A Novel Framework for Compliance to the LGPD in a Federal Higher Education Institution

Uma Proposta de Metodologia para Adequação à LGPD em uma Instituição Federal de Ensino Superior

Willdson Gonçalves de Almeida[1,2], Nelcileno Virgílio de Souza Araújo[3], Pedro Carlos Oprime[1]

[1]Programa de Pós-Graduação Profissional em Engenharia de Produção – Universidade Federal de São Carlos (UFSCAR) – São Carlos – SP – Brasil

[2]Secretaria de Tecnologia da Informação, Universidade Federal de Mato Grosso (UFMT)
Cuiabá – MT – Brasil

[3]Instituto de Computação, Universidade Federal de Mato Grosso (UFMT)
Cuiabá – MT – Brasil

{willdson.almeida,nelcileno.araujo}@ufmt.br, pedro@dep.ufscar.br

Abstract. *Recently, the topic of data protection has been on the rise in Brazil due to the entry into force of Law No. 13,709/2018, denominate General Personal Data Protection Law (LGPD). The objective of this article, characterized in terms of the research method as a case study, is to present a proposal for a methodology to adapt to the LGPD based on the method developed by the Digital Government Secretariat (SGD) of the Federal Government and describe the adapted adoption at the Federal University of Mato Grosso (UFMT), based on the analysis of the actions planned and carried out in the compliance project. The results provide insights into innovations in the actions developed, aiming to contribute to other public institutions that seek to implement the LGPD.*

Passwords*: LGPD, Compliance, Framework, Higher Education Institution.*

Resumo. *Recentemente, o tema proteção de dados está em alta no Brasil devido a entrada em vigor da Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD). O objetivo deste artigo, caracterizado quanto ao método de pesquisa como estudo de caso, é apresentar uma proposta de metodologia de adequação à LGPD baseada no método desenvolvido pela Secretaria de Governo Digital (SGD) do Governo Federal e descrever a adoção adaptada na Universidade Federal de Mato Grosso (UFMT), a partir da análise das ações planejadas e realizadas no projeto de conformidade. Os resultados fornecem percepções de inovações nas ações desenvolvidas, visando contribuir com outras instituições públicas que buscam implementar a LGPD.*

Palavras-chave*: LGDP, Adequação, Framework, Instituição Federal de Ensino Superior.*

1. Introdução

Nas Instituições Federais de Ensino Superior (IFES), a adequação à Lei Geral de Proteção de Dados (LGPD) se apresenta como um desafio imediato, considerando a

natureza das instituições de ensino, pesquisa e extensão, a quantidade e a variedade dos dados pessoais processados e armazenados. De acordo com dados do cadastro nacional de cursos e instituições de educação superior, plataforma digital do Ministério da Educação, existem atualmente 68 universidades federais [MEC 2023], que compartilham da necessidade de se adequar à lei.

Diante de tal desafio, e, como consequência da necessidade da proteção de dados para garantir a privacidade dos titulares de dados pessoais, a transparência das ações governamentais e a conformidade com as normas legais, a Secretaria de Governo Digital (SGD) desenvolveu o Guia de Elaboração de Programa de Governança de Privacidade com o objetivo de fornecer diretrizes, melhores práticas e orientações específicas para a implementação das medidas necessárias à proteção dos dados pessoais e ao cumprimento das exigências legais, para colaborar com as entidades da Administração Pública Federal (APF) na adequação à LGPD [SGD 2023], do qual a Universidade Federal de Mato Grosso (UFMT) adotou como principal subsídio para direcionamento das ações do processo de conformidade.

De acordo com UFMT (2022), a universidade possui quatro campus, Araguaia, Cuiabá (Reitoria), Sinop e Várzea Grande; 3050 servidores, entre técnicos administrativos e docentes, 87 cursos de graduação presencial, seis cursos de educação à distância, 51 programas de mestrado e doutorado que somam em torno 17 mil alunos matriculados.

Diante desse cenário, o presente estudo parte da questão de pesquisa “As IFES têm à disposição um método de conformidade à LGPD adaptado a sua realidade?”. Com isso, o objetivo do trabalho é apresentar uma proposta de metodologia elaborada no processo de conformidade à LGPD da UFMT. Com base nesse objetivo, espera-se contribuir para a compreensão e aprimoramento das práticas de privacidade e proteção de dados nas IFES, fortalecendo a segurança e a confiabilidade dos sistemas de informações e promovendo a garantia dos direitos fundamentais dos cidadãos em relação à privacidade de seus dados pessoais.

2. Métodos

O estudo se caracteriza como uma pesquisa empírica com abordagem qualitativa, de acordo com os objetivos é uma pesquisa descritiva, utilizando o método estudo de caso. A coleta de dados é predominantemente documental, partindo da análise dos procedimentos adotados e artefatos produzidos. O objetivo geral deste estudo é apresentar uma nova metodologia no processo de conformidade da UFMT à LGPD, descrevendo suas etapas, ações, produtos e resultados. Como objetivos específicos, identificar as boas práticas implementadas, os desafios encontrados e os resultados alcançados até o momento, visto que o processo está em andamento.

Considerando as buscas realizadas nas bases Scopus, Web of Science, Scielo, Periódicos CAPES e Google Acadêmico por estudos que abordem a conformidade de instituições federais de ensino à LGPD, foram encontrados nove documentos que permeiam o assunto deste trabalho, entre eles artigos, dissertações e monografias. Destacam-se, Souza (2022) analisou a conformidade de 18 IFES, na perspectiva dos servidores envolvidos ou não com privacidade e proteção de dados, Marques (2022) avaliou a adequação da Universidade Federal do Rio Grande do Sul pelos normativos

publicados pela instituição, Teodoro *et al.* (2023) propôs um modelo teórico do processo de adaptação à LGPD aplicado à Universidade do Estado de Santa Catarina (UDESC), Jesus (2022) elaborou um método para conformidade utilizando a ISO 27701 para a Universidade de Rio Verde. No entanto, um diferencial deste trabalho em relação aos encontrados é a utilização do Guia do Programa de Governança em Privacidade (PGP) elaborado pela SGD, ilustrado na Figura 1, como modelo referencial. Este método foi definido pelo órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), do qual fazem parte as IFES. Tendo esta, estreita relação de proximidade e entendimento das necessidades dos órgãos da APF.

Figura 1 – Marcos do Programa de Governança de Privacidade (SGD).

Na metodologia implementada na UFMT, descrito na Figura 2, foram priorizados os grandes marcos do PGP, tais como: Análise de Maturidade - Diagnóstico do atual estágio de adequação à LGPD, Inventário de Dados Pessoais (IDP), Relatório de Impacto à Proteção de Dados Pessoais (RIPD), Política de Segurança da Informação e Privacidade de Dados (PSIPD) e Cultura de Segurança da Informação e Proteção de Dados. A observação pretendida nesse método é verificar a viabilidade de uma metodologia mais enxuta para realizar uma adequação mínima à LGPD num período de 1 ano de implantação e nos anos subsequentes ajustar os outros marcos necessários para funcionamento cíclico dessa conformidade.

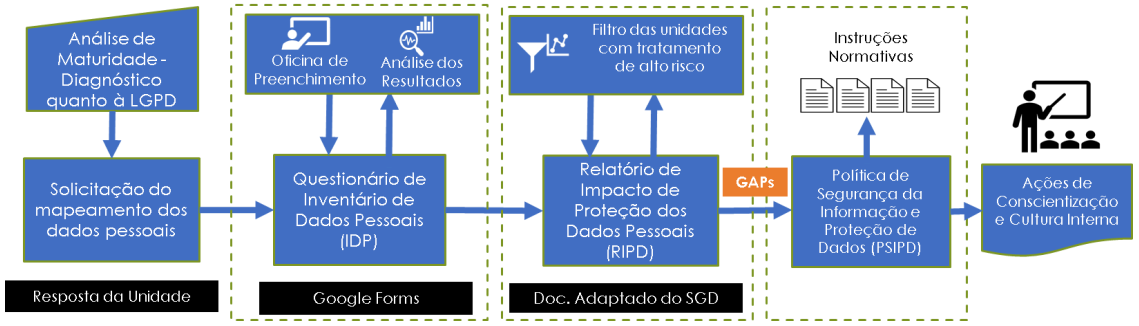

Figura 2 – Método de implantação da LGPD na UFMT.

A seleção desses marcos principais para metodologia proposta é baseada na própria LGPD, como pode ser observado em Brasil (2018), quando afirma no Art. 32

que "*A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais*(...)". Sendo assim, é uma obrigação das IFES ter o RIPD da sua instituição elaborado, caso seja cobrada pelos órgãos fiscalizadores.

Ainda de acordo com Brasil (2018), o RIPD é um documento que *"(...) 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.*". Dessa forma, para realizar o RIPD é necessário, primeiramente, a construção do IDP.

O IDP é um documento que cataloga as operações de tratamento de dados pessoais realizadas pela instituição, por meio, da descrição das seguintes informações: (1) identificação do serviço/processo; (2) identificação dos agentes de tratamento e encarregado; (3) atuação do operador no ciclo de vida do dado pessoal; (4) fluxo de tratamento dos dados pessoais; (5) escopo e natureza dos dados pessoais; (6) finalidade do tratamento dos dados pessoais; (7) categorias de dados pessoais; (8) categorias de dados pessoais sensíveis; (9) frequência e totalização das categorias de dados pessoais tratados; (10) categorias de titulares de dados pessoais; (11) compartilhamento de dados pessoais; (12) medidas de segurança/privacidade; (13) transferência internacional de dados pessoais [Machado 2021]. Com o mapeamento de dados realizado no IDP, torna-se possível a elaboração do RIPD.

Contudo, para a construção do IDP e do RIPD, é necessário entendermos o grau de maturidade da instituição com relação à conformidade a LGPD, dessa forma, o marco "Análise de Maturidade - Diagnóstico do atual estágio de adequação à LGPD" também é um documento essencial para saber em que ponto a instituição se encontra e o percurso para a conformidade.

Com os riscos apresentados pelo RIPD, a instituição deve propor um conjunto de ações para atenuá-los, conforme o que dispõe no Art. 50 da LGPD [Brasil 2018], onde "*o controlador deve implementar um programa de governança em privacidade que estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade*". Sendo assim, uma PSIPD da instituição cumpre essa função de mitigação dos riscos no tratamento de dados pessoais.

Por fim, ações de conscientização e cultura interna na instituição pretendem atender também ao Art. 50 da LGPD [Brasil 2018] com relação às ações educativas que tenham "*o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular*" no processo de tratamento de dados pessoais.

3. Processo de Adequação à LGPD na UFMT

Nesta seção serão detalhados os principais marcos da adoção da lei pela UFMT, bem como descrita as ações de adequação à LGPD previstas na metodologia proposta.

Para contextualizar o cenário da UFMT no que diz respeito à lei, a Figura 3 apresenta o panorama histórico da LGPD na instituição, com ações que compreendem o período entre 2018 e 2023.

Figura 3 - Panorama histórico da LGPD na UFMT.

3.1 Diagnóstico de maturidade à LGPD

O diagnóstico tem o objetivo de avaliar o nível de aderência à LGPD antes de serem iniciadas as ações de conformidade. Realizado com base no artefato próprio desenvolvido pela SGD, denominado "Diagnóstico e Índice de Maturidade de Segurança para adequação à Lei Geral de Proteção de Dados – LGPD", que avalia uma instituição de acordo com o índice calculado a partir das respostas em sete dimensões de perguntas: (1) Governança, (2) Conformidade legal e respeito aos princípios, (3) Transparência e direitos do titular, (4) Rastreabilidade, (5) Adequação de contratos e de relações com parceiros, (6) Segurança da Informação e (7) Violações de dados. As respostas possíveis para cada questão estão relacionadas às ações tomadas, sendo a) não adota, b) iniciou plano para adotar, c) adota parcialmente e d) adota integralmente.

O índice de avaliação varia entre 0,00 a 1,00, correspondendo ao respectivo nível de adequação, sendo 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 e 0,90 a 1,00 Aprimorado.

De acordo com as respostas da avaliação realizada no início do processo de adequação, a universidade demonstrou possuir controles mais efetivos nas dimensões de Governança, Transparência e Direitos do titular e Violação de Dados. O resultado obtido pela UFMT foi de 0,14, correspondente ao nível de adequação "Inicial", esperado para instituições em início de conformidade.

3.2 Inventário de Dados Pessoais

O Inventário de Dados Pessoais foi adaptado do *template* da SGD, disponibilizado no formato planilha e o mapeamento é organizado em serviços ou processos. A comissão de adequação em análise ao modelo, decidiu simplificar o IDP para ser realizado por unidades superiores da instituição, a ferramenta de coleta utilizada foi o *Google Forms*. O formulário contou com 49 categorias de dados pessoais segmentados por seções, 207 tipos de dados pessoais e dez tipos de dados sensíveis.

As unidades superiores de nível estratégico (reitoria, vice-reitoria, pró-reitorias, secretarias, escritórios, institutos e faculdades) deveriam reunir-se com suas unidades subordinadas (coordenações, gerências, supervisões, departamentos, entre outros) para analisar os tratamentos de dados pessoais nos serviços e processos para posterior consolidação em um mesmo formulário com as respostas de toda a unidade. Com objetivo de subsidiar respostas assertivas das unidades, a comissão elaborou uma oficina de preenchimento do Inventário de Dados Pessoais, ao vivo em formato digital[1].

Das 53 unidades superiores relacionadas para o IDP, 34 (64,1%) responderam o formulário. No entanto, devido a possibilidade de correlação de dados da unidade superior com as unidades subordinadas, foi incentivada a resposta direta também das unidades subordinadas. Dessa forma, foram recebidas um total de 78 respostas, descrevendo as operações de tratamento de dados pessoais.

Considerando as operações inventariadas, cabe relatar que o tratamento de dados pessoais sensíveis realizados pelas unidades respondentes ocorre, principalmente, em dados de origem racial ou étnica fornecidos por titulares de dados do tipo Discente, tendo como fonte de retenção, em sua maioria, o Sistema Eletrônico de Informações (SEI). As fontes de dados utilizadas para coleta dos dados pessoais foram, em geral, dos titulares de dados.

Um outro aspecto a ser salientado no IDP é a existência em muitas unidades de tratamento de dados de crianças, adolescentes e grupos vulneráveis. As principais medidas de segurança/privacidade adotadas pelas unidades foram gerenciamento por senha, não permitir o compartilhamento de contas e senhas e evitar transferência de dados para outros dispositivos se não os da instituição.

3.3 Relatório de Impacto à Proteção de Dados Pessoais

Das 34 unidades superiores respondentes do IDP, foi desenvolvido uma ferramenta para análise da unidade quanto ao tratamento de alto risco. Conforme ANPD (2023), para ser caracterizado como tratamento de alto risco, um tratamento deve atender ao menos a um critério geral e um específico. O critério geral compreende o tratamento em larga escala ou tratamento que possa afetar significativamente os interesses e direitos fundamentais do titular. O critério específico se constitui de quatro possibilidades de tratamento: uso de tecnologias emergentes ou inovadoras, vigilância ou controle de zonas acessíveis ao público, decisões tomadas unicamente com base em tratamento automatizado de dados pessoais para perfilamento ou a utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

Com isso, das 34 unidades, 24 foram caracterizadas com baixo/médio risco e dez consideradas de alto risco, que se fez necessário a elaboração do RIPD. A comissão de adequação desenvolveu um modelo adaptado do *template* do SGD para RIPD, com campos e dados que representam o contexto do tratamento de dados pessoais da instituição. A identificação e avaliação dos riscos foi realizada com base na Metodologia de Gestão de Riscos da UFMT para definição da probabilidade e impacto a Política de Gestão de Riscos da UFMT[2].

---

[1]https://eduplay.rnp.br/portal/video/183209
[2]https://cms.ufmt.br/files/galleries/121/CGGRC/Metodologia_Gest%C3%A3o_Riscos_UFMT_2023.pdf

Dentre os riscos evidenciados nos RIPDs elaborados, os que se destacaram foram: 1) coleção excessiva de dados pessoais com informação insuficiente sobre a finalidade desse tratamento; 2) Tratamento de dados pessoais sensíveis e de criança e adolescente ou grupo vulnerável, com informação insuficiente sobre a finalidade ou com retenção prolongada sem necessidade; 3) Tratamento de dados pessoais em larga escala, com informação insuficiente sobre a finalidade ou com retenção prolongada sem necessidade.

Para atenuar esses riscos relacionados pretende-se por meio da PSIPD apresentar normativas sobre controle de acesso, gestão de permissões, plano de backup, plano de continuidade de negócios e recuperação de desastres, histórico de acesso/alterações, coleta de dados, classificação e eliminação de dados (sanitização).

3.4 Política de Segurança da Informação e Proteção de Dados

Tendo em vista a necessidade de se fortalecer a estrutura de Governança de Segurança da Informação, foi planejada a elaboração de uma nova Política de Segurança da Informação e Proteção de Dados para a universidade.

A estratégia é utilizar o documento como instrumento basilar de direcionamento das medidas de segurança que permitirá o incremento da capacidade de prevenir, detectar, remediar e recuperar. A ação será embasada nas boas práticas do CIS, NIST, ISO e no PPSI SGD.

3.5 Cultura e Conscientização

A ação de treinamento e conscientização iniciou com a Oficina de Preenchimentos do Inventário de Dados Pessoais, descrita na seção 3.2, bem como na elaboração de cursos no modelo massivos (MOOC) com certificação em conjunto com a Secretaria de Gestão de Pessoas (SGP), em alinhamento ao Plano de Desenvolvimento de Pessoas (PDP), Workshops e Oficinas.

Planeja-se também a elaboração de material gráfico para divulgação no site institucional, envio em lista de e-mail, afixação nos ambientes, sempre de forma personalizada ao perfil de titular e operador que se pretende abordar: aluno, técnico administrativo, docente, colaborador terceirizado, pesquisador, aluno de extensão, cidadão, entre outros que possam figurar como titular de dados em tratamento realizado pela universidade.

4. Conclusão

A metodologia proposta neste artigo se mostrou uma ferramenta robusta como subsídio à implementação das diretrizes da LGPD. Com respaldo do método do SGD, em especial nos guias e *templates,* permitiram à comissão reduzir o tempo de planejamento e execução das ações. A abordagem da instituição foi de nortear-se pelo método, adaptar o método à realidade da universidade quanto a tempo, recursos humanos e materiais, além das adaptações com o objetivo de detalhar pontos que o guia não aborda com o detalhe suficiente à utilização. Cabe ressaltar que a lei ainda está em fase de maturação, necessitando de regulamentação sobre vários aspectos, que torna o método ainda vago

em alguns cenários. Os modelos de inventário de dados pessoais e relatório de impacto à proteção de dados pessoais foram indispensáveis para a instituição, que utilizou outros modelos de órgãos públicos para complementar a aplicação das ações. A UFMT está empenhada em evoluir a maturidade com as diretrizes da lei, com 6 de 17 ações realizadas (35,29%), as demais ações em estado de planejadas ou previstas. Como trabalhos futuros, pretende-se complementar esse modelo proposto de adequação à LGPD, com os restantes dos marcos do modelo da SGD, bem como buscar as unidades que não foram alcançadas nesse primeiro ciclo de conformidade à lei. Além disso, realizar um estudo comparativo com outras metodologias de adequação realizadas em outras IFES para analisar os pontos fortes e fracos do nosso método.

5. Referências

BRASIL (2018) "Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais", https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

MEC (2023) "Cadastro Nacional de Cursos e Instituições de Educação Superior. Portal de Governo", https://emec.mec.gov.br/.

UFMT (2022) "Relatório de Gestão e Prestação de Contas da Universidade Federal de Mato Grosso", https://cms.ufmt.br/files/galleries/121/Relato%20Integrado/Relat%C3%B3rio_Integrado_2022.pdf.

Marques, A. F. (2022), A implantação da Lei Geral de Proteção de Dados na Universidade Federal do Rio Grande do Sul: uma análise a partir da noção de regime de informação e seus componentes, Universidade Federal do Rio Grande do Sul.

Machado, D. D. (2021). Guia de Elaboração de Inventário de Dados Pessoais. In: *Revista Científica Multidisciplinar Núcleo do Conhecimento*, páginas 93–98.

Teodoro, J., Oliveira, L. S., Junior, J. F. S. (2023). Um modelo Canvas do processo de adaptação à Lei Geral de Proteção de Dados: o caso da Universidade do Estado de Santa Catarina (UDESC). In: *Revista Brasileira de Biblioteconomia e Documentação*, v. 19, páginas 1–28.

Jesus, D. C. (2022), Proposta de um projeto de conformidade a partir da ISO 27701 para implementação de um programa de compliance de proteção de dados à luz da LGPD na Universidade de Rio Verde, UNISINOS.

SGD (2023) "Guia de Elaboração de Programa de Governança de Privacidade", https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_programa_governanca_privacidade.pdf.

ANPD (2023) "Relatório de Impacto à Proteção de Dados Pessoais", 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.