PREFEITURA
TERESÓPOLIS

Ciência e
Tecnologia

PLANO DE AÇÃO

ADEQUAÇÃO À LGPD

Lei Federal 13.709/2018

Versão 1.0

Março / 2023

TERÊGOV
DIGITAL

Prefeitura Municipal de Teresópolis

Secretaria Municipal de Ciência e Tecnologia
Departamento de Governança e Dados

GESTÃO

Vinicius Cardoso Claussen da Silva
Prefeito

Vinicius Oberg Guedes
Secretário Municipal de Ciência e Tecnologia

Yara da Rocha Medeiros
Secretária Municipal de Controle Interno

Cleiton Evandro Corrêa Pimentel
Diretor do CPD
Setor de Governança e Dados

Ricardo Gomes Fonseca
Encarregado de Proteção de Dados (DPO)

André Washington Garcia Suarez
Operador de Dados

Daniel da Cruz Miranda Pereira
Analista e Desenvolvedor de Sistemas

SUMÁRIO

APRESENTAÇÃO

O presente plano de ação é o documento para adequação para a implantação da Lei Geral de Proteção de Dados é conjunto das regras de boas práticas e de governança de dados pessoais que tem como proposta estabelecer as condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos e obrigações específicas para os diversos agentes envolvidos no tratamento.

A Lei Geral de Proteção de Dados (Lei Federal 13709, de 14 de agosto de 2018, “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”, de acordo com o texto da própria lei.

A LGPD é uma lei que busca garantir a segurança de dados pessoais, respeitando a liberdade individual e a privacidade. Neste sentido, o arcabouço legal traz importantes análises sobre a preservação da integridade da pessoa para que não seja objeto de apropriação criminosa, expositiva ou constrangedora.

INTRODUÇÃO

O Plano de Ação para adequação do Município de Teresópolis à Lei Geral de Proteção de Dados Pessoais é o documento que norteia a implementação da Lei n.º 13.709, de 14 de agosto de 2018, no âmbito da Administração Pública Municipal.

O planejamento da implementação da Lei Geral de Proteção de Dados no Município de Teresópolis, tem por parâmetro o estabelecimento de normas legais em consonância com legislação vigente sobre a proteção de dados pessoais.

O PA-LGPD-TERESÓPOLIS reúne diretrizes para que a administração pública municipal, por meio de adoção de medidas estratégicas, se consolida em métodos conceituais para assegurar a observância dos princípios contidos na Lei Geral de Proteção de Dados, reservando aos direitos garantidos aos titulares de dados pessoais.

O seu referencial teórico está fundamentado nas orientações da Autoridade Nacional de Proteção de Dados, de autores renomados especialistas em proteção de dados e, se coaduna com os preceitos do Programa TerêGov Digital, como Estratégia de Governo Digital do Município de Teresópolis. Ainda como referenciais teóricos adotados para constituir o PA-LGPD-TERESÓPOLIS, citem-se os Marcos de conformidade com a LGPD, materializados por Guias Operacionais para adequação à LGPD, os quais fazem parte do conjunto de ações preparadas pela Secretaria de Governo Digital do Ministério da Economia (SGD-ME) para fomentar a cultura de proteção de dados e apoiar a evolução da maturidade necessária às adequações da lei nos órgãos do Governo Federal (alinhando-se com os objetivos 10 e 11 do princípio Governo Confiável da Estratégia de Governo Digital – EGD, que prevê a entrega de importantes Marcos de Conformidade com a LGPD, com o objetivo de auxiliar os órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação no processo de adequação à Lei Geral de Proteção de Dados Pessoais).

Na construção do PA-LGPD-TERESÓPOLIS foram considerados os dispositivos pertinentes da LGPD, aspectos atinentes ao Contexto Organizacional, à Liderança, à Capacitação, à Conformidade do Tratamento, aos Direitos do Titular, ao

Compartilhamento de Dados Pessoais, à Violação de Dados Pessoais e às Medidas de Proteção, por meio uma abordagem atinente a aspectos de Governança, de Conformidade Legal e Respeito aos Princípios, de Transparência e Direitos do Titular, de Rastreabilidade, de Adequação de Contratos e Relações com Parceiros, de Segurança da Informação, e de Violação de Dados.

O PA-LGPD-TERESÓPOLIS será atualizado, sempre que necessário, para se adequar às determinações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD) e dos órgãos de controle interno e de controle externo, bem como para melhor esclarecer algum trecho específico, ou diante de eventuais atualizações legislativas ou de novos entendimentos preponderantes sobre a matéria.

Na elaboração do PA-LGPD-TERESÓPOLIS, considerou-se o arcabouço jurídico que trata sobre os dados pessoais:

Lei n° 9.507/1997, que regula o direito de acesso a informações e disciplina o rito processual do habeas data.

Lei n° 12.527/2011 (Lei de Acesso à Informação), que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

Decreto n° 7.724/2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição

Decreto Municipal n° 5857/2022, que dispõe sobre o acesso à informação no âmbito do Município de Teresópolis;

Lei n° 12.965/2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

Decreto n° 8.771/2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014, (Marco Civil da Internet), para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

Lei n° 13.460/2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

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

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

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

OBJETIVOS

Objetivo Geral

Nortear a implementação da Lei n.º 13.709/18 (Lei Geral de Proteção de Dados Pessoais – LGPD), no âmbito do Município de Teresópolis.

Objetivos Específicos

Identificar as atividades prioritárias a serem desenvolvidas para o atendimento das disposições da LGPD Indicar medidas necessárias para a adequação do Município de Teresópolis à Lei Geral de Proteção de Dados Pessoais.

Fixar parâmetros para assegurar a transparência e o respeito aos direitos dos titulares de Dados Pessoais nos serviços prestados pelo município de Teresópolis e seus prestadores de serviços.

Fomentar a cultura de Proteção de Dados Pessoais no âmbito da administração pública municipal

Promover o engajamento intersetorial dos órgãos integrantes da administração pública no atendimento aos marcos de conformidade atinentes à LGPD.

MARCOS CONCEITUAIS

Nos termos do inciso X do art. 5º da LGPD, considera-se 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.

É plausível destacar que os princípios trazidos pela Lei Geral de Proteção de Dados Pessoais:

a) **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável (LGPD, art. 5º, I).
b) **dado pessoal sensível:** 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).

TRATAMENTO DE DADOS PESSOAIS

Nesse aspecto, destacamos os princípios elencados no art. 6º da LGPD, os quais devem orientar o tratamento de dados pessoais:

O Art. 6º descreve que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

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;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do trata- mento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

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;

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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

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.

Destacamos o Artigo 7º sobre o tratamento de dados pessoais que orienta que o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, ser- viços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - 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; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

No mesmo sentido, é necessário transcrever as hipóteses de tratamentos de dados pessoais sensíveis referidas no art. 11 da LGPD: Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos da-dos pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

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

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

DIREITOS DO TITULAR

A Lei Geral de Proteção de Dados Pessoais empodera os titulares de dados, fornecendo-lhes direitos a serem exercidos perante os controladores de dados, como se pode verificar na tabela abaixo:

Direitos garantidos aos titulares de dados

Direitos dos Titulares	Princípio	Referência legal
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Princípio da adequação	Art. 6º, II
Direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento	Princípio da necessidade	Art. 6º, III
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais	Princípio do livre acesso	Art. 6º, IV
Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento	Princípio da qualidade dos dados	Art. 6º, V

Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão	Princípio da segurança	Art. 6º, VII
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais	Princípio da prevenção	Art. 6º, VIII
Direito de não ser discriminado de forma ilícita ou abusiva	Princípio da não discriminação	Art. 6º, IX
Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais	Princípio da responsabilização e prestação de contas	Art. 6º, X

Direitos específicos dos titulares de dados

Direitos dos Titulares	Referência Legal
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 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 Administração Pública Federal (APF), em queo tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento	Art. 7º, § 5º
Direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida quando o tratamento for baseado no legítimointeresse do controlador	Art. 10, § 1º
Direito à transparência do tratamento de dados baseado no legítimointeresse do controlador	Art. 10, § 2º
Direito à anonimização dos dados pessoais sensíveis, sempre quepossível, 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 cumprimentode 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 portabilidadede 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 pesquisase 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 resultadosou 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 pelo órgão de pesquisa	Art. 13, § 2º
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	Art. 15

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 Le	
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

A seguir, na tabela abaixo, seguem as hipóteses de tratamento autorizados pela LGPD e respectiva base legal:

Hipótese do Tratamento	Dispositivo Legal Para Tratamento Dados Pessoais	Dispositivo Legal para tratamento / Dados Sensíveis
Hipótese 1: Mediante consentimentodo titular	LGPD, art. 7º, I	LGPD, art. 11, I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, “a”
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, inciso III	LGPD, art. 11, II, “b”
Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, inciso IV	LGPD, art. 11, II, “c”
Hipótese 5: Para a execução oupreparação de contrato	LGPD, art. 7º, inciso V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	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	LGPD, art. 7º, inciso VII	LGPD, art. 11, II, “e”
Hipótese 8: Para a tutela da saúdedo titular	LGPD, art. 7º, inciso VIII	LGPD, art. 11, II, “f”
Hipótese 9: Para atender interesseslegítimos do controlador ou de terceiro	LGPD, art. 7º, inciso IX	Não se aplica
Hipótese 10: Para proteção docrédito	LGPD, art. 7º, inciso X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurançado titular	Não se aplica	LGPD, art. 11, II, “g”

“Fonte: Guia de boas práticas (LGPD), 2020. pág. 23”

INVENTÁRIO DE DADOS PESSOAIS IDP

O inventário é um registro de todas as operações de tratamento de dados pessoais e suas avaliações sob a ótica dos princípios da LGPD. De acordo com o Art 37, “o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse”.

O Inventário de Dados Pessoais deve esclarecer, em cada caso, as seguintes informações: Atores envolvidos (agentes de tratamento e o encarregado);

Finalidade (o que a instituição faz com o dado pessoal); Hipótese (arts. 7º e 11 da LGPD) e previsão legal; Dados pessoais tratados pela instituição;

Categoria dos titulares dos dados pessoais; Tempo de retenção dos dados pessoais;

Instituições com as quais os dados pessoais são compartilhados; Transferência internacional de dados (art. 33 LGPD); e

Medidas de segurança atualmente adotadas.

Inventário de todas as operações de tratamento de dados pessoais e suas avaliações sob a ótica dos princípios da LGPD.

TERMO DE USO

Termo de Uso ou Contrato de Termo de Uso é um documento que estabelece as regras e condições de uso de determinado serviço. Orienta a elaboração de Termos de Uso e Políticas de Privacidade vinculados à utilização de serviços públicos por meio de aplicações (sítios, sistemas ou aplicativos para dispositivos móveis) fornecidas por órgãos e entidades da administração pública.

Caso o Termo de Uso seja aceito pelo usuário, a utilização do serviço será vinculada às cláusulas dispostas nele. O Foco são as regras e condições. Portanto, o termo de uso constitui, um dever do controlador e um direito do titular.

O Termo de Uso deve evidenciar de forma clara quais são as responsabilidades de cada parte envolvida no serviço. Ao definir responsabilidades, a Administração Pública e o cidadão estabelecem direitos e deveres para ambas as partes e compreendem suas obrigações ao utilizar e prover o serviço, de forma a esclarecer

quais situações configuram violações aos Termos e para quais situações cabe reparação de danos.

As seguintes informações devem estar presentes no Termo de Uso:

- O que é o serviço?
- Quais são as informações para contato.
- Qual a sua finalidade?
- Qual o foro?
- Em qual leis e normativos o tratamento está respaldado?
- Como serão comunicadas as mudanças no Termo de Uso?
- Quais são as responsabilidades do usuário e da Administração Pública?

O Titular tem direito a obter do Controlador, em relação aos dados por ele tratados, conferidos pela Lei de Proteção de Dados Pessoais:

- Direito de confirmação e acesso (Art. 18, I e II)
- Direito de retificação (Art. 18, III)
- - Direito à limitação do tratamento dos dados (Art. 18, IV)
- - Direito de oposição (Art. 18, § 2º)
- - Direito de portabilidade dos dados (Art. 18, V)
- - Direito de não ser submetido a decisões automatizadas (Art. 20, LGPD)
- - Direito do acesso à informação (Lei 12.527 - Lei de Acesso à Informação)
- - Direito do respeito à intimidade (Constituição Federal, Art. 5º, X)

Fonte: Apresentação Guia Inventário de dados Pessoais - IDP, (LGPD) 2020

AVALIAÇÃO DE RISCOS

Orienta a identificação e mensuração de riscos de segurança e privacidade, mitigando-os com a utilização dos controles mais indicados.

Constitui um instrumento de identificação de controles que elevem a segurança da informação diante dos pilares de confidencialidade, integridade, disponibilidade e autenticidade no sistema a ser desenvolvido.

É importante destacar, nesse contexto, que os controles podem ser agrupados em dimensões abordando três distintos contextos: estrutura, sistema e privacidade.

Na dimensão estrutura são avaliados controles que tratam de aspectos estruturais do sistema (processos e infraestrutura que o sustentam), características

de ambiente que expandem a análise, mas indispensável para identificar o estado atual da segurança e privacidade na organização responsável pelo tratamento de dados pessoais.

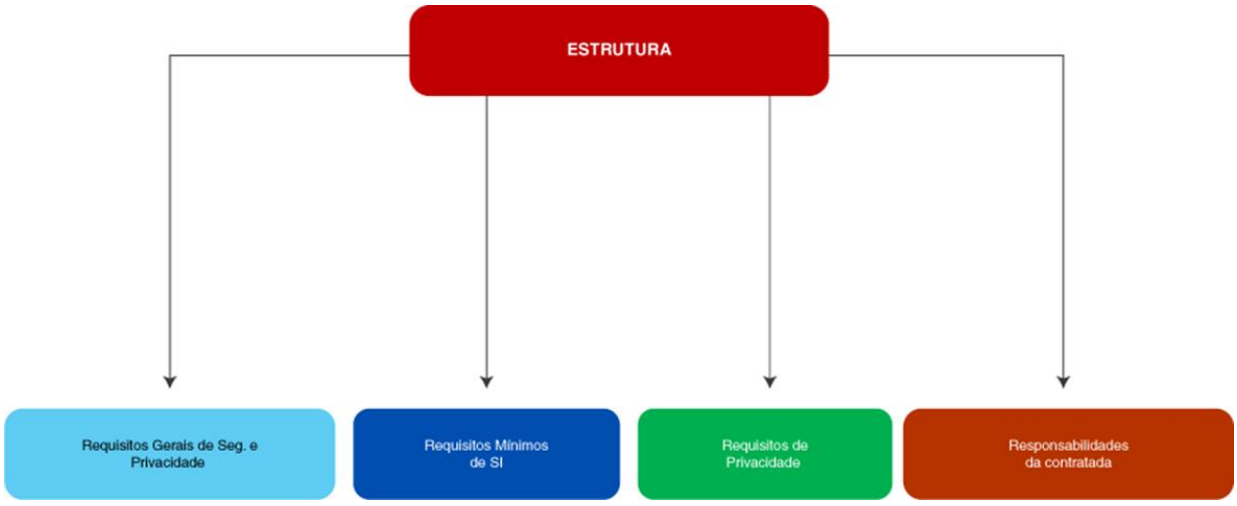
Na dimensão os controles de segurança propostos visam incorporar a segurança da informação durante todo o ciclo de vida do sistema, consequentemente auxiliam a redução da superfície de ataque para vulnerabilidades de sistema, incluindo temas como: desenvolvimento seguro, controles de acesso lógico, segurança web e outros.

Na dimensão privacidade, os controles estão relacionados ao alcance da conformidade legal com a priva- cidade de tratamento de dados pessoais, de forma a permitir que o controlador verifique se os requisitos de adequação à privacidade estão sendo atendidos.

REQUISITOS E OBRIGAÇÕES
SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

- Orienta a adequação do processo de contratação para contemplar os requisitos mais importantes de segurança e privacidade dos dados, conforme Instrução Normativa nº 31, de 23 de março de 2021.

- A Lei Geral de Proteção de Dados Pessoais aborda a implantação de mecanismos de gerenciamento de riscos e análise de impacto na privacidade dos dados pessoais, bem como diversos mecanismos de controle de privacidade.



Destacamos a seguir Requisitos Gerais de Estruturação de Segurança e Privacidade:

- Política de Segurança da Informação (PSIN)
- Análise de Impacto na Privacidade de Dados Pessoais
- Análise e Avaliação de Riscos
- Arquitetura, Controles de Segurança e Matriz de Responsabilidades
- Continuidade Operacional e Contingência
- Gestão de Incidentes
- Coleta e preservação de evidências
- Gestão de Mudanças
- Gestão de Capacidade
- Desenvolvimento Seguro
- Segurança das Redes Corporativas
- Política de Backup

RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS

- Coleta e preservação de evidências;
- Gestão de Mudanças;
- Gestão de Capacidade;
- Desenvolvimento Seguro;
- Segurança das Redes Corporativas;
- Política de Backup.

Nesse contexto, e no que se refere ao conteúdo mínimo que o RIPD deve conter, cumpre destacar o art. 38 da LGPD: “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 da- dos, 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.

É indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais.

A elaboração do RIPD deve compreender as seguintes etapas:

- identificar os agentes de tratamento e o encarregado;
- identificar a necessidade de elaborar o relatório;
- descrever o tratamento;
- identificar partes interessadas consultadas;
- descrever necessidade e proporcionalidade;
- identificar e avaliar os riscos;
- identificar medidas para tratar os riscos;
- aprovar o Relatório;
- manter a revisão.

SEGURANÇA NA WEB

Auxilia os profissionais de desenvolvimento e manutenção de sistemas a atenderem os requisitos de segurança da informação, antes e durante o desenvolvimento da aplicação.

Objetiva auxiliar aos profissionais de desenvolvimento e manutenção de sistemas a atenderem os requisitos de segurança da informação, antes e durante o desenvolvimento da aplicação, utilizando-se da abordagem de desenvolvimento de software e hardware que visa minimizar as vulnerabilidades dos sistemas e reduzir a superfície de ataque em todas as fases do ciclo de vida de desenvolvimento de sistemas (Security by Design).

O Guia de Segurança em Aplicações Web estrutura-se basicamente em requisitos gerais e requisitos específicos.

Requisitos Gerais:

1. Gerenciamento de ambiente
2. Proteção do perímetro da aplicação

Requisitos específicos:

1. Validação dos dados de entrada;
2. Codificação de dados de saída;
3. Autenticação e gerenciamento de credenciais;
4. Gerenciamento de sessões;
5. Controle de acesso;
6. Criptografia;
7. Tratamento de erros e logs;
8. Proteção de dados;

9. Segurança nas comunicações;

10. Configuração do sistema;

11. Segurança em Banco de Dados;

12. Gerenciamento de Arquivos;

13. Gerenciamento de memória;

14. Práticas Gerais de Codificação.

No que se refere ao requisito Proteção de Dados, a aplicação deve proteger os dados tratados por ela, de forma que o acesso às suas informações se restrinja ao mínimo necessário (política de privilégio mínimo, restringindo aos usuários apenas às funcionalidades, dados e informações do sistema que são necessárias para executarem suas tarefas).

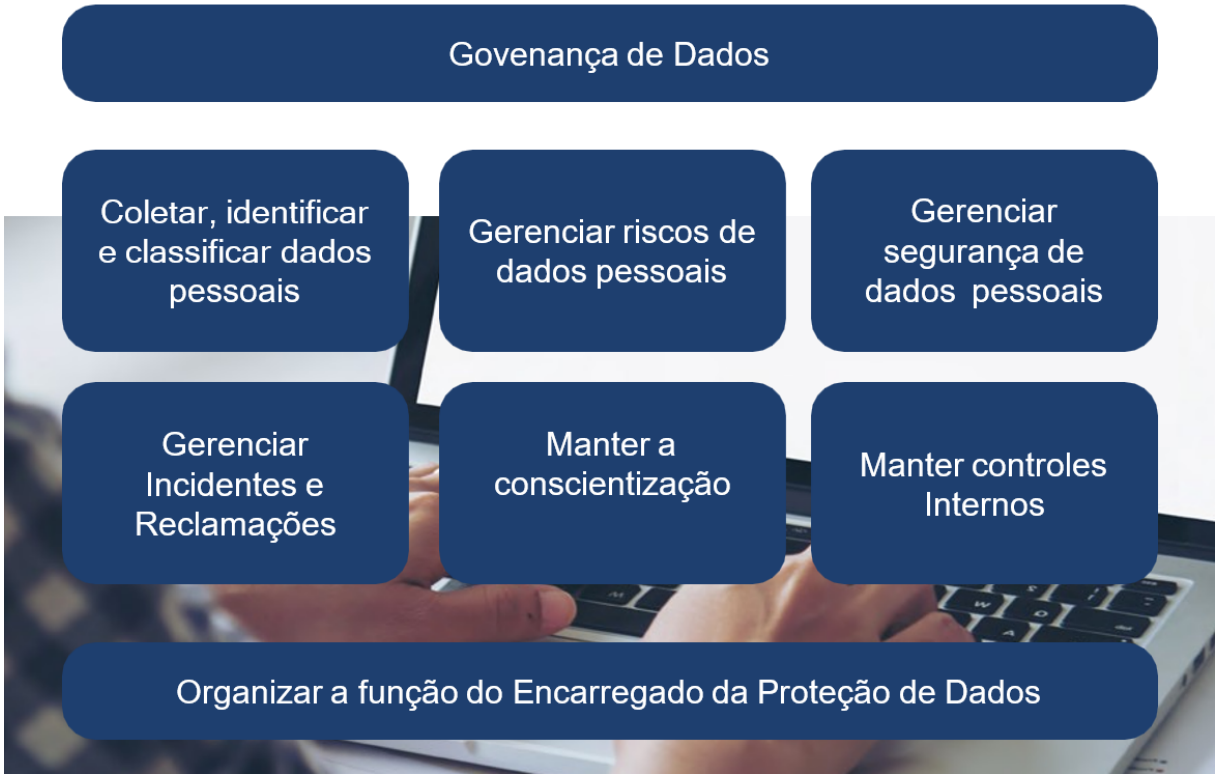
Deve-se ainda adotar controles de segurança ao armazenar as informações para garantir que os dados necessários sejam criptografados (criptografar informações altamente sensíveis quando armazenadas – como dados de verificação de autenticação – mesmo que estejam no lado servidor, usando sempre algorit- mos conhecidos, padronizados e bem testados).

FRAMEWORK DE SEGURANÇA

Fornece aos profissionais de segurança da informação uma maneira de iniciar a identificação, o acompanhamento e o preenchimento das lacunas de segurança presentes na instituição com um conjunto de ações priorizadas que atuam coletivamente na defesa de sistemas e infraestrutura, por meio das melhores práticas para mitigar os tipos mais comuns de ataques.

O processo de proteção de dados pessoais deve estar alinhado com os procedimentos operacionais, segurança da informação, normas de governança, definindo as finalidades, limitações e controles.

É também oportuno promover mecanismos que garantam a proteção de dados pessoais e de dados pessoais sensível, a exemplo do disposto do que a LGPD (art. 6º, XI) conceitua como anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.



Ao tratar de dados pessoais a instituição deve promover a governança de forma a agir conforme os requisitos da LGPD.

Seus processos devem possibilitar que todos os envolvidos contem com um conjunto claramente definido de princípios, políticas e procedimento que estabeleçam a forma como os dados pessoais possam ser tratados e processados, passando por:

1. Estabelecer framework de proteção de dados pessoais;

2. Realizar a gestão do registro de processamento;

3. O estabelecimento de regras para consentimento;

4. A gestão de solicitações e de reclamações de dados pessoais; e

5. Garantia de Gestão imparcial.

Neste momento deve-se proceder a coleta, gerenciamento e controle dos novos dados pessoais, identificando os já existentes para classificar de acordo com a LGPD e com o princípio da minimização de dados.

Os dados pessoais devem ser qualificados em níveis de classificação, analisando o nível de proteção em segurança da informação garantindo que os dados pessoais sejam corretamente reconhecidos e tratados

Todos os dados pessoais existentes (funcionários, ex-funcionários e terceiros) devem ser devidamente identificados e documentados, englobando ativos de informação existentes e os dados pessoais recém coletados.

Os dados pessoais sensíveis devem ser tratados com mais cautela de forma que seu processamento seja legítimo e justificado.

O processo de proteção de dados pessoais deve estar alinhado com os procedimentos operacionais de segurança da informação e normas de governança, definindo as finalidades, limitações e controles.

Os dados pessoais devem ser gerenciados usando um ciclo de vida relacionado com a classificação do dado, desde a coleta inicial até o arquivamento e eliminação.

Nesse sentido, seus subprocessos devem:

1. Realizar Avaliação de Riscos;

2. Conduzir Avaliação de Impacto da Proteção de Dados;

3. Gerenciar o Tratamento de Risco; e

4. Realizar a Validação de Risco.

Gerenciar Segurança de Dados Pessoais

Os dados pessoais devem ser qualificados em níveis de classificação, analisando o nível de proteção em segurança da informação, buscando garantir que os dados pessoais sejam corretamente reconhecidos e tratados de acordo com a LGPD.

Com isso deve-se buscar gerenciar:

1. O anonimato;
2. A criptografia;
3. Os níveis de proteção
4. Recuperação dos dados;
5. Os acessos; e
6. Testes e a maturidade da segurança.

Gerenciar Incidentes e Reclamações

Quaisquer incidentes ou violações relacionadas a dados pessoais devem ser informados, de acordo com a LGPD, para a Autoridade Nacional de Proteção de Dados e aos titulares dos dados, sejam eles reais ou potencialmente afetados por sua violação.

Assim, deve-se gerenciar:

As Notificações;

A comunicação de dados pessoais;

Crises; e

As reinvindicações, reclamações e evidências.

Manter a Conscientização

A proteção de dados e a privacidade devem ser tratados como valores fundamentais da instituição e para tanto exigem conhecimento e informações contínuas sobre Proteção de Dados Pessoais. Seu processo dá suporte a todos os outros processos, explicando, comunicando e reforçando os requisitos da LGPD.

O processo de conscientização inclui educação, treinamento, engajamento e elementos de qualificação para garantir que a instituição tenha os conjuntos de habilidades necessários, devendo para atingir seus objetivos:

1. Manter a conscientização em toda a instituição;

2. Gerenciar educação e habilidades; e

3. Gerenciar treinamentos

Manter Controles Internos

A LGPD exige um conjunto abrangente de controles que garanta a conformidade no tratamento de dados pessoais, fazendo com que seu processamento esteja alinhado com o sistema geral de controles internos da instituição.

Para atingir esse objetivo é necessário:

1. Manter controles de coleta de dados;

2. Manter Controles de Processamento;

3. Manter controles de armazenamento de dados;

4. Manter controles de exclusão;

5. Manter controles de monitoramento; e

6. Realizar revisão da qualidade.

A LGPD determina a designação de um encarregado de proteção de dados. Assim, é necessária a organização de um processo para garantir que este encarregado realize tarefas regulares e interaja com outras partes da instituição. Ao fazer isso, deve garantir ainda a conformidade com leis e regulamentos, estruturado e bem-organizado. Este processo deve englobar os seguintes subprocessos:

1. Manter a Função do DPO;
2. Gerenciar Orçamento e Recursos;
3. Gerenciar Interfaces Organizacionais;
4. Gerenciar Relatórios; e
5. Gerenciar Serviços Externos

DISPOSIÇÕES FINAIS

Compete à Secretaria Municipal de Ciência e Tecnologia a elaboração de normas técnicas, diretrizes, estudos, análises e pareceres que visem atender a esta à legislação vigente, bem como acatar todas as orientações da Autoridade Nacional de Proteção de Dados (ANPD).

Para a efetivação deste plano a administração pública municipal deverá observar dentre as suas obrigações:

I - publicidade das informações relativas ao tratamento de dados em veículos de fácil acesso, preferencialmente nas páginas dos órgãos e entidades na internet, bem como no Portal da Transparência;

II - atendimento das exigências que vierem a ser estabelecidas pela Autoridade Nacional de Proteção de Dados, nos termos do art. 23, § 1º, e do art. 27, parágrafo único da Lei Federal nº 13.709, de 2018;

III - manutenção de dados em formato interoperável e estruturado para o uso compartilhado de dados com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

REFERENCIAL TEÓRICO / EMBASAMENTO

- Plano de adequação à LGPD da Advocacia Geral da União