



Governo do Estado de
RONDÔNIA

GUIA DE CONFORMIDADE: Lei Geral de Proteção de Dados Pessoais (LGPD)

Versão 2.0

2023



GUIA DE CONFORMIDADE: LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Versão 2.0 | Jul. 2023

GOVERNO DO ESTADO DE RONDÔNIA

Marcos José Rocha dos Santos
Governador

Sérgio Gonçalves da Silva
Vice-Governador

SUPERINTENDÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - SETIC

Delner Freire
Superintendente

DIRETORIA TÉCNICA DA SETIC

Gabriel Carrijo Bento Teixeira
Diretor Técnico

ELABORAÇÃO

Tiago Lopes de Aguiar
Encarregado pelo Tratamento de Dados Pessoais da SETIC

CAPA

Idan Luiz Souza Santos



EQUIPE DE REVISÃO

Sara Grécia Nogueira

Luzia Martins

Comitê Gestor de Privacidade e Proteção de Dados Pessoais – CGPD do
Governo do Estado de Rondônia

Coordenação do CGPD

Tiago Lopes de Aguiar – Titular

Larissa Ananda Paiva Maciel – Suplente

Membros Titulares – CGPD

Ândria Aparecida dos Santos de Mendonça

Paulla Pollyany Barbosa Sousa

Tiago Lopes de Aguiar

Larissa Ananda Paiva Maciel

Luísa Rocha Carvalho Bentes

Ana Claudia Guarim dos Santos

Magnun Barros Leite

Neuracy da Silva Freitas Rios

Jaime Fernandes da Silva

Maíra Tamires Lujan Rodrigues da Silva

Carlos Augusto Antunes Malty Júnior

Anna Polliana Oliveira Arivabene Coelho

Membros Suplentes – CGPD

Ítalo Raphael Ferreira Reis

Cássio Bruno Castro de Souza

Maria Gabriela dos Santos Galvão

Rodrigo Cesar Silva Moreira

Boniek Bezerra Santos

Sarita Pantoja Pereira

Adeilson Bandeira Silva

Ariane Dias de Almeida

Jones Bonays Barros da Rocha

Wanderlei Ferreira Leite

Paulo Eduardo da Silva de Vasconcelos

Ander Cledioney Reis



HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autoria
07/06/2021	1.0	Primeira versão do Guia de Conformidade: Lei Geral de Proteção de Dados Pessoais (LGPD).	Tiago Lopes de Aguiar
18/07/2023	2.0	Adequação do Guia para abranger todos os órgãos e entidades do Governo do Estado.	Equipe de Revisão



SUMÁRIO

	INTRODUÇÃO	5
1	PECULIARIDADES DO NEGÓCIO	7
1.1	Diagnóstico inicial	8
2	WORKSHOP	10
3	MOBILIZAÇÃO INICIAL	11
3.1	Encarregado pelo Tratamento de Dados Pessoais	12
3.2	Agentes de Tratamento	15
3.3	Comitê Interno de Privacidade e Proteção de Dados Pessoais	16
3.4	Comissão Tática e Operacional	17
3.5	Ampla divulgação	18
3.6	Diagnósticos intermediários	18
4	INVENTÁRIO DE DADOS PESSOAIS	19
5	PARECER DIAGNÓSTICO	21
6	PLANO DE AÇÃO	22
7	EXECUÇÃO	26
	REFERÊNCIAS	27



INTRODUÇÃO

A Lei Federal 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 (pública ou privada), abrangendo inclusive o tratamento realizado nos meios digitais, e tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade bem como o livre desenvolvimento da personalidade da pessoa natural. A LGPD entrou em vigor em 18 de setembro de 2020, à exceção das sanções administrativas, que passaram a ser exigíveis somente a partir de 1º agosto de 2021.

Recentemente, por meio da Emenda Constitucional nº 115/2022, a proteção de dados pessoais passou a pertencer ao rol dos direitos e garantias fundamentais.

No contexto da administração pública, conforme art. 23 da LGPD, o tratamento de dados pessoais deve ser realizado para atender a “finalidade pública, na persecução do interesse público, com objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”. Devem ainda, os órgãos e entidades públicas, informarem as hipóteses em que realizam o tratamento de tais dados, fornecendo informações sobre a previsão legal, finalidade, procedimentos e práticas utilizadas, bem como indicar um encarregado pelo tratamento desses dados. Nesse sentido, a LGPD constitui marco importante para a administração pública, seja municipal, estadual ou federal, pois deve cumprir com suas diretrizes.

Dentre as características da aplicação da LGPD, destaca-se a sua transdisciplinaridade, pois permeia os mais variados órgãos e departamentos na administração pública, cujo tratamento de dados pessoais pode envolver diferentes titulares, desde os próprios servidores até usuários dos serviços públicos.

Dessa forma, objetivando entrar em conformidade às exigências da LGPD, agindo com responsabilidade e transparência, a Superintendência Estadual de Tecnologia da Informação e Comunicação (SETIC), como parte integrante da administração pública do Governo do Estado de Rondônia, apresenta o **“Guia de Conformidade: Lei Geral de Proteção de Dados (LGPD)”**, em sua **segunda edição**, sob a revisão do Comitê Gestor de Privacidade e Proteção de Dados Pessoais - CGPD/RO, procurando adequá-lo à realidade do Poder Executivo Estadual.



Este Guia, elaborado com base em normas de boas práticas, experiências de especialistas na área e guias operacionais do Governo Federal, tem por objetivo descrever o conjunto das principais ações voltadas para alcançar a conformidade com a LGPD, buscando facilitar a difusão do conhecimento para todos os servidores, órgãos e entidades do Governo de Rondônia.

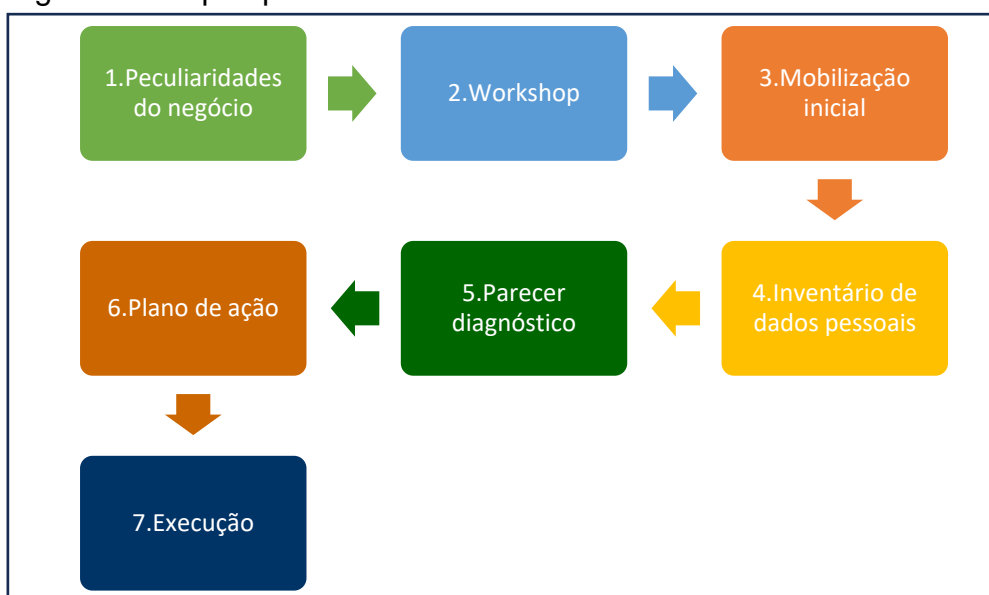
Destaca-se que as orientações aqui contidas poderão ser aplicadas a qualquer órgão ou entidade pública, devendo, entretanto, atentarem-se para possíveis adaptações perante sua realidade.

O conjunto de ações se resume em 7 (sete) etapas, a saber:

1. Conhecer as peculiaridades do negócio;
2. Realizar *workshop* com alta administração, diretoria e coordenadorias das áreas de negócio;
3. Conduzir a mobilização inicial;
4. Inventariar os dados pessoais;
5. Desenvolver parecer diagnóstico;
6. Criar plano de ação; e
7. Executar plano de ação.

A figura abaixo apresenta, de forma sintetizada, cada uma dessas etapas, que serão detalhadas mais adiante.

Figura 1 - Etapas para conformidade com a LGPD.



Fonte: Próprio Autor (2023).



1 PECULIARIDADES DO NEGÓCIO

Inicialmente vale destacar a importância do órgão ou entidade já ter indicado o Encarregado pelo Tratamento de Dados Pessoais (Oficial de Proteção de Dados Pessoais - DPO) para colaborar com a jornada de conformidade ou até conduzi-la. E, dependendo do caso, designar uma equipe para realizar as ações operacionais (**vide item 3.1 e 3.4 deste Guia**).



Essa primeira etapa consiste em conhecer as peculiaridades do órgão ou entidade, elencando suas finalidades e competências, bem como evidenciando sua área de atuação e funcionamento.

Nesse sentido, é importante realizar o levantamento dos seguintes itens:

- normas que tratam de sua organização e estrutura, abrangendo criação, atribuições, competências, funcionamento etc.;
- normas já aprovadas, ou em fase de aprovação, que tratem da temática, tais como política de privacidade, modelo de termo de uso, política de segurança da informação, procedimentos de *backup*, modelos de termos de compromisso, uso de repositórios, uso de mídias sociais, acesso remoto, desenvolvimento seguro de *softwares*, procedimentos de compras e aquisições etc.;
- relação com clientes, usuários do serviço público, parceiros, fornecedores, prestadores de serviço, estagiários etc.;
- contratos, convênios, acordos, termos ou instrumento congêneres que tratem da temática; e
- ações existentes, ou já realizadas, visando a adequação do órgão à LGPD tais como *workshops*, treinamentos, reuniões, nomeação de Encarregado/DPO etc.

Esse levantamento permitirá consolidar as informações iniciais sobre o órgão ou entidade evidenciando sua estrutura, organização e atribuições. De posse de tais



informações, o Encarregado/DPO e a equipe responsável pela adequação, caso tenha sido criada, terão uma melhor compreensão sobre o atual cenário do órgão ou entidade.

1.1 Diagnóstico inicial

O diagnóstico inicial tem por objetivo mensurar o grau de maturidade do órgão ou entidade no que diz respeito à conformidade com a LGPD.

Os dados coletados na 1ª etapa (peculiaridades do negócio) serão muito úteis para o desenvolvimento do diagnóstico inicial, pois será possível identificar as ações já executadas, as que estão em execução e as que deverão ser idealizadas.

Dentre as diversas ferramentas existentes para realizar o diagnóstico de maturidade, recomenda-se o uso da **ferramenta que automatiza a implementação do Framework de Privacidade e Segurança da Informação**¹ desenvolvida pelo Governo Federal, por intermédio da Secretaria de Governo Digital (SGD), do Ministério da Gestão e da Inovação em Serviços Públicos. Trata-se uma ferramenta em formato de planilha eletrônica que conta com o uso de macro, construída em Excel, utilizada para obter e acompanhar indicadores de maturidade em privacidade e em segurança da informação, possibilitando realizar a priorização de ações necessárias para a entrada em conformidade com a LGPD. Os diagnósticos trazem consigo uma tabela contendo os índices de maturidade e seus níveis de adequação, conforme figura abaixo:

Figura 2 – Índices de adequação à LGPD.

Índice	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: Secretaria de Governo Digital – SGD (2023).

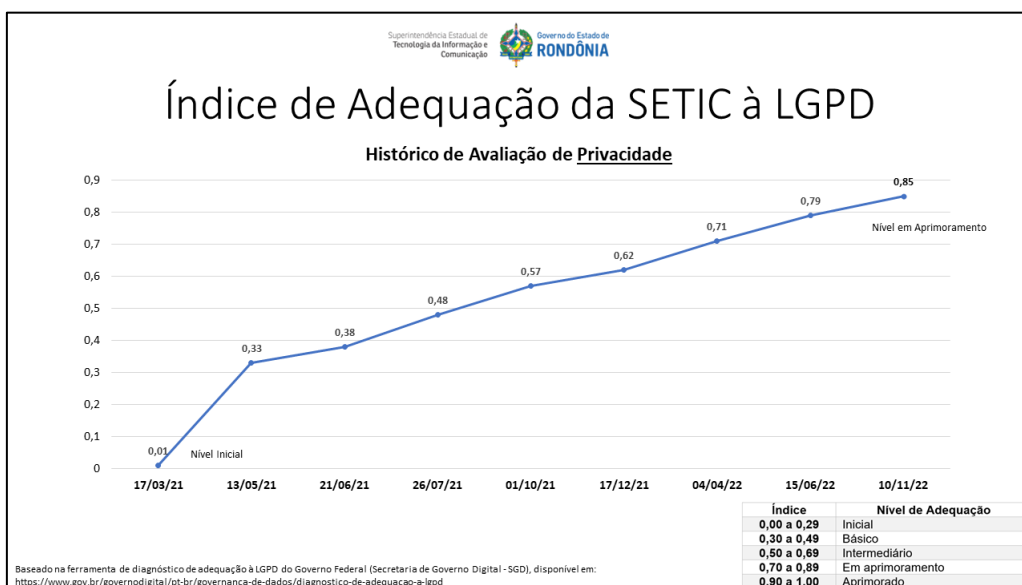
¹ Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protacao-de-dados/pspsi/ferramenta_frameworkpsi_pt-2.zip. Acesso em: 12 jul. 2023.



É importante destacar que esse diagnóstico deverá ser repetido em outras etapas, permitindo a realização da comparação dos resultados, com intuito de avaliar o progresso do órgão ou entidade em busca da conformidade. É um instrumento que permite inclusive demonstrar para a alta gestão, bem como para seus demais líderes, sociedade e para os próprios servidores, os resultados das ações que estão sendo adotadas.

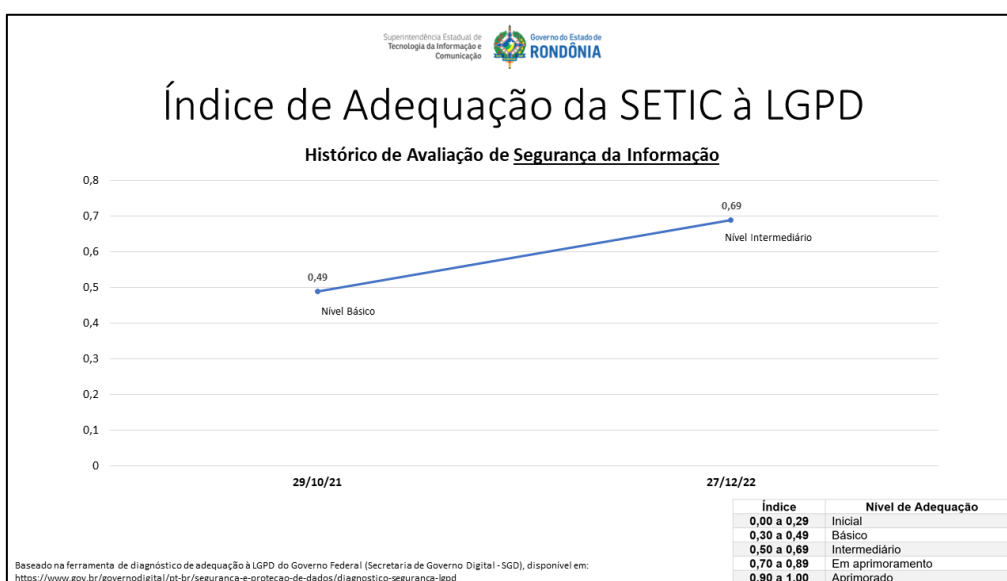
Observe o exemplo apresentado nas figuras abaixo:

Figura 3 – Histórico de avaliação de privacidade à LGPD.



Fonte: Governo do Estado de Rondônia, SETIC (2023).

Figura 4 – Histórico de avaliação de segurança da informação à LGPD.



Fonte: Governo do Estado de Rondônia, SETIC (2023).

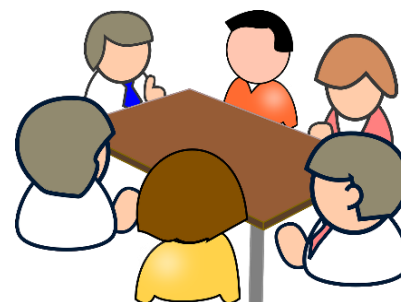


Destaca-se que tal ferramenta é apenas sugestiva, pois, dependendo das peculiaridades do órgão ou entidade, pode ser que outra seja mais adequada.

2 WORKSHOP

A etapa seguinte é a realização de *workshop* com a alta gestão do órgão, incluindo as diretorias e os demais líderes setoriais.

O objetivo é explanar para toda a liderança do órgão ou entidade, bem como sensibilizá-los, sobre a importância do cumprimento das diretrizes



estabelecidas pela LGPD, abordando brevemente sobre seus principais tópicos (entrada em vigor, tratamento de dados pessoais pelo poder público, agentes de tratamento, encarregado pelo tratamento de dados pessoais, sanções administrativas e boas práticas).

Salienta-se que outras abordagens podem ser realizadas por meio de novos *workshops* ou treinamentos temáticos, inclusive abrangendo todos os demais servidores (sugere-se a relação de cursos gratuitos disponível na sessão “Material de Apoio” do sítio institucional do Governo Estadual sobre LGPD, acessível em <https://rondonia.ro.gov.br/material-de-apoio/>).

Os líderes deverão estar cientes de que será necessária a realização de entrevistas no decorrer da jornada e conformidade, objetivando facilitar a compreensão do fluxo de tratamento dos dados pessoais nos departamentos do órgão ou entidade.

Destaca-se que a alta gestão necessita prestar o apoio necessário para que as ações de conformidade com a LGPD sejam executadas. Esse apoio também refletirá no comportamento dos liderados, que terão seus líderes como exemplo. Nessa etapa já se inicia o processo de incorporação de uma nova cultura organizacional no que diz respeito ao adequado tratamento de dados pessoais, por meio da conscientização sobre a importância que a LGPD traz para a administração pública e para a sociedade.



Também é oportuno que seja apresentado o *roadmap*, ou seja, as ações necessárias para entrada em conformidade. Neste Guia, o *roadmap* se traduz nas 7 (sete) etapas apresentadas na **Figura 1**.

Os líderes deverão ser orientados de que a conformidade com a LGPD não se resume em uma única ação, tal como a aquisição de um sistema ou a incorporação ou alteração de um novo procedimento, mas sim em um conjunto de ações que envolve estratégia, governança, políticas, procedimentos, ferramentas, gestão de mudança, conscientização, treinamento, monitoramento, responsabilidade, transparência etc.

Essa etapa poderá ser conduzida pelo Encarregado/DPO e pela equipe responsável pela adequação, caso tenha sido criada.

3 MOBILIZAÇÃO INICIAL

A mobilização inicial se resume na nomeação do encarregado pelo tratamento de dados pessoais, na criação da comissão tática e operacional e na criação do comitê interno, que conduzirão os trabalhos de conformidade do órgão ou entidade com a LGPD.



Importante destacar que existem diferentes maneiras de fazer frente aos trabalhos de conformidade, incluindo a necessidade ou não da criação de colegiados como a comissão e o comitê citados. Neste Guia será abordada a criação de ambos, com intuito de apresentar as diferentes possibilidades.

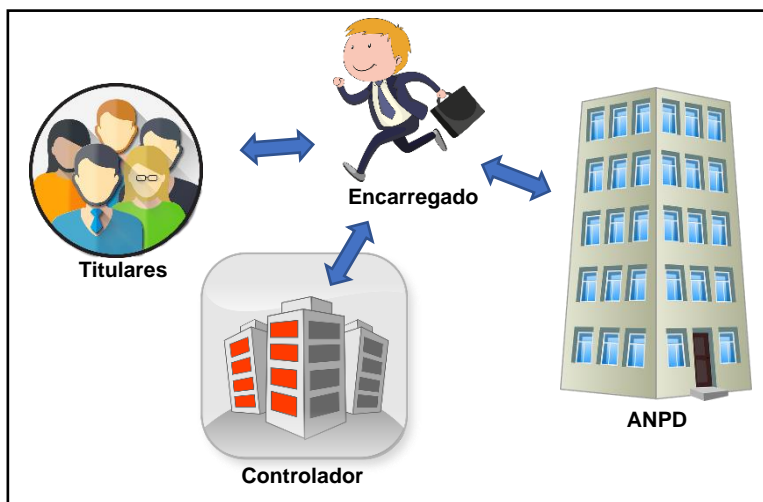
Nessa etapa também será preciso trabalhar com a ampla divulgação interna no órgão ou entidade, explicitando o início da jornada de conformidade e apresentando os profissionais e equipes que estarão conduzindo o processo. Também será necessário realizar outros diagnósticos de adequação à LGPD, com o objetivo de identificar e registrar o nível de progresso.



3.1 Encarregado pelo Tratamento de Dados Pessoais

O encarregado pelo tratamento de dados pessoais, conforme inciso VIII, art. 5º, da LGPD, é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre controlador, titulares e Autoridade Nacional de Proteção de Dados (ANPD):

Figura 4 – Encarregado/DPO, titulares, controlador e ANPD.



Fonte: Governo de Rondônia, SETIC (2023).

Muitas vezes o encarregado é conhecido como *Data Protection Officer* – DPO, uma tradução para Oficial de Proteção de Dados, nomenclatura utilizada na legislação europeia que também versa sobre privacidade e proteção de dados pessoais, norma de referência para a criação da LGPD. No Brasil, conforme **Classificação Brasileira de Ocupações – CBO**², do Ministério do Trabalho, existe a denominação para Oficial de Proteção de Dados Pessoais – DPO registrada sob código ID nº 1421-35.

A nomeação do encarregado é requisito para que os órgãos e entidades públicas possam realizar o tratamento de dados pessoais, conforme explicitado no inciso III do art. 23, e no *caput* do art. 41, ambos da LGPD, devendo ser indicado pelo controlador.

Vale ressaltar que também é mandatória a divulgação pública da identidade e informações de contato do encarregado, preferencialmente no sítio eletrônico do controlador, atendendo os requisitos da clareza e objetividade, conforme ditames do

² Disponível em: <http://www.mtecbo.gov.br/cbosite/pages/home.jsf>. Acesso em: 17 jul. 2023.



§ 1º, art. 41, da LGPD. Nesse sentido, o Governo do Estado, por meio do Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD), publicou a [Instrução Normativa nº 5/2023/CGPD](#), que estabelece diretrizes sobre tal publicização, criando um [canal único](#) para isso.

Conforme **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**³ da ANPD, o “encarregado pode desempenhar um importante papel de fomentar e disseminar a cultura da proteção de dados pessoais na organização”.

O Governo do Estado de Rondônia publicou o [Decreto nº 26.451, de 4 de outubro de 2021](#)⁴ regulamentando a adoção de medidas para aplicação da LGPD no âmbito do Poder Executivo. Dentre as diretrizes relativas ao Encarregado/DPO, destacam-se as seguintes:

- a) o encarregado deve ser agente público formalmente designado (inciso V, art. 2º);
- b) a nomeação do encarregado deve atender as prerrogativas e qualificações necessárias ao exercício da função, possuindo conhecimentos multidisciplinares, preferencialmente aqueles relacionados à privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados, tecnologia da informação e acesso à informação no setor público (inciso I, § 1º, art. 4º);
- c) o encarregado deverá participar de ações de capacitação disponibilizadas pelo Poder Executivo, conforme indicações do Comitê Gestor de Privacidade e Proteção de Dados Pessoais – CGPD do Governo Estadual (§ 3º, art. 4º); e
- d) ao encarregado é assegurado o acesso direto à alta administração, amplo acesso à estrutura organizacional, pronto apoio das unidades administrativas e contínuo aperfeiçoamento relacionado aos temas de

³ Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado_defeso_eleitoral.pdf. Acesso em: 17 jul. 2023, p. 22.

⁴ Disponível em: <http://ditel.casacivil.ro.gov.br/COTEL/Livros/Files/D26451%20-%20COMPILADO.pdf>. Acesso em: 17 jul. 2023.



privacidade e proteção de dados pessoais, observada a disponibilidade orçamentária e financeira (art. 5º).

A mais disso, o Decreto nº 26.451/2021, em seu art. 13, estabelece as competências do encarregado no âmbito do Poder Executivo Estadual:

Art. 13. Compete ao encarregado pelo tratamento de dados pessoais:

I - auxiliar o órgão ou entidade a adaptar seus processos de acordo com a LGPD, incluindo a responsabilidade quanto à orientação e aplicação de boas práticas e governança;

II - trabalhar de forma integrada com os respectivos agentes de tratamento, considerando a necessidade de monitoramento regular e sistemático das atividades destes;

III - receber reclamações e comunicações dos titulares, prestar esclarecimentos, alertar o controlador, sugerir e monitorar a implementação de medidas pertinentes;

IV - receber comunicações da Autoridade Nacional de Proteção de Dados Pessoais - ANPD, alertar o controlador, bem como sugerir e monitorar a implementação de medidas pertinentes;

V - orientar os funcionários, servidores e contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e às normas internas estabelecidas, se houver;

VI - recomendar as salvaguardas para mitigar quaisquer riscos aos direitos dos titulares de dados pessoais tratados pelo órgão, inclusive salvaguardas técnicas e medidas organizacionais;

VII - assessorar os responsáveis pelo tratamento de dados pessoais na realização de inventários de dados pessoais e emissão de relatórios de impacto à proteção de dados pessoais; e

VIII - executar outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Não obstante, é importante destacar a [Instrução Normativa nº 3/2022/CGPD](#), que dispõe sobre os requisitos para indicação do encarregado em órgãos e entidades do Poder Executivo Estadual. A referida norma foi elaborada pelo Comitê Gestor de Privacidade e Proteção de Dados Pessoais – CGPD do Governo Estadual e traz algumas inovações no que diz respeito à atuação do encarregado, tais como:

- a) emissão de declaração para o encarregado, confeccionada pelo órgão ou entidade que representa, com informações de seu tempo de atuação para comprovação de experiência (parágrafo único, art. 1º);
- b) possibilidade de um mesmo encarregado atuar em nome de diferentes órgãos e entidades do Poder Executivo Estadual, principalmente aqueles subordinados ou vinculados por força da desconcentração administrativa, desde que realize suas atribuições com eficiência (§ 5º, art. 2º);



- c) recomendação, objetivando afastar possíveis conflitos de interesse, da vinculação do encarregado ao Controle Interno ou setor similar do órgão ou entidade, e que não exerça cargo que o leve a determinar as finalidades e os meios de tratamento de dados pessoais (art. 4º);
- d) criação e uso de *e-mail* institucional padronizado - <sigla_do_órgão>@lgpd.ro.gov.br (art. 5º);
- e) criação e uso de unidade padronizada no Sistema Eletrônico de Informações – SEI, denominada Unidade de Proteção de Dados Pessoais – <SIGLA_DO_ÓRGÃO>-LGPD (art. 6º); e
- f) anexos de modelos de portaria de indicação do encarregado e de instituição de Unidade de Proteção de Dados Pessoais no SEI.

A escolha do encarregado pelo tratamento de dados pessoais deve levar em conta seus conhecimentos multidisciplinares, destacando-se a imprescindibilidade quanto ao apoio da alta administração na condução jornada de conformidade com a LGPD.

3.2 Agentes de Tratamento

Apesar de não ser o intuito deste Guia de Conformidade, torna-se importante tratar dos conceitos básicos sobre os agentes de tratamento, uma vez que são referenciados no decorrer da jornada de conformidade.

Os agentes de tratamento são os controladores e o operadores, conforme definição trazida no art. 5º, IX, LGPD.

O **controlador** é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (art. 5º, VI, LGPD), já o **operador** é “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (art. 5º, VII, LGPD).

O Governo do Estado de Rondônia, no âmbito da Administração Pública Direta, é considerado o controlador por direito, já seus órgãos e entidades são caracterizados controladores de fato, pois exercem funções típicas de controlador por força da desconcentração administrativa, conforme § 1º, art. 2º, do Decreto nº 26.451/2021.



Destaca-se ainda que os integrantes das pessoas jurídicas (empregados, administradores, sócios, servidores públicos, funcionários e equipes de trabalhos) não são caracterizados como controladores ou operadores, tendo em vista sua subordinação e atuação sob o poder diretivo dos agentes de tratamento, conforme § 2º, art. 2º, do Decreto nº 26.451/2021.

3.3 Comitê Interno de Privacidade e Proteção de Dados Pessoais

A constituição de um comitê interno para deliberações sobre privacidade e proteção de dados pessoais é considerado um importante marco para alcançar a conformidade com a LGPD, a composição do comitê interno deve ser multidisciplinar, ou seja, seus membros devem representar as diferentes áreas de negócio do órgão ou entidade.

Em razão da constituição multidisciplinar do comitê interno, torna-se importante o nivelamento do conhecimento sobre a temática entre seus membros, bem como sobre suas atribuições e competências, o que pode ocorrer por meio da realização de treinamentos.

A recomendação é que os membros do comitê não só representem as áreas de negócio do órgão, mas que sejam seus líderes, pois detêm conhecimentos em nível estratégico, tático e operacional do funcionamento de seu departamento. Tais membros também desempenharão papel importante na incorporação de uma nova cultura organizacional, pois serão considerados verdadeiros influenciadores no que diz respeito ao adequado tratamento de dados pessoais, servindo de referência para seus liderados. Além disso, tais líderes terão poder de voto em deliberações sobre o tema, fazendo parte das decisões e diretrizes que o órgão deverá seguir em busca da conformidade com a LGPD.

Recomenda-se ainda que o Encarregado/DPO faça parte da composição do comitê interno.

Caso já exista um comitê interno no órgão ou entidade, é possível que este assumas as atribuições relativas à LGPD, ajustando sua norma de criação e competências.



O Comitê Interno tem atuação estratégica e tática frente à conformidade com a LGPD. Dentre suas atribuições destacam-se:

- colaborar com a elaboração e implementação do Programa de Governança em Privacidade – PGP;
- facilitar a promoção cultural de privacidade e proteção de dados pessoais;
- deliberar sobre processos, procedimentos e propostas de medidas relacionadas ao tratamento e proteção de dados pessoais;
- propor ações e diretrizes voltadas ao tratamento e proteção de dados pessoais;
- propor e apreciar propostas de iniciativas para melhorar a segurança da informação e a proteção de dados pessoais; e
- auxiliar o encarregado pelo tratamento de dados pessoais no cumprimento de suas competências.

3.4 Comissão Tática e Operacional

A comissão tática e operacional, diferentemente do comitê interno, desenvolverá ações de cunho operacional. Seu objetivo principal é a construção do plano de ação visando a adequação do órgão ou entidade às exigências da LGPD, bem como a elaboração do Programa de Governança em Privacidade (PGP).

Observem que o plano de ação é a 6ª etapa do *roadmap* apresentado, entretanto, para alcançá-la, a comissão deverá necessariamente executar as etapas de número 4 (inventário de dados pessoais) e 5 (parecer diagnóstico).

Recomenda-se que a comissão tática e operacional preste informações periódicas sobre o desenvolvimento de seus trabalhos ao comitê interno. Ao final dos trabalhos, deverá apresentar os registros de suas atividades, bem como o plano de ação e o PGP ao comitê interno, que deliberará sobre suas aprovações.

A comissão deverá ser composta por equipe técnica, sob presidência do Encarregado/DPO, devendo ser constituída por pessoas que detenham, preferencialmente, os seguintes conhecimentos: privacidade e proteção de dados



peçoais, análise jurídica, gestão de riscos, governança de dados, tecnologia da informação e acesso à informação no setor público.

Destaca-se ainda a necessidade de nivelamento de conhecimento entre seus membros no que diz respeito às exigências que a LGPD traz para a administração pública, pois é importante que a equipe esteja alinhada.

3.5 Ampla divulgação

A ampla divulgação se traduz na apresentação, para todos os servidores e departamentos do órgão ou entidade, do início da jornada de conformidade com a LGPD.

Deve-se introduzir uma mensagem positiva, enfatizando-se a responsabilidade e o comprometimento de todos, inclusive da alta gestão e que a condução dessa jornada será realizada por profissionais comprometidos, destacando-se o papel do Encarregado/DPO, da comissão tática e operacional e do comitê interno.

Essa atitude também tem por objetivo a promoção de uma nova cultura organizacional, enfatizando-se a responsabilidade quanto à proteção de dados pessoais, procurando conscientizar todos os envolvidos.

3.6 Diagnósticos intermediários

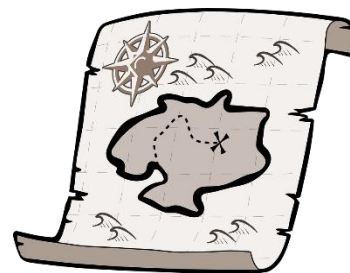
Os diagnósticos intermediários consistem no uso da mesma ferramenta utilizada no diagnóstico inicial e tem por objetivo permitir a comparação entre os índices de maturidades e direcionar esforços para consecução de ações específicas para entrada em conformidade com a LGPD. Recomenda-se que os diagnósticos sejam realizados a cada um ou dois meses.

Até aqui, várias etapas da jornada de conformidade já foram realizadas, tais como o *workshop* com a alta administração, criação de comitê, criação da comissão tática e operacional, nomeação do Encarregado/DPO e ampla divulgação interna, tratando-se, a seguir, do inventário de dados pessoais.



4 INVENTÁRIO DE DADOS PESSOAIS

A etapa de Inventário de Dados Pessoais (IDP) é uma das mais importantes na jornada de conformidade. Contempla uma das exigências da LGPD, prevista em seu art. 37, estabelecendo que “o controlador e o operador devem manter registro de operações de tratamento de



dados pessoais que realizarem”. Além disso, o IDP visa subsidiar a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), termo de uso e outras ações necessárias como a identificação de lacunas frente às exigências da LGPD.

O objetivo é realizar o levantamento dos processos /serviços que tratam dados pessoais, evidenciando, por exemplo, a finalidade do tratamento, fluxo, hipótese legal, amparo legal e identificação dos dados pessoais tratados.

A metodologia sugerida para realizar o IDP é a *top-down*, iniciando-se a análise pelos serviços/processos, e não pelo dado propriamente dito, conforme recomendação contida no **Guia de Elaboração de Inventário de Dados Pessoais**⁵, disponibilizado pela Secretaria de Governo Digital (SGD), desenvolvido com base em metodologias adotadas na França, Bélgica e Inglaterra.

O Governo do Estado, por meio do Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD), publicou a [Instrução Normativa nº 4/2023/CGPD](#), que disciplina a elaboração do IDP no âmbito dos órgãos e entidades do Poder Executivo Estadual, disponibilizando um modelo (*template*) em planilha eletrônica como referência.

Entretanto, é importante esclarecer que o IDP é apenas uma das etapas de toda a jornada de conformidade com a LGPD, e que não há sistema que garantirá a adequação à referida norma, pois muitas das etapas envolvem a aplicação de medidas técnicas e administrativas.

Os resultados dessa etapa refletirão na avaliação quanto às medidas de segurança e suas aplicações, bem como na mitigação ou resolução de possíveis lacunas.

⁵ Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_inventario_dados_pessoais.pdf. Acesso em: 17 jul. 2023, p. 10 e 14.



Destaca-se que é importante manter os registros de tratamento atualizados, estabelecendo-se um ciclo de periodicidade para revisão (a cada ano, por exemplo), bem como a realização de atualização sempre que houver mudança no ciclo de tratamento de dados pessoais do serviço/processo relacionado.

Recomenda-se que o IDP seja elaborado antes do início do tratamento de dados pessoais, nos casos de novos serviços ou processos de negócio.

5 PARECER DIAGNÓSTICO

Esta etapa se caracteriza pela avaliação e validação do Inventário de Dados Pessoais (IDP), devendo serem apreciadas questões que envolvam, dentre outras: o ciclo de tratamento dos dados pessoais; o fluxo de tratamento; as hipóteses legais; finalidade; previsão legal; os tipos de dados pessoais tratados; frequência de tratamento; as categorias dos titulares; possíveis compartilhamentos; medidas de segurança e privacidade; transferências internacionais; e contratos ou acordos existentes.



Por meio dessa ação, a comissão tática e operacional deverá identificar os serviços ou processos de negócios que precisam se adequar à LGPD, bem como as lacunas (*gaps*) existentes, recomendando soluções para resolver ou mitigar os problemas encontrados.

É o momento para realizar a avaliação crítica sobre todas as operações de tratamento de dados pessoais que são realizadas pelo órgão ou entidade. Tais informações subsidiarão a elaboração da próxima etapa, ou seja, do Plano de Ação para adequação à LGPD. Nesse processo de avaliação crítica, recomendando-se a aplicação, no que couber, das orientações presentes no guia orientativo “**Tratamento de Dados Pessoais pelo Poder Público**”⁶, elaborado pela ANPD.

No decorrer desta etapa é possível que alguns problemas identificados já possam ser resolvidos, dependendo do nível de complexidade.

⁶ Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 7 jul. 2023.



6 PLANO DE AÇÃO

Com base no IDP e no parecer diagnóstico, a comissão tática e operacional desenvolverá o plano de ação, elencando as atividades necessárias para que o órgão ou entidade entre em conformidade com as exigências da LGPD, devendo estabelecer uma ordem de priorização.



O plano de ação deverá ser apresentado ao comitê interno e à alta gestão, que deliberarão por sua aprovação e priorizarão as ações que julgar serem mais importantes.

Dentre as ações que poderão ser apresentadas no Plano, destacam-se as seguintes:

	Ação	Justificativa
1	Instituir um Programa de Governança em Privacidade (PGP)	<p>O Programa de Governança em Privacidade (PGP) deve propor ações permanentes de conformidade com o adequado tratamento de dados pessoais e está previsto art. 50 da LGPD.</p> <p>O PGP deve demonstrar o comprometimento do órgão ou entidade em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à temática. Estabelecer políticas e salvaguardas adequadas. Propor ações de melhoria contínua quanto às diretrizes estabelecidas na LGPD, sugerindo-se a adoção de um ciclo que estabeleça o monitoramento e auditoria dessas ações.</p> <p>O PGP deve prever ações de nível estratégico e tático, podendo resultar na criação de projetos de níveis operacionais.</p> <p>Destaca-se que é de competência da autoridade máxima do órgão ou entidade estadual implementar o PGP ou Plano de Adequação à LGPD atendendo os requisitos mínimos elencados no inciso I, §2º, art. 50, da LGPD, sempre que, na sua avaliação, a estrutura, a escala e o volume das operações de tratamento de dados pessoais na sua repartição recomendarem, conforme previsto no art. 6º do Decreto Estadual nº 26.451/2021.</p> <p>Exemplo de PGP: A SETIC, publicou em julho/2021 seu Programa de Governança em Privacidade, acessível em https://wiki.setic.ro.gov.br/home/compliance/programa_privacidade</p>



2	Implementar o <i>Privacy by Design</i>	<p>O <i>Privacy by Design</i> consiste em desenvolver projetos, produtos ou serviços já inserindo medidas de privacidade desde a concepção, ou seja, desde sua construção.</p> <p>O art. 6º da LGPD elenca um rol de princípios que devem ser observados desde a concepção de um projeto, produto ou serviço, relacionando-se diretamente com o <i>Privacy by Design</i>.</p> <p>Destaca-se ainda que a LGPD (art. 46, § 2º) determina que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais, sendo que tais medidas devem ser observadas desde a fase de concepção do produto ou do serviço até sua execução.</p>
3	Implementar campanha de publicidade e conscientização	<p>A implementação de uma campanha de publicidade e conscientização é uma ação que visa principalmente a criação de uma nova cultura organizacional, que revela a importância do adequado tratamento de dados pessoais, considerando que a LGPD é transdisciplinar e deve ser cumprida no decorrer de todo o ciclo de vida do tratamento de dados pessoais.</p> <p>Exemplo de campanha de conscientização:</p> <p>Como exemplo, destaca-se a campanha interna de conscientização criada pela SETIC, denominada “Frame LGPD”, que promove <i>workshops</i> e palestras bimestrais para seus servidores sobre a temática. Acesse as matérias: https://rondonia.ro.gov.br/setic-promove-campanha-de-conscientizacao-frame-lgpd-sobre-tratamento-de-dados-pessoais/ e https://rondonia.ro.gov.br/campanha-de-conscientizacao-frame-lgpd-sobre-tratamento-de-dados-pessoais-e-fortalecida-pela-setic/.</p>
4	Implementar portfólio de treinamento e desenvolvimento	<p>O treinamento e desenvolvimento objetivam o nivelamento e constante aperfeiçoamento envolvendo as boas práticas no tratamento de dados pessoais.</p> <p>Trata-se de uma necessidade, uma vez que a LGPD é transdisciplinar, devendo ser aplicada durante todo o ciclo de vida do tratamento de dados pessoais.</p> <p>O curso intitulado “Tratamento de Dados Pessoais pelo Poder Público – LGPD”, disponível no Ambiente Virtual de Aprendizagem da Escola de Governo, é considerada uma dessas ações. O Curso é destinado a servidores em exercício e para aqueles recém efetivados, devendo ser incluído no processo de ambientação (<i>onboarding</i>), conforme Instrução Normativa nº 2/2022/CGPD.</p>



5	Elaborar Relatório de Impacto de Proteção de Dados (RIPD)	<p>De acordo com o art. 5º, XVII, da LGPD, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) consiste em uma “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”.</p> <p>Conforme art. 38 da LGPD o RIPD deverá conter, no mínimo: a descrição dos tipos de dados pessoais; a metodologia usada para o tratamento e para a garantia da segurança das informações; e a análise com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.</p> <p>Assim como no caso do IDP, a recomendação é que o RIPD seja elaborado para cada processo/serviço de negócio que possuam finalidades distintas.</p> <p>O RIPD deve ser continuamente revisado, especialmente quando houver novos fatos que possam ensejar mudanças nos riscos.</p> <p>Acesso a perguntas e respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais, elaboradas pela ANPD: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais</p>
6	Instituir uma Política de Privacidade	<p>A Política de Privacidade, conforme Guia de Elaboração de Termo de Uso e Política de Privacidade (SGD, 2023, p. 35), tem como objetivo “descrever ao titular dos dados pessoais, os procedimentos e processos adotados no tratamento de dados pessoais realizado pelo serviço, bem como informá-lo sobre as medidas de proteção de dados pessoais adotadas”.</p> <p>O Governo de Rondônia, por meio do Comitê Gestor de Privacidade e Proteção de Dados Pessoais – CGPD, instituiu a Política de Privacidade e Proteção de Dados Pessoais no âmbito do Poder Executivo (Instrução Normativa nº 1/2022/CGPD), descrevendo os preceitos gerais para o tratamento de dados pessoais pelos órgãos e entidades governamentais.</p>
7	Instituir uma Política de Segurança da Informação (PSI)	<p>Política de Segurança da Informação (PSI), conforme “Glossário de Segurança da Informação” (Portaria GSI/PR nº 93, de 18 de setembro de 2019), consiste em um documento com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.</p> <p>No Governo do Estado, a SETIC é a competente pela elaboração de diretrizes gerais de PSI, conforme inciso IV, art. 10, do Decreto Estadual nº 26.451/2021.</p> <p>Portanto, os órgãos e entidades devem considerar tais diretrizes no momento de elaborar suas políticas de segurança, considerando inclusive a PSI Estadual, caso existente.</p>



8	Vincular termo de uso aos serviços ofertados	<p>O Termo de Uso, conforme Guia de Elaboração de Termo de Uso e Política de Privacidade (SGD, 2023, p. 10), “é uma espécie de contrato de adesão cujas cláusulas são estabelecidas de forma unilateral pelo fornecedor do serviço sem que o usuário possa discutir ou modificar substancialmente seu conteúdo. Esse contrato é celebrado entre o prestador e o usuário do serviço e estabelece os direitos e obrigações de cada uma das partes”.</p> <p>No Governo de Rondônia, o Comitê Gestor de Privacidade e Proteção de Dados Pessoais – CGPD tem a competência de elaborar e manter atualizado o modelo de termo de uso, inteligência do inciso IV, § 1º, art. 14, do Decreto Estadual nº 26.451/2021.</p>
9	Instituir um plano de resposta a incidentes e remediação	<p>A instituição de um plano de resposta a incidentes e remediação está prevista na alínea “a”, inciso I, § 2º, art. 50, da LGPD, como parte integrante do Programa de Governança em Privacidade.</p> <p>O plano de resposta deve contar com procedimentos para o tratamento do incidente de segurança envolvendo dados pessoais, bem como com o fluxo de comunicação interna e externa.</p> <p>Dentre as personalidades que deverão ser levadas em consideração no processo de comunicação de incidentes de segurança destacam-se: Encarregado/DPO, controlador, operador, titular de dados e ANPD.</p> <p>O Comitê Gestor de Privacidade e Proteção de Dados Pessoais – CGPD criará o Plano Geral de Respostas a Incidentes de Segurança e Remediação, conforme previsto na alínea “a”, inciso IV, item 17, da Instrução Normativa Conjunta nº 1/2023/OGE-OUVGER.</p>
10	Revisar contratos, termos, convênios e instrumentos congêneres	<p>A adequação e revisão dos atuais contratos com parceiros ou terceiros deve ser realizada objetivando o cumprimento dos dispositivos da LGPD, tanto pelo controlador quanto pelo operador, e demais envolvidos no tratamento de dados pessoais.</p> <p>Nesse sentido, deve-se procurar atender principalmente aos princípios da adequação, responsabilização e prestação de contas, elencados no art. 6º, LGPD, buscando cumprir com a compatibilidade entre o tratamento e as finalidades elencadas em contrato, bem como com a observância e o cumprimento de normas de proteção de dados pessoais pelos envolvidos no ciclo de tratamento.</p> <p>A LGPD, no <i>caput</i> do seu art. 42 estabelece a responsabilidade do controlador ou operador por qualquer dano ou violação referente ao tratamento de dados pessoais, inclusive prevendo, em seu inciso I, art. 42, a responsabilidade solidária do operador quando este não cumprir com suas obrigações legais e com instruções lícitas do controlador.</p> <p>Dessa forma, é importante que os contratos, termos, convênios e congêneres estejam adequados à LGPD, destacando-se ainda a necessidade de realizar diligências junto aos parceiros para validação de cumprimento das exigências da LGPD (<i>Due Diligence</i>).</p> <p>A Procuradoria-Geral do Estado – PGE é a responsável por “examinar, registrar, elaborar, lavrar e fazer publicar os instrumentos jurídicos de contratos, acordos e outros ajustes em que for parte o Estado de Rondônia”, nos termos do inciso IX, art. 3º, da Lei Complementar 620/2011, devendo ser consultada a respeito.</p>

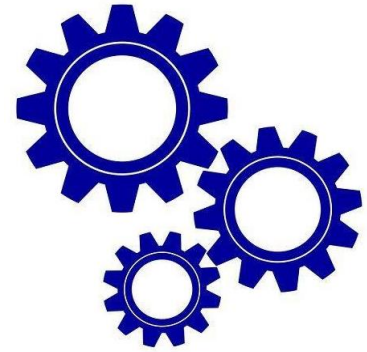
O rol acima é apenas exemplificativo, podendo haver outras ações necessárias para que o órgão ou entidade entre em conformidade com a LGPD.



7 EXECUÇÃO

De posse do plano de ação, o órgão ou entidade, por intermédio do comitê interno e do Encarregado/DPO, executará as ações previstas objetivando sua adequação à LGPD, considerando a ordem de priorização.

Dentre as ações, é importante destacar a implementação do Programa de Governança em Privacidade – PGP, cuja aprovação se dará por meio do comitê interno, caso existente, e pela autoridade máxima do órgão ou entidade, pois será o documento norteador das ações permanentes de conformidade com a LGPD, visando a melhoria contínua.



REFERÊNCIAS

BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. **Data protection officer (encarregado)**: teoria e prática de acordo com a LGPD e o GDPR. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

BRASIL. **Guia de boas práticas**: Lei Geral de Proteção de Dados Pessoais (LGPD). Comitê Central de Governança Digital. Versão 2. Brasília: ago. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 17 jul. 2023.

BRASIL. **Guia de elaboração de inventário de dados pessoais**. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital (SGD). Brasília: mar. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_inventario_dados_pessoais.pdf. Acesso em: 17 jul. 2023.

BRASIL. **Guia de elaboração de programa de governança em privacidade**. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital (SGD). Brasília: mar. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: 17 jul. 2023.

BRASIL. **Guia de elaboração de termo de uso e política de privacidade**. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital (SGD). Brasília: mar. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_termo_uso_politica_privacidade.pdf. Acesso em: 17 jul. 2023.

BRASIL. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. ANPD. Brasília: abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado_defeso_eleitoral.pdf. Acesso em: 17 jul. 2023.

BRASIL. **Guia orientativo**: tratamento de dados pessoais pelo poder público. ANPD. Brasília: jun. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 17 jul. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação (LAI). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm. Acesso em 28 mar. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 28 mar. 2021.



BRASIL. **Portaria nº 93, de 26 de setembro de 2019.** Aprova o Glossário de Segurança da Informação. Presidência da República/Gabinete de Segurança Institucional. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em 6jun. 2021.

BRASIL. **Programa de Governança em Privacidade do MCOM.** Ministério das Comunicações. Disponível em: https://www.gov.br/mcom/pt-br/composicao/secretaria-executiva-novo/planejamento-e-tecnologia-da-informacao/programa-de-governanca-em-privacidade/ProgramadeGovernanaemPrivacidadedoMCalGPD_mcom.pdf. Acesso em: 6 jun. 2021.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados comentada.** 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

CRESPO, Marcelo Xavier de Freitas. **Compliance no Direito Digital.** São Paulo: Thomson Reuters Brasil, v. 3, 2020.

MALDONADO, Viviane Nóbrega. **LGPD: Lei Geral de Proteção de Dados Pessoais: manual de implementação.** São Paulo: Thomson Reuters Brasil, 2019.

_____. **LGPD: Lei Geral de Proteção de Dados comentada.** 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

PINHEIRO, Patricia Peck. **Direito digital.** 6. ed. São Paulo: Saraiva, 2016.

POZZO, Augusto Neves Dal. MARTINS, Ricardo Marcondes. **LGPD e administração pública: uma análise ampla dos impactos.** São Paulo: Thomson Reuters Brasil, 2020.

RONDÔNIA. **Decreto nº 26.451/2021.** Disponível em: <http://ditel.casacivil.ro.gov.br/COTEL/Livros/Files/D26451%20-%20COMPILADO.pdf>. Acesso em: 17 jul. 2023.

RONDÔNIA. **Instrução Normativa nº 1/2022/CGPD.** Disponível em: https://wiki.setic.ro.gov.br/home/compliance/cgpd/normativas/instrucao_normativa_n1_2022_cgpd. Acesso em: 17 jul. 2023

RONDÔNIA. **Instrução Normativa nº 2/2022/CGPD.** Disponível em: https://wiki.setic.ro.gov.br/home/compliance/cgpd/normativas/instrucao_normativa_n2_2022_cgpd. Acesso em: 17 jul. 2023

RONDÔNIA. **Instrução Normativa nº 3/2022/CGPD.** Disponível em: https://wiki.setic.ro.gov.br/home/compliance/cgpd/normativas/instrucao_normativa_n3_2022_cgpd. Acesso em: 17 jul. 2023



Rondônia. **Instrução Normativa nº 4/2023/CGPD**. Disponível em:
https://wiki.setic.ro.gov.br/home/compliance/cgpd/normativas/instrucao_normativa_n4_2023_cgpd. Acesso em: 17 jul. 2023

Rondônia. **Instrução Normativa nº 5/2023/CGPD**. Disponível em:
https://wiki.setic.ro.gov.br/home/compliance/cgpd/normativas/instrucao_normativa_n5_2023_cgpd. Acesso em: 17 jul. 2023





Governo do Estado de
RONDÔNIA



setic@lgpd.ro.gov.br
comite@lgpd.ro.gov.br



Acesse:
lgpd.ro.gov.br