FUNDAÇÃO UNIVERSIDADE FEDERAL DE RONDÔNIA

PLANO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

RONDÔNIA, BRASIL
MARÇO/2022

PLANO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Reitora
Marcele Regina Nogueira Pereira

Vice-Reitor
José Juliano Cedaro

Chefe de Gabinete
Elyzania Torres Tavares

Pró-Reitor de Administração
Vastinei Sena de Farias

Pró-Reitor de Planejamento
George Queiroga Estrela

Pró-Reitora de Graduação
Verônica Ribeiro da Silva Cordovil

Pró-Reitor de Pós-Graduação e Pesquisa
Artur de Souza Moret

Pró-Reitora de Cultura, Extensão e Assuntos Estudantis
Neiva Cristina de Araújo

Assessor de Comunicação
Sandro Adalberto Conferai

Ouvidora institucional
Ivanda Soares da Silva

Coordenadora do Serviço de Acesso à Informação
Patrícia Santos Araújo

COMISSÃO[1]

José Juliano Cedaro
Presidente

Aurineide Alves Braga
Vice-Presidente

Elyzania Torres Tavares
Membro

André Luiz de Souza Freitas
Membro

Ivanda Soares da Silva
Membro

Patrícia Santos Araújo
Membro

George Queiroga Estrela
Membro

Fabrício Donizeti Ribeiro Silva
Membro

Vastinei Sena de Farias
Membro

Verônica Ribeiro da Silva Cordovil
Membro

Sandro Adalberto Colferai
Membro

Sézani Moraes Gonçalves Carvalho
Membro

Cristiane Marina Teixeira Girard
Membro

Pablo Diego Leão
Membro

[1] (Portaria Nº 14/2022/GR/UNIR, de 06 de janeiro de 2022, publicada no Boletim de Serviço UNIR n° 02 de 06/01/2022, p. 13, em substituição à Portaria Nº 405/2021/GR/UNIR, de 29 de junho de 2021)

Bruno Gomes da Silveira
Membro

EQUIPE DE ELABORAÇÃO DO TEXTO

Patrícia Santos Araújo
Bacharel em Direito, Técnica em Assuntos Educacionais, Coordenadora do Serviço de Informação ao Cidadão, Ouvidora substituta.

Ivanda Soares da Silva
Contadora, Ouvidora Institucional. Encarregada da LGPD na UNIR.

José Juliano Cedaro
Vice-Reitor, Autoridade de Monitoramento da Lei de Acesso à Informação da UNIR.

Aurineide Alves Braga
Profa. do Departamento Acadêmico de Ciências da Informação

Bruno Gomes da Silveira
Arquivista.

Ficha Catalográfica elaborada pela Biblioteca Central da UNIR

Fundação Universidade Federal de Rondônia. Comissão de Adequação da Universidade Federal de Rondônia à Lei Geral de Proteção de Dados Pessoais (Lei n°13.709, de 14 de agosto de 2018), PORTARIA Nº 14/2022/GR/UNIR, DE 06 DE JANEIRO DE 2022, publicada no Boletim de Serviço da UNIR n° 02 de 06.01.2022, p. 13).

F981

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxx. – Porto Velho, RO, 2021.

xxp.: il.

Modo de acesso:

1. Plano de Adequação. 2. Lei Geral de Proteção de Dados Pessoais. 3. Universidade. 4. xxx. I. xxxxxxxxxx IX. Título.

CDU:

Bibliotecária Responsável: Cristiane Marina T. Girard / CRB 11-897

Fundação Universidade Federal de Rondônia (UNIR)

Biblioteca Central da UNIR

E-mail: bc-unir@unir.br

Site: www.bibliotecacentral.unir.br

VERSÃO	DATA	EQUIPE RESPONSÁVEL	DESCRIÇÃO
1.0 (2022/2024)	Março/2022	Portaria Nº 14/2022/GR/UNIR, de 06 de janeiro de 2022, publicada no Boletim de Serviço da UNIR n° 02 de 06.01.2022, p. 13.	Plano de adequação da UNIR à Lei Geral de Proteção de Dados Pessoais

SUMÁRIO

I - INTRODUÇÃO

O desenvolvimento tecnológico que vivenciamos nos últimos anos trouxe grandes possibilidades para as mais diversas áreas da atuação humana, como o comércio, educação, divulgação científica, tratamento em saúde, entre tantos outros. A rede mundial de computadores ensejou um aumento incomensurável no compartilhamento de informações, entre os quais incluem dados pessoais, que muitas vezes são utilizados para finalidades inadequadas e até na prática de crimes. Com isso, os cidadãos vêm se sentindo incomodados e ameaçados com a utilização de informações sensíveis[2] sobre sua vida pessoal e de sua família, muitas vezes por meio de ações sem que tenha dado qualquer autorização ou tenha confiado em empresas (e até em órgãos governamentais) ao fazer cadastros corriqueiros, compras ou uma simples matrícula, por exemplo. Por tais razões, essa temática está presente nos debates nas casas de leis de várias nações democráticas no mundo e deve pautar nossas preocupações por um longo tempo, levando a mudanças nas condutas individuais e nas práticas organizacionais.

A Lei Geral de Proteção de Dados Pessoais, conhecida como LGPD (Lei n° 13.709, de 14 de agosto de 2018, alterada pela Lei 13.853, de 8 de julho de 2019) tem como principal finalidade ordenar/proteger o uso dos dados pessoais, alterando a Lei n° 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e o Decreto 8.771, de 11 de maio de 2016.

A LGPD tem gerado significativa repercussão, pois envolve o tratamento de informações pessoais, seja no meio digital ou físico, por pessoa natural ou jurídica. Considera-se que representa um extraordinário avanço em direção ao fortalecimento de um sistema de proteção de dados no País, pois traz princípios, direitos e obrigações, sendo um movimento essencial para a consolidação da confiança do cidadão no trato com as instituições. Traz a garantia instrumental de dois direitos já previstos na Constituição: 1) direito à privacidade, que é um conceito antigo, tratado de forma clássica ligado a questões relativas à intimidade e à vida privada; 2) o *habeas data*, conforme previsto no artigo 5°, inciso LXXII da Carta Magna, que assegura a todo cidadão acesso a dados e informações pessoais que estejam sob a posse de instituições públicas ou privada. Assim, o princípio da autodeterminação informativa[3] previsto na LGPD pode ser considerado uma extensão material do *habeas data*.

[2] Dado pessoal sensível se refere à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, bem como dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural (Lei n°13.709/2018, art.5°, inciso II).

[3] Significa que o titular do dado pessoal tem o controle absoluto sobre o que é feito com os seus dados.

A implantação dessa Lei tem representado um grande desafio, pois implica na mudança de uma cultura e na adoção de práticas pouco valorizadas. E, mesmo passando mais de três anos depois da promulgação, ainda damos os primeiros passos, salientando que desde o último mês de agosto o não cumprimento implica na possibilidade de aplicação de penalidades.

É exatamente dentro desse contexto que o presente Plano de Adequação se apresenta para a UNIR. Trata-se da primeira versão sobre mudanças que estão sendo implementadas e da proposição de ações que precisam ser efetivadas para atender a legislação vigente, as quais implicam na adoção de procedimentos que estejam alinhados com a legislação, sobretudo no que diz respeito ao relacionamento e prestação de serviços aos cidadãos/usuários. Portanto, pretende-se definir como será a governança dos dados pessoais, criação das normas de segurança, padrões técnicos no tratamento dos dados e ações educativas. Além disso, há também o desafio de definir papéis e um cronograma de adequação e implantação da LGPD na UNIR.

II – OBJETIVOS

2.1 Objetivo geral

O objetivo principal deste plano é oferecer orientações para que os procedimentos acadêmicos e administrativos da Fundação Universidade Federal de Rondônia/UNIR sejam adequados às exigências previstas na Lei Geral de Proteção de Dados Pessoais/LGPD (Lei n° 13.709, de 14 de agosto de 2018) e normativas correlatas.

2.2 Objetivos específicos

1. Criar uma política de proteção e privacidade de dados pessoais.

2. Estabelecer premissas, estratégias e táticas, operacionais e comunicacionais que contribuam para o cumprimento dos requisitos mínimos elencados pela LGPD.

3. Garantir que as atividades que envolvem o tratamento de dados pessoais e dados pessoais sensíveis na instituição sejam realizadas de forma transparente e segura.

4. Assegurar aos titulares dos dados proteção às suas informações e acesso facilitado, incluindo direito de atualização e eliminação deles, dentro das prerrogativas legais.

5. Apresentar canais de comunicação e de denúncias para os titulares dos dados.

6. Capacitar e orientar servidores (incluindo terceirizados e estagiários) quanto aos cuidados a serem adotados para garantir a privacidade dos dados pessoais.

7. Promover transparência ativa sobre o uso dos dados pessoais.

8. Adequar os processos (SEI e/ou outros sistemas utilizados) à LGPD.

9. Possibilitar que haja consulta pública aos processos do SEI, respeitando as limitações impostas pela legislação pertinente.

III- CONCEITOS ESSENCIAIS

Para adequação da UNIR à LGPD faz-se necessário adentrar em alguns aspectos dessa norma para que haja maior clareza sobre o melhor caminho a seguir. Nesse sentido é imperioso conhecer as hipóteses legais e buscar a aplicação dos princípios no decorrer de todo o processo de adequação.

O primeiro capítulo da LGPD trata das disposições preliminares, com os fundamentos, propósitos, definições dos novos termos e seus princípios. Segundo Garcia (2020, p. 6), essa Lei:

> (...) pretende proteger direitos fundamentais como liberdade, privacidade e direito ao desenvolvimento de pessoas naturais, que sejam feridos por outra pessoa natural ou mesmo por pessoa jurídica. Todo esse esforço tem o intuito de não deixar dúvidas de que se está falando de todo e qualquer sistema que utilize o dado de uma pessoa natural.

A LGPD[4] traz um grande avanço para assegurar não só a privacidade, como também a proteção de dados pessoais da pessoa natural, e apresenta uma definição mais detalhada dos princípios, termos e procedimentos. Foi promulgada em agosto de 2018, sendo concedido um período de 24 meses para adequação das instituições, posteriormente ampliado por mais 12 meses. Com isso, passou a vigorar com previsão de penalidades em caso de descumprimento a partir de agosto de 2021.

É importante destacar que a LGPD observa o princípio da transparência e autodeterminação no tratamento de dados pessoais. Por essa razão assegura ao titular que a qualquer momento possa questionar as informações relacionadas, podendo acessá-los de forma rápida e ser atendido por meio de linguagem simples e objetiva (LUNA, 2020).

O artigo 2º da LGPD aborda os fundamentos que irão disciplinar a proteção de dados pessoais. Tais fundamentos merecem atenção e ganham relevância na exegese da lei, afastando interpretações que os ofendam. Dentre os fundamentos elencados nesse artigo estão o da proteção dos dados pessoais com base no respeito à privacidade, autodeterminação informativa, liberdade de expressão, de informação, de comunicação e de opinião, além da inviolabilidade da intimidade, da honra e da imagem.

[4] Foi inspirada na *General Data Protection Regulation* - GDPR, da União Europeia, que foi aprovada em 2016 e teve naquele continente uma *vacatio legis* de dois anos, entrando em vigência em 25 de maio de 2018.

O conceito de proteção de dados e privacidade são distintos. Por exemplo: se uma pessoa publicar um dado em sua página pessoal numa rede social, ele se torna público. Entretanto, isso não significa que esse dado pode ser utilizado indiscriminadamente. Esses dados, não estão sob o amparo do princípio constitucional da privacidade, mas sob a determinação da proteção de dados (GARCIA, 2020).

O artigo 2º ainda preconiza o fundamento de autodeterminação informativa. Significa que o titular do dado tem o direito de decidir o que será feito com a sua informação, quais dados as instituições podem possuir a seu respeito e como poderão ser utilizados. Nesse mesmo sentido, podem requerer correções e pedir exclusão. Em síntese, cada usuário tem o direito de determinar como sua informação pode (e se vai) ser utilizada (GARCIA, 2020).

Destaca-se ainda que esses fundamentos sobre a inviolabilidade da intimidade, honra e imagem, aliado ao direito do desenvolvimento da personalidade, respeito à dignidade da pessoa humana, que fazem parte do exercício livre da cidadania, estão previstos na Constituição Federal e são pontuados na LGPD para reiterar sua relevância. E, nesse sentido, o legislador foi cuidadoso ao definir que os dados são fundamentais para a proposição e execução de políticas públicas, para as pesquisas científicas e até mesmo para o bom funcionamento do mercado, garantindo que esteja consonante com os fundamentos do desenvolvimento econômico e tecnológico, promoção da inovação e valorização da livre iniciativa e da concorrência. Mas, por outro lado, deve-se garantir que os direitos inalienáveis da privacidade, intimidade e respeito à honra, bem como outros elementos relacionados à defesa do consumidor em particular e do cidadão como um todo, sejam respeitados. Entende-se, portanto, que houve um reconhecimento da importância do tratamento dos dados pessoais para a sociedade e para o desenvolvimento do conhecimento, mas respeitando os direitos individuais.

No artigo 5°, a LGPD dispõe os conceitos importantes, conforme descrito no quadro abaixo:

Quadro 1- Conceitos

Tipos de dados (Art. 5º, Lei 13.709/2018)	
Pessoal	Informação relacionada a pessoa natural identificada ou identificável (Art. 5º, inciso I).
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 (Art. 5º, inciso II).
Anonimizado	Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (Art. 5º, inciso III).

	Demais Conceitos
Banco de Dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (Art. 5°, inciso IV).
Titular	Pessoa natural a que se referem os dados pessoais que são objeto de tratamento (Art. 5°, inciso V).
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 (Art.5°, inciso X).
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 (Art. 5°, inciso XI).
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Art. 5°, inciso XII).
Bloqueio	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados (Art. 5°, inciso XIII).
Eliminação	Exclusão de dado ou de conjunto de dados armazenados em banco de dados independente do procedimento empregado (Art.5°, inciso XIV).
Uso compartilhado de dados	Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgão e entidades públicas no cumprimento de suas competências legais, ou entre esses entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (Art. 5°, inciso XVI).

Fonte: Guia de Boas Práticas para Implementação na Administração Pública Federal (Abri/2020).

As definições trazidas no artigo 5° contribuem para a compreensão dos procedimentos de adequação, inclusive com dispositivos para harmonização com a Lei de Acesso à Informação (LAI), como por exemplo nas situações que oferecem a possibilidade ou implicam na necessidade de procedimentos de pseudoanonimização e anonimização de dados para evitar a exposição de pessoas envolvidas com a questão que precisa ser divulgada. É imprescindível que haja o equilíbrio entre a Proteção de Dados (como um direito individual) e a proteção da segurança pública (como um direito coletivo), para que se fortaleça o combate ao crime organizado, à fraude digital e ao terrorismo (PINHEIRO, 2018).

Em razão da LGPD estar em vigência recentemente, principalmente no tocante às penalidades, há ainda muitas dúvidas quanto à aplicação de alguns itens dessa norma. No artigo 5º, por exemplo, há o questionamento se a lista de dados sensíveis é taxativa ou exemplificativa. Existem argumentos para ambas as posições. Alguns juristas defendem que tem que ser taxativa para fins de segurança jurídica, visto que a classificação de um dado como sensível acarreta

diferenças quanto às bases legais e as hipóteses de tratamento. Outros, argumentam que a lista deveria ser exemplificativa dada a própria categoria de dados sensíveis, pois teria sido criada para evitar tratamentos discriminatórios.

Como registrado anteriormente, a LGPD se caracteriza como um marco regulatório para o tratamento de dados pessoais. Além disso, traz um forte caráter de proteção a direitos individuais que estão expressos nos princípios estabelecidos no seu artigo 6° (conforme síntese abaixo) e nos demais artigos da referida lei.

Quadro 2 – Direitos garantidos aos titulares de dados (Art. 6º Lei 13.709/2018)

Direitos dos Titulares de Dados que decorrem dos princípios	Princípio Correspondente
Direito ao tratamento subordinado aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades	Princípio da Finalidade
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Princípio da Adequação
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
Direito a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais	Princípio do Livre Acesso
Direito a 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
Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.	Princípio da Transparência
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
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
Direito de não ser discriminado de forma ilícita ou abusiva	Princípio a não discriminação
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

Fonte: Guia de Boas Práticas para Implementação na Administração Pública Federal (Abri/2020).

No capítulo II da LGPD estão elencados os requisitos para o tratamento dos dados pessoais, que pode ser realizado desde que tenha previsão em uma das hipóteses previstas no

Art. 7°, uma vez que garantidas tais condições permitam a verificação por parte do Controlador e do Operador se o tratamento de dados que foi definido pela instituição é permitido.

O quadro abaixo traz uma síntese dessas hipóteses para tratamento de dados pessoais:

Quadro 04 – Hipótese de tratamento de dados pessoais (Art.7°, da Lei 13.709/2018)

HIPÓTESE DE TRATAMENTO
Mediante consentimento do titular
Para cumprimento de obrigação legal ou regulatória
Para execução de políticas públicas
Para realização de estudo e pesquisas
Para execução ou preparação de contrato
Para exercício de direitos em processo judicial, administrativo e arbitral
Para proteção da vida ou da incolumidade física do titular ou de terceiro
Para tutela da saúde do titular
Para atender interesses legítimos do controlador ou de terceiro
Para proteção do crédito
Para garantia da prevenção à fraude e à segurança do titular

Fonte: Guia de Boas Práticas para Implementação na Administração Pública Federal (Abri/2020).

A LGPD também dispõe de critérios para situações que pode haver a dispensa do consentimento do titular dos dados, conforme destacado no quadro abaixo;

Quadro 05 - Hipóteses nas quais o tratamento de dados é permitido com dispensa da exigência do consentimento do titular.

Hipóteses (Art.7º da Lei 13.309/2018)	
Questões legais	Para o cumprimento de obrigação legal ou regulatória pelo controlador (Art. 7º, inciso II).
Políticas públicas	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 (Art. 7º, inciso III).
Pesquisas	Para a realização de estudos por órgão de pesquisa, garantida sempre que possível, a anonimização dos dados pessoais (Art. 7º, inciso IV).
Contratos	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 (Art. 7º, inciso V).
Processo Judicial	Para o exercício regular de direitos em processo judicial, administrativo ou arbitral (Art. 7º, inciso VI).
Vida	Para a proteção da vida ou da incolumidade física do titular ou de terceiros (Art. 7º, inciso VII).

Saúde	Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (Art. 7º, inciso VIII).
Legítimo interesse	Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso que prevalecer direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (Art. 7º, inciso IX).
Crédito	Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (Art. 7º, inciso X).

No entanto, é necessário ponderar a respeito desse tipo de autorização listado no Quadro 05, pois deve-se manter a circulação de dados pessoais de forma restrita e só podem ser usados em consonância com a finalidade que ensejou a sua solicitação. Por outro lado, a Lei de Acesso à Informação (Lei 12.527/2011) estabelece a possibilidade de divulgação quando houver interesse preponderante e irrestrito para fins de transparência, como em nos casos de contratos públicos firmados entre empresas e a administração pública. De qualquer forma, não temos dúvida que a ampla divulgação de dados pessoais pode gerar impactos negativos para os titulares e por essa razão merecem atenção redobrada.

IV - ETAPAS DO PLANO DE ADEQUAÇÃO

A adequação da UNIR à LGPD está diretamente condicionada a um esforço para transformação cultural da instituição e visa alcançar todas as dimensões, e precisa envolver algumas ações fundamentais ou desde a estratégica até a operacional, essa transformação envolve:

1. Conscientização da Comunidade Universitária.
2. Apoio da alta administração.
3. Definição dos atores envolvidos.
4. Capacitação/Treinamento especializado.
5. Criação de uma Política Institucional de Proteção e Privacidade de Dados Pessoais.
6. Constituição de grupo de trabalho para gestão de riscos e incidentes relacionados à LGPD.

Nesse contexto apresenta-se um fluxo (Apêndice 1) que traz uma síntese das ações para adequação à LGPD a seguir consta a descrição das etapas a serem seguidas, cuja representação visual está no Apêndice 2.

4.1 Identificação dos agentes de tratamento de dados

Esta etapa consiste em identificar os agentes de tratamento de dados pessoais (controlador e operador) e o encarregado. A definição dos papéis serve para resguardar ambas as partes, os agentes públicos ou privados e os titulares de dados pessoais. Os agentes de tratamento de dados pessoais desempenham um importante papel no levantamento das informações necessárias para adequação da universidade à LGPD.

Controlador: é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. No âmbito da Administração Pública será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade que representa a instituição, a qual está imbuída de adotar as decisões acerca do tratamento de tais dados (ANPD, 2021, p.7).

Operador: é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. São agentes públicos que exercem tal função, bem como pessoas jurídicas representante do Controlador, que exercem atividade de tratamento no âmbito de contrato ou instrumento congênere (ANPD,2021, p.16).

Encarregado: Pessoa indicada (natural ou jurídica) pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD, 2021, p.22).

4.2 Alinhamento de expectativas com a alta administração

Consiste na apresentação das expectativas da alta administração e das prioridades às ações mais urgentes que guiarão a cultura de proteção de dados na instituição.

4.3 Análise da maturidade - Diagnóstico do atual estágio de adequação à LGPD

Nessa etapa será analisado o nível de maturidade da instituição à LGPD com o objetivo de fornecer informações necessárias para um diagnóstico. Os resultados apresentarão um índice de maturidade que possibilitará o direcionamento de esforços e a priorização das ações necessárias, visando a melhoria do tratamento e da proteção de dados.

4.4 Análise e adoção de medidas de segurança inclusive diretrizes e cultura externa

Nesta etapa deve ocorrer o planejamento com a análise de quais medidas de segurança podem ser adotadas (Art. 46 da LGPD). Cada medida deve acompanhar o objetivo que se espera alcançar com a aplicação da medida, para o aprimoramento de diretrizes e cultura de respeito e proteção de dados pessoais[5].

Quadro 06: medidas de segurança

MEDIDA DE SEGURANÇA	DESCRIÇÃO
CLASSIFICAÇÃO DA INFORMAÇÃO	Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a instituição.
COMPARTILHAMENTO, USO E PROTEÇÃO DA INFORMAÇÃO	Assegurar a privacidade e proteção das informações de identificação pessoal, conforme requerido por legislação e regulamentação pertinente.
CONTINUIDADE DAS ATIVIDADES	A proteção de dados deve ser contemplada nos sistemas de gestão da continuidade das atividades da instituição
CONTROLE DE ACESSO LÓGICO	Limitar o acesso à informação e aos recursos de processamento da informação.
CONTROLES CRIPTOGRÁFICOS	Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.
CONTROLES DE COLETA E PRESERVAÇÃO DE EVIDÊNCIAS	A instituição deve definir e aplicar procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências para a proteção de dados pessoais.
CÓPIA DE SEGURANÇA	Cópias de segurança das informações, de softwares e das imagens do sistema devem ser efetuadas e testadas regularmente, conforme a política de segurança definida.
DESENVOLVIMENTO SEGURO	Garantir que a proteção de dados está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.
GESTÃO DE MUDANÇAS	Mudanças na organização, nos processos de negócios, nos recursos de processamento da informação e nos sistemas que afetam a proteção de dados devem ser controladas.
GESTÃO DE RISCOS	Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a instituição. Destinado a fornecer segurança razoável quanto à proteção dos dados pessoais e à realização de seus objetivos.
ORGANIZAÇÃO DE SEGURANÇA	Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança dos dados dentro da organização.
POLÍTICA DE SEGURANÇA	Prover orientação da direção e apoio para a segurança dos dados pessoais de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

[5] Guia de Elaboração de Programa de Governança em Privacidade, 2020.

PROTEÇÃO FÍSICA E DO AMBIENTE	Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento e informações institucionais
REGISTRO DE EVENTOS E RASTREABILIDADE	Registrar eventos e gerar evidências a fim de proporcionar rastreabilidade
SEGURANÇA EM REDES	Assegurar a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.
SEGURANÇA NAS OPERAÇÕES	Garantir a operação segura e correta dos recursos de processamento da informação.
TRATAMENTO E RESPOSTA A INCIDENTES	Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais, incluindo a comunicação sobre fragilidades e eventos de segurança.

Fonte: ENAP/2020/ABNT/ISO 27002:2013; ISO/IEC 29151:2016.

Para cada medida de segurança deverão ser elencados controles a serem aplicados sobre os ativos organizacionais, que são bases de dados, documentos, equipamentos, locais físicos, sistemas e até mesmo pessoas que compõem uma instituição.

Sugere-se que seja criada uma planilha de controle na qual deve constar a descrição do controle em formato de pergunta que tem a finalidade de verificar se o controle está sendo aplicado no ativo organizacional. Para tanto, propõe-se no Apêndice 3 um quadro para controle das ações específicas de segurança que podem ser aplicadas sobre os ativos organizacionais.

4.5 Instituição de estrutura organizacional para governança e gestão da proteção de dados pessoais

A execução do Plano de Adequação à LGPD, bem como a realização das atividades pertinentes às atribuições do Encarregado, deve ocorrer de forma estruturada e planejada. Sugere-se que tenha como base a Portaria da Anatel n°1197, de 25 de agosto de 2020, que estabelece as competências de um Escritório de Apoio a Proteção de Dados[6]., que obedece a estrutura recomendada, embora num primeiro momento possa ser exercido pela própria Comissão de Segurança da Informação e Avaliação de Processos Sigilosos (Resolução 374/Consad/2021).

4.6 Inventário de dados pessoais

Essa etapa consiste no mapeamento dos dados pessoais tratados na instituição que indicará em que grau a universidade atende o que está disposto na LGPD e quais controles ainda não foram observados. É uma ferramenta que identifica quais dados pessoais são tratados, onde

[6] Ver Guia de Elaboração de Programa de Governança em Privacidade, 2020.

ficam armazenados e que operações são realizadas com eles e a partir deles, devendo observar o previsto no Art. 37 da LGPD. Atualmente a ferramenta mais utilizada para mapear os dados de instituições públicas ou privadas é conhecida como Record Of Processing Activities/ROPA, que segue princípios General Data Protection Regulation-GDPR, que é regulamento adotado para a proteção de dados na Europa. Para Pinheiro (2018) consiste em criar uma matriz de tratamento de dados pessoais que será alimentada com as informações de quais são os tipos de tratamento de dados e para quais finalidades.

4.7 Levantamento dos contratos relacionados a dados pessoais

Para as adequações contratuais (já existentes e futuras) deverão ser utilizadas as informações mapeadas no Inventário de dados. Para tanto é fundamental a existência de um Grupo de Trabalho para analisar os dados que já foram mapeados no inventário e se criar um Programa de Gerenciamento de Privacidade/PGP para proteger os direitos do cidadão. Sugere-se que sejam observados os aspectos listados no quadro 07.

Quadro 07: Orientações para o Programa de Gerenciamento de Privacidade.

Gerenciamento de Direitos Individuais	Consentimento e rastreamento de Preferência	Redução de responsabilidade por violação
1- Respeito aos direitos individuais de privacidade. 2- Respeito ao direito de o titular acessar seus dados pessoais tratados na instituição. 3- Direito de o titular solicitar atualização de seus dados. 4- Adoção de procedimentos de preparação para recebimento das demandas (incluindo reclamações), realização de triagem e respostas aos titulares dos dados (demandantes).	1- Reunir o consentimento. 2- Rastrear solicitações de preferências tanto dos titulares de dados como dos agentes de tratamento.	1- Criptografia. 2- Anonimização de dados

Fonte: Guia de Elaboração de Programa de Governança em Privacidade, 2020 (adaptado)

4.8 Políticas e práticas para proteção da privacidade do cidadão

Nessa etapa são especificadas as políticas e práticas para proteger a privacidade do cidadão e garantir que o uso dos dados pessoais seja adequado, de acordo com a legislação. Para tanto, é necessário definir os papéis específicos dos servidores envolvidos na coleta,

retenção, processamento, compartilhamento e eliminação dessas informações[7]. Outro ponto a se destacar nessa etapa são as ações educativas que devem ser ofertadas a servidores (incluindo terceirizados) que atuem ou tenham acesso a dados de usuários ou outras pessoas que tenham vínculo com a instituição.

4.9 Cultura de segurança e proteção de dados pessoais desde a concepção (*privacy by design*)

Um dos maiores desafios para o Plano de Adequação da UNIR à LGPD será uma mudança na cultura organizacional da instituição, envolvendo um processo de orientação e sensibilização de todos os envolvidos. Neste aspecto, algo a ser difundido é o conceito de privacidade desde a concepção de práticas, serviços, projetos, produtos e sistemas, persistindo em todo o ciclo em que haja dados pessoais sendo trabalhados, sobretudo naqueles que estejam presentes nas tecnologias da informação e comunicação.

4.10 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais/RIPD é o documento de comprovação por meio do qual o Controlador pode apresentar o registro de todas as etapas de uma avaliação de riscos nas operações que envolvam essas informações, incluindo a coleta, tratamento, uso e compartilhamento. Para tanto, precisam estar estabelecidas e implementadas quais são medidas adotadas para mitigar os riscos que possam afetar os direitos fundamentais dos titulares, conforme está previsto no inciso XVII do art. 5°, combinado com o parágrafo único do Art. 38, da LGPD.

> Art. 5° Para fins desta Lei, considera-se:
> (...)
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
> (...)
>
> Art.38. A autoridade Nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

[7] Guia de Elaboração de Programa de Governança em Privacidade, 2020.

> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O RIPD deverá ser produzido antes da instituição iniciar o tratamento das informações pessoais dos seus usuários e servidores. Deve ocorrer na fase inicial da implantação do Plano de Adequação (ENAP/2021), contemplando as várias ações que se inserem nas etapas que ora estão sendo descritas e que o esquema do trabalho em espiral consta no Anexo 1, que são "Etapas da fase de Elaboração do RIPD", presente no "Guia de boas práticas sobre a LGPD", produzido pelo Comitê Central de Governança de Dados.

4.10. Etapas da fase de elaboração do RIPD

1ª Etapa: Identificar os Agentes de Tratamento e o Encarregado

A primeira etapa na elaboração do Relatório de Impacto à Proteção de Dados Pessoais - RIPD, compreende a identificação dos agentes de tratamento de dados pessoais (Controlador e Operador) e o Encarregado, que ficarão responsáveis pelo levantamento das informações primordiais para a elaboração do RIPD.

O artigo 5° da LGPD, em seus incisos VI, VII e VIII trazem a definição desses atores conforme segue abaixo:

> Art.5° Para fins desta Lei, considera-se:
> VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII -operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado pessoa indicada pelo controlador e operador para atuar como canal de comunicação de Dados (ANDP).

2ª etapa: Identificar a necessidade de elaborar o Relatório

O Relatório de Impacto à Proteção de Dados Pessoais é o documento que serve de norteador para a adequação da Universidade à LGPD. Portanto, recomendamos sua elaboração. Nesse documento deverá constar informações de quais dados pessoais são coletados, tratados, usados, compartilhados e quais são as medidas adotadas para a mitigação de possíveis riscos. Além dos casos específicos previstos pela LGPD, o RIPD também poderá ser elaborado ou

atualizado nas situações em que haja a possibilidade de ocorrência de impactos a privacidade dos dados pessoais, resultante de:

A - Uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados.

B - Rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art.12 §2°).

C - Tratamento de dado pessoal sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (LGPD, art. 5º, II).

D - Processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20).

E - Tratamento de dados pessoais de crianças e adolescentes (LGPD, art.14).

F - Tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art.42).

G - Tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art.4°, §3°).

H - Tratamento no interesse legítimo do controlador (LGPD, art. 10, §3º).

I - Alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operações do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados etc.

J - Reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Obs.: Quando houver a necessidade de elaboração de um RIPD, devem se esclarecer qual (ais) dos itens acima demonstram essa necessidade.

3ª etapa: Descrever o tratamento

Nessa etapa são descritos os processos de tratamento de dados pessoais e dados pessoais sensíveis que podem gerar riscos às liberdades civis e aos direitos fundamentais, contempla a especificação da natureza, escopo, contexto e finalidade do tratamento.

O objetivo dessa descrição é reunir as informações que permitirão conhecer a conjuntura institucional referente aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos (ENAP/2020).

É importante destacar que a LGPD (Art. 5°, X), considera tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Se a instituição entender mais condizente com sua realidade de tratamento de dados pessoais, pode reunir a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD.

- **Natureza do tratamento**: representa como a instituição pretende tratar ou trata o dado pessoal;
- **Escopo do tratamento**: representa a abrangência do tratamento de dados;
- **Contexto do tratamento**: inclui fatores internos e externos que podem afetar as expectativas do titular.
- **Finalidade do Tratamento**: é a razão ou motivo pelo qual se pretende tratar os dados pessoais. A definição da finalidade é uma etapa importante pois, justificará o tratamento e base para informar o titular dos dados.

Ao detalhar a finalidade de tratamento de dados pessoais deve se considerar:

A. Que indicam qual (is) o (os) resultado (s) pretendido (os) para os titulares dos dados pessoais, informando o quão importante são esses resultados.
B. Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

4ª etapa: Identificar partes interessadas consultadas

Devem ser identificadas as partes interessadas relevantes internas e externas, consultadas a fim de obter opiniões legais técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento. Nessa etapa, deve-se destacar:

A. Quais partes foram consultadas, como por exemplo operador (LGPD, art. 5°, VII), encarregado (LGPD, art.5°, VIII), gestores, especialistas em segurança da informação, consultores jurídicos etc.

B. O que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve-se observar os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).

Obs.: Na impossibilidade de registrar o que foi consultado, é necessário justificar o motivo de não ter realizado o registro.

5ª etapa: Descrever necessidade e proporcionalidade

Nessa etapa deve ser demonstrado que as operações realizadas sobre os dados pessoais se limitam ao mínimo necessário para o alcance de suas finalidades, com alcance dos dados adequados proporcionais e não excessivos em relação às finalidades do tratamento de dados (Art. 6°, III da LGPD).

Outro ponto a ser destacado é a fundamentação legal para o tratamento que se deseja realizar. Se o embasamento for o legítimo interesse[8] do controlador (Art. 10, LGPD), deve por exemplo ser provado que:

A. O tratamento de dados pessoais é indispensável.
B. Inexistência de outra base legal possível de se utilizar para alcançar o mesmo propósito.
C. O processamento proposto de fato auxilia no propósito almejado.
D. Como será garantida a qualidade (exatidão, clareza, relevância e atualização dos dados e minimização dos dados).
E. Quais medidas são adotadas a fim de assegurar que o operador (Art. 5º, VII, LGPD), realize o tratamento de dados pessoais, conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (Art.5°, VI, LGPD).
F. Como estão implementadas as medidas que assegurem o direito de o titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
G. Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
H. Quais são as salvaguardas para as transferências internacionais de dados.

É necessário também criar os procedimentos para atender os direitos previstos no art. 18 da LGPD, que trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os seus dados pessoais. Além

[8] O legítimo interesse consiste em que o tratamento de dados seja pautado em fundamentações claras e legítimas e somente dados rigorosamente necessários sejam coletados com garantia de uso para a finalidade informada, proteção e privacidade do titular (PINHEIRO,2018, p.04).

disso, é necessário estabelecer quem na instituição representa o controlador na coleta, tratamento e proteção de dados.

6ª etapa: Identificar e avaliar os riscos

O relatório deve ter uma seção que trata da identificação e avaliação de riscos na qual deverá tratar das ações necessárias para identificar e avaliar os riscos que podem comprometer a privacidade dos dados pessoais tratados pela instituição.

No art. 5°, XVII da LGPD está disposto o que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco".

O procedimento inicial é a identificação dos riscos que geram impacto potencial sobre o titular dos dados pessoais.

Para cada risco identificado, deve ser definida a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

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

7ª etapa: Identificar medidas para tratar os riscos

Nessa etapa devem ser reunidas as informações que se referem às medidas que serão adotadas para cada situação que podem ser de segurança, técnicas ou administrativas.

O art. 46 da LGPD determina que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Durante esse processo, a instituição pode decidir que alguns riscos são aceitáveis, até um risco de nível alto, em razão dos benefícios do processamento dos dados pessoais e dificuldades de mitigação. Se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.

No primeiro momento deve-se identificar em qual fase do ciclo de vida de dados pessoais o risco pode gerar algum tipo de impacto, com essa informação determina-se a medida a ser aplicada para o tratamento do risco.

A efetivação das medidas de segurança ocorre mediante a aplicação dos controles sobre os ativos organizacionais.

8ª etapa: Aprovar o relatório

Essa etapa compreende a formalização da aprovação do RIPD por meio da obtenção das assinaturas do responsável pela elaboração do RIPD e pelas autoridades que representam o controlador e operador. O responsável pela elaboração do relatório pode ser o próprio encarregado, ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar essa tarefa.

9ª etapa: Manter revisão

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados na instituição. As mudanças podem ser motivadas por alterações:

A. Significativas na finalidade do tratamento de dados pessoais que impacte no processo de como esses dados são tratados
B. Expressivas na quantidade de dados pessoais coletados e no contexto do tratamento de dados resultantes de identificação de falta de segurança no uso de uma nova tecnologia, nova preocupação pública sobre o tipo de tratamento de dados realizado pela instituição ou vulnerabilidade de um grupo específico de titulares de dados pessoais.

A instituição deve manter a revisão do RIPD para demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações na conjuntura tecnológica, normativa, política e institucional.

4.11 POLÍTICA DE PRIVACIDADE E DE SEGURANÇA DA INFORMAÇÃO

Segundo a Instrução Normativa n°1 de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, nessa etapa ocorre a atualização das diretrizes internas de proteção de dados pessoais. Para tanto, é feita uma revisão para verificar se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessária a retenção de determinados dados tratados e se é necessário revisar alguns contratos. Também é necessário fazer uma busca se já existe uma Política de Privacidade na Instituição para que seja atualizada ou construída conforme o Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos.

A Política de Privacidade é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário. A Política de Privacidade, que faz parte do Termo de Uso, origina-se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados e informarem como as atividades de tratamento de dados atendem os princípios dispostos no artigo 6° da LGPD.

A Política de Privacidade é um dever do controlador e um direito do usuário, portanto, deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares dos dados seja garantida de forma eficiente e como os princípios da: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

A Política de Privacidade deve contemplar os seguintes tópicos:

- Controlador;
- Operador;
- Encarregado;
- Quais dados são coletados;
- Qual o tratamento realizado e para qual finalidade;
- Compartilhamento de dados;
- Segurança dos dados;
- Uso de Cookies;
- Tratamento posterior dos dados para outras finalidades;
- Transferência internacional de dados.

Os direitos dos titulares precisam ser gerenciados e para início desse processo é necessário que as informações referentes às obrigações quanto ao fornecimento de informações aos titulares com relação ao tratamento dos dados pessoais, termo de uso e política de privacidade sejam bem explicadas para dirimir qualquer tipo de dúvida que possa surgir.

4.12 Adequação de cláusulas contratuais

Para adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados pelo Inventário realizado na etapa de Iniciação e Planejamento da Adequação da UNIR à LGPD é necessário revisar os documentos vigentes e

os dados já coletados. No âmbito dos contratos administrativos, pode ser necessário que a Administração Pública revisite as cláusulas contratuais econômicas firmadas, mesmo após concluído o certame. Pode ser necessário incluir novas cláusulas, conforme os princípios da LGPD, preconizados no seu art. 6º.

4.13 Termo de uso

O Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele. Representa o compromisso do Controlador e Operador com a transparência ao titular de dados pessoais e comunica como as atividades de tratamento desses dados observam os princípios dispostos na LGPD.

Para assegurar aos cidadãos o amplo acesso às informações é fundamental que os termos devam ser regularmente atualizados a fim de refletir, de modo claro e preciso, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares, que comumente serão utilizados pela instituição no exercício de suas competências legais ou execução de políticas públicas com previsão legal. Os tópicos que devem constar no Termo de Uso são:

- Aceitação dos Termos e Políticas,
- Definições,
- Arcabouço Legal,
- Descrição do serviço,
- Direitos do usuário,
- Responsabilidade do usuário e da Administração Pública,
- Mudanças no Termo de Uso,
- Informações para contato e foro[9].

4.14 Indicadores de Conformidade e Performance

Os indicadores de Performance (Key Performance Indicator - KPI), incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no Plano de Adequação. Recomenda-se o uso dos seguintes indicadores:

A. Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais.

[9] Guia de Elaboração de Programa de Governança em Privacidade (2020).

B. Resultados do Diagnóstico de Adequação à LGPD - índice de adequação.
C. Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados, número de serviços com dados pessoais do órgão *100[10].
D. Índice de serviços com termo de uso elaborado: quantidade de serviços com termo de uso elaborado/ quantidade de serviços do órgão *100.
E. Índice de serviços com RIPD elaborado: quantidade de serviços com RIPD elaborado/quantidade de serviços do órgão *100.
F. Índice de conscientização em segurança: quantidade de treinamentos realizados/quantidade de treinamentos previstos *100.
G. Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço/quantidade total de controles de segurança e privacidade identificados para o serviço *100.

4.15 Gestão de Incidentes

Deve ser criado um processo de Gestão de Incidentes, que registre os incidentes ou eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente e as medidas tomadas para mitigá-los para evitar as reincidências. Pode-se implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação e privacidade, de forma a reduzir o nível de risco ao qual a Solução de TIC e/ou órgão estão expostos, considerando os critérios de aceitabilidade de risco definidos pelo órgão.

Outra recomendação a ser seguida é a construção de um Plano de Comunicação orientando a forma que os incidentes de segurança, que acarretem risco ou dano, sejam informados aos órgãos fiscalizatórios e à imprensa, bem como a construção de uma política de comunicação da UNIR. [11].

4.16 Análise e Reporte de resultados

Para demonstrar o valor do Plano de Adequação para a alta administração é indicado que seja realizado um monitoramento que contenha a análise e reporte registro dos resultados.

[10] Indicadores de desempenho de processos, quantificam o desempenho de atividades relacionadas à produção de bens e serviços, medem a eficiência de determinado processo de trabalho (BAHIA, 2021).
[11] Guia de Elaboração de Programa de Governança em Privacidade (2020).

Dar publicidade a evolução das ações e resultados obtidos e a função da privacidade para o cidadão reforçam e fortalecem a cultura de privacidade dos dados[12].

Na etapa de monitoramento o Encarregado deve assumir a articulação desse processo exercendo a função de:

A. Gerenciamento do estabelecimento de métricas para auxiliar no acompanhamento das ações do Plano de Adequação à LGPD.
B. Divulgação dos resultados entre as diversas áreas da instituição - estabelecimento de uma estrutura de divulgação de resultados para a alta direção dos órgãos e entidades.

[12] Guia de Elaboração de Programa de Governança em Privacidade (2020.

REFERÊNCIAS E BIBLIOGRAFIA CONSULTADA

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS - ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**, Brasília, ANPD, 2021.

BAHIA, Leandro Oliveira. **Guia referência para construção e análise de indicadores**, Brasília, ENAP: 2021.

BRASIL, **Constituição da República Federativa do Brasil**. Brasília: Senado Federal,1988.

BRASIL, **Lei n°13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). In Diário Oficial da República Federativa do Brasil, DF, 14 de agosto de 2019.

BRASIL. Ministério da Economia. Comitê Central de Governança de Dados/CCGD**. Guia de Boas Práticas para Implementação na Administração Pública Federal**. Brasilia/DF, Abril/ 2020.

BRASIL. SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL. **Guia de Elaboração de Programa de Governança em Privacidade**. Ministério da Economia Outubro, 2020.

DONDA, Daniel. Guia Prático de Implementação da LGPD: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020, 144p.

GARCIA, Lara Rocha; FERNANDES, Edson Aguilera; GONÇALVES, Rafael Augusto Moreno; PEREIRA-BARRETO, Marcos Ribeiro. Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implantação. São Paulo: Editora Blucher, 2019.

LUNA, Francisco Djalma Silva. Instituições de Ensino Superior Brasileiras e sua Jornada para a Transformação Digital,2020. 139p. Dissertação de Mestrado (Programa de Mestrado Profissional em Empreendedorismo). Faculdade de Economia, Administração e Contabilidade de São Paulo, Universidade de São Paulo, São Paulo, 2020.

OLIVEIRA, Sandro Lima. **LGPD – Como aplicar na sua organização**. [S.I.] E-book,2020. Disponível em: https://ler.amazon.com.br.

PINHEIRO, Patricia Peck. Proteção de Dados Pessoais – Comentários a Lei n°13709/18 – LGPD. São Paulo: Ed. Saraiva Educação, 2018.

PIRONTI, Rodrigo. **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021.

SOUZA NETO, José Luiz de. A Proteção dos Dados Pessoais na Era da Informação. [S.I] Ebook, 2020. Disponível em: Kindle Cloud Reader (amazon.com.br)

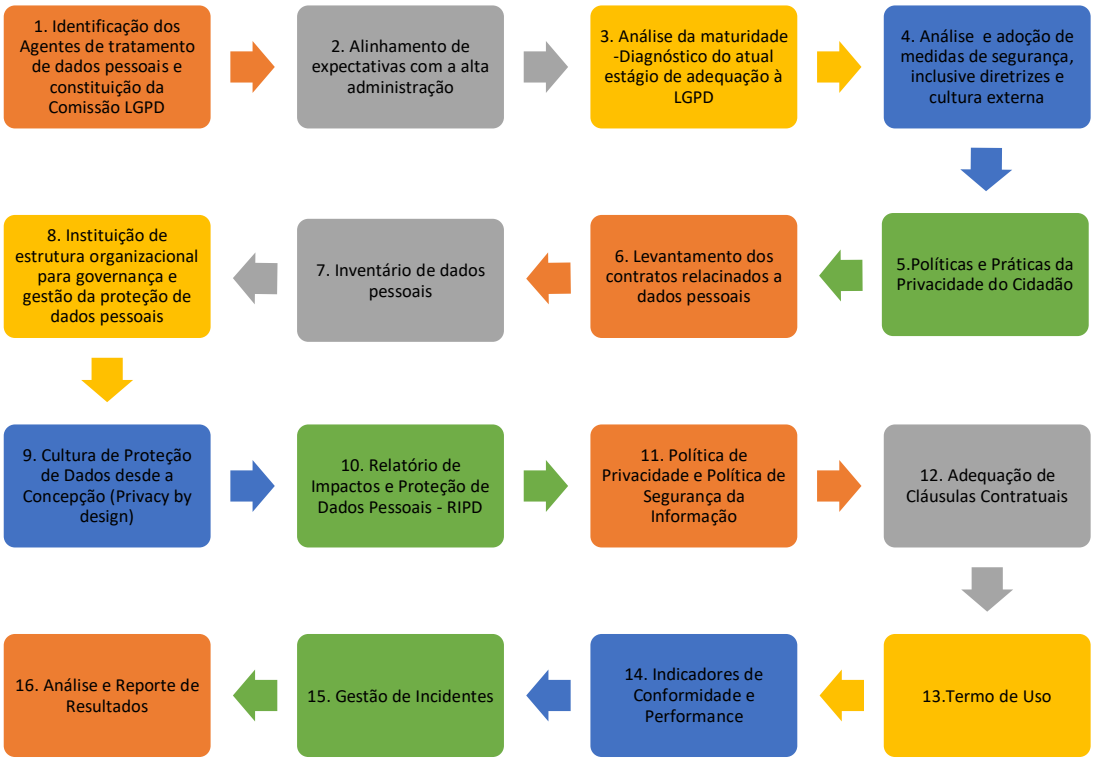
TEIXEIRA, Ilderlandio. **Fundamentos Jurídicos – LGPD**. [S.I] Ebook, 2020. Tratamento de Dados Pessoais no Setor Público. ENAP Fundação Escola Nacional de Administração Pública, 2020.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO/UFRJ. COMITÊ DE GOVERNANÇA DIGITAL – CGD. **Plano de Adequação à Lei Geral de Proteção de Dados Pessoais – LGPD**. Universidade Federal do Rio de Janeiro -UFRJ, Rio de Janeiro, 2020.

APÊNDICES

APÊNDICE 1: FLUXO DA AÇÕES PARA ADEQUAÇÃO DA UNIR À LGPD

APÊNDICE 2: ETAPAS DO PLANO DE ADEQUAÇÃO



APÊNDICE 3: CONTROLE DE AÇÕES DE MEDIDAS DE SEGURANÇA (SIM/NÃO)

	Existe e é executado um processo formal de Gestão de Mudanças na organização?	**É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC**	**Mudanças significativas são identificadas e registradas**
Bases de Dados			
Documentos			
Equipamentos			
Locais			
Pessoas			
Sistemas			
Unidades Organizacionais			

Fonte: ENAP/2020 (adaptado)

ANEXOS

Anexo 1: ETAPAS DA FASE DE ELABORAÇÃO DO RIPD

Fonte: Guia de Boas Práticas – Lei Geral de Proteção de Dados - LGPD