MMAI-LGPD: A Maturity Model for Governance and Data Compliance in Information Systems Institutions

Juliana Saraiva
Departamento de Ciências Exatas
UFPB
Rio Tinto, PB, Brasil
julianajags@dcx.ufpb.br

Cleidson de Souza
Departamento de Informática
UFPA
Belém, PA, Brasil
cdesouza@ufpa.br

Sérgio Soares
Centro de Informática
UFPE
Recife, PE, Brasil
scbs@cin.ufpe.br

ABSTRACT

Context: The General Data Protection Law (LGPD) in Brazil demands organizations implement governance, compliance, and data security frameworks. This requirement is particularly significant for institutions managing Information Systems (IS), which face challenges in aligning technological innovation with regulatory demands. The MMAI-LGPD addresses this gap by integrating legal, organizational, and technological dimensions into a structured compliance framework tailored for IS institutions. **Problem**: Despite the urgency of LGPD compliance, there is no widely adopted maturity model specifically designed for IS institutions, leaving organizations struggling to balance governance, security, and operational efficiency while meeting legal and ethical requirements. **Solution**: This paper presents the MMAI-LGPD, a model that categorizes compliance into five maturity levels and defines 57 items across six dimensions, offering a pathway for improving governance, security, and data management practices. **IS Theory:** The research adopts a sociotechnical approach, building on maturity models in Information Systems to integrate governance, technology, and legal perspectives. **Method**: A qualitative, prescriptive approach was used, including content analysis of LGPD requirements and case studies with six IS institutions. Axial coding validated the model's applicability and identified organizational gaps in compliance practices. **Results**: The MMAI-LGPD provides a practical tool for assessing and improving compliance maturity. Validation results demonstrate its effectiveness in aligning governance, technology, and legal frameworks in IS institutions. **Contributions and Impact on IS**: This research bridges academia and practice, advancing maturity model studies in IS. The MMAI-LGPD enables IS institutions to meet regulatory demands while fostering ethical and sustainable practices in digital ecosystems.

KEYWORDS

LGPD, Compliance Maturity Model, Information Systems Company Governance

1 Introdução

Numa era onde há um amplo uso de tecnologias de monitoramento de dados em tempo real, é crucial que o desenvolvimento de software assegure a proteção e privacidade dos dados pessoais. Com o crescimento das soluções inteligentes e da interconexão de dispositivos digitais na rotina das pessoas, há um aumento significativo na coleta, compartilhamento e processamento dessas informações. Considerando a importância desses dados e o impacto das consequências na realidade das pessoas, diversas regulamentações de privacidade e proteção de dados foram propostas ao redor do mundo, como a *General Data Protection Regulation* (GDPR) na Europa [1] e da Lei Geral de Proteção de Dados (LGPD) no Brasil [2].

Apesar da LGPD ter sido publicada em 2018, muitas instituições ainda não se adequaram à lei, decorrente da falta de conscientização, orientação e cultura de proteção de dados [3]. Essa falta de conformidade viola direitos constitucionais e prejudica a competitividade global do país, especialmente no cenário das empresas de software, uma vez que há uma crescente interconexão de redes e do uso massivo de dados em tecnologias como Inteligência Artificial e dispositivos da internet das coisas (IoT). É neste cenário que se encontram as empresas de software que fornecem sistemas de informação como produto ou serviço.

Embora algumas diretrizes iniciais tenham sido divulgadas, ainda não existe um padrão claro para implantar e avaliar a conformidade à LGPD dentro das instituições. No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) é a entidade responsável por garantir a conformidade com a LGPD [4]. Apesar dos esforços da ANPD nos últimos anos, ainda há uma carência de um modelo de referência para adequação institucional à lei, que claramente exponha quais os itens de conformidade devem ser atendidos, quais ferramentas podem ser adotadas e processos de apoio que podem dar suporte à adequação da LGPD. Além disso, não há um instrumento ou meio transparente de auditoria e inspeção desse processo, que poderia ser adotado internamente nas empresas de software ou pela própria ANPD.

Um Diagnóstico de Adequação à LGPD foi proposto pela Secretaria do Governo Digital[1], mas a falta de clareza nos critérios de avaliação e na adoção das práticas, dificulta a transparência no processo de auditoria. Por vezes, inclusive, este site não está disponível ou instável. Adicionalmente, não há definição clara sobre melhores práticas a serem seguidas nos níveis estratégicos, táticos e operacionais de uma empresa de software, podendo comprometer assim a governança dos dados pessoais e a conformidade legal da instituição.

Como consequência, há (i) uma baixa adesão das instituições aos processos de adequação à LGPD [13], (ii) a adoção de práticas é ultrapassada ou não mais eficiente para os tipos de ataques cibernéticos atuais [14], e (iii) controle e aplicação de sanções administrativas e judiciais de órgãos governamentais pode acontecer com alta subjetividade, dificultando a eficácia da lei de proteção de dados [5]. Além disso, negócios que possuam transações comerciais internacionais podem ser afetados, num curto prazo, por falta de adesão e cumprimento de normas internacionais de privacidade e proteção a dados pessoais, como é o caso da GPDR [6] [7] [8] [9] [10] [11].

Assim, esta pesquisa propõe uma estrutura básica para um modelo de referência a ser adotado pelas empresas de software, especificamente aquelas baseadas em sistemas de informação, contemplando níveis estratégicos, táticos e operacionais de planejamento – MMAI-LGPD (Modelo de Maturidade de Adequação Institucional à LGPD). Ele tem como objetivo principal estabelecer um conjunto de diretrizes para implantar, avaliar e aprimorar a conformidade dessas instituições no *Compliance* com a LGPD. Além da apresentação do modelo de referência, um estudo de empírico foi realizado através de um processo de auditoria para avaliar a conformidade legal à LGPD de 7 empresas de software através do MMAI-LGPD.

Espera-se que o modelo MMAI-LGPD sirva como um arcabouço para (1) Governança de dados, (2) Controle e registro das operações de tratamento de dados pessoais, (3) Atendimento ao titular do dados, (4) Implantação de controles de Segurança da Informação, (5) Gestão de incidente de segurança, e (6) Elaboração de termos e políticas necessárias. O atendimento a todos esses itens é exigido por lei e precisam estar sistematicamente estruturados nas empresas de software. Este planejamento sistemático auxilia a proposição e evolução sistemática de soluções de desenvolvimento e avaliação de software que garantam à inovação tecnológica segura, protegendo os dados pessoais dos usuários.

Diferentemente de abordagens que avaliam a conformidade de sistemas de informação ou de softwares, este modelo foca na instituição, não no produto comercializado, uma vez que a responsabilidade a eventuais danos aos titulares não recai sobre o software, mas sim, sobre pessoas físicas e jurídicas que desenvolvem ou utilizam estes sistemas de informação.

Este artigo está organizado em 8 seções incluindo esta. A Seção 2 aborda as teorias, normativas e materiais de referências adotados na elaboração desta proposta, enquanto a Seção 3 detalha a metodologia utilizada para construção do modelo de maturidade. O MMAI-LGPD está descrito na Seção 4, sendo apresentados todos os seus elementos. A Seção 5 descreve os resultados encontrados no processo de avaliação inicial do modelo proposto. A Seção 6 discute lições aprendidas após a realização do estudo empírico e as limitações do trabalho são expostas na Seção 7. Por fim, a Seção 8 expõe as considerações finais do trabalho.

2 A LGPD e as Resoluções da ANPD

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira aprovada em 2018 e que entrou em vigor em 2020. Seu propósito principal é garantir a proteção da privacidade e dos dados pessoais dos cidadãos brasileiros. Abrange tanto pessoas físicas (CPF) quanto jurídicas (CNPJ) que lidam com informações pessoais no país, seja através da oferta de serviços ou de produtos. A LGPD é fundamentada em princípios amplos e conceituais, em vez de abordar cenários específicos de forma detalhada, o que permite uma interpretação e aplicação flexíveis desses princípios em diferentes contextos. Algumas diretrizes da lei ainda aguardam regulamentação por parte da ANPD.

Além da LGPD, as resoluções da ANPD desempenham um papel crucial na implementação e regulamentação efetiva da proteção de dados no Brasil. Essas resoluções têm como objetivo detalhar e esclarecer aspectos específicos da lei, fornecendo diretrizes mais concretas para sua aplicação prática. As resoluções abaixo foram consideradas na construção do MMAI-LGPD:

1. **Resolução nº 01/2021**: Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.
2. **Resolução nº 02/2022**: Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.
3. **Resolução nº 04/2023**: Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.
4. **Resolução nº 08/2023**: Institui a Política de Governança de Processos da Autoridade Nacional de Proteção de Dados (ANPD).
5. **Resolução nº 15/2024**: Aprova o Regulamento de Comunicação de Incidente de Segurança.
6. **Resolução nº 18/2024**: Aprova o Regulamento da Atuação do Encarregado de Dados Pessoais.
7. **Resolução nº 19/2024**: Regulamenta os artigos da LGPD que tratam da transferência internacional de dados.

Essas resoluções são essenciais para orientar as instituições na adequação à LGPD, fornecendo um instruções mais detalhadas e práticas para a proteção dos dados pessoais. É importante ressaltar

[1] https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd

que o descumprimento das resoluções pode acarretar diversas consequências para as organizações, incluindo sanções administrativas, medidas corretivas e reparatórias e até mesmo a aplicação de multas significativas pela ANPD. Portanto, fica claro que elas são extensões da própria lei e tem força impositiva semelhante às regras dispostas nos artigos da LGPD.

A ANPD tem o papel de fiscalizar e aplicar penalidades às instituições que não cumprem as diretrizes estabelecidas pelas resoluções, o que pode resultar em danos à reputação, perda de confiança dos clientes e parceiros, além de possíveis impactos financeiros e legais. Portanto, é fundamental que as empresas de software estejam em conformidade também com as resoluções da ANPD e adotem medidas efetivas para proteger os dados pessoais, garantindo a segurança e a privacidade dos indivíduos.

3 Metodologia Adotada

Além da própria LGPD, resoluções mencionadas na Seção 2 também foram empregadas na elaboração do Modelo MMAI-LGPD. Adicionalmente, as normas ISO - parâmetros orientativos internacionais, voltadas à segurança da informação e privacidade de dados pessoais, também foram aplicadas na construção do modelo, uma vez que servem como guia de boas práticas. Especificamente as ISOs 27002 e 27701 foram usadas pois versam sobre segurança e governança de sistemas de informação. A Figura 1 ilustra a metodologia abordada na construção do MMAI-LGPD.

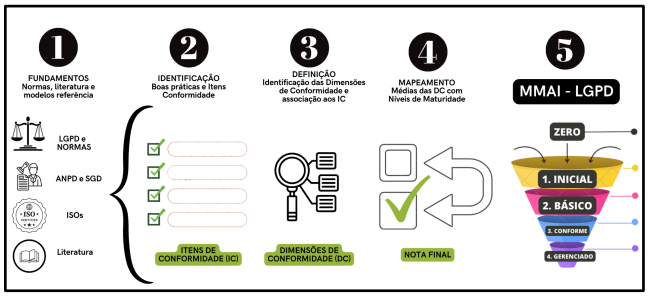

Figura 1: Passos Metodológicos

3.1 Identificação dos Itens de Conformidade (IC) do MMAI-LGPD

Ao analisar a LGPD, foram identificados os artigos da lei que continham verbos indicativos de **ação, ordem ou mandamento** a ser seguido. Assim, todos os artigos que se enquadraram neste contexto foram mapeados como um "Item de Conformidade (IC)". O mesmo método foi usado para identificar estes itens nas resoluções da ANPD. A seguir está um exemplo deste processo:

*LGPD: "Art. 37. O controlador e o operador **devem manter registro das operações** de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."*

IC01: Construção do Inventário de Dados Pessoais conforme art. 37 da LGPD e Guia Orientativo da ANPD.

É importante ressaltar que os artigos da LGPD que abordam definições gerais e aspectos transitórios de implantação da lei não foram utilizados para definir os IC. Segue um exemplo de dispositivo da lei que não foi mapeado em nenhum IC: "*Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;*".

Como mencionado anteriormente, além da LGPD e das resoluções da ANPD, as ISO 27701 e a ISO 27002 também foram contempladas na construção do modelo de referência. A ISO 27701 tem como objetivo estabelecer diretrizes e requisitos para um sistema de gestão de privacidade da informação, ampliando os princípios e controles da ISO 27001, a fim de abordar especificamente a proteção de dados pessoais. Já a ISO 27002 é vista como um código de práticas para controles de Segurança de Informação, fornecendo diretrizes e boas práticas para o estabelecimento, implantação, manutenção e melhoria contínua de um sistema de gestão de segurança da informação. Nos casos destas ISOs, o controles de segurança previstos em cada uma foram mapeados como IC, conforme exemplo abaixo:

*ISO 27002: Controle 6.2.1 Política para o uso de dispositivo móvel: Convém que uma política e medidas que apoiam a segurança da informação sejam adotadas para gerenciar os riscos decorrentes do **uso de dispositivos móveis**.*
IC02: Elaboração e Implantação de Política de Uso de Dispositivo Móvel.

3.2 Identificação das Dimensões de Conformidade (DC) do MMAI-LGPD

Dada a natureza multidisciplinar da LGPD, que contempla os âmbitos jurídico, de tecnologia da informação e governança, o MMAI-LGPD agrupou os Itens de Conformidade (IC) baseando-se na relação do item com os Capítulos e Seções dispostas na lei. O método utilizado para categorizar os IC baseou-se na análise temática dos itens, além da avaliação dos objetivos principais de cada dimensão. Este é um processo análogo à codificação axial na análise qualitativa de dados usando *grounded theory* [15] e envolveu três etapas principais: (1) análise de propósito (2) identificação de similaridades e (3) organização por áreas de atuação.

A LGPD é composta por 10 Capítulos e cada um deles refere-se a um tema particular. Essa divisão tem o objetivo de organizar e subdividir o conteúdo em seções mais gerenciáveis e compreensivas sobre a norma, sendo eles: I. Disposições Preliminares, II. Do Tratamento de Dados Pessoais, III. Dos Direitos do Titular, IV. Do Tratamento de Dados pelo Poder Público, V. Da Transferência Internacional de Dados, VI. Dos Agentes de Tratamento, VII. Da Segurança e das Boas Práticas, VIII. Da Fiscalização, IX. Da ANPD, X. Disposições Finais e Transitórias.

A cada agrupamento deu-se o nome de Dimensão de Conformidade (DC). A criação das DC é essencial para estruturar e organizar os IC em categorias temáticas que facilitam a compreensão, mensuração e implementação das exigências da LGPD. Essa categorização torna possível direcionar auditorias a profissionais específicos, conforme a área de atuação ou *expertise*, promovendo maior clareza e eficiência nos processos de avaliação e adequação. Além disso, as dimensões proporcionam uma abordagem mais prática e acessível para que as instituições identifiquem lacunas e priorizem ações corretivas de forma estratégica, alinhando-se aos requisitos legais de maneira mais objetiva. Neste modelo é proposta a adoção de 6 dimensões conforme a apresentação do Quadro 1.

Quadro 1: Mapeamento entre os Capítulos LGPD/ISO com as Dimensões de Conformidade do MMAI-LGPD

DIMENSÃO DE CONFORMIDADE (DC)	CAPÍTULO LGPD/ISO
1. Governança	Capítulos I, VII, VIII, IX e X
2. Registro de Operações Tratamento	Capítulos II, IV e V
3. Atendimento ao Titular	Capítulo III
4. Segurança da Informação	VI, VII e as ISO 27002 e 27701
5. Incidente de Segurança	VI, VII e as ISO 27002 e 27701
6. Políticas e Termos	VI, VII e as ISO 27002 e 27701

É importante ressaltar que os outros capítulos da LGPD não foram contemplados nesta classificação porque não continham artigos que impusessem regras de comportamento ou adoção de práticas correlacionadas a qualquer IC. Conforme mencionado, os 57 Itens de Conformidade (IC) foram agrupados em 6 Dimensões de Conformidade (DC), sendo elas:

1. **GOVERNANÇA**: Dimensão que observa um conjunto de procedimentos, estratégias e práticas estabelecidas para garantir a gestão adequada, controle, qualidade, segurança, privacidade e conformidade dos dados dentro da instituição – itens dispostos no Quadro 2.

Quadro 2: IC da Dimensão GOVERNANÇA

ITEM DE CONFORMIDADE (IC)	JUSTIFICATIVA LEGAL
Todos os funcionários realizam Leitura de Guias de Boas Práticas Continuamente	LGPD - art. 50
É adotado Programa Institucional de Proteção e Privacidade de Dados (PIPPr)	LGPD - art. 46 e 50
É adotado um Procedimento para revisão de medidas PDCA	LGPD - art. 50
É adotado um Plano de Comunicação Interno	LGPD - art. 46, 48 e 50
Há a Oficialização Encarregado	LGPD - art. 23 e 41
Todos os Recursos para Encarregado estão disponibilizados	RECOMENDAÇÃO
Há Indicação líderes setor	RECOMENDAÇÃO
Há Indicadores de Resultados da PIPPr	RECOMENDAÇÃO
O Relatório de Impacto de Dados (RIDP) foi elaborado	LGPD - art. 10 e 38
O RIDP basea-se na Recomendação ANPD	LGPD - art. 10 e 38
É adotado um Procedimento retificação dados pessoais	LGPD - art. 17 e 18
Há Publicidade de ausência de consentimento, quando aplicável	LGPD - Art. 7o, III
Há Aplicação princípios LGPD	LGPD - Art. 6o
Os princípios Privacy by design e default foram adotados em todos produtos e serviços	LGPD - Art. 46 § 2º
Houve Treinamento de áreas em Proteção de Dados e Privacidade	LGPD - art. 46 e 50

2. **REGISTRO DE OPERAÇÕES DE TRATAMENTO**: Tem o foco em analisar como o mapeamento de dados pessoais está sendo usado nos sistemas e de forma física, para a construção do Inventário de Dados Pessoais, conforme prevê o artigo 37 da LGPD, analisando finalidades de tratamento, ciclo de vida dos dados pessoais e bases legais estabelecidas itens dispostos no Quadro 3.

Quadro 3: IC da Dimensão REGISTRO DE OPERAÇÕES DE TRATAMENTO

ITEM DE CONFORMIDADE (IC)	JUSTIFICATIVA LEGAL
Há um Plano para Evitar Coleta Excessiva	LGPD - art. 6o e 18
Foi realizada a Construção do Inventário de Dados Pessoais	LGPD - art. 37
Finalidade de tratamento e bases legais estão definidas	LGPD - art. 6o e 37
Há a Classificação dos Dados (mínimo em comuns e sensíveis)	LGPD - art. 37
Há um Conscientização dos stakeholders sobre o Tratamento pelo Poder Público	LGPD - art. 6o, 26

3. **ATENDIMENTO AO TITULAR DE DADOS PESSOAIS**: Destina-se a avaliar o atendimento ao titular de dados pessoais conforme a LGPD de forma eficiente, através de procedimentos adotados pela instituição no trato das solicitações e demandas dos indivíduos em relação aos seus dados - itens dispostos no Quadro 4.

Quadro 4: IC da Dimensão ATENDIMENTO AO TITULAR

ITEM DE CONFORMIDADE (IC)	JUSTIFICATIVA LEGAL
Há a Publicidade do Encarregado para o titular	LGPD - art. 23 e 41
É adotado um Plano de Comunicação sobre os Objetivos PIPPri	LGPD - art. 27, 30, 36
Há a Publicização da Política de Privacidade e Proteção de Dados (PPPD)	LGPD - art. 46 e 50
É adotado um Procedimento Padrão de Atendimento ao Titular	LGPD - art. 17 e 18
Houve a Conscientização do Titular do Dados sobre o tratamento realizado	LGPD - art. 17 e 18
A PPPD está escrita de uma forma simples e clara	LGPD - art. 6o, 46 e 50

4. **SEGURANÇA DA INFORMAÇÃO**: Objetiva verificar a robustez, eficácia e conformidade dos sistemas, procedimentos e políticas implementadas pela organização para proteger os dados contra ameaças internas e externas, garantindo que os controles de segurança da informação sejam adequados, atualizados e alinhados com as melhores práticas - itens dispostos no Quadro 5.

Quadro 5: IC da Dimensão SEGURANÇA DA INFORMAÇÃO

ITEM DE CONFORMIDADE (IC)	JUSTIFICATIVA LEGAL
Foram adotados Controles de Segurança para gestão de Riscos	LGPD - art. 34, 44, 46 e 55-J
Há o Monitoramento de Vulnerabilidades	LGPD - art. 34, 44, 46 e 55-J
Há Comprovações de Medidas de Segurança implantadas	LGPD - art. 34, 44, 46 e 55-J
Há Proteção dos ambientes e meios físicos	LGPD - art. 6o, VII, VIII e art. 46
É adotada Autenticação bifator ou multifator	RECOMENDAÇÃO
Há Monitoramento de Redes e Detecção de Intruso	LGPD - art. 34, 44, 46 e 55-J
É adotada riptografia nos softwares (produtos ou serviços)	LGPD - art. 34, 44, 46 e 55-J
Há Instauração de Backups e Redundância de Dados	LGPD - art. 34, 44, 46
As Medidas de segurança são adotadas desde fase de Concepção (by design)	LGPD - art. 6o, art. 46, §2o

5. **INCIDENTE DE SEGURANÇA**: Observa a capacidade da instituição em responder de forma eficaz a eventos adversos que possam comprometer a segurança da informação, garantindo a eficiência das medidas de resposta e recuperação, identificar possíveis lacunas ou falhas no plano - itens dispostos no Quadro 6.

Quadro 6: IC da Dimensão INCIDENTE DE SEGURANÇA

ITEM DE CONFORMIDADE (IC)	JUSTIFICATIVA LEGAL
É adotado um Plano de Comunicação quando houver violações	LGPD - art. 7o, 11, 15, 18, 26, 27, 30, 36, 41, 46, 48, 55-J
É adotado um Plano de Gestão de Incidentes	LGPD - art. 34, 44, 46 e 55-J
Há Canal de Recebimento de Denúncia e Alertas Ocorrência	LGPD - art. 7o, 11, 15, 18, 26, 27, 30, 36, 41, 46, 48, 55-J
É adotado um Procedimento de Rastreabilidade de Tratamento de Dados	LGPD - art. 10, 38, 46 e 50
É adotado um Procedimento para Gestão de Riscos Jurídico e de Segurança da Informação	LGPD - art. 46, 50 e 51
É adotado um Procedimento para Plano de Mitigação e Continuidade do Negócio	LGPD - art. 46, 50 e 51
É adotado um Procedimento retificação dados	LGPD - art. 18

6. **DOCUMENTOS E POLÍTICAS**: Dimensão que tem como objetivo principal verificar a implementação, compreensão e conformidade dos colaboradores e da organização em relação às diretrizes estabelecidas nas políticas internas, avisos, documentos, editais, contratos e termos de uso - itens dispostos no Quadro 7.

Quadro 7: IC da Dimensão DOCUMENTOS E POLÍTICAS

ITEM DE CONFORMIDADE (IC)	JUSTIFICATIVA LEGAL
Houve Adequação Instrumentos Convocatórios (Ex.: Editais e Processos Seletivos)	LGPD - 8o, 33 e 35
Existe um Termo de Consentimento Padrão	LGPD - art. 7o, 11
Houve Revisão de Contratos	LGPD - 8o, 33 e 35
É adotada uma Política de Segurança da Informação	LGPD - art. 46, 50 e 51
É adotada uma Política de Cookies	RECOMENDAÇÃO ANPD
Existe um Aviso de Cookies	RECOMENDAÇÃO ANPD
É adotada uma Política de Retenção e Exclusão	LGPD - art. 46, 50 e 51
Existe um Termo de Confidencialidade	RECOMENDAÇÃO ISO
É adotada uma Política de Criptografia	RECOMENDAÇÃO ISO
É adotada uma Política de Monitoramento de Redes	LGPD - art. 34, 44, 46
É adotada uma Política de Patches e Atualizações	RECOMENDAÇÃO ISO
É adotada uma Política de Backups e Restaurações	LGPD - art. 34, 44, 46
É adotada uma Plano de Continuidade de Negócio	RECOMENDAÇÃO ISO
Existe Termos de Uso dos Softwares Desenvolvidos	RECOMENDAÇÃO ANPD
É adotada uma Política de Transferência internacional de Dados	LGPD - art. 33, 34, 35, 36

3.3 Status de Conformidade dos Itens

No modelo MMAI-LGPD, um valor é atribuído a cada IC. A metodologia que embasou a escolha dos valores assumidos pelos ICs foi a proposta pelo Diagnóstico de Adequação LGPD, elaborado pelo Ministério da Economia[2]. Este diagnóstico teve o intuito de fornecer as informações necessárias para um diagnóstico do atual estágio de adequação à LGPD pelos órgãos públicos federais. Os ICs podem assumir 4 status:

- **Não adota**: A organização ainda não adota a prática, bem como não iniciou planejamento para adotá-la.
- **Iniciou plano para adotar**: A instituição ainda não adota a prática, mas iniciou ou concluiu planejamento visando adotá-la, o que se evidencia por meio de documentos formais (planos, atas de reunião, estudos preliminares, etc).
- **Adota parcialmente:** A instituição iniciou a adoção da prática, que ainda não está completamente implementada, conforme planejamento realizado; ou a prática não é executada uniformemente em toda a organização.
- **Adota integralmente:** A instituição adota integralmente a prática apresentada, de modo uniforme, o que se evidencia em documentação específica ou por meio do(s) produto(s) ou artefato(s) resultante(s) de sua execução.

[2]https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd.

Conforme descrição do modelo sugerido pelo Ministério da Economia, adotado neste trabalho, cada IC pode assumir os seguintes valores numéricos, associativos ao status: (i) Não adota = 0; (ii) Iniciou plano para adotar = 0,25: (iii) Adota parcialmente = 0,5; (iv) Adota integralmente = 1. É importante ressaltar que os valores (ii) e (iii), apesar de não representarem uma adequação total à LGPD, são considerados neste modelo como relevantes em função da incorporação do Princípio da Boa-fé, previsto pela LGPD. A implantação desse princípio pode ser observado num contexto em que a instituição, apesar de não adotar integralmente uma prática recomendada descrita no IC, ela tem um planejamento de adoção ou em adoção parcial. Nestes casos, as penalidades administrativas e judiciais são minimizadas, justificando-se assim, a pontuação do IC no modelo de referência aqui proposto.

Atribuindo-se o status para cada IC, é realizada valoração de cada um e um índice para cada dimensão. Após isso, é calculada a **Nota Final** para a instituição. Esta nota é obtida pela média aritmética dos valores de ICs, e assim, é possível determinar qual o Nível de Adequação à LGPD a instituição está. Ela pode ser classificada em um dos cinco níveis, apresentados na seção a seguir, sendo o "Zero" o nível mais incipiente e o "Gerenciado" o nível mais eficiente de adequação à LGPD.

4 O Modelo de Referência MMAI-LGPD

O Modelo Maturidade de Adequação Institucional que tem como objetivo fornecer, minimamente, informações necessárias para um diagnóstico de maturidade de Adequação à LGPD à uma instituição que possui como produto sistema de informação. O objetivo é indicar o alinhamento dos processos à governança de dados, assim como direcionar o desenvolvimento de sistemas de informação com adoção das melhores práticas de privacidade e proteção aos dados dessoais, conforme preconiza a LGPD. A Figura 2 apresenta cada nível do modelo e uma breve descrição.

Figura 2: Níveis de Maturidade do MMAI-LGPD

- Nível "ZERO": as instituições que não têm nenhuma adoção de práticas que dizem respeito à implantação da LGPD - **Nota Final = 0**.
- Nível "INICIAL": enquadram-se aquelas que possuem algumas iniciativas e práticas de privacidade e proteção de dados de maneira *ad hoc*, sem processo de adequação definido, possuindo sua **0 < Nota Final < 0,5**.
- Nível "BÁSICO": ainda possuem pendências no processo de adequação à LGPD - parcialmente adequadas, e precisam atender a dois requisitos: (i) possuírem um **Programa de Adequação e boas práticas LGPD** que está sendo implantado na instituição e (ii) **0,5 < Nota Final < 1.**
- Nível "CONFORME": Instituições atendem a todos os ICs, com Programa de Adequação estruturado, mas não possuem métricas e indicadores para gerir a melhoria contínua deste programa - **Nota Final = 1**.
- Nível "GERENCIADO": Precisam atender a todos os critérios do Nível "CONFORME" e possuírem um Programa de Melhoria e Revisão contínua de através da adoção de métricas e indicadores de Privacidade e Proteção de dados que avaliam as esferas Jurídica, de Segurança da Informação e Governança de Dados Pessoais, simultaneamente.

Os resultados apresentados por este modelo ainda possuem um caráter meramente informativo, visando dar suporte à adoção de medidas organizacionais estratégicas, táticas e operacionais para que cada instituição aumente a conformidade à referida lei. Suas metas fundamentais incluem:

- Estruturar a Avaliação e Níveis de Conformidade: Oferecer uma estrutura para avaliar o nível de conformidade das instituições com os requisitos estabelecidos pela LGPD.
- Identificação de Lacunas: Identificar lacunas existentes entre as práticas atuais das instituições e os requisitos da LGPD, apontando áreas que precisam ser melhoradas ou ajustadas para estar em conformidade.
- Estabelecimento de Boas Práticas: Fornecer diretrizes e práticas recomendadas para garantir uma gestão adequada e segura dos dados pessoais, alinhadas com os princípios e exigências da LGPD.
- Progressão na Adequação: Permitir uma progressão gradual das instituições em direção a um maior nível de maturidade em relação à conformidade com a LGPD, possibilitando melhorias contínuas.
- Promoção da Cultura de Proteção de Dados: Estimular uma cultura organizacional que valorize a privacidade e a proteção dos dados pessoais, incorporando esses princípios no cerne das operações das instituições.

5 Auditorias Internas adotando o MMAI-LGPD

5.1 Metodologia do Estudo Empírico

A fim de avaliar a viabilidade de adoção do modelo MMAI-LGPD, ele foi utilizado num processo de auditoria em seis empresas de tecnologia, sediadas em um parque tecnológico brasileiro. O convite para as empresas foi realizado diretamente àquelas que participaram de uma reunião com os autores deste trabalho e a administração do referido parque tecnológico. Neste encontro foi exposta a necessidade das empresas de software se adequarem à LGPD, sendo apresentados também o impacto jurídico e administrativo que poderiam sofrer sem a devida adequação, eventuais perdas de contratos e oportunidades no mercado.

Neste estudo empírico, os ICs compuseram o *checklist* de inspeção da auditoria caracterizando-se como modelo de avaliação do MMAI-LGPD. Esta inspeção foi realizada presencialmente, *in loco*, através de uma entrevista com profissionais responsáveis pela gestão empresarial, pela segurança da informação e gestão de desenvolvimento de sistemas da instituição. Adicionalmente, foram feitas visitas às instalações das instituições, uma vez que o MMAI-LGPD também possui IC que lidam com a segurança física das informações. Cada inspeção durou em média duas horas e foi composta por 4 momentos:

1. Apresentação do objetivo do estudo e entrega dos Termos de Confidencialidade e Sigilo;
2. Explicação sobre a metodologia adotada e processo avaliativo da instituição;
3. Apresentação do MMAI-LGPD;
4. Realização das perguntas sobre a adoção dos ICs.

A entrevista também serviu como meio de esclarecimento de dúvidas sobre o processo de adequação da LGPD. As respostas foram persistidas em planilha eletrônica e cada IC valorado de acordo com a metodologia apresentada na subseção anterior.

Em seguida, a Nota Final foi calculada e um Relatório de Auditoria enviado para as instituições. Este relatório continha (i) uma visão geral da instituição com relação a cada dimensão de conformidade, (ii) sua Nota Final e (iii) o Nível de Maturidade de instituição de acordo com enquadramento em uma das 5 possibilidades. Adicionalmente, o relatório listou (iv) um conjunto de recomendações e indicações de boas práticas que poderiam ser adotadas num primeiro momento pelas instituições, levando em consideração os ICs não atendidos por elas.

5.2 Visão Geral das Instituições Auditadas

Por questões de sigilo e anonimização das instituições participantes, mais detalhes sobre a caracterização delas não serão descritas. Entretanto, abaixo está uma visão geral sobre as entidades que participaram do estudo.

- EMPRESA 01 (E01): Uma empresa que se dedica à informatização de diferentes segmentos de mercado, desenvolvendo aplicativos web e mobile para simplificar

o cotidiano de pessoas e organizações. Com certificação MPS-BR em Serviço e Desenvolvimento e utilizando tecnologia totalmente em nuvem, cria soluções inovadoras, práticas e objetivas para auxiliar na gestão de diversos negócios.

- EMPRESA 02 (E02): é uma empresa que propõe soluções de software com IA para o mercado do setor automotor. O foco de suas soluções é a organização eficiente dos processos e investimentos em funcionários qualificados para realizar cotações.
- EMPRESA 03 (E03): é uma empresa de consultoria e prestação de serviços de outsourcing especializada em soluções de *Business Intelligence* e Engenharia de Dados, que atua no mercado desde 2018. Suas soluções oferecem uma abordagem Data-Driven para impactar organizações e transformar a realidade dos clientes, além de disponibilizar uma tecnologia exclusiva de integração de dados.
- EMPRESA 04 (E04): é uma empresa dedicada à integração de soluções computacionais para impulsionar a Pesquisa, Desenvolvimento, Inovação e Engenharias, tendo como missão projetar, integrar e implementar sistemas de hardware, software e serviços integrados, incluindo servidores, workstations e clusters computacionais de alto desempenho.
- EMPRESA 05 (E05): ela desenvolve tecnologia para o agronegócio, especialista em segurança de dados e oferece soluções de videomonitoramento com insights estratégicos para tomada de decisões eficientes.
- EMPRESA 06 (E06): empresa se destaca na criação de websites, e-commerces, aplicativos e sistemas personalizados, oferecendo soluções de alta qualidade que resultam em confiança e em um portfólio extenso de projetos desenvolvidos não só para o Brasil, mas também para outros países.

5.3 Níveis de Maturidade Institucionais

Conforme a metodologia previamente descrita, os níveis de maturidade instituições sobre a adequação da LGPD levam em consideração a "Nota Final" e a aderência a um Programa estruturado de adequação à lei. É importante lembrar que a "Nota Final" é resultado da média aritmética dos valores atribuídos a cada dimensão.

Observando detalhadamente cada DC (1ª coluna), a Tabela 1 apresenta as notas obtidas por cada instituição participante. A primeira coluna explicita a DC, enquanto as colunas subsequentes indicam as notas de cada uma das instituições. As últimas linhas apresentam respectivamente a Nota Final e o Nível de Maturidade da Instituição.

De acordo com a Tabela 1, é possível observar que o "*Registro de Operações*" possuem as piores notas. Neste sentido, o Inventário de Dados Pessoais, que sintetiza todas as informações de registros de tratamento de dados pessoais está construído de forma incompleta, dificultado várias outras etapas do processo de adequação à LGPD, uma vez que ele é base para tomada de decisões no processo de adequação. Assim, os softwares desenvolvidos pela empresa não possuem aderência às exigências legais e nem boas práticas legais de desenvolvimento de software seguro, pois o ciclo de vida dos dados não está identificado conforme prevê o art. 37 da LGPD.

Tabela 1: Avaliação das instituições por DC e Nota Final

DIMENSÃO	EP01	EP02	EP03	EP04	EP05	EP06
1. GOVERNANÇA	0,28	0,18	0,54	0,41	0,87	0,29
2. REGISTRO DE OPERAÇÕES	0,20	0	0,2	0,3	0,4	0,1
3. ATENDIMENTO AO TITULAR	0,25	0,33	0,41	0,83	0,93	0,16
4. SEGURANÇA DA INFORMAÇÃO	0,75	0,76	0,93	0,25	0,93	0,25
5. INCIDENTE DE SEGURANÇA	0,28	0	0,5	0,14	0,75	0,12
6. POLÍTICAS E TERMOS	0,31	0,18	0,75	0,11	0,84	0,28
NOTA FINAL	0,35	0,24	0,56	0,34	0,79	0,20
NÍVEL DE MATURIDADE LGPD	INICIAL	INICIAL	**BÁSICO**	INICIAL	**BÁSICO**	INICIAL

Além disso, é preocupante que a DC 3 "*Atendimento ao Titular*" teve também um dos piores desempenhos. Isto significa que os procedimentos de atendimento aos direitos dos titulares conforme preveem a LGPD estão longe de serem atendidos pela maioria das instituições. Ou seja, seus sistemas não possuem funcionalidades que deem suporte ao titular para que ele exerça seus direitos, nem há garantia de que as funcionalidades implementadas nos softwares sigam padrões que garantam a privacidade do usuário (titular do dado).

Esta circunstância pode levar a empresa a responder não apenas processos **administrativos** sancionatórios, pela ANPD, mas a processos **judiciais** em diferentes esferas, a pedido do titular dos dados pessoais. No âmbito judicial, o não atendimento aos direitos do titular dos dados pode acarretar ações do tipo criminal, civil, trabalhista, dentre outros, a depender do caso concreto. Ressalta-se ainda que, os processos judiciais e os processos administrativos provenientes da ANPD podem transcorrer de forma simultânea.

Outra observação que vale destaque é que a Dimensão "*Segurança da Informação*" foi a mais atendida pela maioria das instituições participantes do estudo (excetuando E04). Este resultado se deve ao fato de que empresas software participantes do estudo vinham adotando boas práticas apenas de segurança da informação na instituição, no processo de desenvolvimento de sistemas, não limitando-se à proteção aos dados pessoais. É importante também destacar as altas pontuações da E05 neste quesito, visto que ela tem clara preocupação com o tema conforme descrito na seção 5.2.

Até o momento da realização desta pesquisa, nenhuma instituição estava em conformidade com a LGPD, nas perspectivas jurídicas, de tecnologia e de governança. A maioria delas encontra-se no **Nível Inicial (4/6)**, tendo adotado algumas boas práticas de proteção de privacidade de dados pessoais, mas sem um processo definido de adequação e sem contemplar de forma satisfatória todos os ICs das 6 dimensões diferentes.

Esta realidade não é exceção no Brasil e vem com preocupação se tornando regra. Apesar da LGPD ter 6 anos, a maioria das empresas brasileiras ainda não estão adequadas, incluindo as de software [3] [12]. Existe uma complexidade inerente ao processo de adequação, uma vez que vários profissionais precisam atuar num **programa multidisciplinar de atividades** envolvendo desenvolvedores de software, analistas de segurança da informação, gestores de projetos, gestores da informação, advogados e qualquer profissional que compreenda da legislação e de boas práticas de segurança da informação, como encarregado de dados pessoais.

A única empresa que mais se aproximou do cenário de conformidade foi a EP05, mas ainda em **Nível Básico**, havia recentemente obtido a certificação da ISO 27001 e tinha implantado um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

É importante ressaltar que não apenas o conhecimento e conscientização sobre a LGPD, mas também a natureza dos serviços ofertados pelas instituições são cruciais para essa aderência a um programa de adequação. Esta empresa, por exemplo, oferta serviços de software críticos, onde uma falha de segurança poderia levá-los a perdas de contratos ou de credibilidade no mercado. Portanto, precisam naturalmente ser mais rigorosos com a segurança da informação.

Outro ponto relevante que precisa ser levado em consideração é a opacidade normativa das entidades governamentais no Brasil. A ANPD ainda não publicou um guia, protocolo ou arcabouço para que as instituições possam facilmente compreender como a lei deve ser efetivada. Além disso, pesquisas apontam que a maior parte das empresas de software no Brasil são microempresas, empresas de pequeno porte ou startups [12]. Assim, elas possuem recursos limitados e muitas vezes, equipes enxutas, prejudicando a implementação de políticas de privacidade robustas, a garantia da segurança dos dados pessoais, a obtenção do consentimento dos titulares de dados de forma adequada e respostas a possíveis vazamentos de informações. Adicionalmente, a falta de conhecimento especializado sobre a legislação e seus requisitos técnicos pode tornar o processo de adequação à LGPD ainda mais complexo.

6 Lições Aprendidas no Estudo na Adoção do MMAI-LGPD

A avaliação de um de modelo de maturidade envolve uma análise de diversos aspectos, como a compreensão dos objetivos e a justificativa da proposta, incluindo sua relevância para as necessidades e metas da instituição que o adere. É também essencial analisar diversos critérios para garantir sua eficácia e conformidade. Primeiramente, deve-se compreender os objetivos do modelo e verificar se ele abrange os requisitos da LGPD. Neste sentido, o MMAI-LGPD foi inteiramente construído a partir das regras e mandamentos previstos pela própria lei e resoluções publicadas pela ANPD, que devem ser encaradas como normas jurídicas no Brasil. Além disso, os critérios de avaliação propostos precisam ser claros, mensuráveis e alinhados aos princípios da lei. Para isto, estes critérios foram estabelecidos em formato de Itens de Conformidade (IC) que podem se desdobrar nos âmbitos jurídico, tecnológico e/ou de governança. As métricas e indicadores foram propostos para permitir uma avaliação objetiva do progresso em direção à conformidade. Essas métricas basearam-se em princípios da LGPD, justificativas legais e tecnológicas sobre o status de atendimento e valoração da nota de cada IC: não adota, tem plano, adota parcialmente ou adota integralmente.

Também é importante verificar a progressão lógica dos níveis de maturidade, certificando-se de que representam uma evolução prática na implementação das medidas de conformidade. Como explicitado anteriormente, existe uma pontuação dada para cada IC que leva ao cálculo de uma "Nota Final". Esta nota embasa o enquadramento institucional em cada Nível de Conformidade.

Finalmente, é crucial considerar a adequação do modelo à realidade da instituição, garantindo que seja viável e aplicável aos recursos disponíveis. Uma vez que a LGPD é uma lei federal que deve ser cumprida por todas as pessoas, empresas e instituições públicas que ofertam bens ou serviços, a ponderação de estar ou não em conformidade não tem espaço. O que existe é a avaliação de proporcionalidade sobre o rigor e a adesão de soluções vanguardistas (ou menos complexas/custosas) para atender a algum IC. Entretanto, todos eles precisam ser atendidos para que as instituições possam estar em conformidade com a LGPD. É importante pontuar que este trabalho não possui o escopo sobre avaliação de sistemas de informação, mas sim, de instituições que desenvolvem estes sistemas. A LGPD deixa clara que adequação à ela deve ser institucional e não adequação de requisitos, arquitetura ou componentes de sistemas. Não adianta, portanto, o software desenvolvido na empresa adotar boas práticas de privacidade e proteção à dados pessoais, mas a empresa não ter um processo estruturado para governança de dados pessoais, ou mesmo falhar no atendimento a todos os direitos dos titulares dos dados.

Durante a realização da auditoria LGPD utilizando o MMAI-LGPD, foi possível estabelecer algumas *lições aprendidas*. Primeiro, o processo de conscientização da empresa foi um aspecto crucial, pois permitiu que os entrevistados compreendessem melhor os requisitos e princípios da lei. Segundo, a auditoria proporcionou a oportunidade de esclarecer dúvidas e desmistificar conceitos mal compreendidos sobre a LGPD, contribuindo para uma melhor assimilação e aplicação das medidas necessárias. Terceiro, ficou evidente que ainda é necessário contar com a *expertise* de um ou mais especialistas para aplicar o modelo de maturidade em uma auditoria de forma eficaz, garantindo uma avaliação completa e precisa. Isso se deve porque este(s) especialista(s) em LGPD devem possuir um conhecimento mínimo técnico e jurídico para interpretar corretamente os requisitos da lei e aplicá-los de maneira adequada durante a auditoria. Este cenário garante que a avaliação seja realizada de acordo com as diretrizes legais e evita interpretações equivocadas que possam comprometer a conformidade da empresa.

Como outra lição aprendida, faz-se necessário que um ou mais profissionais entrevistados estejam familiarizados com as melhores práticas e padrões do setor, para que sejam possíveis uma análise mais abrangente e a identificação de áreas de melhoria no modelo de maturidade em questão. Por fim, é importante ressaltar que, embora os documentos e termos das instituições não tenham sido analisados durante a auditoria, foi possível confirmar a sua existência e sua elaboração adequada a boas práticas de privacidade e proteção de dados.

É mister lembrar que estudos vêm sendo realizados na literatura propondo checklists de inspeção de código ou de produto de software com relação à LGPD [16] [17] [18] [19] [20] [21]. Além disso, modelos de maturidade de governança de dados também já foram propostos como o DMM (*Data Maturity Model)* [22]. Entretanto, é importante pontuar que conforme à LGPD não é apenas o produto de software que precisa ser desenvolvido e disponibilizado de acordo com a lei, mas toda a empresa ou órgão público que desenvolve e disponibilize software.

Portanto, para que a cultura de proteção de dados seja de fato implantada na instituição, modelos de referência como MMAI-LGPD precisam ser adotados, antes ou simultaneamente, à adoção de práticas de programação e desenvolvimento de sistemas de informação. O modelo oferece um arcabouço de conformidade legal e proposições de requisitos legais através de seus IC. Desta forma, na perspectiva de empresas de software, com uma visão geral do nível de maturidade de adequação da instituição à LGPD, fornecida pelo MMAI-LGPD, é possível direcionar esforços para efetivamente desenvolver e manter softwares que garantam a privacidade dos dados pessoais desde a fase de concepção e durante todo o seu ciclo de vida.

7 Limitações

Apesar da contribuição da proposta do modelo, compreende-se a existências de limitações, comum a estudos desta natureza. Em primeiro lugar, a aplicação do MMAI-LGPD em um número maior de instituições e de diferentes nichos de mercado poderia fornecer uma visão mais abrangente e representativa das práticas de conformidade na realidade institucional. Além disso, deve-se considerar que a interpretação sobre o rigor de conformidade com a LGPD pode ser subjetiva e variar entre diferentes avaliadores, o que pode influenciar os resultados obtidos.

Outro ponto a ser mencionado é que este estudo se baseou em uma avaliação inicial por meio de autoavaliação (*self-service assessment*) do entrevistado(a), sem a análise detalhada dos documentos, políticas e processos dessas instituições. Uma abordagem mais aprofundada, envolvendo a análise por especialistas numa segunda etapa do processo de auditoria, poderia fornecer resultados mais precisos e completos.

Apesar dessas limitações, o estudo empírico foi conduzido em seis organizações diferentes, o que proporcionou uma visão ampla da eficácia do modelo de maturidade proposto em diferentes cenários. A diversidade de contextos organizacionais analisados contribui para validar a aplicabilidade e a relevância do modelo, mesmo diante das dificuldades mencionadas. Deste modo, espera-se que este trabalho represente um primeiro passo para entender o estado atual da conformidade com a LGPD e identificar áreas de melhoria nas práticas de proteção de dados das instituições que fornecem sistemas de informação.

8 Considerações Finais

O Modelo de Maturidade de Adequação à LGPD (MMAI-LGPD) representa um pontapé inicial para as instituições no caminho da conformidade com a lei. Ao estabelecer uma estrutura de referência, o modelo orienta e educa essas instituições sobre os requisitos mínimos que devem ser observados para garantir a proteção adequada dos dados pessoais. Isso é crucial não apenas para cumprir com as exigências legais, mas também para promover a confiança dos clientes e parceiros comerciais, fortalecendo a reputação e a credibilidade da organização. E ainda, não se limite à requisitos legais de software, pois o foco não é limitado ao processo de desenvolvimento de sistemas, mas sim, a estrutura organizacional da empresa e seu modelo de governança de dados pessoais.

Além disso, o MMAI-LGPD vai além de simplesmente indicar o que deve ser observado minimamente, pois ele fornece uma direção sobre como as instituições podem progredir de um nível de conformidade para outro. Ao definir os critérios e as práticas recomendadas (ICs) para cada nível de maturidade, o modelo auxilia na identificação de suas deficiências, estabelece metas realistas para serem implementadas as melhorias necessárias em suas práticas de gestão de dados. Essa abordagem graduada e orientadora do modelo proposto não apenas facilita o processo de adequação à LGPD, mas também promove uma cultura contínua de proteção de dados dentro das organizações. Ao passar de um nível de maturidade para o próximo, as instituições não apenas melhoram sua conformidade legal, mas também aprimoram sua capacidade de gerenciar e proteger os dados pessoais de forma eficaz e responsável, adaptando-se às demandas de um ambiente regulatório em constante evolução. Consequentemente, o modelo proposto mostra-se não apenas como uma ferramenta essencial para a conformidade, mas também como um catalisador para a excelência na governança de dados e na proteção da privacidade.

O estudo empírico feito com seis empresas de TI constatou que nenhuma delas está em plena conformidade com a LGPD, retrato da realidade comum em muitas organizações [3]. Além disso, um dos principais gargalos identificados no estudo foi o atendimento ao titular dos dados, que se apresenta como uma área crítica e frequentemente negligenciada pelas instituições e este critério está como meta de fiscalização por parte da ANPD. Essa constatação ressalta a necessidade urgente das organizações direcionarem seus esforços para melhorar o tratamento e a resposta às demandas dos titulares de dados, garantindo o exercício efetivo dos direitos previstos pela LGPD.

Como trabalhos futuros, há diversas oportunidades de aprimoramento e expansão do modelo proposto. Primeiramente, é necessário refiná-lo, levando em consideração os *insights* obtidos nesta pesquisa e as práticas emergentes de conformidade com a LGPD. Isso inclui a inclusão de novos ICs relacionados às novas alterações da LGPD e resoluções da ANPD, bem como a proposição de critérios de avaliação mais procedimentais, detalhando os processos e o conteúdo presente em cada documento. Por exemplo, a ponderação dos ICs pode ser revista baseando-se nos tipos de sanções administrativas da ANPD, proporcionando uma análise de valores que reflita a importância relativa de cada aspecto para a conformidade. Isso permitirá uma abordagem mais estratégica na priorização das ações de adequação e mitigação de riscos.

Além disso, a elaboração de um Plano de Implantação do modelo é demandada a fim de embasar um Programa de Adequação à LGPD que guie as instituições desde o estágio inicial até a implementação efetiva das melhorias necessárias com medição e melhoria contínua. Esse plano deve ser detalhado, acompanhado de um sistema de monitoramento e avaliação contínuos para garantir a eficácia e o sucesso do modelo de maturidade proposto ao longo do tempo. Uma outra área promissora a ser trabalhada é a automatização da avaliação e da documentação por meio de técnicas de Processamento de Linguagem Natural (NPL) e recuperação da informação, que já está em andamento. Isso possibilitará uma análise mais rápida e precisa dos dados, reduzindo a carga de trabalho manual e permitindo uma abordagem mais escalável e eficiente na gestão da conformidade com a LGPD.

Finalmente, é essencial ressaltar que o MMAI-LGPD representa apenas um passo inicial, identificando os elementos-chave e estabelecendo uma base sólida para a adequação às exigências legais na jornada de conformidade com a Lei Geral de Proteção de Dados. Para uma abordagem mais abrangente e eficaz, dois elementos complementares são necessários: (i) um modelo de processo que detalhe as etapas e atividades a serem realizadas em cada nível de maturidade - Programa de Adequação LGPD, e (ii) um modelo de avaliação que permita medir de forma objetiva e precisa o grau de conformidade alcançado em relação ao modelo de referência proposto - Processo de Auditoria LGPD. Esses elementos são essenciais para guiar as instituições de forma prática e orientada a resultados em sua jornada rumo à conformidade total com a LGPD, promovendo uma gestão eficaz da privacidade e proteção de dados. Estes dois modelos serão parte dos nossos estudos futuros.

REFERÊNCIAS

[1] European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 27 April 2016.

[2] Brasil. (2018). Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018.

[3] Daryus. (2023). LGPD está fora da realidade de 80% das empresas no Brasil, diz estudo. FEBRABRAN TECH. Recuperado de https://febrabantech.febraban.org.br/blog/lgpd-esta-fora-da-realidade-de-80-das-empresas-no-brasil-diz-estudo.

[4] Autoridade Nacional de Proteção de Dados (ANPD). (2023). Guia de Elaboração de Inventário de Dados Pessoais. Brasília, DF: ANPD. Recuperado de https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_inventario_dados_pessoais.pdf

[5] Souza, C. A. A. de. (2022). Os reflexos das leis protetivas de dados nos contratos. Monografia de Especialização, Pontifícia Universidade Católica de São Paulo, São Paulo, Brasil.

[6] McGruer, J. (2020). Emerging Privacy Legislation in the International Landscape: Strategy and Analysis for Compliance. Wash J Law Tech Arts, 15, 120. Recuperado de https://digitalcommons.law.uw.edu/wjlta/vol15/iss2/3.

[7] Branche, P., & Thomaz, A. (2018). Brazilian Data Protection Law – A New Scenario For Business In Brazil Compared To Eu-GDPR. Computer Law Review International, 19(4), 130-132. https://doi.org/10.9785/cri-2018-190405.

[8] Abigayle, E. (2019). Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD. 44 Brooklyn Journal of International Law, 859. Recuperado de https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9

[9] Espindola, H. A. (2022). How does the legal bases for processing personal data differ between GDPR and LGPD? [Tese de mestrado, University of Oslo].

[10] Ringmann, S. D., Langweg, H., & Waldvogel, M. (2018). Requirements for Legally Compliant Software Based on the GDPR. In H. Panetto et al. (Eds.), On the Move to Meaningful Internet Systems. OTM 2018 Conferences. OTM 2018. Lecture Notes in Computer Science, 11230. Springer. https://doi.org/10.1007/978-3-030-02671-4_15.

[11] Lincke, S. (2024). Complying with the European Union General Data Protection Regulation (GDPR). In Information Security Planning. Springer. https://doi.org/10.1007/978-3-031-43118-0_17.

[12] SEBRAE. (2020, 11 de maio). Painel de Empresas Dashboard. SEBRAE. Recuperado de https://datasebrae.com.br/totaldeempresas-11-05-2020/.

[13] Data Center Dynamics (2023). LGPD Brasil. Aderência à LGPD: apenas 36% das empresas brasileiras estão em conformidade total. LGPD Brasil. Disponível em https://www.lgpdbrasil.com.br/aderencia-a-lgpd-apenas-36-das-empresas-brasileiras-estao-em-conformidade-total/#:~:text=para%20o%20conte%C3%BAdo-,Ader%C3%AAncia%20%C3%A0%20LGPD%3A%20apenas%2036%25%20das%20empresas,brasileiras%20est%C3%A3o%20em%20conformidade%20total&text=Desde%20a%20entrada%20em%20vigor,para%20se%20adequar%20%C3%A0s%20exig%C3%AAncias.

[14] NIC.br. (2024). Cinco falhas de segurança cibernética que não podem se repetir em 2024. NIC.br. Disponível em https://www.nic.br/noticia/na-midia/cinco-falhas-de-seguranca-cibernetica-que-nao-podem-se-repetir-em-2024/.

[15] Bryant, A., & Charmaz, K. (2019). The SAGE Handbook of Current Developments in Grounded Theory. SAGE Publications Ltd.

[16] Muncinelli, G., Pinheiro de Lima, E., Deschamps, F., Gouvea da Costa, S., Lara Souza, J., dos Santos Pereira, A., & Cestari, J. (2020, April). Components of the Preliminary Conceptual Model for Process Capability in LGPD (Brazilian Data Protection Regulation) Context. Advances in Transdisciplinary Engineering, https:// 10.3233/ATDE200125.

[17] Muncinelli, G., Pinheiro de Lima, E., Deschamps, F., Gouvea da Costa, S., Lara Souza, J., dos Santos Pereira, A., & Cestari, J. (2021, April). Process Capability in LGPD Context: Characterization and Potential Future Directions. In 2nd South American International Conference on Industrial Engineering and Operations Management, https://doi.org/10.46254/SA02.20210121.

[18] Neitzke, C., Mendes, J., Rivero, L., Teixeira, M., & Viana, D. (2023). Enhancing LGPD Compliance: Evaluating a Checklist for LGPD Quality Attributes within a Government Office. In Anais do XXII Simpósio Brasileiro de Qualidade de Software, (pp. 218–227). Porto Alegre: SBC.

[19] Pereira, I., Mendes, J., Viana, D., Rivero, L., Ferreira, W., & Soares, S. (2022). Extending an LGPD Compliance Inspection Checklist to Assess IoT Solutions: An Initial Proposal. In Anais Estendidos do XIII Congresso Brasileiro de Software: Teoria e Prática, (pp. 28-31). Porto Alegre: SBC. doi:10.5753/cbsoft_estendido.2022.226679.

[20] Canedo, E., Cerqueira, A., Gravina, R., Ribeiro, V., Camões, R., Reis, V., Mendonça, F. and Sousa Jr., R. Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD). DOI: 10.5220/0010398200190030 In Proceedings of the 23rd International Conference on Enterprise Information Systems (ICEIS 2021) - Volume 1, pages 19-30 ISBN: 978-989-758-509-8.

[21] Mendes, J., Viana, D., & Rivero, L. (2021). Developing an Inspection Checklist for the Adequacy Assessment of Software Systems to Quality Attributes of the Brazilian General Data Protection Law: An Initial Proposal. In Anais do XXXV Simpósio Brasileiro de Engenharia de Software. Porto Alegre: SBC.

[22] Marques, L. N. (2020). O mapeamento do modelo data management maturity (DMM) à Lei Geral de Proteção de Dados (LGPD) [Trabalho de conclusão de curso, Pontifícia Universidade Católica de Goiás]. Repositório PUC Goiás. https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1289