CONTROLADORIA GERAL DO ESTADO DE RONDÔNIA

PLANO DE AÇÃO PARA ADEQUAÇÃO À LGPD

EXERCÍCIO DE 2021

CONTROLADOR-GERAL DO ESTADO

Francisco Lopes Fernandes Netto

COORDENADOR TÉCNICO

Rodrigo Cesar Silva Moreira

EQUIPE TÉCNICA DE ELABORAÇÃO

Comissão Multidisciplinar de Implementação e Adequação da Lei Geral de Proteção de Dados Pessoais

Ádrian Breno Cavalcante do Nascimento

Alan Negri Feitosa

Alessandra Nunes Silva

Cíntia da Silva Rodrigues Costa

Fagna da Silva Paiva

Franklin Ribeiro

Henrique Ferreira Guimarães

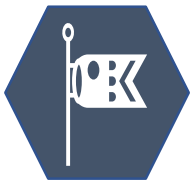
Jeferson Leal Maia

Juscélia Nunes dos Santos

Pablo Jean Vivan

Rodrigo Cesar Silva Moreira

Ronaldo Aparecido Avanzi



MISSÃO

Zelar pela adequada aplicação dos recursos públicos com transparência, publicidade e participação social, fortalecendo o combate à corrupção.

VISÃO

Ser reconhecida como órgão efetivo de controle dos recursos públicos e de defesa dos interesses da sociedade.

VALORES

Comprometimento com o serviço público
Transparência e Credibilidade
Ética
Humanização
Participação Social
Foco no Cidadão
Valorização dos Servidores

SUMÁRIO

1. CAPÍTULO 1: CONTEXTUALIZAÇÃO DA LGPD NO ÂMBITO DA CGE

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) dispõe sobre o tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica, de direito público ou privado, abrangendo inclusive o tratamento realizado nos meios digitais, e tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

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

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

Destarte, a Controladoria Geral do Estado (CGE), como parte integrante da administração pública do Estado de Rondônia, visando se adaptar às diretrizes e às exigências da LGPD, agindo com responsabilidade e transparência, apresenta o presente Plano de Ação para Adequação à LGPD. Este Plano tem por objetivo descrever o conjunto das principais ações voltadas para alcançar a conformidade com a LGPD.

2. CAPÍTULO 2: OBJETIVOS DO PLANO DE AÇÃO

2.1. OBJETIVOS GERAIS

- Implementar a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito da Controladoria Geral do Estado de Rondônia;
- Implantar as diretrizes estratégicas e operacionais da LGPD nos processos da instituição;
- Conscientizar o órgão para garantir a proteção da privacidade de dados pessoais tratados na CGE/RO;
- Atender aos direitos dos titulares de dados.

2.2. OBJETIVOS ESPECÍFICOS

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

3. CAPÍTULO 3: GESTÃO DOS STAKEHOLDERS

O conceito de *stakeholder*, criado em 1984 pelo filósofo norte-americano Robert Edward Freeman, engloba qualquer indivíduo ou ente que, de alguma forma, é afetado pelas ações de uma organização. Em tradução livre para o português, o termo significa parte interessada. A Teoria dos *Stakeholders* considera que a empresa deve coordenar o interesse dos diversos públicos interessados, e vê as organizações como uma coleção de grupos cujos objetivos devem ser coordenados pelos gestores (Freeman, 1984). Nesse sentido, "a compreensão mais abrangente e ambiciosa do conceito de stakeholder representa uma redefinição das organizações e de como devem ser conceituadas" (Freeman & Phillips, 2002, p. 1).

Designar o encarregado pelo tratamento de dados, a rastreabilidade do tratamento de dados, a forma de atender as demandas dos titulares dos dados e a comunicação com a Autoridade Nacional. Sumariamente, a LGPD visa atender a uma das mais recentes demandas da sociedade digital, a proteção de dados, alinhada aos pressupostos do maior engajamento dos *stakeholders* no papel a ser desempenhado pelas organizações. As organizações estão se adequando à nova sociedade, sendo impactadas e impactando as novas relações impostas pelos avanços tecnológicos.

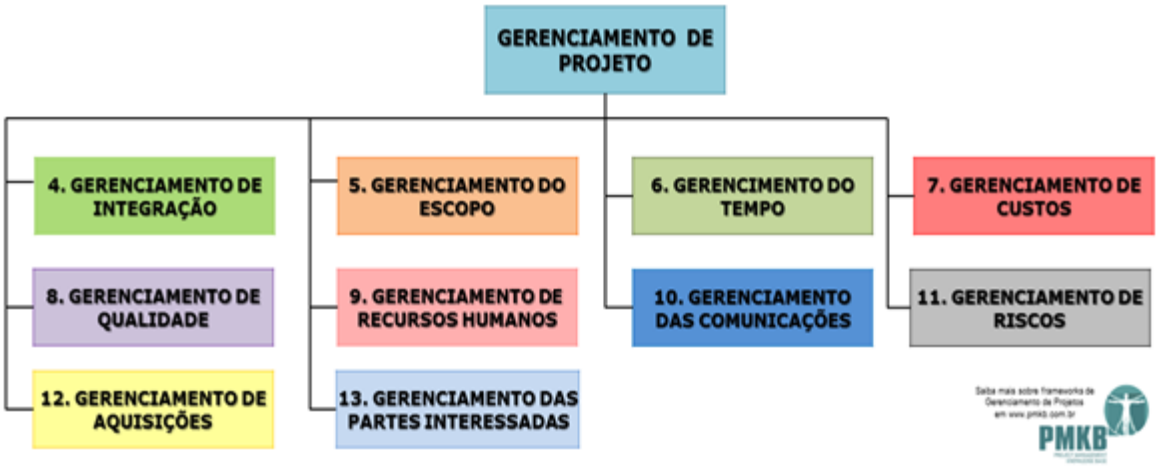
Para o sucesso do presente Plano de Ação, é necessário o envolvimento de todos as partes interessadas: apoio da alta administração; comprometimento das unidades e gerências da CGE; empenho da Comissão Multidisciplinar de Implementação e Adequação da Lei Geral de Proteção de Dados; e interesse de todos os atores envolvidos.

4. CAPÍTULO 4: METODOLOGIA DE ELABORAÇÃO DO PLANO DE AÇÃO

Para a elaboração do Plano de Ação para implementação e adequação da LGPD no âmbito da Controladoria Geral do Estado de Rondônia, foi publicada a **Portaria nº 104 de 07 de junho de 2021.** Essa portaria possui entre seus membros representantes de todos os setores da CGE-RO, desde o gabinete, passando pela gerência técnica e setor administrativo e financeiro.

Essa composição da comissão visou trazer para o processo de implementação e adequação à LGPD uma discussão multidisciplinar, além de abranger a pluralidade de visões técnicas e operacionais do processo de armazenamento, tratamento e utilização das informações públicas.

Por se tratar de um projeto cujo produto final é a implementação e a adequação de sua gestão, utilizou-se como metodologia o **Guia PMBOK** *Project Management Body of Knowledge*, que pode ser traduzido como o Conjunto de Conhecimentos em Gerenciamento de Projetos, desenvolvido pelo *Project Management Institute* (**PMI**). Em seu ciclo de gerenciamento são definidas entradas, ferramentas, técnicas e saídas para o produto do projeto.



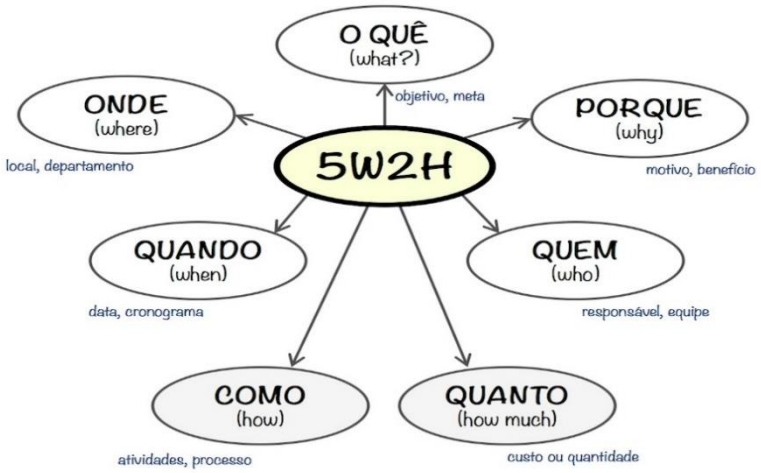
Fonte: *https://pmkb.com.br/sig/padroes-frameworks/pmbok-pmi/*

As áreas de conhecimento do Guia PMBOK utilizadas foram: gestão da integração, gerenciamento do escopo, gerenciamento do cronograma, gerenciamento da qualidade, gerenciamento dos recursos, gerenciamento de comunicações, gerenciamento de riscos e gerenciamento dos *stakeholders*.

O guia também prevê o gerenciamento de custos e de aquisições que ainda não foram tratados na presente fase. Pois, nessa etapa busca-se a formulação do plano de ação para adequação completa da CGE à LGPD e que os custos e

aquisições só podem ser detalhados com maior precisão após a elaboração do diagnóstico, da publicação da política geral de proteção de dados da CGE.

Quanto ao plano de ação em si, em termos de procedimento, utilizou-se, para sua formulação, a ferramenta 5W2H que, nas palavras de Silva *et al*. (2013) atua como suporte estratégico e permite que as informações básicas e mais fundamentais sejam claramente definidas e as ações propostas sejam minuciosamente descritas, porém utilizando linguagem simples.



Fonte: *https://dkvr.wordpress.com/2017/12/13/5w2h-ferramenta-para-elaboracao-de-planos-de-acao-blog-da-iproce*

Para aplicação da ferramenta foram realizadas reuniões para discutir as atividades do plano de ação, bem como seus respectivos produtos e serão realizadas consultas técnicas em forma de entrevistas com profissionais de áreas de conhecimento chave para a qualidade da gestão das informações no âmbito da LGPD, definidas atividades, ações e produtos, foi realizada nova rodada de encontros para montagem da estrutura analítica do projeto, distribuição das tarefas, definição de responsáveis, cronogramas e prazos.

Após essas etapas construiu-se o documento formal do Plano de Ação seguindo o modelo proposto pela Resolução nº 228/2016/TCE-RO e Resolução nº. 260/2018/TCE-RO em termos de estrutura mínima somando com as especificidades estabelecidas pela iniciativa.

5. CAPÍTULO 5: FASE 1 – DIAGNÓSTICO E CONSCIENTIZAÇÃO

5.1. COMPOSIÇÃO DA EQUIPE DE PLANEJAMENTO

Para elaborar o plano de adequação à LGPD, é necessário o engajamento das principais áreas da instituição, cujas lideranças devem compor a equipe de planejamento, implementação e monitoramento das atividades a serem desenvolvidas.

Neste contexto, a CGE instituiu, por meio da Portaria nº 104 de 07 de junho de 2021, a **Comissão Multidisciplinar de Implementação e Adequação da Lei Geral de Proteção de Dados**, no âmbito Controladoria Geral do Estado de Rondônia, com objetivo de definir e implementar estratégias de atuação preventiva nas frentes de segurança da informação e privacidade de dados, bem como fomentar a cultura de proteção de dados visando sobretudo avançar no processo de adequação da CGE à LGPD.

Em vista da estrutura limitada da CGE, em primeira análise foram definidas apenas as áreas estratégicas para possuírem representantes na **Comissão Multidisciplinar** juntamente com o encarregado de dados nomeado por meio da Portaria nº 103, de 07 de junho de 2021, que são: Diretoria Executiva – DIREX, Assessoria de Tecnologia da Informação, Transparência e Prevenção da Corrupção – ASTIPC, Gerência Administrativa e Financeira – GAF, Gerência de Análise e Certificação de Contas – GACC, Gerência de Fiscalização e Auditoria Interna – GFAI, Gerência de Gestão de Risco e Monitoramento – GGRM, reunindo assim, as principais lideranças responsáveis por atividades de tratamento de dados pessoais relevantes da instituição.

A Comissão Multidisciplinar foi constituída com competências para elaboração e execução de todas as etapas do presente plano de adequação da CGE às regras da LGPD, bem como para apresentar o programa de Governança em Privacidade de dados, e prestar apoio direto ao encarregado de dados.

De acordo com inciso III, do art. 23 da LGPD, o Encarregado de dados ou DPO é figura de natureza obrigatória em instituições públicas, que deve estar envolvido em todas as questões de proteção de dados pessoais da instituição, deve contar com suporte e acesso a recursos adequados para cumprir suas funções e manter suas habilidades e conhecimentos técnicos.

Nos termos da LGPD, as principais atribuições do Encarregado são:

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

b) receber comunicações da autoridade nacional e adotar providências;

c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Posto que a CGE possui uma estrutura administrativa limitada, ressalta-se que a LGPD estabelece que a Autoridade Nacional de Proteção de Dados – ANPD – poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, e as melhores práticas internacionais indicam que o encarregado pode assumir um papel mais central no apoio à conformidade do controlador representado.

O Encarregado pelo Tratamento de Dados da Controladoria Geral do Estado, além das atribuições definidas pela Portaria nº 103 de 07 de junho de 2021, será responsável por:

e) monitorar a conformidade à LGPD, incluindo o gerenciamento de atividades internas de proteção de dados pessoais, treinamento de pessoal e realização de pareceres internos; e

f) elaborar/fornecer aconselhamento sobre o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) e monitorar o seu desempenho.

Os demais membros da Comissão multidisciplinar irão auxiliá-lo a realizar suas atividades, assim como outras tarefas essenciais para a correta implementação do plano de adequação da Controladoria Geral à LGPD.

5.2. DIAGNÓSTICO INICIAL DA CGE PERANTE A LGPD

A adequação da CGE à Lei Geral de Proteção de Dados, assim como em outras instituições, envolve, dentre outros, uma mudança cultural que deve atingir todos os níveis da entidade, desde o estratégico até o operacional, o que exige a conscientização dos servidores, no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas, bem como a reflexão sobre a privacidade dos dados pessoais em todas as fases que envolvem seu tratamento.

Nesse sentido, é essencial a realização de um diagnóstico da cultura organizacional com objetivo de mensurar o nível de percepção dos servidores em relação à LGPD, possibilitando a identificação da necessidade de ampliação da conscientização dos agentes públicos em relação ao assunto.

Na CGE, essa avaliação será realizada de forma ampla, com participação do maior número possível de servidores, por meio de pesquisa/questionário cujas respostas possam ser espontâneas e/ou parametrizadas.

Tão importante quanto o diagnóstico cultural em relação à proteção de dados é a apuração do diagnóstico do grau de maturidade de conformidade da unidade à LGPD, este tem o condão de calcular um índice que identifica o estágio de conformidade em que a

unidade se encontra, com vistas a fornecer as informações necessárias à adequação, e o emprego de ações direcionadas e precisas na busca pela conformidade.

Para o diagnóstico do grau de conformidade, a CGE utilizará a ferramenta de Diagnóstico de Adequação à LGPD do Governo Federal, cuja metodologia é baseada em questões formuladas acompanhadas de referências legais e ou normativas e pode ser respondida com as opções "Não adota", "Iniciou plano para adotar", "Adota parcialmente" e "Adota Integralmente", o que subsidia a formalização e cálculo de um índice de maturidade e seu nível de adequação correspondente, conforme tabela abaixo:

Indíce	Nível de Adequação
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Fonte: Governo Federal https://limesurvey.sgd.nuvem.gov.br/index.php/798411?lang=pt-BR

Ressalta-se que essas avaliações serão realizadas de forma periódica, com a finalidade de acompanhar a evolução e a necessidade de eventuais melhorias, fundamentais à governança do tratamento de dados.

5.3. PLANO DE CONSCIENTIZAÇÃO E ENGAJAMENTO DOS STAKEHOLDERS

É imprescindível que todos os stakeholders conheçam as regras estabelecidas na LGPD, particularmente aqueles que tratam diretamente os dados pessoais. Esse alinhamento garante que todos estejam a par das mudanças, afastando eventuais irregularidades.

Nesse contexto, é importante o desenvolvimento de ações de conscientização interna que envolvem o uso de ferramentas para propagação de conhecimentos acerca das regras a serem observadas nas atividades que implicam tratamento de dados pessoais no âmbito da CGE e por seus parceiros.

Como é cediço que colaboradores das diversas unidades internas são quem executarão as atividades diárias, esses precisam estar envolvidos com o tema, para isso serão realizadas campanhas de conscientização visando criar e disseminar uma cultura de proteção de dados aos servidores da CGE e estabelecer tal postura perante os demais parceiros.

Métodos de publicidade e disseminação de conhecimentos podem variar, desse modo a campanha de conscientização deve contemplar a promoção de palestras,

workshops e treinamentos presenciais, *e-learning*, reuniões de equipes, pôsteres, *slogan*, bem como orientações por meio de redes interna e grupos de aplicativos.

Importante destacar que as atividades de conscientização devem ser mantidas durante todo o processo de planejamento, execução e monitoramento do Plano de adequação da CGE à LGPD para desenvolver continuamente a cultura da privacidade, mostrando a importância da LGPD e sua aplicabilidade prática, alcançando uma cultura de segurança da informação e privacidade de dados (*privacy by design e privacy by default*), dentro da instituição.

6. CAPÍTULO 6: FASE 2 – PROPOSIÇÃO DA POLÍTICA GERAL DE PROTEÇÃO DE DADOS DA CGE

A Política de Privacidade tem por objetivo estabelecer as diretrizes da CGE para resguardo e uso de dados pessoais que venham a ser tratados em suas atividades e aplicações (sítios, sistemas ou aplicativos para dispositivos móveis), tendo como referência a Lei Geral de Proteção de Dados Pessoais, entre outras normas nacionais e internacionais relativas à privacidade e proteção de dados pessoais, com especial atenção à *General Data Protection Regulation* e a ISO/IEC 27001.

A Política de Privacidade de Dados é um documento endereçado ao usuário, esclarece papéis e responsabilidades, a forma, os processos e os procedimentos adotados no tratamento dos dados pessoais e as medidas de privacidade empregadas, e busca atender aos princípios da transparência, do livre acesso e da prestação de contas previstos na LGPD.

Nesse contexto, em relação ao conteúdo do instrumento, recomenda-se que contenha as seguintes informações:

I- Informação sobre a CGE como entidade responsável pelo tratamento;

II- Especificar os dados pessoais tratados e respectivas finalidades do tratamento, incluindo-se dados não informados pelo usuário (exemplo: IP, localização, etc.), quando aplicável;

III- Fundamento legal do tratamento;

IV- Prazo de retenção dos dados pessoais;

V- Informações de contato do encarregado de proteção de dados;

VI- Canais de atendimento ao titular e a forma como são atendidos os direitos do titular, informando como ele pode acessar, retificar, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento, e retirar o consentimento;

VII- Informações quanto à existência de compartilhamento de dados com terceiros e qual a finalidade (quando aplicável);

VIII- Se há transferência internacional de dados (quando aplicável);

IX- Proteção de dados de menores de idade, se for o caso;

X- Proteção de dados sensíveis.

Quanto à validação da política de privacidade e proteção de dados da CGE, recomenda-se que, antes da publicação, esta seja submetida à revisão por parte da equipe técnica da Assessoria de Tecnologia da informação e Diretoria Executiva.

6.1. DA DIVULGAÇÃO DA POLÍTICA GERAL DE PRIVACIDADE E PROTEÇÃO DE DADOS DA CGE

É importante garantir a divulgação e conscientização organizacional da política de privacidade de dados. Assim, após a publicação do instrumento, orienta-se o compartilhamento com todo corpo funcional da CGE, utilizando-se os meios de conscientização definidos no item 5.3, disponibilizando-a em linguagem apropriada, clara e precisa para melhor entendimento do seu público-alvo.

De igual forma, a Política de Privacidade de dados deverá ser disponibilizada ao usuário no site da CGE na área destinada ao tema LGPD.

7. CAPÍTULO 7: FASE 3 – ESTRUTURAÇÃO E ESTRATÉGIA PARA IMPLEMENTAÇÃO DA PGPD-CGE

7.1. ELABORAÇÃO DA MATRIZ DE PRAZOS E RESPONSABILIDADES

Com fito de desenvolver o Plano de Adequação, a participação de diversos atores é necessária em cada etapa do processo com a finalidade de engajar e priorizar as ações que se mostrarem mais relevantes para o atingimento dos objetivos.

Assim, tendo em vista o volume e a complexidade, além das limitações inerentes aos órgãos públicos e obediência aos princípios e normas que regem a Administração Pública, torna-se fundamental a cristalina divisão de competências.

Com efeito, o quadro abaixo apresenta os atores engajados no processo de elaboração do Plano de Adequação:

Quadro 1: Atores e suas responsabilidades na elaboração do Plano de Adequação da LGPD na CGE

Atores	Responsabilidades
Controlador	Adequação da CGE à LGPD, além de priorizar as ações e auxiliar as equipes.
Operadores	Inventariar os dados e adequar os processos pelos quais são responsáveis pelo tratamento à LGPD.
Encarregado	Intermediar a comunicação entre a CGE e a ANPD, além dos titulares dos dados.
Comissão CGE	Propor e dar encaminhamento à execução de medidas para adequação à LGPD.

Fonte: *Elaboração própria*.

Como metodologia de visualização das responsabilidades e prazos, de modo a dar transparências na distribuição das atividades, sugere-se que seja utilizada a Matriz RACI, que significa: R (responsabilidade), A (Aprovador), C (Consultado), I (Informado).

Responsável: Grupo de pessoas ou indivíduo responsável pela execução, pelo desenvolvimento, pela conclusão e pela entrega da atividade;

Aprovador: Parte que tem autoridade para organizar tarefas, acompanhar seu desenvolvimento e aceitar ou recusar formalmente uma entrega;

Consultado: Especialista ou pessoa que detém informações essenciais para a execução das ações;

Informado: Quaisquer pessoas que devem ser comunicadas sobre o progresso das ações.

7.2. LEVANTAMENTO DE SISTEMAS E OPERAÇÕES QUE ENVOLVAM PROTEÇÃO DE DADOS

Para fins de identificar a atual maturidade da CGE em relação à proteção de dados, revela-se necessária a realização de diagnóstico acerca do rol de soluções tecnológicas responsáveis pela produção, compartilhamento e retenção de dados passíveis de tratamento.

Dessa forma, as seguintes informações apresentam-se como preferenciais a compor o levantamento:

I- Nome do Sistema/Ferramenta/Solução Tecnológica;

II- Finalidade;

III- Meio de Acesso;

IV- Pessoas que fazem parte do tratamento;

V- Fonte de dados;

VI- Gestor responsável e contato;

VII- Analista responsável e contato;

VIII- Tipos de dados pessoais coletados;

IX- Forma de coleta;

X- Previsão legal do tratamento;

XI- Processos relacionados;

XII- Compartilhamento;

XIII- Retenção/armazenamento.

Salienta-se que, inicialmente, não serão incluídos processos físicos e sistemas sujeitos a regulamentação e/ou controle de outros controladores, por exemplo, o sistema de folha de pagamento e o sistema de viagens e diárias.

7.3. PROPOSIÇÃO DE TOOLKIT

Preliminarmente, cumpre destacar que não há metodologia para a realização do inventário de dados, documentos de trabalho, produção de relatório de impacto e plano de respostas, sendo necessário a busca de boas práticas em organizações públicas ou privadas com intuito de adequá-los às especificidades da CGE.

Assim, com intuito de adequar a CGE à LGPD poderá ser encaminhado aos setores responsáveis pelo tratamento de dados alguns formulários para alimentação, com o objetivo de dar uniformidade e celeridade às informações necessárias para a avaliação da Comissão Multidisciplinar e consequente adoção de providências.

7.4. ELABORAÇÃO DO PLANO DE ADEQUAÇÃO

Para cumprimento desta fase, os membros designados por meio da Portaria nº 104, de 07 de junho de 2021, devem participar de capacitações, realizar pesquisas e reuniões de modo a melhor planejar e decidir as ações a serem implementadas.

As ações que forem elencadas para execução serão produto de levantamento realizado por cada setor da CGE, por meio de planilha ou formulário, de modo a selecionar os objetos mais prioritários.

Com efeito, após a realização do levantamento, as ações deverão ser validadas pela Comissão para servir de insumo ao Plano de Adequação.

7.5. GESTÃO DE RISCOS

Ulterior à fase de inventário, será iniciado o estágio da gestão de riscos cujo objetivo é a avaliação das informações do inventário, identificando as lacunas de segurança da informação e de privacidade sobre os sistemas, demonstrando, aos setores do processo e tomadores de decisão, onde se encontram os riscos dos processos priorizados e o impacto dimensionado, com ações propostas de mitigação destes.

Dessa forma, serão identificados os riscos inerentes à CGE e a proposição de medidas mitigadoras.

8. CAPÍTULO 8: DEFINIÇÃO DOS PRODUTOS

8.1. PUBLICAÇÃO DA POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS DA CGE

A Política de Privacidade tem como objetivo descrever ao usuário o método, os processos e os procedimentos adotados no tratamento de dados pessoais pelo serviço e informá-lo sobre as medidas de privacidade empregadas.

Para isso, o serviço deve informar ao titular do dado como é assegurada a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares dos dados seja garantida de forma eficiente.

Sendo assim, a Política de Privacidade e Proteção de Dados da CGE será disponibilizada conforme o item 6.1.

8.2. ELABORAÇÃO DO 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. Caso o Termo de Uso seja aceito pelo usuário, a utilização do serviço será vinculada às cláusulas dispostas nele.

O Termo de Uso origina-se da responsabilidade de os agentes de tratamento de dados serem transparentes no relacionamento com o titular de dados e informem como as atividades de tratamento de dados atendem aos princípios dispostos no artigo 6º da Lei Geral de Proteção de Dados Pessoais (LGPD). Portanto, o documento constitui, ao mesmo tempo, um dever do controlador e um direito do titular.

Em se tratando da elaboração do Termo de Uso da CGE, será utilizado por base o "Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos", Versão 1.1, de 08 de junho de 2021, do Governo Federal ou versão mais atual, caso seja publicada, no qual consta os tópicos a serem inseridos no referido Termo, em que cada tópico contém uma descrição e um campo com as informações que devem constar em cada um deles. Os tópicos apresentam referências ao Guia de Boas Práticas da LGPD, elaborado pelo Comitê Central de Governança de Dados, instituído pelo Decreto 10.046, de 9 de outubro de 2019, de modo a ajudar na compreensão e aprofundamento dos temas tratados.

Ressaltando que não é obrigatória a elaboração do Termo estritamente conforme o referido Guia, visto que cada Entidade tem suas especificidades, portanto, o Guia serve de orientação na elaboração do Termo do Uso.

8.3. PUBLICAÇÃO DO PLANO DE ADEQUAÇÃO À LGPD

O Plano de Adequação à LGPD da Controladoria Geral do Estado tem como objetivo adequar os principais processos e tecnologias à LGPD, bem como conscientizar

todo o órgão para garantir a privacidade de dados pessoais tratados na Controladoria e em nome desta.

Quanto à publicação do Plano de Adequação à LGPD, o mesmo será disponibilizado no site oficial da CGE, bem como no portal da transparência, na área referente à LGPD, dando amplo conhecimento a todos os s*takeholders*.

8.4. INVENTÁRIO DE DADOS PESSOAIS – IDP

O Inventário de Dados Pessoais – IDP consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição (LGPD. Art. 37). Refere-se a um documento essencial quando se está no processo de adequação às normas de proteção de dados.

De uma forma geral, esse registro mantido pelo IDP envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade como:

a) atores envolvidos (agentes de tratamento e o encarregado);
b) finalidade (o que a instituição faz com o dado pessoal);
c) hipótese (arts. 7º e 11 da LGPD);
d) Previsão legal;
e) Dados pessoais tratados pela instituição;
f) Categoria dos titulares dos dados pessoais;
g) Tempo de retenção dos dados pessoais;
h) Instituições com as quais os dados pessoais são compartilhados;
i) Transferência internacional de dados (art. 33 LGPD); e
j) Medidas de segurança atualmente adotadas.

Desta feita, a CGE elaborará o IDP com base no "Guia de Elaboração de Inventário de Dados Pessoais", versão 2.0, de 26 de abril de 2021, elaborado pelo Governo Federal, ou versão mais atual.

O referido Guia apresenta a estrutura do IDP que é inspirado nos modelos propostos pelas autoridades de proteção de dados da França, Bélgica e Inglaterra.

Na elaboração dos formulários do IDP da CGE, serão utilizados os *Templates* disponibilizados pelo Governo Federal (disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd), com as devidas adaptações à realidade da própria CGE, visto que o modelo proposto pelo Guia não é obrigatório.

8.5. PLANO DE CONTINGÊNCIA A INCIDENTES

Plano de Contingência a Incidentes é o processo que descreve como uma organização deverá lidar com um incidente de segurança de TI, seja ele um ataque cibernético, uma violação de dados, a presença de um aplicativo malicioso (como um vírus), uma violação das políticas e padrões de segurança do órgão, dentre outros exemplos. O objetivo é minimizar os danos que poderiam ser causados pelo incidente, reduzir o tempo de ação e os custos de recuperação.

No mais, a própria LGPD é clara no sentido de que:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;
>
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
>
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
>
> I - ampla divulgação do fato em meios de comunicação; e
>
> II - medidas para reverter ou mitigar os efeitos do incidente.
>
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Portanto, faz-se necessária a elaboração de Plano de Contingência a Incidentes, para que a CGE esteja preparada para o caso de "violação da segurança que provoque, de modo acidental ou ilícito a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (definição constante no art. 4º da GDPR), e que seja amplamente divulgada para todos os servidores quanto às medidas que deverão ser adotadas no caso de incidente com segurança de dados pessoais, inclusive, a comunicação apropriada e tempestiva à Autoridade Nacional de Dados Pessoais – ANDP;

O Plano de Respostas a Incidentes deve conter:

a) A definição de incidente para o órgão;
b) Descrição dos procedimentos a serem executados quando um incidente ocorrer;
c) As ferramentas, tecnologias e recursos a serem utilizados em caso de incidentes;
d) Descrição dos colaboradores que fazem parte do processo e quais são suas responsabilidades e ações.

Ou seja, o Plano de Respostas a Incidentes consiste de um documento interno do órgão que deve ser amplamente conhecido por todos os servidores e que disponha sobre as medidas que devem ser tomadas no caso de um incidente de segurança em dados pessoais.

O Plano de Resposta aos Incidentes deve ser implementado com o apoio total de todas as áreas envolvidas, deve ser visto como a maneira essencial de minimizar os danos de qualquer incidente que possa vir a acontecer, de minimizar o tempo de resposta ao incidente e de normalização das operações e, consequentemente, de minimização dos danos em reputação que podem ser causados por um incidente de grande proporção ou não devidamente respondido.

8.6. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

Segundo o inciso XVII, do artigo 5º, da Lei 13.709/2018 (LGPD), o Relatório de Impacto à Proteção de Dados Pessoais - RIPDP 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".

A referida lei também faz menção ao conteúdo mínimo exigido no RIPDP, em seu parágrafo único, do artigo 38, devendo conter 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 importante que o RIPD seja revisto e atualizado anualmente ou quando houver mudança que atinja o tratamento dos dados pessoais realizado pela instituição.

Dessa forma, na elaboração do RIPDP da CGE, será utilizado o modelo disponibilizado pelo Governo Federal, que foi estruturado em formato a ser preenchido por editor de textos. O modelo não é de utilização obrigatória, tratando-se apenas de sugestão e sendo adaptável à realidade de cada entidade.

8.7. MECANISMOS DE TRANSPARÊNCIA

É fato que hoje há diversos mecanismos de transparência, principalmente com o surgimento da *internet*, ao passo que foi promulgada, em 2011, a Lei de Acesso à Informação (12.527/2011), resultando em um grande avanço na transparência pública e participação da sociedade nas atividades do Estado.

Quanto à Lei Geral de Proteção de Dados – LGPD, o grande avanço veio na transparência quanto ao tratamento e proteção de dados pessoais, dispondo a LGPD, em seu Capítulo III, sobre os direitos do titular, assegurando que toda pessoa natural tenha os direitos fundamentais de liberdade, de intimidade e de privacidade garantidos.

A transparência na LGPD nada mais é do que informar ao titular, de forma clara e em momento anterior, a razão pela qual os seus dados estão sendo coletados e tratados, a finalidade e todo o caminho pelo qual o dado irá percorrer ao longo do seu ciclo de vida.

Assim, após a conclusão e implementação do Roteiro para Elaboração do Plano de Ação para Adequação à LGPD da CGE, serão garantidos todos os mecanismos de transparência quanto à finalidade do tratamento, ao tempo de armazenamento, às medidas de segurança que são adotadas para protegê-los e com quem serão compartilhados os dados pessoais.

Com exceção do segredo industrial e comercial, a Lei Geral de Proteção de Dados revela grande importância com o princípio da transparência, o qual está intimamente ligado ao princípio da *accountability*.

9. CAPÍTULO 9: MONITORAMENTO

Mormente, é necessário o monitoramento de forma contínua, visando a implementação dos planos de ação e medidas recomendadas para adequação à LGPD, sendo os seguintes processos recomendados:

1- Diagnosticar o impacto da LGPD na CGE-RO. Desse modo, o diagnostico ocorrerá por meio da avaliação estratégica do impacto da LGPD nas atividades da Controladoria, envolvendo a elaboração de inventário e mapeamento dos dados pessoais que trafegam na instituição, além da identificação dos processos de trabalho e documentos afetados.

2- Identificar as tarefas e atividades principais e secundárias que envolvam tratamento de dados pessoais. Diante do exposto, necessita-se rastrear o ciclo de tratamento de dados pessoais, desde a coleta e exibição, até o descarte em redes sociais, portais de transparência, serviço de informação ao cidadão, entre outros.

3- Identificar normativas internas impactadas pela LGPD (dados pessoais, privacidade e segurança da informação). Nesse sentido, efetuar levantamento das normativas e providenciar adequação.

4- Catalogar oportunidades de melhoria ligadas aos processos, sistemas e normativas. Diante disso, deve-se focar, a princípio, na ocultação de dados a fim afastar a aplicação da LGPD e a redução do uso de dados pessoais nos processos sempre que não houver relação com a finalidade.

5- Adaptar canais de comunicação, políticas, processos e mecanismos de tratamento de dados pessoais com vistas a atender a LGPD. Logo, os canais de comunicação deverão estar aptos a tratar as demandas relativas aos dados pessoais da maneira mais célere e efetiva possível.

6- Avaliar política institucional de segurança da informação com base na LGPD. Portanto, realizar avaliação e, se possível, a adaptação, ainda que mínima, dos instrumentos afetos à segurança da informação no tocante à proteção de dados, fortalecendo e ampliando as políticas existentes.

7- Identificar e tratar riscos relacionados à proteção de dados pessoais, visto que isso fortalece a gestão de riscos já instituída, estabelecendo indicadores relativos à Proteção de Dados.

8- Promover ações de capacitação e sensibilização sobre o tratamento de dados pessoais. Uma vez que tornará servidores, contratados, jurisdicionados e parceiros capacitados quanto aos requisitos de conformidade e de implementação da LGPD.

9- Instituir e divulgar políticas de governança em privacidade. Visando, com isso, promover a aplicação da LGPD, assim como reafirmar a necessidade de proteção dos dados.

10- Correção de processos e erros para garantir a minimização dos dados e a remoção de dados pessoais que não atendem aos critérios de finalidade de processamento. A partir disso, busca-se evitar a incidência de dados que não atendam aos critérios definidos na LGPD.

Além disso, em relação à Gestão das Informações dos Relatórios gerados em função da LGPD, ressalta-se que serão ofertadas às partes interessadas as informações de acordo com o nível de acesso que a parte possuir, sendo separado em informações abertas ao público e informações a indivíduos restritos.

Por fim, as atividades de monitoramento retromencionadas ficam a cargo da Gerência de Gestão de Riscos e Monitoramento – GGRM, a qual acompanhará a execução do plano nos setores da controladoria, tendo por objetivo a mitigação dos riscos relacionados à proteção de dados pessoais e a promoção de melhorias relacionadas à LGPD.

10. CAPÍTULO 10: REVISÃO E APRIMORAMENTO DOS PLANOS E POLÍTICA DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), entrou em vigor em 2020 e por isso as organizações, ainda, estão se adaptando a essa nova realidade.

Em decorrência da rapidez com que os cenários atuais se transformam, a organização deve manter revisão e atualização dos planos e políticas a fim de demonstrar que avalia continuamente os riscos de tratamento de dados pessoais. A conformidade com a LGPD é um trabalho contínuo.

Sendo assim, a Controladoria Geral do Estado revisará e atualizará seus manuais anualmente, no mês de setembro, ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.

Para isso, a Controladoria Geral do Estado contará com o auxílio de todas as gerências, que, impreterivelmente até o mês de junho, elaborarão um relatório contendo as principais dificuldades encontradas para o atendimento da lei supramencionada e encaminharão à Gerência de Gestão de Riscos e Monitoramento - GGRM.

De posse dessas informações, a GGRM coletará as informações prestadas e apresentará, até o mês de agosto de cada ano, ao Controlador-Geral do Estado, as sugestões das providências a serem atualizadas.

O Controlador analisará as sugestões enviadas e publicará, até o final de setembro, a revisão dos procedimentos para o atendimento da LGPD.

11. CAPÍTULO 11: MATRIZ DE PRAZOS E RESPONSABILIDADES

	Ações Planejadas	Setor Responsável	Indicador de Resultado	Prazo
1	Diagnóstico do Cenário da CGE perante a LGPD	**Comissão** de Implementação da LGPD na CGE	Diagnóstico Elaborado	**30** dias
2	Companha de Conscientização e Engajamento dos Stakeholders	**Comissão** de Implementação da LGPD na CGE	Campanha Realizada para todos os colaboradores da CGE	**60** dias
3	Inventário de Dados Pessoais	**Gerências**	Inventário de Dados Pessoais elaborado	**75** dias
4	Publicação da Política de Privacidade e Proteção de Dados da CGE	**Comissão** de Implementação da LGPD na CGE	Publicação da Política de Privacidade e Proteção de Dados	**90** dias
5	Elaboração do Termo de Uso	**Comissão** de Implementação da LGPD na CGE	Termo de Uso elaborado	**90** dias
6	Plano de Contingência a Incidentes	**Comissão** de Implementação da LGPD na CGE	Plano de Contingência a Incidentes elaborado	**120** dias
7	Relatório de Impacto à Proteção de Dados	**Comissão** de Implementação da LGPD na CGE	Relatórios publicados	**120** dias
8	Relatórios de Monitoramento da Implementação da LGPD na CGE	**GGRM/CI**	Relatórios publicados	**150** dias

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: Seção 1, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jul. 2021.

DATA Protection Brasil. *In*: **STAKEHOLDER X LGPD**. 31 out. 2019. Disponível em: https://dataprotectionbrasil.com.br/2019/10/31/stakeholder-x-lgpd/. Acesso em: 14 jul. 2021.

PROJECT MANAGEMENT INSTITUTE (PMI). **Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK)**. Globalstandard, 6ª ed. 2017. ISBN: 978-1-62825-192-0. Disponível em: https://dicasliderancagp.com.br/wp-content/uploads/2018/04/Guia-PMBOK-6%C2%AA-Edi%C3%A7%C3%A30.pdf.

SILVA, A. O da.; RORATTO, L.; SERVAT, M. E.; DORNELAS, L.; POLACINSKI, E. **Gestão da Qualidade: aplicação da ferramenta 5W2H como plano de ação para projeto de abertura de uma empresa**. 3ª SIEF – Semana Internacional das Engenharias da FAHOR. Horizontina, 2013. Disponível em: https://www.fahor.com.br/publicacoes/sief/2013/gestao_de_qualidade.pdf.

BRASIL. *In*: **Ferramenta de diagnóstico de adequação à LGPD do Governo Federal (Secretaria de Governo Digital - SGD)**. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnosticode-adequacao-a-lgpd.