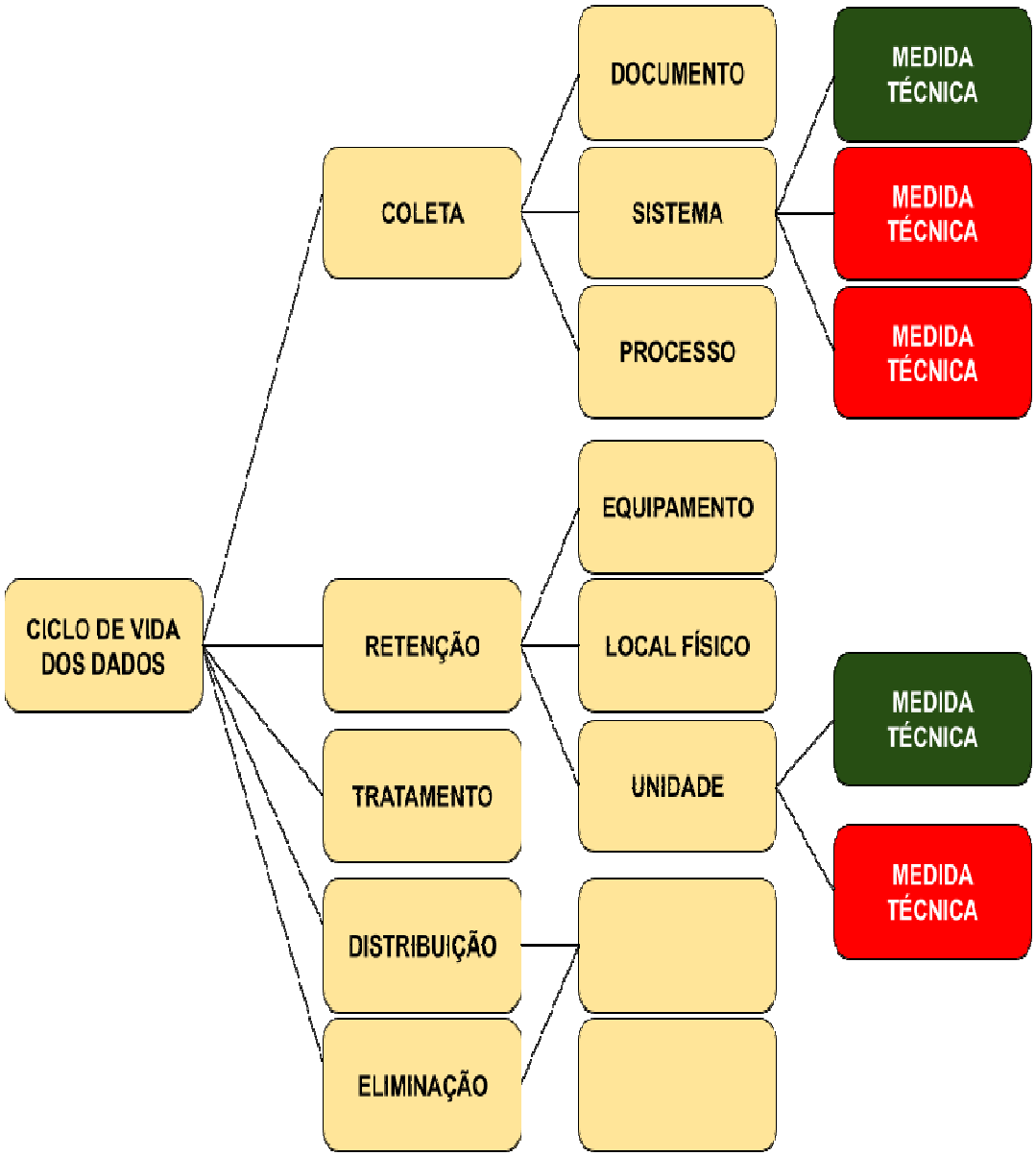
Esse processo demanda esforço considerável, principalmente para grandes unidades, com vários departamentos e divisões, ou, ainda, unidades descentralizadas como é o caso de UBSs, escolas, CRAS, CREAS e etc. O ideal é que se estabeleçam ações de **mapeamento e análise dos processos organizacionais**, tendo em vista que, desta forma, o órgão conseguirá identificar de maneira mais eficaz os ativos envolvidos em cada competência administrativa.

O quadro seguinte apresenta o relacionamento entre as fases do ciclo de tratamento de dados pessoais e os ativos que podem ser utilizados em cada etapa. É importante registrar, assim, que existem ativos presentes em todas as fases do ciclo (ex: Documento) e outros que estarão em apenas algumas delas (ex: Pessoa).



Uma vez identificados os ativos, é necessário analisá-los para verificar quais medidas técnicas de segurança estão efetivamente implementadas nesses ativos, com vistas a prover a adequada proteção aos dados pessoais de que trata a LGPD. Recomenda-se a utilização de alguma metodologia framework, boa prática ou norma técnica aplicável como as que foram apresentadas no Capítulo 2 de nosso documento e serão sugeridas na parte prática.

O resultado dessa análise vai determinar quais medidas de segurança devem ser implementadas em cada ativo e quais devem ser ajustadas para que o órgão público possua o adequado grau de proteção de dados exigido pela LGPD. A **Figura 7** apresenta esquema de mapeamento dos ativos e suas respectivas **medidas de segurança** implementadas (destacadas em verde) e não implementadas (destacadas em vermelho).


CICLO DE VIDA DOS DADOS
COLETA
RETENÇÃO
TRATAMENTO
DISTRIBUIÇÃO
ELIMINAÇÃO
DOCUMENTO
SISTEMA
PROCESSO
EQUIPAMENTO
LOCAL FÍSICO
UNIDADE
MEDIDA TÉCNICA
MEDIDA TÉCNICA
MEDIDA TÉCNICA
MEDIDA TÉCNICA
MEDIDA TÉCNICA

6

BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

Neste capítulo iremos abordar:

- ***o que a LGPD espera como política preventiva de segurança e como estabelecer o "Privity by desing" no local de trabalho;***
- ***8 passos básicos para implementação de um plano de ação para colocar em prática todo o nosso conteúdo junto a equipe.***

Quando tratamos de boas práticas em segurança da informação o assunto toma uma dimensão que vai além de simplesmente aplicar mais uma nova legislação em nossa rotina administrativa de servidor municipal, trata-se de uma mudança cultural irreversível, impactada por um mundo cada vez mais globalizado e digital, onde as práticas de "compliance"[15], estão tornando a Administração Pública cada vez mais dinâmica e alinhada com práticas de qualidade de gestão do mundo corporativo.

A grande notícia é que somos parte desta mudança e, ainda que a maioria ainda não perceba, temos a oportunidade de realizar o que Mahatma Gandhi pontuou: **"*Seja a mudança que você quer no mundo*".**

Em nosso contexto, **que tal trocar "mundo" pela Prefeitura?**

[15] O termo compliance vem do inglês "to comply" e significa estar em conformidade. Na prática, o compliance tem a função de proporcionar segurança e minimizar riscos de organizações públicas e privadas, garantindo o cumprimento dos atos, regimentos, normas e leis estabelecidos interna e externamente.

6.1 PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO (*PRIVACY BY DESIGN E BY DEFAULT*)

6.1.1 Privacidade desde a concepção

Não apenas os agentes de tratamento, mas qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais são obrigados a assegurar a segurança da informação para proteção dos dados pessoais, pois ambas estão relacionadas.

Segundo o previsto pelo caput do art. 46 da LGPD, a proteção dos dados pessoais é alcançada por meio de **medidas de segurança**, técnicas e administrativas.

> **Art. 46. 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.**
>
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados: a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
>
> **§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.**

O art. 46, § 2º menciona que as **medidas de segurança**, técnicas e administrativas para proteção de dados pessoais deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Isso apresenta um conceito fundamental para a proteção da privacidade dos dados pessoais denominado Privacidade **desde a Concepção** (do inglês Privacy by Design).

O conceito de Privacidade desde a Concepção foi criado por Ann Cavoukian, ex-comissária de Informação e Privacidade da Província de Ontário, no Canadá, significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Tal privacidade pode ser alcançada por

meio da aplicação dos 7 Princípios Fundamentais criados por ´Cavoukian[16], que serão destacados nas próximas subseções deste tópico.

6.1.1.1 Proativo, e não reativo; preventivo, e não corretivo

A Privacidade desde a Concepção (PdC) é caracterizada por medidas proativas e não reativas. Ou seja, essa abordagem antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem nem ofereçam soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram. Em resumo, a Privacidade desde a Concepção vem antes do fato, não depois.

Se aplicada a tecnologias da informação, práticas organizacionais, projeto físico ou em rede de ecossistemas de informação, a PdC começa com um reconhecimento explícito do valor e dos benefícios de adoção de práticas de privacidade fortes, de forma precoce e consistente.

Por exemplo, prevenir a ocorrência de violações de dados, internas ou externas. Isso implica:

• um compromisso claro da Administração em definir e fazer cumprir altos padrões de privacidade;

• um compromisso de privacidade comprovadamente compartilhado pelas comunidades de usuários de serviços públicos e pelas partes interessadas administração direta e indireta e terceiros contratados, no exercício de sua atividade pública, e inserido em uma cultura de melhoria contínua; e

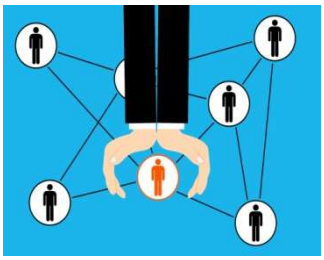
• métodos estabelecidos para reconhecer projetos de privacidade inadequados, antecipar práticas inadequadas de privacidade e corrigir quaisquer impactos negativos, muito antes de ocorrerem.

Tais providências não são rápidas e tampouco fáceis de se conseguir implementar, mas contarão com todo o apoio que os órgãos de Gestão e Controladoria Geral puderem proporcionar.

6.1.1.2 Privacidade deve ser o padrão dos sistemas de TI ou práticas de rotina

[16] CAVOUKIAN, Ann. *Privacy by Design: The 7 Foundational Principles*. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>.

administrativa.



A privacidade por padrão procura oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

O Departamento de Informática e Telecomunicações estará atuando concomitantemente com todas as demais áreas auxiliando-as dentro de suas realidades locais, fornecendo diretrizes de segurança através de Notas Técnicas e implantação de Políticas Públicas voltadas à segurança em TI.

Com relação aos documentos arquivísticos, a privacidade precisa ser resguardada de acordo com a legislação vigente, seguindo os procedimentos de gestão de documentos. Os sistemas que mantêm e gerenciam documentos arquivísticos devem ter controles para garantir esse resguardo, tanto do ponto de vistas do acesso quanto de sua guarda em segurança. Ex. a guarda de documentos em locais sem segurança ou cuja disposição a fatores ambientais como goteiras e umidade possam comprometer sua integridade.

6.1.1.3 Privacidade incorporada ao projeto (*design*)

A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas administrativas. Isto significa que não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

A privacidade deve ser incorporada às tecnologias, operações de sistemas e arquiteturas de informação de maneira holística, integrativa e criativa:

• holística significa que contextos adicionais mais amplos devem sempre ser considerados;

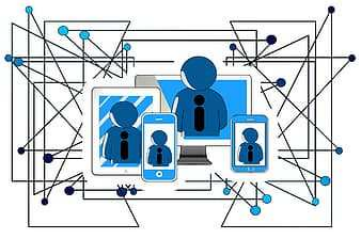
• integrativa indica que todas as partes interessadas devem ser consultadas; e
• criativa, pois incorporar privacidade às vezes significa reinventar as escolhas

atuais quando as alternativas forem inaceitáveis.

Para alcançar esse objetivo, deve-se adotar uma abordagem sistemática apoiada em padrões e frameworks reconhecidos, os quais necessitam ser revistos e passíveis de auditorias externas. Todas as práticas de informação equitativa precisam ser aplicadas com igual rigor a cada etapa do projeto e da operação.

O impacto do uso, configuração incorreta ou erros relativos à tecnologia, à operação ou à arquitetura de informações sobre a privacidade devem ser comprovadamente minimizados. Por isso, avaliações de impacto e risco na privacidade devem ser realizadas e publicadas, documentando claramente os riscos à privacidade e todas as medidas tomadas para mitigá-los. A seção 4.7 deste documento apresenta orientações referentes à elaboração do Relatório de Impacto à Proteção dos Dados Pessoais.

6.1.1.4 Funcionalidade total



A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos da atividade administrativa, não apenas os objetivos de privacidade. A PdC é habilitadora duplamente em natureza, permitindo funcionalidade total com resultados reais e práticos.

Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do resultado daquele trabalho sejam atendidas.

A questão da privacidade é frequentemente vista como de nenhuma ou baixa relevância e que compete com a objetividade do projeto, com as capacidades técnicas de um produto ou serviço e com outros interesses das partes envolvidas. A PdC visa justamente contrapor essa visão, pois objetiva satisfazer todos os objetivos da instituição, e não somente os de privacidade. Evitando a pretensão de dicotomias falsas, como privacidade X segurança, o PdC demonstra que é possível — e mais desejável — ter ambos.

6.1.1.5 Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados

Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.

A privacidade deve ser protegida continuamente em todo o domínio e ao longo do ciclo de vida do tratamento dos dados em questão. Não deve haver lacunas na proteção ou na prestação de contas. O princípio “Segurança” tem relevância especial porque, em sua essência, sem segurança forte, não pode haver privacidade.

As instituições devem assumir a responsabilidade pela segurança dos dados pessoais, geralmente proporcional ao grau de sensibilidade, durante todo o ciclo de tratamento, consistente com os padrões que foram definidos por organismos reconhecidos de desenvolvimento de padrões.

Os padrões de segurança aplicados devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de tratamento, incluindo, entre outros, métodos de destruição segura, criptografia apropriada, e métodos fortes de controle de acesso e registro.

Na LGPD, a segurança é um princípio a ser observado no tratamento de dados pessoais, destacado pelo art. 6º, inciso VII.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> **VII - segurança:** 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;

6.1.1.6 Visibilidade e Transparência

A PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Esse cenário pode ser sintetizado pelo seguinte lema: confie, mas verifique!

Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança. A avaliação independente deste princípio fundamental deve concentrar-se, especialmente, sobre os seguintes aspectos:

• **Responsabilização** - A coleta de dados pessoais implica um dever de cuidar de sua proteção. A responsabilidade por todas as políticas e procedimentos relacionados à privacidade deve ser documentada e comunicada conforme apropriado e atribuído a um indivíduo especificado. E ao transferir dados pessoais para terceiros, medidas equivalentes de proteção à privacidade devem ser asseguradas por contratos ou outros tipos de acordos formais.

• **Abertura** - Abertura e transparência são fundamentais para a prestação de contas. Informações sobre as políticas e práticas relacionadas ao gerenciamento de dados pessoais devem estar prontamente disponíveis para consulta dos titulares de dados. Mecanismos de reclamação e reparação dos dados pessoais devem ser estabelecidos e comunicados para os titulares dos dados.

• **Conformidade** - As etapas necessárias para monitorar, avaliar e verificar a conformidade com as políticas e procedimentos de privacidade devem ser estabelecidas.

A responsabilização, abertura e transparência estão expressas na LGPD pelos seguintes princípios destacados no art. 6º:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> **IV - livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> **VI - transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; e
>
> **X - responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de

proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

6.1.1.7 Respeito pela privacidade do usuário

Acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados.

Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

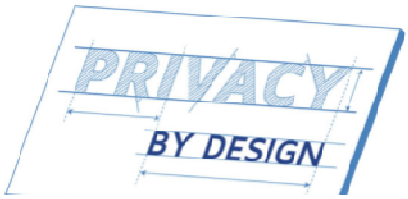
Empoderar os titulares de dados a desempenhar um papel ativo no gerenciamento de seus próprios dados pessoais pode ser o meio mais eficaz de verificação contra abusos de e uso indevido. O respeito à privacidade do titular dos dados pessoais é suportado pelos seguintes aspectos:

• **Consentimento ou hipótese de tratamento prevista em lei** - é necessário o consentimento livre e específico do titular dos dados para a coleta, uso ou divulgação de dados pessoais, exceto onde permitido por lei. As hipóteses de tratamento de dados pessoais e dados pessoais sensíveis estão preconizadas pelos arts. 7º e 11 da LGPD.

• **Precisão** - os dados pessoais devem ser precisos, completos e atualizados, conforme necessário para cumprir finalidades especificadas.

• **Acesso** - os titulares devem ter acesso aos seus dados pessoais e ser informados do uso e divulgação de tais dados. Os mencionados titulares devem ser capazes de contestar a precisão e integridade dos dados e alterá-los conforme apropriado.

• **Conformidade** - as instituições devem estabelecer mecanismos de reclamação e reparação e comunicar informações sobre eles ao público.



6.1.2 Privacidade por padrão

Também seguindo o conceito sugerido pela nomenclatura, a privacidade por padrão, *"by default"*, diz respeito à adoção da proteção de dados pessoais como padrão em todos os processos e atividades desenvolvidos pelo Município, por meio da definição de medidas de segurança, técnicas e organizacionais que devem ser aplicadas de forma padronizada e constante, em todas as áreas, projetos, serviços.

Quer dizer, antes de a Municipalidade iniciar qualquer processo, é necessário que seja verificado se o mínimo necessário em termos de proteção de dados está sendo observado, como finalidade específica e legítima para o tratamento de dados pessoais, ou a minimização dos dados sempre que aplicável.

Os agentes de tratamento devem implementar medidas adequadas para garantir que, por padrão, apenas serão processados os dados pessoais necessários para cumprimento da(s) finalidade(s) específica(s) definida(s) pela instituição que desempenha o papel de controlador dos dados pessoais.

Essa obrigação de implementação significa que a Unidade deve limitar a quantidade de dados pessoais coletados, extensão do tratamento, período de armazenamento e acessibilidade ao mínimo necessário para a concretização da finalidade do tratamento dos dados pessoais. Essa medida deve garantir, por exemplo, que nem todos os usuários dos agentes de tratamento tenham acesso ilimitado e por tempo indeterminado aos dados pessoais tratados pela instituição.

Na LGPD, a **Privacidade por Padrão** (do inglês Privacy by Default) está diretamente relacionada ao princípio da necessidade, expresso pelo art. 6º, inciso III.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> **III - necessidade: 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 de dados;**

A privacidade por padrão é obtida por meio da adoção das seguintes práticas:

• **Especificação da finalidade** - os objetivos para os quais os dados pessoais são coletados, usados, retidos e divulgados devem ser comunicados ao titular dos dados antes ou no momento em que as informações são coletadas. As finalidades especificadas devem ser claras, limitadas e relevantes em relação ao que se pretende ao tratar os dados pessoais.

• **Limitação da coleta** - a coleta de dados pessoais deve ser legal e limitada ao necessário para os fins especificados.

• **Minimização dos dados** - a coleta dos dados pessoais que possa identificar individualmente o titular de dados deve obter o mínimo necessário de informações pessoais. A concepção de programas, tecnologias e sistemas de informação e comunicação deve começar com interações e transações não identificáveis, como padrão. Qualquer vinculação de dados pessoais deve ser minimizada. A possibilidade de informações serem usadas para identificar o titular de dados deve ser minimizada.

• **Limitação de uso, retenção e divulgação** - o uso, retenção e divulgação de dados pessoais devem limitar-se às finalidades relevantes identificadas para o titular de dados, para as quais ele consentiu ou é exigido ou permitido por lei. Os dados pessoais serão retidos apenas pelo tempo necessário para cumprir as finalidades declaradas e depois eliminados com segurança.

Quando a necessidade ou uso de dados pessoais não forem claros, deve haver uma presunção de privacidade e o princípio da precaução deve ser aplicado. Dessa forma, as configurações padrão devem ser as de maior proteção à privacidade.

6.2 PADRÕES FRAMEWORKS E CONTROLES DE SEGURANÇA DA INFORMAÇÃO

A CGU recomenda aos entes públicos que, ao implantarem a LGPD em suas respectivas

Unidades, observem as orientações das normas internacionais e nacionais de segurança conforme foi reportado no capítulo 2 do presente documento.

6.3 OS 8 PASSOS BÁSICOS PARA MONTAR UM PLANO DE AÇÃO EM SEU LOCAL DE TRABALHO.

Após toda essa explicação, você deve estar se perguntando “como eu transformo todas essas informações em prática em meu local de trabalho”? Pensando nisso, está sendo incluído ao final deste material esta proposta com 8 passos básicos para que você consiga desenvolver um plano de ação baseado nas melhores estratégias para executá-la, não apenas na concretização da implementação LGPD na Administração do Município, como qualquer outro projeto que se necessite trabalhar em equipe. Confira:

6.3.1 Defina claramente seus objetivos

Primeiramente, você precisa considerar as competências administrativas que lhe são legalmente atribuídas e, em nosso caso, sua combinação com os princípios da LGPD. Os objetivos devem ser claros e atingíveis, pois servem como base para o plano de ação.

Nessa etapa, crie ou extraia do planejamento estratégico todos os elementos que vão guiar as ações dos envolvidos na equipe, incluindo:

Missão: Propósito que se pretende alcançar. Por exemplo: aplicar as normas da LGPD nas rotinas internas, através do mapeamento das atividades e confluência no tratamento de dados pessoais.

Visão: Inspiração que a Municipalidade pretende alcançar. Pode ser “conquistar conformidade legal com segurança para servidores e usuários dos serviços públicos municipais”;

Valores: Princípios que guiam o comportamento, como “sempre primar pelos princípios da legalidade, impessoalidade, moralidade, supremacia do interesse público, eficiência e todos os demais princípios que norteiam o Ato Administrativo”.

6.3.2 Torne suas metas mensuráveis

Metas consistem em desdobramentos dos objetivos. É fundamental que elas atendam a determinados requisitos para que orientem as tarefas do plano de ação precisamente.

Uma estratégia interessante para isso é a técnica corporativa americana chamada de “SMART” (“inteligente” ou “esperto” em uma tradução livre). Ela estabelece que uma meta deve ser:

6.3.3 Liste todas as tarefas que devem ser realizadas

Nesta etapa, é importante observar que é preciso estruturar um *checklist* dos atos que devem ser executados no plano de ação. Portanto, siga os seguintes passos:

➢ Faça uma reunião com a equipe de cada setor e discuta as tarefas;

➢ Crie uma lista contendo a atividade, com o seu respectivo responsável.

É importante que haja equilíbrio das funções. Um servidor não pode ficar sobrecarregado de atividades, bem como outro não pode ficar com tempo ocioso. Cada um terá um papel claro, de acordo com suas virtudes individuais e responsabilidades já assumidas previamente.

6.3.4 Estabeleça prazos

Todas as metas e tarefas devem ter prazos. Essa é uma etapa fundamental para o cumprimento do plano de ação. Além disso, lembre-se de que cada atividade deve ter o tempo adequado para ser realizada.

Os prazos devem ser compatíveis entre si. Ou seja, no ciclo produtivo eles devem se encaixar, sem deixar que um colaborador do estágio posterior permaneça ocioso enquanto aguarda uma nova atividade.

6.3.5 Delegue tarefas

Estude as tarefas e as classifique pelo nível de complexidade. Dessa forma, é mais fácil conseguir delegar sem sobrecarregar nenhum membro da equipe.

Uma dica aqui é desmembrar as atividades mais complexas em tarefas menores, para que existam entregas em menos tempo e que possam ser monitoradas regularmente. Assim, o colaborador terá mais clareza sobre seu trabalho.


Planos de Ação

Ação	Responsável	Prazo Início	Prazo Término	Custo
1. Contratar nova agência de Propaganda, buscando ideias inovadoras.	Ana Bernardes - Marketing	Jan/2010	Mar/2010	R$
2. Elaborar com a nova agência os materiais para a campanha de lançamento do perfume 'Aventura'.	Flávio Cavalcanti - Marketing	Abr/2010	Mai/2010	R$
3. Veicular anúncios em Revistas voltadas a esportes radicais.	Carla Campos - Marketing	Jun/2010	Ago/2010	R$
4. Veicular comerciais em TV, nos intervalos de programas sobre esportes radicais.	Carla Campos - Marketing	Jun/2010	Ago/2010	R$
5. Patrocinar eventos relacionados a esportes radicais.	Júlio Mello - Marketing	Set/2010	Out/2010	R$

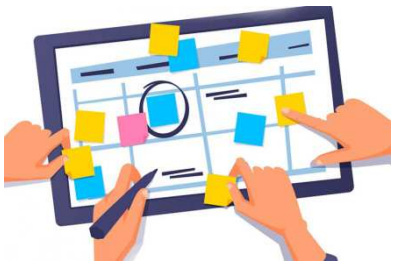
6.3.6 Crie uma representação visual do plano de ação

Nesse ponto, você deve elaborar um cronograma visualmente claro de todas as ações, prazos, metas etc. É preciso que todos os envolvidos consigam identificar suas obrigações e responsabilidades. Durante a parte prática do nosso manual apresentaremos um modelo de cronograma com vistas a auxiliar visualmente em sua conclusão.

Por exemplo, você pode estruturar apresentações com relatórios contendo o ciclo produtivo, metas que já foram cumpridas e resultados já alcançados.

Após isso, exponha o cronograma em um local que todos possam ver. Dessa maneira, a equipe não se perde no processo produtivo e se motiva ao ver que seu trabalho impacta positivamente nos resultados.

6.3.7 Preveja situações de riscos e estruture planos de contingência



Nem sempre tudo ocorre como o planejado. São inúmeros os fatores que podem prejudicar o seu objetivo, como mudanças de chefia, alteração no quadro de servidores, acidentes de trabalho, entre outras ocorrências fora do seu controle.

Para solucionar esses problemas, preveja o máximo de situações de risco possível e, então, elabore planos de ação para solucioná-las. Quando você se deparar com esses acontecimentos, saberá exatamente o que fazer para manter a estratégia ativa. Ou seja, tenha sempre um Plano “B” e se possível, um Plano “C”, também é recomendável.

6.3.8 Monitore o andamento das ações

Por fim, monitore toda a execução do plano de ação. Assim, você garante que as tarefas estejam sendo cumpridas no prazo e na ordem correta.

Inclusive, crie um cronograma de envio de relatórios e de reuniões periódicas (quinzenal ou semanalmente), para que os responsáveis de cada setor apresentem seus resultados.

Com os dados em mãos, registre tudo que não sair conforme o planejado e detecte eventuais entraves no trabalho dos colaboradores. Por fim, identifique suas causas e apresente soluções para os problemas.

Tome todas as medidas necessárias para corrigi-las e verifique se as mudanças estão garantindo o andamento do plano.

Aqui, também é importante pensar em medidas que aprimorem os processos e acelerem o alcance de metas. Nesse caso, pode haver a necessidade de revisar o plano de ação, pois suas metas serão alcançadas antes do esperado.

Seguindo esses passos, você será capaz de criar um plano de ação que resolve as não conformidades e possibilita o desenvolvimento saudável da implantação da LGPD, da forma mais ágil e segura possível.

6.4 Vantagens de utilizar planos de ação

Como pode ser observado, o plano de ação bem aplicado é útil, principalmente, em dois cenários: alcançar resultados específicos e resolver falhas nos processos internos.

Dessa forma, sua unidade vai conseguir identificar situações que estão causando ameaças à segurança de dados pessoais e encontrar as soluções ideais e personalizadas com cada uma delas, ou pelo menos, criar mecanismos de minimização de riscos. Com isso, o processo de crescimento da segurança é acelerado e a eficiência de sua equipe também.

Por este motivo, os planos de ação são essenciais para criar projetos de implementação duradouros e sustentáveis.

Além disso, essa ferramenta também traz benefícios como:

- ➔ Prevenção de problemas;
- ➔ Identificação de vulnerabilidades;
- ➔ Apresentação de soluções;
- ➔ Coleta de informações relevantes para a gestão de cada unidade;
- ➔ Tomada de decisão pelos gestores;
- ➔ Feedback construtivo e aprendizagem de todos envolvidos;
- ➔ Conquista de objetivos;
- ➔ Gestão apropriada de não conformidades legais e estruturais;
- ➔ Resolução de problemas.

Por fim, planejamentos estratégicos variam de unidade para unidade e, consequentemente, o uso dos planos de ação também. Logo, conhecer as melhores estratégias e metodologias é fundamental para que a sua unidade possa usufruir de todos os benefícios que são possíveis de alcançar.

ANEXO - PERGUNTAS E RESPOSTAS SOBRE A LGPD

Perguntas e Respostas sobre a LGPD

1) Que pessoas devem observar a Lei Geral de Proteção de Dados?

A Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, devendo ser observadas pela União, Estados, Distrito Federal e Municípios, ou seja, ela regula o tratamento de dados pessoais feito por pessoa jurídica de direito público ou privado, abrangendo secretarias, autarquias, fundações, empresas públicas e sociedades de economia mista. Ela alcança todos os entes da Administração Pública direta e indireta.

2) A Lei Geral de Proteção de Dados se aplica apenas a dados armazenados em meios digitais?

Não. Os dispositivos da LGPD se aplicam tanto a dados armazenados em meios digitais, quanto a dados armazenados em meios físicos.

3) O que o legislador espera de você?

Ao aplicar os dispositivos da LGPD, o legislador quer que você: respeite a privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

4) O que é autodeterminação informativa?

É saber quais dados pessoais estão sendo coletados e qual a finalidade.

5) A Lei Geral de Proteção de Dados deve ser observada em que atividades?

A LGPD aplica-se a qualquer operação de tratamento: realizada no território nacional; que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou que tenham sido coletados no território nacional, considerando-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

6) A Lei Geral de Proteção de Dados se aplica em casos de segurança pública, segurança do Estado ou atividades de investigação e repressão de infrações penais?

Essa Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: segurança pública; segurança do Estado; ou atividades de investigação e repressão de infrações penais, sendo vedado, nestas hipóteses, o tratamento dos dados por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à Autoridade Nacional, não podendo, em hipótese alguma, a totalidade dos dados pessoais de banco de dados ser tratada por pessoa de direito privado, a menos que possua capital integralmente constituído pelo Poder Público. Em tempo, o tratamento de dados pessoais para estes fins será objeto de legislação específica.

7) O que é dado pessoal?

É toda informação relacionada à pessoa natural identificada ou identificável.

8) O que é dado pessoal sensível?

É toda informação que se refere à 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 relacionado a uma pessoa natural.

9) O que é dado anonimizado?

É o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, ou seja, o dado que, submetido a técnicas próprias, não possa ser levado a identificar uma pessoa.

10) O que é banco de dados?

É o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

11) Quem é titular?

É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

12) Quem é o controlador?

É a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Em tempo, a própria entidade controladora poderá realizar o tratamento dos dados.

13) Quem é o operador?

É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. É possível que o operador e o controlador sejam pessoas diferentes (se, por exemplo, uma pessoa jurídica armazena dados a pedido de uma autarquia, a autarquia será controladora e a pessoa jurídica será operadora).

14) Quem é encarregado?

É a 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).

15) O que é tratamento?

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

16) O que é anonimização?

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

17) O que é consentimento?

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

18) O que é bloqueio?

É a suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

19) O que é eliminação?

É a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

20) O que é transferência internacional de dados?

É a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o controlador seja membro.

21) O que é uso compartilhado de dados?

É a 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.

22) O que é relatório de impacto à proteção de dados pessoais?

É 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.

23) O que é órgão de pesquisa?

É o 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.

24) O que é Autoridade Nacional de Proteção de Dados?

É o órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. Suas competências e estrutura regimental constam da LGPD e do Decreto Federal n. 10.474, de 26 de agosto de 2020.

25) Quais os princípios gerais que devem ser seguidos nas atividades de tratamento de dados?

Toda atividade de tratamento de dados pessoais deverá observar a boa-fé e, também, os seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

26) O que é o princípio da finalidade?

É a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

27) O que é o princípio da adequação?

É a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

28) O que é o princípio da necessidade?

É a 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 de dados.

29) O que é o princípio do livre acesso?

É a garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

30) O que é o princípio da qualidade dos dados?

É a garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

31) O que é o princípio da transparência?

É a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

32) O que é o princípio da segurança?

É a 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.

33) O que é o princípio da prevenção?

É a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

34) O que é o princípio da não discriminação?

É a impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

35) O que é o princípio da responsabilização e prestação de contas?

É a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

36) O tratamento de dados pessoais sensíveis pode ser realizado em quais condições?

O tratamento de dados pessoais sensíveis somente poderá ocorrer com consentimento do titular ou seu responsável legal, de forma destacada e para finalidades específicas.

Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) pela Administração Pública, de políticas públicas previstas em leis ou regulamentos; c) estudos por órgão de pesquisa; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) proteção da vida; f) tutela da saúde; e g) garantia da prevenção à fraude e à segurança do titular.

37) Quem é o setor público de acordo com a LGPD?

O denominado setor público, para fins de aplicação da LGPD, é composto pelos órgãos integrantes da Administração dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, Judiciário e Ministério Público, assim como pelas autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas, direta ou indiretamente, pela União, Estados, Distrito Federal a Municípios, nos termos do que prevê o parágrafo único do art. 1º da Lei Federal n. 12.527/2011 (LAI).

Merece, porém, especial atenção o enquadramento de empresas públicas, sociedades de economia mista e demais entidades controladas no conceito de setor público para fins da LGPD, pois, a depender da atividade que desempenharem ao tratar dados pessoais, deverão transitar entre os capítulos II e IV da LGPD, ou seja, é a finalidade a que está vinculado determinado tratamento de dado pessoal – se em regime concorrencial ou se para a execução de políticas públicas - que determinará se a entidade deve atender aos requisitos exigidos na LGPD para o setor privado ou para o setor público.

Portanto, ao ser verificado, no caso concreto, a necessidade de tratar dados pessoais, a entidade que compõe a Administração indireta cuja personalidade jurídica seja de direito privado, especialmente as empresas públicas e sociedades de economia mista, deverão identificar sob qual condição atuam, já que as consequências de atuar em regime concorrencial ou para atendimento de política pública são diversas, desde os requisitos a serem atendidos até as consequências por eventual descumprimento da Lei.

Por fim, a LGPD efetuou a equiparação com o setor público dos serviços notariais e de registro exercidos por delegação, os quais receberam o mesmo tratamento dispensado aos entes públicos quando realizarem o tratamento de dados pessoais.

38) Quando o setor público pode tratar dados pessoais?

Para a execução de políticas públicas previstas em leis, decretos, portarias do órgão ou da entidade, em contratos administrativos, acordos de parceria, termos de cooperação, termos de ajustamento de conduta, convênios ou instrumentos jurídicos congêneres ou para o atendimento de finalidade

pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Verifica-se, assim, que a execução de políticas públicas é indubitavelmente a principal justificativa para que o setor público realize qualquer tipo de tratamento de dados, já que é inerente à existência do Estado a formulação e implementação de políticas públicas em benefício dos cidadãos.

39) Quais as obrigações que o Poder Público assume ao realizar o tratamento de dados pessoais?

Ainda que voltado à execução de política pública, a Administração, ao realizar o tratamento de dados pessoais, deverá efetuar o correto enquadramento da situação fática em uma das hipóteses autorizadoras listadas no art. 7º da LGPD.

O ato de tratamento deve ser motivado e voltado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Atendendo-se ao princípio da transparência, exige a LGPD que o Poder Público divulgue, preferencialmente em seus sítios eletrônicos, informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas, no exercício de suas competências, voltadas para o tratamento de dados pessoais.

Também é dever da Administração indicar um servidor que exercerá a função de encarregado, conforme preconiza o inciso III do art. 23 da LGPD.

Por fim, embora sendo exceção no setor público, há casos em que o consentimento do titular dos dados precisará ser colhido e considerado. É o que ocorre por exemplo nos tratamentos de dados de crianças e adolescentes.

40) Sempre que o Poder Público efetuar o tratamento de dados pessoais deverá informar o titular do dado?

Não. De acordo com a LGPD, não há necessidade de consentimento do titular ou de garantir publicidade à referida dispensa de consentimento, conforme preconiza o inciso I do art. 23 da LGPD nos casos em que o tratamento de dados pessoais voltar-se para:

a) realização de estudos por órgão de pesquisa;

b) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

c) proteção da vida ou da incolumidade física do titular ou de terceiro;

d) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; e

e) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

41) Quais os instrumentos que podem ser utilizados pelo Poder Público como bases legais justificadores do tratamento de dados pessoais?

No exercício de suas competências legais, o órgão ou entidade poderá, por meio de portaria da autoridade superior, discriminar as hipóteses autorizadoras, a finalidade, os procedimentos e as práticas que serão utilizadas para o tratamento de dados pessoais. O citado ato administrativo deverá ser amplamente divulgado no âmbito interno e ainda publicado pela Administração preferencialmente em seus sítios eletrônicos.

É importante, ainda, que no bojo de convênios, contratos administrativos, termos de cooperação técnica, acordos de parceria, termos de outorga e demais instrumentos jurídicos utilizados pelo Poder Público, conste cláusula expressa a respeito da possibilidade de tratamento de dados pessoais eventualmente coletados, devendo, nesse caso, ser observadas todas as regras previstas na LGPD.

42) Como ficam os dados pessoais que estão publicamente disponíveis após o advento da LGPD?

Dados pessoais que estejam publicamente disponíveis devem ser analisados de acordo com a base legal existente para essa disponibilização. Assim, por exemplo, no caso das remunerações de servidores públicos expostas no Portal da Transparência, impõe a Lei de Acesso à Informação que tais dados devem ser expostos, para fins de controle da sociedade.

Todavia, embora estejam públicos, esses dados devem ser protegidos, visto que não poderão ser utilizados para qualquer outra finalidade que não aquela prevista na LAI, não podendo um terceiro captá-los para fazer listas de fornecimento de crédito ou, então, a Administração Pública cedê-los para que terceiros os utilizem para qualquer fim.

43) Como diferenciar a aplicação da LGPD da LAI (Lei de Acesso à Informação)?

O acesso à informação, contida em registros ou documentos, produzidos ou acumulados por órgãos públicos ou entidades da Administração Pública indireta, é de interesse coletivo, sendo regido pela LAI. Isso significa, por exemplo, que qualquer pessoa poderá ter acesso, para fins de controle da atividade administrativa do Estado, a processos licitatórios, contratos administrativos, prestações de contas e demais documentos, salvo os considerados sigilosos segundo a Lei.

A finalidade central do acesso à informação na esfera da Administração Pública perante a LAI consiste no princípio constitucional da publicidade.

No tocante à LGPD, o acesso à informação é amparado pelo princípio do acesso livre por interesse particular, ou seja, apenas o titular dos dados pessoais tem direito a requerer, em regra.

Desse modo, o agente público, diante de uma solicitação de acesso à informação pelo particular, deve verificar qual o teor do acesso, se pessoal ou coletivo, pois a depender do requerimento poderá ser aplicada a LAI ou a LGPD ou até mesmo as duas legislações.

44) É necessário registrar as operações sobre o tratamento de dados pessoais?

A Lei obriga que o controlador e o operador mantenham registro das operações relativas ao tratamento de dados pessoais que realizarem, principalmente quando baseado no legítimo interesse (art. 37). Esses registros são importantes para demonstrar o cumprimento da Lei e em caso de apuração de responsabilidade. Por outro lado, a Lei prevê a possibilidade de a Autoridade Nacional determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive quanto aos dados sensíveis, de acordo com o previsto no art. 38. Veja-se que o art. 10, § 3º, indica que o relatório poderá ser solicitado quando o tratamento tiver como fundamento o interesse legítimo. O parágrafo único do art. 38 já estabelece um regramento quanto às exigências mínimas desse documento, como:

a) descrição dos tipos de dados coletados;

b) metodologia utilizada para a coleta e para a garantia da segurança das informações; e

c) análise do controlador em relação a medidas, salvaguardas e mecanismos de mitigação de riscos.

45) A instauração de processo fiscalizatório pela ANPD impede, suspende ou, de alguma forma, influencia a apuração funcional na esfera administrativa?

Não. O poder disciplinar da Administração Pública é independente e desvinculado da fiscalização realizada pela ANPD. Eventual condenação em uma esfera não vincula ou prejudica outra. Apesar disso, a ANPD, antes de aplicar as penalidades referentes à suspensão do banco de dados, suspensão do tratamento de dados e proibição parcial ou total do tratamento de dados, deverá ouvir os respectivos órgãos e entidades com competências sancionatórias.

46) A ANPD pode aplicar penas diretamente a agentes públicos com base na LGPD?

Não há previsão expressa nesse sentido.

A título exemplificativo, os agentes públicos paraenses, pessoalmente, estão sujeitos ao Regime Jurídico Único dos Servidores Civis do Estado do Pará (Lei Estadual n. 5.810/1994), à Lei de Acesso à Informação (Lei Federal n. 12.527/2011) e à Lei de Improbidade Administrativa (Lei Federal n. 8.429/1992).

Nesse sentido, a ANPD, para aplicar as penalidades referentes à suspensão do banco de dados, suspensão do tratamento de dados e proibição parcial ou total do tratamento de dados, deverá ouvir os respectivos órgãos e entidades com competências sancionatórias, a fim de considerá-las para efeito de dosimetria da sanção.

7

IMPLEMENTAÇÃO DA LGPD – FASE – EXECUÇÃO – ADEQUAÇÃO E CONFORMIDADE

7.1 CONTEXTO DA PRÁTICA

Como já visto, temos a Lei Nacional que trata da proteção de dados e o Decreto Municipal para sua regulamentação no âmbito do Poder Executivo, além de outros documentos já elaborados e os novos que serão editados para o atendimento inicial às exigências da Lei Geral de Proteção de Dados e manutenção do processo contínuo de melhorias, como a orientação técnica, cartilha, termos de uso e responsabilidade, e as políticas necessárias para implantar a cultura da proteção de dados pessoais e sensíveis.

Logo, chegamos ao momento da execução de tarefas que têm por objetivo a implantação de medidas para o correto tratamento de dados pessoais e sensíveis na Administração Pública Direta, de forma que os requisitos iniciais e mínimos para o tratamento de dados pessoais e sensíveis sejam aplicados como boas práticas em cumprimento às legislações vigentes, bem como ser multiplicado e adotado por outras entidades, por meio de consulta aos demais interessados na adoção e no processo de colaboração para as melhorias contínuas.

Também, para que as referências legais sejam atendidas, é importante ter ciência de que a metodologia de apoio descrita nas próximas seções está alinhada com o disposto nos arts. 21 e 22 do Decreto Municipal n. 38.145/2021, referente aos prazos de entrega dos planos de adequação e dos termos de conformidade, sendo que os modelos serão disponibilizados como anexos e em planilha no formato digital na página da LGPD, no endereço eletrônico: https://www.guarulhos.sp.gov.br/lei-geral-de-protecao-de-dados .

Cabe lembrar que, é fundamental que todos os atores participem desse projeto, desde a implantação aos processos que serão gerados, sendo que, para os efeitos deste manual, o termo “atores” é amplo e atinge a todos os agentes públicos que participarem direta ou indiretamente para atender aos objetivos da Lei Geral de Proteção de Dados, incluídos o encarregado de dados, os controladores de dados, os operadores centrais, os operadores de dados, os auxiliares e as comissões e comitês existentes, em especial a Comissão de Acesso à Informação – CAI.

É importante ressaltar, que não existe hierarquia entre as funções atribuídas para a implementação e monitoramento das ações necessárias ao atendimento da LGPD, desde o primeiro momento é importante que todos sejam sensibilizados no sentido de que as atividades devem ser realizadas em equipe com responsabilidades mútuas entre todos os atores.

Então, este manual contém a edição de diretrizes com as orientações para a proteção de dados e a elaboração dos relatórios de impacto à proteção de dados pessoais - RIPD para os esforços iniciais indispensáveis à adequação e conformidade às exigências da Lei Geral de Proteção de Dados Pessoais – LGPD, bem como passou por deliberação da Comissão de Acesso à Informação, conforme exigência do art. 13 do Decreto Municipal n. 38.145/2021.

Os arts. 7° e 9° do referido Decreto, que estão no Capítulo das Responsabilidades da Administração Pública trata sobre as atribuições do encarregado de dados, em especial nos incisos III, IV e IX, quanto à orientação para proteção de dados pessoais, edição de diretrizes para a elaboração dos planos de adequação, conforme o inciso III, do art. 7º:

> *VIII - providenciar a publicação dos relatórios de impacto à proteção de dados pessoais previstos pelo art. 32, da Lei Federal nº 13.709, de 2018; (...)*
> *IX - recomendar a elaboração de planos de adequação relativos à proteção de dados pessoais aos Encarregados das entidades integrantes da Administração Indireta.*
>
> *Art. 13. Cabe à Comissão de Acesso a Informação - CAI, por solicitação do Encarregado de dados pessoais que, por sua vez, poderá ser provocado pelo Controlador de dados pessoais:*
> *I - deliberar sobre proposta de diretrizes para elaboração dos planos de adequação no tratamento de dados pessoais e sensíveis, conforme os termos da*
> *II - deliberar sobre qualquer assunto relacionado à aplicação da Lei Federal em vigor, e do presente Decreto pelos órgãos do Poder Executivo.*

Sendo assim, nas próximas linhas iniciaremos a explicação das ações que precisam ser realizadas na fase de conformidade pelos agentes públicos nomeados nas suas respectivas unidades e, ao final, como a realização dessas ações precisam ser apresentadas no cronograma de adequação para o cumprimento aos prazos descritos no Decreto Municipal.

O Encarregado de dados, os agentes de tratamento e os auxiliares da Controladoria Geral do Município - CGM, por meio da Ouvidoria do Município, estarão disponíveis para esclarecer as dúvidas e auxiliar na implementação e manutenção da LGPD, dentro de suas atribuições, por meio dos seguintes canais de contato.

Telefone: 2475-7300 – Ramal 7484
e-mail: encarregadodedados@guarulhos.sp.gov.br
Encarregado de dados: Renato Corte Lopes

7.2 INICIANDO AS ATIVIDADES

7.2.1 PASSO A PASSO

1. Quem participará da implementação?

Para que os dados e as informações sejam protegidos com base na LGPD, foi adotada como primeira medida no município de Guarulhos a nomeação dos responsáveis pela implementação do projeto para direcionar as atividades e multiplicar os conceitos que darão causa à mudança cultural na organização, aqui designados como “atores”, também deverão atuar como ponto de apoio interno e externo na implementação da LGPD. Para isso, procedeu-se com a indicação de agentes públicos que foram devidamente nomeados pelo Prefeito por meio da Portaria 2554/21-GP.

TRABALHO EM EQUIPE

Para este passo, é importante que os nomeados de cada unidade trabalhem em conjunto desde o início em todas as atividades relacionadas com a LGPD, tendo a ciência de que não deve existir hierarquia entre os responsáveis e de que o processo deve ser realizado de forma colaborativa em equipe.

*Ter o registro dos responsáveis pela aplicação da LGPD em suas respectivas unidades e enviar qualquer atualização para o Encarregado de dados, que deverá ser feito pelo endereço de e-mail:

encarregadodedados@guarulhos.sp.gov.br

O modelo do ***ANEXO I - indicados LGPD*** traz a planilha que deverá ser preenchida e enviada com os dados necessários para registro dos responsáveis nomeados nas unidades.

2. Onde será aplicado?

Nas unidades, subunidades, coordenadorias, departamentos e demais designações das divisões existentes na Administração Pública Direta e Indireta (respeitada a sua autonomia) do Poder Executivo Municipal.

APOIO DA ALTA ADMINISTRAÇÃO E DAS CHEFIAS

Aqui é importante ter o apoio da alta administração e, para isso, é essencial que as autoridades e as chefias tenham o conhecimento da LGPD e compreendam a sua importância para que as atividades sejam organizadas com as demais realizadas rotineiramente de modo a manter a eficiência.

*Adotar o modelo ***ANEXO II - carta de comprometimento***, que é documento que contém a carta de apoio e comprometimento da alta administração na implantação e revisão das atividades da LGPD.

Encaminhar e-mail para a autoridade máxima da pasta com confirmação de entrega ou leitura e guardar o comprovante de que a referida carta foi enviada para ciência.

3. Quando será realizado?

Por meio da realização das atividades nos prazos previstos no cronograma de adequação, que traz a conformidade mínima exigida neste manual e em respeito aos artigos dispostos no Decreto Municipal n. 38.145/2021, sendo a execução composta pelas seguintes fases:

Fase de adequação: art. 21 - entrega do cronograma com o plano de adequação até 20 de setembro de 2021; e

Fase de Conformidade: art. 22 - entrega dos termos de conformidade até o dia 05 de novembro de 2021, podendo ser prorrogado por igual período, com prazo final em 20 de dezembro de 2021.

DA ADEQUAÇÃO - CRONOGRAMA

Adiante será visto que ao elaborar o cronograma próprio de adequação, que será apresentado até o dia 20 de setembro de 2021. As unidades deverão se comprometer a cumprir com os prazos na realização das atividades na fase de conformidade, sendo que eventuais atrasos devem ser reajustados de forma a não impactar o prazo final do projeto.

*Encaminhar em meio físico – Processo Administrativo e por e-mail – Encarregado de dados, as documentações da execução das fases de adequação e conformidade nos seus respectivos prazos, utilizando os modelos existentes neste manual e indicados no item 4, a seguir.

Dados da unidade administrativa: CGM-LGPD

4. Como será implementado?

Por meio dos entregáveis previstos no cronograma com a evidência das ações que serão executadas em adequação e conformidade com a LGPD.

Para a fase de adequação será exigida a elaboração do cronograma com as necessárias descrições do plano de trabalho e do plano de ação, conforme os modelos que poderão ser utilizados como referência e estão contidos nos seguintes modelos: ***ANEXO III - plano de trabalho***, ***ANEXO IV - plano de ação*** e ***ANEXO V - cronograma***.

Para a fase de adequação será exigida a execução das atividades elencadas no cronograma e a apresentação dos termo de conformidade, conforme o modelo de referência contido no ***ANEXO VI - termo de conformidade.***

Na fase de adequação deverão ser apresentados o plano de trabalho, o plano de ação e o cronograma, contendo o prazo e as medidas mínimas para assegurar os esforços de proteção aos ativos físicos e digitais relacionados aos dados pessoais e sensíveis.

Na fase de conformidade as medidas mínimas apresentadas na fase de adequação deverão ser executadas e demonstradas por meio de termos.

DOS ENTREGÁVEIS

Trata-se da entrega dos artefatos, sendo estes descritos como produto mecânico resultado da realização das atividades previstas em cronograma com prazo e responsáveis definidos em plano de ação, respeitando as especificidades de cada unidade.

*Entrega dos documentos apresentados nos ***ANEXOS III, IV e V***, por cada uma das unidades, para o cumprimento deste passo, sendo eles, o plano de trabalho, o plano de ação e o cronograma, são modelos com tarefas iniciais que deverão ser complementadas de acordo com as especificidades de cada órgão.

Entrega do modelo apresentado no **ANEXO VI - termo de conformidade** - por cada uma das unidades, de modo a se comprometerem de que as medidas previstas e elaboradas na fase de adequação foram atendidas.

Encaminhar em meio físico – Processo Administrativo e por e-mail – Encarregado de dados, as documentações da execução das fases de adequação e conformidade nos seus respectivos prazos, utilizando os modelos existentes neste manual e indicados no item 4, a seguir:

Dados da unidade administrativa: CGM-LGPD

5. Quanto será demandado de esforço?

Na elaboração deste manual foram adotadas medidas para que na implantação sejam utilizados recursos humanos e ferramentas já existentes na Administração Pública, de forma a evitar nesse primeiro momento qualquer impacto orçamentário para o ano corrente.

No entanto, para a manutenção e melhorias necessárias nas próximas ações, será necessário que cada unidade tenha sempre a LGPD como obrigações a cumprir na elaboração da sua previsão orçamentária.

Como já visto, a implementação da LGPD provocará mudança cultural na organização e isso refletirá na necessidade de atualizações, sejam

sob o aspecto intelectual com os treinamentos e capacitações, ou mesmo na infraestrutura com a aquisição de equipamentos que permitam proteger os ativos físicos e digitais que contêm dados pessoais e sensíveis.

DOS RECURSOS

Nesse primeiro momento, alinhado ao propósito deste manual, o objetivo é buscar a aplicação de medidas iniciais que não causem impacto financeiro na organização, sem prejuízo futuro de que as mudanças decorrentes e necessárias sejam apontadas no orçamento para que o processo de melhoria contínua seja observado.

*Registrar os recursos necessários para aquisição e utilizados desde a fase de adequação até o final da conformidade e, nas posteriores revisões, sejam eles materiais, financeiros, humanos, mercadológicos (divulgação) ou administrativos. O modelo a ser utilizado está no ***ANEXO VII - registro de recursos.***

6. Dos requisitos da conformidade.

A conformidade está relacionada com a adequação das unidades da Administração Pública com a LGPD, sendo que para essa adequação é necessária a realização de medidas emergenciais com requisitos mínimos com o objetivo de garantir a proteção de dados pessoais e sensíveis.

Deste ponto até a etapa de realização do cronograma – fase de adequação, serão apresentadas as diretrizes que auxiliarão na implantação da LGPD de forma prática, com as ações necessárias que têm por objetivo cumprir as exigências legais.

DA CONFORMIDADE

Compreender o que está sendo demandado como requisito mínimo de atendimento inicial às medidas necessárias ao cumprimento da LGPD, de forma que seja possível elaborar o cronograma dessas ações em prazo de execução que seja viável.

*Ao final da leitura desta fase de conformidade, será exigida a apresentação de cronograma no prazo disposto no Decreto Municipal n. 38.145/2021 alterado pelo Decreto n. 38.257/2021, daí decorre a importância em ter a compreensão da complexidade que será exigida na fase de conformidade, visto que o cronograma que deverá ser apresentado na fase de adequação.

7. Conhecer o ambiente e sua atuação na organização.

É necessário que a organização tenha conhecimento do conceito de dados, informação e o valor agregado para a melhor tomada de decisão, como já apresentado neste manual, mas tão importante é conhecer o propósito da sua organização.

Nesse sentido, conhecer a missão, a visão e os valores das unidades dentro da visão do negócio, é ter um norte para que os resultados alcançados estejam alinhados com o propósito da organização com eficiência.

MISSÃO: é saber para que a unidade ou órgão existe. Declarar a missão é construir a estratégia com suas metas, objetivos e indicadores. Quando bem definida, a missão corresponde ao benefício que ela produz para o seu público-alvo, no caso, o interesse público primário (a sociedade) e o interesse público secundário (Administração Pública). A entidade pública deve cumprir com suas obrigações não apenas para realizar tarefas e cumprir suas atribuições legais, mas sim, para beneficiar e atender as expectativas do seu público. Ex. Carta de Serviços ao Usuário.

VISÃO: é o futuro. É ter de forma clara os objetivos para o futuro da unidade ou órgão. Por isso é necessário indicadores e metas, assim é possível analisar o crescimento. Os indicadores vão demonstrar se as metas para os objetivos que se esperam estão sendo alcançados.

VALORES: são os princípios da organização. Esses princípios possibilitam a edição de diretrizes que vão orientar o comportamento da unidade ou órgão. Por comportamento entende-se o modo de atuar da unidade na execução das suas ações, pode ser no seu relacionamento interno e externo, nos processos de medições que permitem analisar se as suas metas estão sendo alcançadas, entre outros.

DO ALINHAMENTO COM A ORGANIZAÇÃO

Ao conhecer as funções do ambiente em que trabalha, os agentes públicos passam a entender melhor a importância da realização das suas atividades, mesmo que em pequenas tarefas, tendo conhecimento da importância do seu esforço e nível de participação na entrega do resultado.

*Ter conhecimento que o agente público é parte integrante do todo que á a Administração Pública, sendo a sua atividade indispensável para a execução das políticas públicas.

8. Elaborar organograma com a estrutura do órgão.

O organograma representa de forma visual a estrutura do órgão e é necessário que na sua elaboração seja possível visualizar a complexidade da

unidade quanto aos seus departamentos, subunidades, seções e cargos, sejam internos ou externos quanto à infraestrutura.

Essa etapa é relevante, pois com base nessas informações será possível analisar os fluxos dos processos e seguir com os demais levantamentos necessários para mapear os dados pessoais e sensíveis.

DA IDENTIFICAÇÃO DA ESTRUTURA

O objetivo dessa tarefa é facilitar a compreensão das relações hierárquicas e a integração entre as áreas e seus cargos, sendo aplicável tanto para visualização do seu público-alvo como internamente pela organização.

*Para essa atividade deverá ser preenchido modelo do ***ANEXO VIII - visão do negócio*** - que contém exemplo da estrutura e informações necessárias para seguir com as próximas etapas. Na elaboração da representação gráfica é recomendável utilizar qualquer programa que permita fazer imagens em hierarquia, lembrando que a imagem gerada deverá ser carregada no arquivo modelo quando não for criada no mesmo.

Para auxiliar na elaboração dessa tarefa indicamos a página da prefeitura no seguinte endereço eletrônico: http://portaldoservidor.guarulhos.sp.gov.br/servicos.php?serv=34, que contém os cargos das unidades, de forma que esses cargos precisam estar demonstrados quanto aos setores de trabalho na elaboração da estrutura organizacional e os respectivos nomes dos agentes públicos, conforme o modelo ***ANEXO IX - cargos das unidades***, a ser preenchido por cada órgão.

A página do portal do servidor é uma referência e caso exista divergência é fundamental que a informação conste na observação da planilha modelo.

9. Conhecer a legislação de cada unidade e subunidades.

Os atores responsáveis pela implementação da LGPD e pela execução das tarefas rotineiras devem ter conhecimento claro da legislação às quais estão submetidos enquanto agentes públicos, sejam as relacionadas aos seus departamentos e cargos quanto às relacionadas ao seu comportamento.

DA LEGISLAÇÃO VIGENTE

Conhecer a legislação é um dos pontos de atenção para a execução das tarefas às quais os agentes públicos estão designados, pois auxilia no cumprimento das suas obrigações, legitima as ações para maior segurança jurídica e possibilita multiplicar as boas práticas ao trazer conceitos e definições alinhados à maior eficiência.

*Os agentes públicos têm o dever de conhecer as diretrizes legais relacionadas à sua atuação, sendo assim, recomenda-se a leitura, no mínimo, das legislações abaixo aplicáveis no Poder Executivo de Guarulhos:

- Lei do Regime Jurídico dos Funcionários Públicos - Lei 1.429/1968;

- Lei da Estrutura Organizacional - Lei 7.550/2017 com alterações;

- Leis, Decretos, Portarias e Regimentos que regem o funcionamento da sua organização (unidades e subunidades);

- Leis, Decretos, Portarias e Regimentos que afetam o funcionamento da sua organização:

Lei n. 12.527/2011 e Decreto 36.140/2019
Acesso à Informação;

Lei n. 13.709/2018 e Decreto n. 38.145/2021 com alterações
Proteção de Dados Pessoais;

Lei n. 12.846/2013 e Decreto n. 35.460/2021
Responsabilidade Administrativa de Pessoas Jurídicas;

Decreto n. 35.459/2019
Código de Conduta e Ética Profissional;

Decreto n. 25.624/2008
Temporalidade; e

- Procedimentos e outros documentos publicados de apoio em cumprimento às legislações vigentes - Lei n. 13.460/2017 - Carta de Serviços ao Usuário - Cartas documentadas em Guarulhos, acessar endereço: https://www.guarulhos.sp.gov.br/cartasdeservico .

10. Do nível de maturidade em adequação à LGPD.

Disponibilizados pela Secretaria do Governo Digital, unidade pertencente à estrutura do Governo Federal, o nível de maturidade apresentado neste manual refere-se aos dois questionários contendo perguntas relacionadas com a privacidade e a segurança para adequação à LGPD.

Ao preencher cada um dos questionários, é possível obter ao final as respectivas notas que representam a proximidade ou distanciamento quanto à adequação para a LGPD.

DA MATURIDADE EM PRIVACIDADE E SEGURANÇA

O preenchimento dos questionários é importante para que a unidade conheça seu cenário atual e possa atuar na adoção de melhorias contínuas. O nível de maturidade também auxilia a medir a evolução no decorrer do tempo quanto à aplicação de medidas adotadas às exigências da LGPD,

*Uma vez que existe a proximidade com as legislações anteriormente citadas e conhecendo um pouco mais sobre o tema aqui tratado, é necessário realizar o registro inicial do cenário em que a unidade se encontra em relação às exigências da LGPD. Assim, adotamos inicialmente o modelo do Governo Digital e solicitamos que sejam respondidos os questionários dos níveis de maturidade que tratam sobre a privacidade e segurança em suas unidades, disponíveis nos seguintes endereços:

Maturidade de privacidade
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/diagnostico-privacidade-lgpd

Maturidade de segurança
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/diagnostico-seguranca-lgpd

Futuramente, estará disponível em formulário na ferramenta do Google a ser disponibilizado na plataforma da ESAP, na área LGPD em curso, o link para respostas aos questionamentos com relação ao nível de maturidade de privacidade e de segurança, os quais irão gerar os respectivos anexos, a saber: ***ANEXO X - nível de maturidade em privacidade*** e ***ANEXO XI - nível de maturidade em segurança***.

11. Conhecer os processos internos nas subunidades de cada órgão.

Processo interno é o conjunto de atividades ou tarefas com entrada, transformação e saída, para gerar um resultado de valor que ocorre por meio da entrega de um produto ou serviço e possui recorrência. Um processo estruturado permite visualizar o que deve ser realizado, como será realizado e por quem será realizado.

O processo é formado por:

- Entradas (insumos que podem ser: materiais, serviços, dados e informações);

- Transformações (ferramentas, técnicas e métodos para transformar os insumos);

- Saídas (resultado do insumo transformado).

A saída é direcionada para um cliente que pode ser interno (setor ou colaborador/parceiro) ou externo (munícipe ou fornecedor).

Ex.: de processo de serviço de RH, entra o currículo (entrada), análise e entrevista (processo), sai contratado (saída).

Também, é possível a ocorrência de subprocessos, que são as divisões dentro de um processo, de modo a gerar dependência em nível hierárquico.

Sobre a definição de processos é importante conhecer alguns conceitos para o preenchimento da planilha no modelo ***ANEXO XII - definição de processos.***

Os Processos de internos administrativos são classificados em:

- Processos Primários: são as atividades fundamentais para que a organização cumpra sua missão de negócio, estão conectados com a experiência do público-alvo. Ex.: Administração, Finanças, Comunicação, etc.

- Processos de Suporte: são aqueles que auxiliam a execução dos Processos Primários. Não atingem diretamente o público-alvo, por exemplo: Gestão de Recursos Humanos, Gestão de treinamentos.

- Processos de Gerenciamento: são aqueles onde ocorre a medição, monitoram e controlam as atividades de uma organização, por exemplo: Governança Corporativa, Gestão Estratégica.

O mapeamento de processos tem como finalidade demonstrar a sequência entre as atividades do processo desde a entrada até a sua saída com objetivo de registrar, padronizar, melhorar e transformar as atividades do cotidiano.

É um mecanismo para melhoria por meio da transformação de processos e permite delimitar funções e papéis, atuar na previsão de recursos e mensurar o desempenho do processo, dentre outras medidas.

O mapeamento de processos lista as pessoas que participam do processo, seja o responsável ou o colaborador. Isso auxilia para dar transparência ao processo, pois cada pessoa começa a visualizar e entender seu contexto no todo e como suas ações impactam no trabalho dos demais participantes.

Também, o mapeamento auxilia no controle dos recursos humanos, financeiros e operacionais, que alinhados ao objetivo do processo vão garantir que não ocorram impactos ocasionados pela escassez.

Ainda, é possível visualizar se existe padronização das atividades, estando relacionado diretamente com as medições, pois processos com o

mesmo objetivo na área de atuação que não estão padronizados apresentam distorções em suas medições.

A tabela abaixo auxilia na identificação dos termos utilizados quanto à definição dos temas relacionados ao processo:

Tarefa	O que é executado no aspecto operacional, descreve o que deve ser feito para concretizar, transforma o que precisa ser feito em resultado. Ex.: disponibilizar cadeira, copo dágua, fazer login no sistema, coletar as informações descritas na tela, solicitar esclarecimentos, gerar protocolo no sistema.
Atividade	Descreve o que precisa ser feito, mas não sob o ponto de vista operacional de como será feito. Ex.: disponibilizar local adequado para recepção, tranquilizar conforme o caso, efetuar registro do atendimento.
Subprocesso	Divisão das atividades dentro do processo. Ex.: realizar a triagem para classificar o tipo de solicitação, reclamação, denúncia.
Processo	Combinação das atividades. Ex.: Atender o requerente.
Macroprocesso	Propósito do negócio. Ex: Atendimento ao cliente.

"Se você não é capaz de descrever o que você faz como um processo, então você não sabe o que está fazendo". William Edwards Deming

PRIORIZANDO PROCESSOS

Conhecer o processo é importante para visualizar onde os dados estão circulando de acordo com os serviços prestados ou produtos fornecidos, além de permitir que sejam estabelecidas prioridades para o projeto da implementação, conforme o impacto e a probabilidade do risco, sendo necessário priorizar os processos que contenham dados pessoais e/ou sensíveis em tratamento.

*A planilha disponível no ***ANEXO XII - definição de processos*** - deve ser preenchida de acordo com seus campos. Para isso, recomendamos conversar com os responsáveis em cada seção, divisão, departamento ou subunidade para levantar as informações.

Algumas dicas de como fazer o Mapeamento de Processos:

Definir quais são os processos que serão mapeados, minimamente todos os processos que possuírem dados e informações pessoais e sensíveis deverão ser mapeados.

As perguntas que poderão auxiliar no mapeamento são as seguintes:

- Por que mapear esse processo? Seu objetivo (documentar, aplicar melhoria, padronizar etc.)

- Esse processo possui riscos envolvidos?

- É processo para atender legislações? Em caso positivo, quais?

Na elaboração do mapeamento do processo é necessário envolver as pessoas para que atuem de forma colaborativa, isso vai gerar a troca de experiência entre todos os participantes, visto que a pessoa que está no operacional provavelmente é a que mais tem proximidade e vivência com o processo de forma a trazer a descrição mais próxima da realidade.

Abaixo temos algumas técnicas utilizadas para mapear processos são:

- Entrevistas;
- Questionários;
- Reuniões;
- Oficinas;
- Workshops;
- Análise documental;
- Coleta de evidências;

Não existe técnica correta ou incorreta e sim a mais adequada para o levantamento das informações necessárias de acordo com cada equipe de trabalho.

Validar o mapeamento do processo é a ação final, pois é ela que indicará se o processo faz sentido no meio ao qual está sendo executado, além disso a validação comprova que as pessoas entenderam o significado do processo, o que possibilita a legitimação do mesmo por seus responsáveis.

Lembrando que, os processos necessitam de acompanhamento periódico para que estejam adaptados à realidade de acordo com a LGPD e suas necessárias medidas de proteção aos dados pessoais.

É essencial que cada processo seja identificado, conforme disponível no modelo ***ANEXO XII - definição de processos***, visto que essa identificação permitirá criar o relacionamento do processo com as demais etapas que serão executadas, como: o registro das atividades - inventário de dados, a análise de riscos, a gestão de incidentes, etc. Sendo que as identificações em cada um dos modelos devem guardar a devida correspondência.

12. Identificar os dados pessoais no espaço em que se encontram.

Como vimos anteriormente, conhecer os processos faz parte do exercício de conhecer quais atividades são realizadas em nosso cotidiano, sendo que as atividades realizadas na administração pública decorrem de competências e atribuições definidas em lei.

É importante conhecer os processos, pois na realização das atividades e tarefas que formam esses processos temos uma quantidade enorme de dados e informações que podem estar armazenados de forma estática, mas disponíveis para consulta e utilização, ou podem estar em circulação devido à sua constante necessidade de utilização, tornando-se assim mais dinâmicos.

Nessa etapa, após verificados os processos que são decorrentes das atribuições legais, bem como suas atividades e tarefas, é necessário analisar quais dados e informações fazem parte desses processos para que ocorra a identificação dos dados pessoais e sensíveis nos termos da LGPD.

IDENTIFICANDO OS DADOS PESSOAIS

Temos como objetivo nessa etapa a análise dos dados levantados nos processos para a identificação dos dados pessoais sensíveis, visto que não são todos os dados que se enquadram sob a proteção da LGPD.

Essa etapa merece extrema atenção na análise, visto que os dados identificados como pessoais e sensíveis, quando indicados no inventário de dados pessoais, deverão seguir para as próximas etapas, como: a análise dos riscos, as medidas de segurança, a mitigação e a gestão de incidentes.

Caso ocorra equívoco na classificação, um dado pessoal e sensível que deveria ser tratado não será contemplado pela devida proteção, em outro sentido, caso ocorra a classificação de dado diverso como pessoal e sensível, o trabalho realizado inicialmente será perdido, vez que não deverá constar das próximas etapas.

*Para essa pré-análise deverá ser preenchida a planilha do inventário de dados - ***ANEXO XIII - inventário de dados pessoais - IDP*** - disponibilizado pelo Governo Federal e adaptado às realidades do município de Guarulhos, em especial para essa fase inicial de implantação da LGPD.

13. Do Registro de Tratamento dos Dados Pessoais e Sensíveis.

Quando tratamos sobre a Lei Geral de Proteção de Dados, inevitavelmente vamos nos deparar com novas práticas que precisam ser adotadas. No entanto, essas práticas geralmente decorrem de normas de padronização internacionais já adotadas por entidades privadas, dentre elas, as normas ISO, ISO-IEC, ABNT, além de outros mecanismos como ICO -

Information Commissioner's Office e o Gov.BR – Secretaria do Governo Digital, este último utilizado como referência neste manual.

Após o estudo dos processos e a identificação de dados pessoais e sensíveis, nos deparamos com a necessidade de elaborar um documento que sirva não somente como prova, como também para a devida formalização de como os dados pessoais e sensíveis são tratados sob a luz da LGPD, ou seja, desde a coleta, passando pelo processamento e indo até sua eliminação.

Trata-se de um dos documentos iniciais mais importantes, pois além do registro para visualização, organização, atualização, serve de apoio para a elaboração do RIPD e aos eventuais questionamentos que possam surgir pela Autoridade Nacional de Proteção de Dados – ANPD.

DO INVENTÁRIO DE DADOS PESSOAIS – IPD

Tem por objetivo o registro de diversas informações a fim de permitir a localização e o rastreamento dos dados pessoais e sensíveis, em ativos físicos ou digitais, para garantir minimamente as medidas aplicáveis no contexto da LGPD.

Em segunda análise, permite visualizar melhorias nos processos, em especial os que estão relacionados com a proteção de dados pessoais.

Quanto aos itens que estão presentes no inventário, de uma forma geral tratam sobre:

- Nome da Unidade e subunidade;
- Dados do Controlador e do Encarregado de Dados;
- Identificação, nome e descrição do processo de dados pessoais e sensíveis;
- Data de criação do inventário, atualização e versão;
- A finalidade do tratamento dos dados pessoais e sensíveis;
- Fases do ciclo de vida dos dados;
- Identificação do(s) Operador(es) para cada fase do ciclo;
- Descrição do fluxo de tratamento dos dados para cada fase do ciclo;
- Abrangência da área geográfica do tratamento;
- Fonte de dados da obtenção de dados pessoais;
- Finalidade do tratamento de dados pessoais;
- Categorização dos dados pessoais e dos dados sensíveis;
- Frequência e quantidade de dados pessoais tratados;
- Compartilhamento;
- Transferência internacional;
- Contratos de serviços que tratam de dados pessoais; e
- Contratos de TI que tratam dados pessoais.

* Trata-se de uma planilha – ***ANEXO XIII - inventário de dados pessoais - IDP*** – disponibilizada pela Secretaria de Governo Digital que

contém uma série de informações para preenchimento e que serão brevemente destacadas.

Vale ressaltar que esta planilha foi adaptada durante essa fase de implantação no município de Guarulhos, sem prejuízo da utilização dos materiais de apoio, sendo eles, o guia do inventário e sua apresentação, ambos presentes nos seguintes endereços:

Guia do Inventário
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf

Apresentação
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/apresentacoes/apresentacao_inventario_dados_pessoais.pdf

Finalizado o preenchimento da planilha do inventário de dados pessoais, é recomendável que seja feita a análise imediata sobre a coleta excessiva ou não de dados pessoais, pois durante a análise dos riscos de privacidade e as medidas de segurança aplicáveis são apontadas esses itens, de forma que a coleta excessiva de dados que não estejam alinhados com os princípios da LGPD, sobretudo, da necessidade e adequação, pode gerar esforço adicional na fase de implantação para a conformidade.

14. Dos Riscos ao Tratamento de Dados Pessoais.

Agora que temos a lista dos dados na planilha do inventário de dados pessoais, é possível seguir para a próxima etapa que trata da análise dos riscos no tratamento de dados pessoais.

Como visto, basicamente temos o risco como a probabilidade de ocorrer um fato e pelo impacto que este pode gerar quando da sua ocorrência que não esteja alinhado ao objetivo do projeto.

Então, temos dois pontos para análise ao calcular o risco, a probabilidade que está relacionada com a possibilidade da ocorrência de um fato e o impacto que está relacionado ao quanto o fato irá mudar o resultado que era esperado.

Para esse momento de implantação da LGPD, devemos observar somente os riscos relacionados com o tratamento de dados pessoais, visto que podemos analisar os riscos sob outros aspectos, como riscos de gestão, à operação, à saúde etc. No entanto, qualquer tipo de risco que afete o tratamento de dados precisa ser identificado e analisado para mitigação.

Também, a Secretaria de Governo Digital já fornece uma lista contendo alguns riscos que podem ocorrer no tratamento de dados, a título exemplificativo, ainda nessa fase, recomendamos que os riscos de privacidade sejam descritos com base nessa tabela.

Lembrando que, classificar os riscos nessa tabela poderá simplificar os trabalhos do resultado final da análise, além de adotar um padrão mínimo que possa ser replicado e posteriormente reanalisado.

Caso seja necessária a elaboração de um risco que não esteja descrito dentre os riscos da tabela existente, é possível que seja adicionado, desde que respeitada a sua construção, seguindo o cálculo por meio da matriz apresentada na *figura 2 - matriz de risco*, levando em conta a probabilidade e o impacto com o resultado final de acordo com seus respectivos pesos.

Ainda, é importante lembrar que a análise do risco é subjetiva, ou seja, uma vez que ocorrer a descrição de um ou mais riscos para cada item do inventário, é possível que as notas finais sejam alteradas, visto que a probabilidade e o impacto dependem da situação levantada em cada órgão, sendo assim, a utilização de um risco previsto na planilha não impede que a sua probabilidade e o seu impacto seja reavaliado e a sua nota consequentemente seja alterada.

IDENTIFICANDO E AVALIAR OS RISCOS

Identificar e avaliar os riscos é a fase que precede a definição de medidas e mecanismos para a mitigação do risco.

Para cada item exclusivo descrito no inventário de dados em que está localizada a existência de dados pessoais e sensíveis é necessária a análise para a identificação e o apontamento de um ou mais riscos.

A probabilidade de ocorrência de um evento de risco e o seu possível impacto é o que deve definir o risco para que seja possível ter o produto do nível potencial de cada evento.

A probabilidade e o impacto são calculados com base nos parâmetros escalares em uma matriz, conforme pode ser visualizado na *figura 1 - parâmetros escalares*.

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

Figura 1 – Parâmetros Escalares

Os parâmetros escalares acima indicados demonstram os níveis de probabilidade e impacto que após ocorrer a multiplicação desses fatores teremos como resultado os níveis de risco nas quais poderão orientar a aplicação de medidas de segurança. A necessidade de calcular o nível do risco deve-se ao fato de que é a exigência necessária para que seja elaborada a resposta a esse risco.

O produto da probabilidade e do impacto de cada risco fica representado em uma região da matriz (3x3) apresentada pela Figura 2.

Figura 2 - Matriz de Risco (3x3)

Risco enquadrado na região	
verde	risco baixo
amarelo	risco moderado
vermelho	risco alto

No município de Guarulhos ainda não possuímos uma política exclusiva para a Gestão de Riscos, sendo assim, as definições e conceitos aqui utilizados são adotados como forma de auxiliar a avaliação existente no RIPD. Sendo assim, quando da existência de política que venha a tratar a Gestão de Riscos, esse documento poderá ser revisado para manter a concordância com a norma.

Tendo em vista o modelo de RIPD constante do ***ANEXO XVII - Relatório de Impacto a Proteção de Dados Pessoais***, a identificação e avaliação de riscos envolve elencar os eventos de risco, a probabilidade, o impacto e o nível de risco.

É importante a identificação de qualquer risco que afete o tratamento de dados pessoais, de forma independente de sua natureza, ou seja, quando se trata de segurança da informação, da privacidade ou até mesmo de riscos que tenham como natureza condição técnica ou administrativa.

A tabela abaixo traz uma lista exemplificativa de riscos de privacidade e segurança da informação que guardam relação com os dados pessoais, assim como a probabilidade e o impacto poderão ser revistos.

Observa-se que os doze primeiros itens representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017 seção 6.4.4., conforme descrito no guia da LGPD da Secretaria de Governo Digital e citado adiante.

Tabela de Risco - referente ao tratamento de dados pessoais

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P1	I2	NÍVEL DE RISCO (P X I)3
R01	Acesso não autorizado	10	15	**150**
R02	Modificação não autorizada	10	15	**150**
R03	Perda	5	15	**75**
R04	Roubo	5	15	**75**
R05	Remoção não autorizada	5	15	**75**
R06	Coleção excessiva	10	10	**100**
R07	Informação insuficiente sobre a finalidade do tratamento	10	15	**150**
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente)	10	15	**150**
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	5	15	**75**
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais	10	15	**150**
R11	Retenção prolongada de dados pessoais sem necessidade	10	5	**50**
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	5	15	**75**
R13	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.)	5	15	**75**
R14	Reidentificação de dados pseudonimizados	5	15	**75**

Conforme a tabela acima que é parte integrante do Guia da LGPD, bem como as definições e conceitos trazidos pelo Guia, temos o seguinte modelo:

Probabilidade P1: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente,

qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

Impacto - I2: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

Nível de Risco - (PxI)3: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

RISCO		
P1	I2	(P X I)3

Modelo da Matriz de Risco

*Para executar essa tarefa, é necessário preencher a planilha disponibilizada no modelo ***ANEXO XIV - análise de riscos***, aplicando as definições e conceitos deste manual.

Abaixo temos um conjunto de perguntas para auxiliar nas respostas que deverão ser fornecidas na planilha.

Conhecer os Riscos	**Medir os Riscos**	**Classificar os Riscos**	**Mitigar os Riscos**
Quem sabe apontar?	Qual o valor da probabilidade e sua descrição?	Qual o valor apresentado na tabela?	Quem cuidará da mitigação?
Identificar e Detalhar	Qual o valor do impacto e sua descrição?	Qual o grau de acordo com a região de enquadramento?	Quando ocorrerá a medida de mitigação?

Lembrando que o caráter é subjetivo e que as alterações precisam ser justificadas e registradas nas descrições da probabilidade e do impacto de forma que justifiquem o valor dado a cada item que compõe o nível de risco.

Ainda, é saudável que mais de uma pessoa participe desse levantamento para se chegar a um consenso na análise dos riscos no caso concreto.

15. Das Medidas de Segurança – Proteção de Dados.

As medidas de segurança devem ser adotadas pelos agentes de tratamento com o objetivo de proteger os dados pessoais em qualquer situação que possa comprometer o tratamento de dados pessoais e sensíveis de forma inadequada ou ilícita. A segurança não pode ter como base apenas as regras de acesso não autorizado, a perda de dados, por exemplo, é um dos fatores que podem ocorrer de forma acidental.

Uma vez que os riscos foram identificados e avaliados, as medidas deverão ser indicadas em seu campo respectivo na planilha do ***ANEXO XIII - inventário de dados pessoais - IDP***.

O inventário traz o apontamento para as medidas de segurança, mas aqui é necessário ir além e implementar controles de segurança por meio do conhecimento e utilização de técnicas e métodos, de forma que fique registrado qual ou quais medidas são aplicáveis aos riscos identificados e avaliados.

É importante mencionar que as medidas de segurança para o ambiente tecnológico se aplicam não só aos utilizadores dos recursos computacionais como para os administradores, gestores e responsáveis por essa estrutura, sendo que as medidas específicas de segurança na tecnologia da informação deverão ser apresentadas pelo Departamento de Informática e Telecomunicações - DIT, que poderá solicitar informações para sua elaboração em conjunto com a unidade ao qual a medida estiver relacionada.

> Art. 12. Cabe ao Departamento de Informática e Telecomunicações - DIT, integrante da Secretaria de Gestão:
> I - oferecer os subsídios técnicos necessários à edição das diretrizes pelo Encarregado de dados pessoais para a elaboração dos planos de adequação; e
> II - orientar, sob o ponto de vista tecnológico, as Secretarias e Subsecretarias na implantação dos respectivos planos de adequação.

IDENTIFICAR MEDIDAS PARA TRATAR OS RISCOS

Identificar as medidas que irão tratar os riscos é fundamental para demonstrar a boa-fé no atendimento aos princípios da LGPD, em especial, à proteção de dados pessoais desde a concepção.

Cabe ressaltar que, nem todos os riscos precisam ser eliminados, existem situações em que o risco é aceitável, desde que devidamente justificado, com exceção do risco residual de nível alto, que além da justificativa deverá conter registro de consulta para a ANPD antes de prosseguir com a operação de tratamento de dados pessoais.

*Para que a planilha modelo - ***ANEXO XV - medidas de tratamento*** - seja devidamente alimentada, tem-se alguns exemplos de medidas para tratar riscos que foram extraídas do guia de avaliação de riscos da Secretaria do Governo Digital, de forma que essa tarefa seja simplificada e sirva de apoio ao RIPD.

As medidas adotadas como referência para auxiliar na descrição do tratamento dos riscos têm por base as normas ABNT NBR ISO/IEC 27002:2013 - segurança da informação e ISO/IEC 29100:2011 - privacidade.

A tabela a seguir contém os exemplos de medidas e a descrição com os objetivo dos controles aplicáveis para o tratamento de riscos, e pode ser consultada juntamente com o guia completo na seguinte página da internet da Secretaria de Governo Digital:

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf

Tabela 01. Exposição das medidas de segurança e os objetivos dos controles.

Medidas de Segurança (12)	Descrição (Objetivo dos controles presentes na medida de segurança)
Continuidade de Negócio	Manter a operação da atividade, apesar das adversidades enfrentadas.
Controles Criptográficos	Oferecer um meio seguro para as comunicações e armazenamento de registros (dados, informações e conhecimento).
Controles de Acesso Lógico	Limitar os acessos indevidos ao sistema.
Controles de Segurança em Redes, Proteção Física e do Ambiente	Evitar acessos indevidos às estruturas internas.
Cópia de Segurança	Realizar e manter cópias com temporariedade de execução e testes (simulações) de que os procedimentos adequados foram implantados e estão funcionais.
Desenvolvimento Seguro	Atender critériosde segurança da informação, desde a concepção do produto.

Gestão de Capacidade e Redundância	Manter a disponibilidade do serviço.
Gestão de Mudanças	Acompanhar as mudanças, comunicar aos interessados e identificar potenciais riscos.
Gestão de Riscos	Identificar, avaliar, gerenciar e monitorar os riscos identificados.
Registro de Eventos, Rastreabilidade e Salvaguarda de Logs	Registrar eventos com atributos de rastreabilidade e proteger de alteração e acessos indevidos.
Medidas de Segurança (12)	**Descrição (Objetivo dos controles presentes na medida de segurança)**
Resposta a Incidente	Realizar a coleta, a preservação de evidências, o tratamento e a resposta à incidentes de segurança.
Segurança Web	Elevar os níveis de segurança (da camada de front-end) nos serviços de acessos eletrônicos.
Abertura, Transparência e Notificação	Atender o princípio de transparência da LGPD (art. 6º, inciso VI).
Compliance com a Privacidade	Atender a legislação de proteção de dados, monitorar e auditar a privacidade.
Consentimento e Escolha	Obter consentimento do titular (art. 7º, I), desde que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 da LGPD.
Controles de Acesso e Privacidade	Limitar acessos indevidos às operações de tratamento de dados pessoais (LGPD, art. 6º, Incisos VII e VIII).

Legitimidade e Especificação de Propósito	Realizar tratamento para propósitos legítimos, específicos, explícitos e informados ao titular (LGPD, art. 6º, I).
Limitação da Coleta	Limitar a coleta ao mínimo necessário para a realização de suas finalidades (LGPD, art. 6º, III).
Medidas de Segurança (12)	**Descrição (Objetivo dos controles presentes na medida de segurança)**
Minimização dos Dados	Minimizar os dados utilizados no processamento (LGPD, art. 6º, III).
Participação Individual e Acesso	Assegurar que os direitos do titular dos dados pessoais são atendidos, a exemplo do livre acesso aos seus dados (LGPD, art. 6º, IV).
Precisão e qualidade	Assegurar que os dados coletados são exatos e relevantes para o cumprimento da finalidade do tratamento (LGPD, art. 6º, V).
Responsabilização	Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (LGPD, art. 6º, X).
Uso, Retenção e Limitação de Divulgação	Assegurar aos titulares os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos da LGPD ao realizar o tratamento de dados pessoais.

16. Da Gestão de Incidentes.

Um Incidente com Dados Pessoais é um evento de concretização do risco, ou seja, é quando o risco ocorre de fato com capacidade para alterar as coisas de maneira diversa como deveriam ser ou estar, de maneira que coloque em risco os dados pessoais dos titulares.

Esse evento pode ou não estar listado anteriormente, isso significa que pode existir um incidente com dados pessoais do qual não possui medida para tratar o risco, uma vez que por algum motivo ele não foi identificado previamente.

O incidente é um evento que atinge a segurança e afeta os dados pessoais, o que pode estar relacionado com a alteração, destruição,

perda, divulgação ou acesso não autorizados, e pode ocorrer de forma ilícita ou acidental.

Assim, todo e qualquer incidente que envolva os dados pessoais precisam de medida de tratamento, como visto anteriormente, sendo necessário, no caso da ocorrência de incidente, a aplicação imediata das medidas de tratamento e segurança em plano de resposta, seja para um evento que não tenha sido previamente detectado ou para um evento de incidente já ocorrido, ainda que as medidas preventivas ao risco tenham sido adotadas.

Em observação ao disposto no artigo 48 da LGPD, é obrigação do controlador comunicar para a autoridade nacional e ao titular dos dados, a ocorrência de incidente de segurança que possa acarretar risco ou dano aos titulares.

Esta comunicação ser feita em prazo razoável contendo em seu conteúdo, no mínimo:

- A descrição dos dados pessoais afetados;
- Informações dos titulares envolvidos;
- Quais medidas de segurança para a proteção de dados que foram adotadas previamente;
- Quais os riscos relacionados ao incidente (efetuar revisão na análise de riscos);
- Justificativa da não ocorrência imediata da comunicação, quando for o caso; e
- Quais medidas estão sendo adotadas para mitigar o impacto e eventuais prejuízos.

PLANO DE RESPOSTA

O objetivo da elaboração do Plano de Resposta a Incidentes é para que se tenha um plano de orientação aos agentes públicos acerca dos procedimentos mais adequados para execução quando da ocorrência de Incidentes com Dados Pessoais, preparando a entidade para atuar na gestão de um incidente de dados pessoais de forma organizada, rápida e eficiente, minimizando seus impactos para todos os envolvidos.

Ao ter ciência sobre qualquer incidente com dados pessoais, imediatamente, é dever de qualquer pessoa comunicar o Controlador de Dados que reunirá os envolvidos no processo que atuam de alguma forma no ciclo de vida dos dados do incidente, como o Departamento de Informática e Telecomunicações - DIT, quando este estiver relacionado ao ativo digital, ou a pessoa responsável pela segurança do ativo físico, para que as medidas necessárias sejam aplicadas com o objetivo de proteger os dados pessoais.

Simultaneamente a essa comunicação inicial interna e às medidas de tratamento e segurança que serão aplicadas, o Controlador de Dados deverá comunicar o Encarregado de Dados, bem como este comunicará a Secretaria Executiva da Comissão de Acesso à Informação sobre o evento.

O Encarregado de Dados comunicará a Procuradoria Geral do Município sobre o incidente para que esta tenha ciência e possa, se for o caso, elaborar resposta em defesa a eventual dano que possa ter ocorrido tendo como causa o incidente.

É importante manter sigilo sobre todas as comunicações relacionadas com o incidente de dados pessoais, pois a falta do sigilo poderá prejudicar a averiguação de responsáveis pelo incidente.

Se for o caso, o Controlador de Dados realizará a comunicação do Incidente com Dados Pessoais à ANPD - Autoridade Nacional de Proteção de Dados, com base nas análises técnicas e jurídicas realizadas pelo DIT e pela PGM, além da Comissão de Acesso à Informação - CAI, quando necessária, de forma a sempre manter o alinhamento com o Encarregado de Dados nessas comunicações.

Também, em atendimento ao Decreto que regulamenta a LGPD e ao próprio regimento interno da CAI, surgem ações para realização em conjunto entre os agentes de tratamento, do encarregado de dados, do DIT, da PGM e da CAI, quando necessária a participação desta, a título exemplificativo, conforme elencado a seguir:

- aprovação e autorização da divulgação de comunicado, aos titulares envolvidos no Incidente com Dados Pessoais;
- validação e assinatura quaisquer comunicados ao público, imprensa e outros meios necessários;
- orientação e comunicação com as equipes envolvidas a respeito das medidas que deverão ser adotadas com relação ao Incidente com Dados Pessoais;
- coordenar as ações necessárias para mitigar os impactos ocorridos e rever os riscos apontados preventivamente, quando da ocorrência de Incidente com Dados Pessoais; e
- atuar na comunicação da entidade junto a ANPD, demais autoridades competentes e os titulares de dados;

*Quando da ocorrência de incidente com dados pessoais, temos as seguintes **etapas do plano de resposta** que deverão ser observadas:

DA CONTENÇÃO

Na ocorrência de incidente, a etapa de contenção serve para evitar que outros dados sejam afetados e que os danos não sejam estendidos. Nessa ação é importante efetuar o registro do incidente e suas medidas para que as evidências sejam utilizadas em posterior averiguação. O trabalho exigido quando da ocorrência de um incidente deve ser colaborativo, em especial para os atores elencados a seguir:

- a partir da ocorrência de incidente de segurança de dados pessoais, o responsável da área pelos dados deve imediatamente informar o encarregado de dados;
- o Encarregado de Dados, quando comunicado, irá verificar a existência do plano de ação para o incidente e, se for o caso, preencher o formulário de Comunicação de Incidente para a Autoridade Nacional de Proteção de Dados - ANPD e aos titulares afetados;

- a Procuradoria Geral do Município poderá ser comunicada para auxiliar no processo de comunicação, bem como adotar as medidas jurídicas cabíveis;
- o Departamento de Informática e Telecomunicações será comunicado quando o incidente for relacionado a segurança da informação em ativo digital, para que as medidas cabíveis sejam adotadas;

- o Controlador de dados: deve validar as medidas propostas no Plano de Respostas a Incidentes e oferecer subsídios para que as mesmas sejam efetivamente cumpridas.

DA EXTINÇÃO E DO RESTABELECIMENTO

Após a contenção a ameaça deve ser extinta e todos os processos e seus sistemas atingidos devem ser restabelecidos, porém, a medida de restabelecimento só deve ocorrer após a existência de evidências da extinção da ameaça.

No caso de ativos digitais, os sistemas só poderão funcionar no ambiente de produção após a verificação da existência de perda e a tentativa de recuperação, se for o caso.

DA DOCUMENTAÇÃO

Para que os erros não voltem a ocorrer, é essencial que os incidentes sejam documentados, descrevendo quais procedimentos foram adotados para que se tenha um histórico dos eventos e as medidas realizadas.

Medidas para realização conforme orientações contidas na página de internet da Secretaria de Governo Digital:

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/reportar-incidentes-problemas

https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

- *No caso de dados pessoais de pessoas físicas, a comunicação de incidentes de segurança com dados pessoais, inclusive vazamentos, deve ser efetuada por intermédio de formulário disponível na seguinte página: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.*
- *Para informações adicionais sobre o trabalho da Autoridade Nacional de Proteção de Dados (ANPD), acesse https://www.gov.br/anpd/pt-br.*

O formulário de comunicação imediata ao Encarregado de Dados está disponibilizado no documento modelo ***ANEXO XVI - comunicação de incidentes***.

17. Do Relatório de Impacto à Proteção de Dados.

Para o referido relatório estão sendo consideradas as orientações do guia da LGPD da Secretaria de Governo Digital, listadas abaixo, sendo que todos os documentos anteriores exigidos para se chegar até essa etapa serão utilizados, visto que o RIPD adaptado para adequação no município contém as informações previamente demandadas.

Sendo assim, conforme as orientações do guia da LGPD da Secretaria de Governo Digital, temos as seguintes etapas:

Como Elaborar

O **RIPD** deve ser elaborado antes de a instituição iniciar o tratamento de dados pessoais, preferencialmente, na fase inicial do programa ou projeto que tem o propósito de usar esses dados. A elaboração contempla as etapas destacadas pela figura a seguir.

Identificar os Agentes de Tratamento e o Encarregado

Esta etapa consiste em identificar os agentes de tratamento (controlador e operador) e o encarregado no RIPD (art. 5º da LGPD). Esses atores desempenham papel essencial no levantamento das informações necessárias para elaboração do RIPD.

> *Art. 5º Para os 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 entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019).*

A conclusão desta etapa envolve registrar o e-mail e o telefone de contato do encarregado, já que ele é o canal de comunicação entre o controlador, titulares dos dados e ANPD.

Identificar a necessidade de elaborar o Relatório

Inicialmente, é fundamental conhecer os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado. São eles:

- Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou

atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);

• Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e

• A qualquer momento sob determinação da ANPD (art. 38).

Quando for necessária a elaboração do **RIPD**, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do **RIPD**.

A elaboração de um único **RIPD** para todas as operações de tratamento de dados pessoais ou de um **RIPD** para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um **RIPD** único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único **RIPD** não seja a opção mais indicada, optando por elaborar RIPDs segregados por ser mais adequado à sua realidade.

Além dos casos específicos previstos pela LGPD no início desta seção 2.5.2.2 relativas à elaboração do RIPD, é indicada a elaboração ou atualização do **Relatório de Impacto** sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

• uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;

• 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 § 2º);

• tratamento de 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” (LGPD, art. 5º, II);

• 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);

• tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);

• 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);

• 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. 4º, § 3º);

• tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);

• alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e

• reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Em síntese, nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o **RIPD** ser elaborado ou atualizado pela instituição.

Descrever o tratamento

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, escopo, contexto e finalidade** do tratamento.

Lembrando que a LGPD (art. 5º, 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”.

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.

Natureza do tratamento

A **natureza** representa como a instituição pretende tratar ou trata o dado pessoal. Importante descrever, por exemplo: como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;

Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.

Escopo do tratamento

O **escopo** representa a abrangência do tratamento de dados. Nesse sentido, considerar destacar:

- as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis.
- o volume dos dados pessoais a serem coletados e tratados;
- a extensão e frequência em que os dados são tratados;
- o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
- o número de titulares de dados afetados pelo tratamento; e
- a abrangência da área geográfica do tratamento.

O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.

Contexto do tratamento

Nesta etapa, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.

Finalidade do tratamento

A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.

Nesta etapa, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os exemplos de finalidades elencadas abaixo, embasados nos artigos 7º e 11 da LGPD, no que for aplicável.

Identificar partes interessadas consultadas

Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Descrever necessidade e proporcionalidade

Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o 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 de dados (LGPD, art. 6º, III).

Identificar e avaliar os riscos

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever “medidas, salvaguardas e mecanismos de mitigação de risco“.

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais. Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança.

Identificar medidas para tratar os riscos

Conforme a análise dos riscos identificados, devem ser apontadas as medidas para o tratamento com a revisão constante.

Aprovar o Relatório

Esta etapa visa formalizar a aprovação do RIPD por meio da obtenção das assinaturas do responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador.

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 pela instituição.

A instituição deve manter revisão do RIPD a fim de demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

*Aqui o processo de implantação da LGPD tem sua entrega completa dentro da previsão do cronograma, sendo necessário a partir desse momento, o acompanhamento desse processo, efetuando a constante revisão para a aplicação das medidas cabíveis, como eventuais correções e melhorias.

O RIPD está disponível no modelo - ***ANEXO XVII - Relatório de Impacto a Proteção de Dados Pessoais*** - e será compartilhado para que seja confeccionado de forma colaborativa.

18. Do cronograma para conformidade – fase de adequação.

Inicialmente, algumas tarefas já precisam ser realizadas em conjunto com o cronograma, dentre elas, temos conforme o disposto no Decreto Municipal n. 38.145/2021, que as unidades precisam ter página criada para disponibilização de informações padronizadas sobre a LGPD.

Também, é necessária a disponibilização das cartas de serviços e as finalidades e adequação da lei conforme as respectivas cartas de serviços, devendo comunicar as pessoas que atuam diretamente na prestação do serviço de atendimento ao público para que saibam informar sobre a finalidade do tratamento de dados quando questionado e o andamento da implantação da LGPD.

*Conforme o Decreto que regulamenta a LGPD, será exigida a elaboração do cronograma com etapas mínimas para orientação constantes no modelo - ***ANEXO V - cronograma***, que deverá ser entregue ao Encarregado de dados até a data do dia 20 de setembro de 2021, do qual poderá ser adequado conforme as necessidades de cada secretaria, quanto às suas tarefas .

19. Observações

Da Tecnologia da Informação
O DIT, como departamento alocado na Secretaria de Gestão, deverá adotar as mesmas medidas aplicáveis com vistas aos seus processos internos, porém, devido às suas características próprias existem especificidades que deverão ser realizadas e cumpridas, nas quais deverão constar do cronograma da Secretaria de Gestão a aplicação de medidas de segurança em ativos digitais, sejam eles de ponta, treinamento e orientação quanto às boas práticas no uso dos mecanismos informatizados por seus agentes públicos (conforme termo de referência modelo), quanto às medidas.

Do canal de comunicação.
Externo - sistema de requisição dos titulares em desenvolvimento para questões em que há necessidade de verificação do titular e utilização do sistema-e-SIC para as questões que envolvam o tratamento de forma transparente, quando não disponibilizados ativamente.
Interno - para questões específicas utilizar o e-mail interno do Encarregado de Dados: encarregadodedados@guarulhos.sp.gov.br.

Para questões gerais, dúvidas, esclarecimentos e suporte na implementação que sejam de interesse comum, o canal de cursos da ESAP, LGPD em curso, possui repositórios dos materiais e fórum para troca de experiências do qual servirá para elaborar o campo de dúvidas frequentes.

Disponibilizado na página de internet: eadesap.guarulhos.sp.gov.br

*A comunicação do Controlador com o titular de dados e com a ANPD deve ser feito com ciência do Encarregado de Dados, na situação específica do art. 48 da Lei 13.709/2018. O controlador deve, por definição legal, se comunicar com a ANPD e o titular de dados em situações concretas e quando isso ocorrer

deverá informar o Encarregado de Dados para alinhamento (plano de comunicação interno) no que for necessário providenciar junto à ANPD.

Geração de evidências – qualquer documento, mesmo que a comunicação, que sejam decorrentes de demandas da LGPD, seja na sua implementação ou na sua rotina, deverão ser armazenados e com backup de segurança nas próprias unidades por seus respectivos controladores. Dessa forma institui-se a cultura de registro das evidências e controle para o monitoramento e melhorias.

*Recomenda-se criar pasta na rede interna disponibilizada pelo Departamento de Informática e Telecomunicações – DIT com a estrutura que possa, minimamente, identificar as atividades de Adequação, Conformidade, Comunicação e Controle (monitoramento), sem prejuízo da criação de pastas com outras informações.

8

CONSIDERAÇÕES FINAIS

As boas práticas sobre o tema da Proteção de Dados demandarão a constante atualização de conceitos e condutas nas rotinas técnicas e administrativas desta Municipalidade, sem distinção de cargo ou função.
É de suma importância lembrar que a proteção de dados pessoais, como desdobramento do direito à privacidade, deverá ser instrumento de promoção à personalidade humana, privilegiando-se os direitos individuais.

O trabalho integrado de todas as unidades administrativas será imprescindível para a correta aplicação da Lei Geral de Proteção de Dados Pessoais, que requisitará o constante diálogo de todas as fontes, evitando-se, assim, aplicação de penalidades.

Por fim, informamos que este conteúdo basilar será periodicamente revisado e atualizado por esta equipe técnica de elaboração da Controladoria Geral do Município e todas as sugestões dos destinatários deste Manual serão analisadas de acordo com a sua pertinência.

Lista de Documentos ANEXOS

ANEXO I - Perguntas e respostas sobre a LGPD.

ANEXO I.A – planilha de controle dos agentes de tratamento, disponibilizar modelo em branco para cada unidade cumprir o item 1.

ANEXOS II.C.1, IIC.2, II.C.3 – do plano de trabalho,do plano de ação e do cronograma.

*Cabe lembrar que todos os documentos apresentados como ANEXO estão disponíveis para download na página da LGPD no seguinte endereço eletrônico: https://www.guarulhos.sp.gov.br/lei-geral-de-protecao-de-dados

REFERÊNCIAS BIBLIOGRÁFICAS

Verificados os acessos e conteúdo em: 15/09/2021
https://www.guarulhos.sp.gov.br/lei-geral-de-protecao-de-dados
https://www.guarulhos.sp.gov.br/06_prefeitura/leis/decretos_2019/36140decr.pdf.

POLÍTICA DE RESPOSTA A INCIDENTES. https://www.unoesc.edu.br/unoesc/lgpd/politica-incidentes.

Reportar incidentes de segurança e outros problemas. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/reportar-incidentes-problemas.

O que é o ROPA na LGPD? Conheça os Registros das Atividades de Tratamento. Disponível em: https://www.privacytools.com.br/ropa-lgpd/.

ALMEIDA, Vinicius Nóbile de. *Cadeia de valor: o que é, para que serve e exemplo de aplicação na gestão de processos*. Disponível em: **http://www.euax.com.br/2019/10/cadeia-de-valor/**.

_____. *O que é e como fazer Mapeamento de Processos em 6 passos*. Disponível em: **https://www.euax.com.br/2016/06/como-fazer-mapeamento-de-processos-em-6-passos/**.

BRANDÃO, Graziela. O que é o mapeamento de dados? Disponível em: https://blconsultoriadigital.com.br/mapeamento-de-dados/.

CAVOUKIAN, Ann. *Privacy by Design: The 7 Foundational Principles*. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>.

COPETTE, Fabio. *Data Mapping* versus *Data Discovery*: quais as diferenças e as similaridades? Disponível em: https://pt.linkedin.com/pulse/data-mapping-versus-discovery-quais-diferen%C3%A7as-e-fabio-copette.

GONÇALVES, Mariana Sbaite. *Ocorreu um incidente de segurança com dados pessoais. E agora?* Disponível em: https://www.lgpdbrasil.com.br/ocorreu-um-incidente-de-seguranca-com-dados-pessoais-e-agora/

MARTINS, Thiago Souza. *O "Privacy by Design" na Lei Geral de Proteção de Dados. Disponível em*: https://tico080970.jusbrasil.com.br/artigos/1108185338/o-privacy-by-design-na-lei-geral-de-protecao-de-dados

NAKAGAWA, Marcelo. Missão, Visão e Valores. Disponível em: https://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/ME_Missao-Visao-Valores.PDF

SOARES, João. Data Mapping e Inventário de Dados – O Colete Salva Vidas do DPO. Disponível em https://goadopt.io/blog/mapeamento-ou-inventario-de-dados-lgpd/

GLOSSÁRIO

ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO – atender o princípio de transparência da LGPD (art. 6º, inciso VI).

ACESSO – ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

ACORDO DE COOPERAÇÃO INTERNACIONAL – acordos de Cooperação são ajustes genéricos estabelecidos entre organizações de países distintos ou com organizações supranacionais. Por meio destes instrumentos, definem-se os objetivos da cooperação, áreas de trabalho, formas de implementação, prazos e interlocutores.

ADEQUAÇÃO – a adequação à LGPD é muitas vezes confundida com um processo puramente jurídico. No entanto, um pilar fundamental previsto na lei é a segurança dos dados pessoais. A LGPD estabelece dez princípios que devem nortear o tratamento de dados pessoais. Um deles é justamente a segurança.

ARMAZENAMENTO – ação ou resultado de manter ou conservar em repositório um dado;

ARQUIVAMENTO – ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;

AVALIAÇÃO – analisar o dado com o objetivo de produzir informação;

CERTIFICAÇÃO REGULARMENTE EMITIDA – a certificação foi desenvolvida pela ABRADi e *Bureau Veritas* para apoiar o ecossistema da comunicação digital na adequação à LGPD. A Certificação demonstra também que as instituições públicas e privadas estão engajadas em cumprir a LGPD, além de preparadas para evitar e prevenir violações de dados pessoais.

CLASSIFICAÇÃO – maneira de ordenar os dados conforme algum critério estabelecido;

COLETA – recolhimento de dados com finalidade específica;

COMPLIANCE COM A PRIVACIDADE – Atender a legislação de proteção de dados, monitorar e auditar a privacidade.

COMUNICAÇÃO – transmitir informações pertinentes a políticas de ação sobre os dados;

CONFORMIDADE – para estar em conformidade (*compliance*) com a LGPD, é preciso atualizar a infraestrutura, fazer análises profundas nas operações e mapear processos de negócio, pois as regras de tratamento de dados pessoais são rigorosas.

CONSENTIMENTO E ESCOLHA – obter consentimento do titular (art. 7º, I), desde que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 da LGPD.

CONTINUIDADE DE NEGÓCIO – manter a operação da atividade, apesar das adversidades enfrentadas.

CONTROLE – ação ou poder de regular, determinar ou monitorar as ações sobre o dado;

CONTROLES CRIPTOGRÁFICOS – oferecer um meio seguro para as comunicações e armazenamento de registros (dados, informações e conhecimento).

CONTROLES DE ACESSO LÓGICO – limitar os acessos indevidos ao sistema.

CONTROLES DE ACESSO E PRIVACIDADE – limitar acessos indevidos às operações de tratamento de dados pessoais (LGPD, art. 6º, Incisos VII e VIII).

CONTROLES DE SEGURANÇA EM REDES, PROTEÇÃO FÍSICA E DO AMBIENTE – evitar acessos indevidos às estruturas internas.

CÓPIA DE SEGURANÇA – realizar e manter cópias com temporariedade de execução e testes (simulações) de que os procedimentos adequados foram implantados e estão funcionais.

COOPERAÇÃO JURÍDICA INTERNACIONAL ENTRE ÓRGÃOS PÚBLICOS DE INTELIGÊNCIA, DE INVESTIGAÇÃO E DE PERSECUÇÃO, DE ACORDO COM OS INSTRUMENTOS DE DIREITO – acordo que visa o compartilhamento de informações para o fim de aplicação dos instrumentos legais para manutenção da ordem pública , inclusive a persecução de investigados e infratores.

CRONOGRAMA – é a representação do projeto, de fácil visualização, com a descrição das tarefas e seus respectivos prazos, de modo a permitir o controle na execução, possibilitar o registro de ações no tempo e as necessárias adequações em seu decorrer.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADOR – quando o tratamento realizado decorre de obrigação legal ou regulatória. Ex.: Comunicação de doenças contagiosas.

DESENVOLVIMENTO SEGURO – atender critérios de segurança da informação, desde a concepção do produto.

DIFUSÃO – ato ou efeito de divulgação, propagação, multiplicação dos dados;

DISTRIBUIÇÃO – ato ou efeito de dispor de dados de acordo com algum critério estabelecido;

ELIMINAÇÃO – ato ou efeito de excluir ou destruir dado do repositório;

ENTREGÁVEIS – todos os documentos produzidos relacionados à implantação da LGPD.

EXECUÇÃO DE CONTRATO OU DE PROCEDIMENTOS PRELIMINARES RELACIONADOS A CONTRATO DO QUAL SEJA PARTE O TITULAR – uma das dez bases legais para tratamento de dados da LGPD**.**

EXECUÇÃO DE POLÍTICA PÚBLICA OU ATRIBUIÇÃO LEGAL DO SERVIÇO PÚBLICO – uma das dez bases legais para tratamento de dados da LGPD**.**

EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL – uma das dez bases legais para tratamento de dados da LGPD**.**

EXTRAÇÃO – ato de copiar ou retirar dados do repositório em que se encontrava;

FORNECIMENTO DE CONSENTIMENTO ESPECÍFICO PELO TITULAR DOS DADOS PESSOAIS – o consentimento deve ocorrer com manifestação livre, informada e inequívoca dada pelo titular, ou seja, o titular deve concordar com o tratamento de dados para uma finalidade determinada

GESTÃO DE CAPACIDADE E REDUNDÂNCIA – manter a disponibilidade do serviço.

GESTÃO DE MUDANÇAS – acompanhar as mudanças, comunicar aos interessados e identificar potenciais riscos.

GESTÃO DE RISCOS – identificar, avaliar, gerenciar e monitorar os riscos identificados.

INCIDENTE DE SEGURANÇA – um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

LAI – Lei de Acesso à Informação – Lei Nacional n.12.527/2011;

LEGITIMIDADE E ESPECIFICAÇÃO DE PROPÓSITO – realizar tratamento para propósitos legítimos, específicos, explícitos e informados ao titular (LGPD, art. 6º, I).

LGPD – Lei Geral de Proteção de Dados – Lei Nacional n. 13.709, de 14 de agosto 2018;

LIMITAÇÃO DE COLETA – limitar a coleta ao mínimo necessário para a realização de suas finalidades (LGPD, art. 6º, III).

MINIMIZAÇÃO DE DADOS – minimizar os dados utilizados no processamento (LGPD, art. 6º, III).

MODIFICAÇÃO – ato ou efeito de alteração do dado;

NORMAS CORPORATIVAS GLOBAIS – as normas corporativas globais fazem parte do projeto de alteração proposto para a Lei de Proteção de Dados Pessoais (LGPD).

ORGANOGRAMA – é uma representação gráfica do tempo investido em uma determinada tarefa ou projeto, segundo as tarefas que devem ser executadas no âmbito desse projeto.

PAÍS QUE FORNECE UM NÍVEL ADEQUADO DE PROTEÇÃO – A LGPD é uma Lei derivada da Européia GDPR, a qual prima por manter relações, inclusive comerciais, com países onde a proteção de dados pessoais tem uma proteção de nível considerado adequado.

PARTICIPAÇÃO INDIVIDUAL E ACESSO – Assegurar que os direitos do titular dos dados pessoais são atendidos, a exemplo do livre acesso aos seus dados (LGPD, art. 6º, IV).

PLANO DE ADEQUAÇÃO – Projeto para adequar os principais processos e tecnologias internos à LGPD, bem como, conscientizar toda a Administração para garantir a privacidade de dados pessoais tratados na Municipalidade e em nome desta.

PRECISÃO E QUALIDADE – Assegurar que os dados coletados são exatos e relevantes para o cumprimento da finalidade do tratamento (LGPD, art. 6º, V).

PRIVACY BY DESIGN – é uma estrutura de trabalho que tem como proposta central incorporar a privacidade e a proteção de dados pessoais em todos os projetos desenvolvidos por uma organização, desde a sua concepção.

PROCESSAMENTO – ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;

PRODUÇÃO – criação de bens e de serviços a partir do tratamento de dados;

PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA DO TITULAR OU DE TERCEIRO – uma das dez bases legais para tratamento de dados da LGPD**.**

RECEPÇÃO – ato de receber os dados ao final da transmissão;

RECURSOS ADMINISTRATIVOS – são os recursos gerenciais que as empresas utilizam para planejar, organizar, dirigir e controlar suas atividades.

RECURSOS FINANCEIROS – são recursos monetários, como capital, dinheiro em caixa ou em bancos, créditos, investimentos, contas a receber etc.

RECURSOS HUMANOS – são as pessoas que trabalham em todos os níveis da empresa, desde o presidente até o mais humilde dos operários. na verdade, as pessoas são os únicos recursos vivos e inteligentes de uma empresa, capazes de lidar com todos os demais recursos empresariais.

RECURSOS MATERIAIS – são os recursos físicos, como edifícios, prédios, máquinas, equipamentos, instalações, ferramentas, matérias-primas etc.

RECURSOS MERCADOLÓGICOS – são os recursos comerciais que as empresas utilizam para colocar seus produtos ou serviços no mercado, como vendas, promoção, propaganda, pesquisa de mercado, definição de preços etc.

REGISTRO DE EVENTOS, RASTREABILIDADE E SALVAGUARDA DE LOGS – registrar eventos com atributos de rastreabilidade e proteger de alteração e acessos indevidos.

REPRODUÇÃO – cópia de dado preexistente obtido por meio de qualquer processo;

RESPONSABILIZAÇÃO – adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (LGPD, art. 6º, X).

RESPOSTA A INCIDENTE – realizar a coleta, a preservação de evidências, o tratamento e a resposta à incidentes de segurança.

SEGURANÇA WEB – elevar os níveis de segurança (da camada de front-end) nos serviços de acessos eletrônicos.

SELO REGULARMENTE EMITIDO – uma das formas de comprovação de conformidade com a LGPD, para a transferência de dados. Ex. art, 33, II d, **selos**, certificados e códigos de conduta **regularmente emitidos**;

TRANSFERÊNCIA – mudança de dados de uma área de armazenamento para outra, ou para terceiro;

TRANSFERÊNCIA AUTORIZADA PELA ANPD – é a transferência de dados realizada após consulta e autorização emitida pela Agência Nacional de Proteção de Dados.

TRANSMISSÃO – movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.;

USO RETENÇÃO E LIMITAÇÃO DE DIVULGAÇÃO – assegurar aos titulares os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos da LGPD ao realizar o tratamento de dados pessoais.

UTILIZAÇÃO – ato ou efeito do aproveitamento dos dados.

WEB – a *World Wide Web*, também conhecida pela sigla WWW ou apenas pelo termo Web, pode ser traduzida como teia mundial. Falando também de forma simples e direta, a web nada mais é do que o caminho que permite a você usufruir do conteúdo transferido pela internet.