Modelo de maturidade de processos para avaliação da conformidade com a LGPD: um estudo de caso em uma instituição educacional no Brasil

Jonas Pereira de Andrade Filho[1]*, Gustavo Henrique Matos Bezerra Motta[2]

[1]jonassonjp@gmail.com, [2] gustavo@ci.ufpb.br. Universidade Federal da Paraíba (UFPB), João Pessoa, Paraíba, Brasil
* autor correspondente

Resumo
Nas últimas décadas, o aumento exponencial das atividades digitais trouxe benefícios econômicos e sociais por meio da rápida adoção da Tecnologia da Informação e Comunicação (TIC). No entanto, essa expansão também impulsionou a coleta massiva de dados. As organizações utilizam a TIC para otimizar operações, aprimorar as experiências do público-alvo e tomar decisões estratégicas baseadas em dados. Esse aumento substancial nos dados gerados e compartilhados elevou os riscos de violação de privacidade, necessitando de regulamentações legais específicas. A Lei Geral de Proteção de Dados (LGPD), estabelecida no Brasil em 2018, regulamenta a coleta e o processamento de dados pessoais para proteger a privacidade dos indivíduos. Este estudo propõe um modelo de maturidade de processos para auxiliar as organizações a cumprir os requisitos legais da LGPD, oferecendo uma estrutura clara e eficaz para avaliar o nível de maturidade da organização em relação à Lei. O modelo compreende 27 processos organizacionais derivados dos requisitos da LGPD, categorizados em 5 grupos temáticos, sendo eles: tratamento de dados pessoais, direitos ao titular dos dados, transferência internacional de dados, governança e segurança da informação e sanções administrativas. Um estudo de caso foi conduzido em uma instituição de ensino no Brasil, com análise restrita às informações e documentos públicos da instituição. Foram realizadas duas avaliações dentro de grupos responsáveis por processamento de dados pessoais, governança e segurança da informação. Os resultados deste estudo revelaram um nível de conformidade com a LGPD menor do que o previsto, sugerindo a necessidade de ajustes institucionais para atender aos requisitos da LGPD. Essas descobertas indicam que, embora existam diretrizes e modelos, a aplicação prática desses mecanismos ainda enfrenta desafios, principalmente no que diz respeito à maturidade organizacional e à conformidade regulatória. Nesse sentido, o modelo proposto pode servir como uma ferramenta valiosa para as organizações implementarem e monitorarem processos de proteção de dados.
Palavras-chave: dados pessoais; LGPD; privacidade; proteção; segurança da informação.

Process maturity model for assessing compliance with the LGPD: a case study at an educational institution in Brazil

Abstract
Over the past decades, the exponential growth of digital activities has delivered significant economic and social benefits through the rapid adoption of Information and Communication Technologies (ICT). However, this expansion has also driven massive data collection. Organizations leverage ICT to optimize operations, enhance user experiences, and support data-driven strategic decision-making. Yet, the substantial volume of data generated and shared has amplified privacy risks, creating a pressing need for specific legal frameworks. Brazil's General Data Protection Law (LGPD), enacted in 2018, establishes regulations for collecting and processing personal data, aiming to safeguard individuals' privacy. This study presents a process maturity model to help organizations comply with the LGPD's legal requirements. It offers a structured and practical framework to assess organizational maturity about the law. The model encompasses 27 organizational processes derived from the LGPD's mandates, categorized into five thematic groups: personal data processing, data subject rights, international data transfers, governance and information security, and administrative sanctions. A case study was conducted in a Brazilian educational institution, focusing exclusively on publicly available information and documents. Two assessments were performed with groups responsible for personal data processing, governance, and information security. The results revealed

a lower-than-expected level of compliance with the LGPD, highlighting the need for institutional adjustments to fully meet the law's requirements. The findings emphasize that while guidelines and models are available, their practical application still encounters significant challenges, particularly in organizational maturity and regulatory compliance. In this context, the proposed model is a valuable tool for organizations to implement and monitor data protection processes effectively.
***Keywords**: data protection; LGPD; information security; personal data; privacy.*

1. Introdução

A proliferação das tecnologias digitais e o crescimento exponencial dos volumes de dados trafegados intensificam a necessidade de proteger a privacidade e a segurança das informações. Esse aumento no fluxo de dados impõe desafios significativos a empresas e governos, que precisam adotar medidas robustas para gerenciar e proteger essas informações de maneira eficaz (Saraswat; Meel, 2022). Ademais, a exigência de conformidade com regulamentações legais demanda a adoção de padrões rigorosos de proteção de dados, sem comprometer a eficiência operacional, o que se tem mostrado uma tarefa desafiadora (Fayayola; Olorunfemi; Shoetan, 2024).

Para assegurar a privacidade dos usuários, diversos países têm implementado legislações rigorosas destinadas a regulamentar o uso de dados pessoais. Um exemplo destacado é o Regulamento Geral de Proteção de Dados (GDPR – General Data Protection Regulation) da União Europeia. No Brasil, essa preocupação culminou na criação da Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 14 de agosto de 2018 (Brasil, 2018). Embora promulgada em 2018, a lei entrou em vigor em 18 de setembro de 2020, com a aplicação de sanções administrativas – como advertências, multas e bloqueio de dados pessoais – iniciada em 1º de agosto de 2021. Além das sanções administrativas, a LGPD prevê penalidades de natureza civil e penal. Entre as principais sanções administrativas, destacam-se advertências, multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração, publicização da infração, bloqueio ou eliminação dos dados pessoais envolvidos (Vasconcelos; Salib, 2021).

A nova legislação formaliza a questão pública do uso indevido de dados pessoais, trazendo implicações legais que demandam estratégias complexas para sua implementação. A eficácia da LGPD dependerá da atuação de múltiplos atores internos e externos à organização (Santos, 2020).

Esse marco legal impacta significativamente o Brasil, abrangendo instituições privadas e públicas e todas as formas de tratamento de dados pessoais, independentemente do meio utilizado, seja por pessoas físicas ou jurídicas (Pinheiro, 2020).

Organizações em geral coletam regularmente dados como parte de suas operações, abrangendo informações diversas de seus públicos. No caso específico das instituições de ensino, essa prática é ainda mais comum, dado o caráter de suas atividades, que envolve a coleta de dados pessoais, cadastrais, avaliações educacionais, notas e frequência acadêmica (Barbosa *et al*., 2021).

Em uma pesquisa realizada pela Rede Nacional de Ensino e Pesquisa (RNP) em 2022, foram avaliadas 30 instituições públicas e privadas de ensino e pesquisa. Os resultados revelaram que 50% dessas instituições ainda não haviam definido as bases legais para o tratamento de dados pessoais. Ademais, 44% reconheceram a necessidade de gerenciar o consentimento dos usuários, mas não adotaram práticas para fazê-lo, e 62% ainda não estabeleceram um processo formal para responder às solicitações dos titulares de dados pessoais. A maioria das instituições também não havia nomeado o encarregado pelo tratamento de dados pessoais, uma exigência clara da LGPD (RNP, 2022).

Vazamentos de dados pessoais representam um desafio crítico no atual contexto de digitalização das transações e da economia, gerando crescente preocupação quanto à proteção dessas informações e à segurança cibernética. Um exemplo marcante ocorreu em janeiro de 2018, quando a empresa brasileira Netshoes S.A. teve aproximadamente dois milhões de registros de usuários comprometidos. Dados como nome, CPF, e-mail, data de nascimento e histórico de compras foram expostos, embora informações mais sensíveis, como números de cartão de crédito e senhas, não tenham sido afetadas. Esse incidente evidenciou uma falha de segurança que expôs dados confiados à empresa para transações comerciais online (MPDFT, 2024). Em consequência, o Ministério Público, por meio da homologação judicial de um Termo de Ajustamento de Conduta (TAC), definiu o pagamento de R$ 500.000,00 como indenização pelos danos morais coletivos de caráter nacional (Cunha, 2022).

Uma mudança cultural interna representa um dos principais desafios enfrentados pelas instituições em relação ao tratamento de dados pessoais. Transformações na cultura institucional demandam tempo e investimentos financeiros, como atividades de divulgação, treinamento e conscientização da comunidade envolvida. Alcançar o nível de conformidade com a LGPD exige uma transformação cultural que não é simples nem rápida (Crespo, 2021).

Uma abordagem alternativa para promover a conformidade é o uso de um modelo de maturidade, que permite descrever e avaliar o progresso de uma entidade em direção a um objetivo específico (Knoke; Nwankwo, 2022). No contexto da proteção de dados, isso envolve a análise dos requisitos necessários para cumprir as diretrizes da LGPD, possibilitando a identificação precisa de lacunas e falhas no cumprimento das obrigações legais e promovendo a melhoria contínua no desempenho da proteção de dados.

Diante da diversidade de modelos de maturidade disponíveis na literatura, considerou-se a adoção do *Capability Maturity Model Integration* (CMMI), amplamente utilizado e consolidado na Engenharia de Software (CMMI Institute, 2024). O CMMI é um modelo voltado para o desenvolvimento e manutenção de software, abrangendo todo o ciclo de vida do produto, desde a concepção até a entrega e manutenção. Ele oferece um conjunto de boas práticas organizadas em áreas correlatas e níveis de maturidade, que representam etapas progressivas de eficácia gerencial, fornecendo um caminho evolutivo para organizações que buscam aprimorar seus processos de desenvolvimento e manutenção de software (Chrissis; Konrad; Shrum, 2003).

Com o intuito de auxiliar as organizações na adequação às exigências da LGPD, este trabalho propõe um modelo de processos com maturidade e capacidade para avaliar a conformidade com os requisitos da legislação em organizações brasileiras. Inspirado na abordagem do CMMI, que define diretrizes específicas para cada estágio do desenvolvimento de software, o modelo é adaptado ao contexto da LGPD, com foco na avaliação da conformidade legal exigida por essa lei.

O restante deste trabalho está organizado como segue: a Seção 2 apresenta o referencial teórico necessário para o entendimento do conteúdo. Em seguida, a Seção 3 discute os trabalhos relacionados que abordam questões análogas, identificando lacunas na literatura que esta pesquisa visa preencher. A Seção 4 descreve a abordagem de pesquisa adotada, a motivação da escolha da pesquisa, os níveis de maturidade, processos e sua aplicação. Na Seção 5, são detalhados o estudo de caso e os resultados preliminares da pesquisa, seguidos de uma análise crítica desses elementos. Por fim, a Seção 6 sintetiza os principais achados até o momento, discutindo suas implicações e sugerindo direções para futuros estudos.

2. Referencial teórico

As primeiras iniciativas de proteção e privacidade da informação remontam ao século XVIII, com a Suécia introduzindo, em 1766, um marco legal sobre o acesso à informação. Em 1890, os juristas americanos Samuel Warren e Louis Brandeis publicaram *The Right to Privacy*, no qual definiram a privacidade como o "direito de ser deixado em paz" (Warren; Brandeis, 1890). Na América do Sul, a Colômbia foi pioneira ao estabelecer, em 1888, um código que garantia o acesso a documentos (CGU, 2011).

Com o passar do tempo, o conceito de privacidade evoluiu e foi reconhecido como um direito fundamental na Declaração Universal dos Direitos Humanos de 1948, assegurando a proteção contra intromissões na vida privada. No Brasil, diversas iniciativas governamentais buscaram normatizar e proteger a informação e a privacidade, mas foi na Constituição de 1988 que o direito à intimidade e à proteção da vida privada foi plenamente contemplado (Finkelstein; Finkelstein, 2020).

A crescente pressão da sociedade civil para que o Estado divulgue dados governamentais e proteja a privacidade dos usuários de Internet levou à criação do Marco Civil da Internet criado em 2014. Esse marco regulou o termo "privacidade" no sistema jurídico brasileiro, estabelecendo princípios, garantias, direitos e deveres a serem observados no ambiente digital (Daniel, 2022).

A coleta intensiva de dados de usuários por provedores de internet fomentou o crescimento de grandes corporações de marketing, direcionadas para publicidade personalizada e criação de nichos de mercado específicos. Tal prática evidenciou a necessidade de regulamentação, resultando na criação da LGPD, sancionada em agosto de 2018. A LGPD busca controlar o uso indiscriminado de informações pessoais por meio de princípios como transparência, finalidade e consentimento

obrigatório, assegurando os direitos civis e promovendo a responsabilidade e a transparência das organizações no tratamento de dados pessoais, alinhando-se aos padrões internacionais de proteção de dados (Bioni, 2018; Cots; Oliveira, 2019).

Um dos principais desafios para as instituições é a promoção de uma mudança cultural interna em relação ao tratamento de dados pessoais, o que demanda tempo e investimentos financeiros. Alcançar a conformidade com a LGPD implica em transformações que não são simples, nem céleres (Crespo, 2021).

A melhoria de processos é uma atividade contínua e de longo prazo, essencial para aumentar a qualidade, reduzir custos e tempo de desenvolvimento. Em um ambiente de negócios em constante mudança, uma escala de maturidade de processos se torna necessária, oferecendo uma referência clara de qualidade e possibilitando o planejamento de estratégias para melhorias contínuas.

Modelos de maturidade de processos são ferramentas valiosas para avaliar e aprimorar a eficiência organizacional. O *Process Maturity Framework* (PMF) avalia a maturidade dos processos de gestão de serviços de TI, permitindo tanto a avaliação individual de processos específicos quanto da maturidade global de todos os processos de gestão de serviço (Pereira; Silva, 2010). O *Business Process Maturity Model* (BPMM) é um modelo que avalia o nível de maturidade de processos de negócio, considerando a influência das áreas de processo, a capacidade de monitoramento e controle e o impacto na melhoria contínua dos processos (Lee; Lee; Kang, 2007). O PEMM (*Process and Enterprise Maturity Model*) é uma ferramenta de auditoria de processos que auxilia as organizações no planejamento de mudanças, acompanhamento de progresso e superação de obstáculos. O modelo distingue a maturidade em dois níveis: o dos processos e o da organização como um todo, abordando não apenas a eficiência, mas também o alinhamento estratégico (Kalinowski, 2011).

Por fim, o *Capability Maturity Model Integration* (CMMI) é um modelo amplamente reconhecido para a melhoria de processos organizacionais. Desenvolvido para fornecer uma estrutura que apoia a avaliação e o aprimoramento das capacidades organizacionais, o CMMI oferece um conjunto abrangente de melhores práticas, abrangendo áreas como desenvolvimento de software, serviços e gestão de projetos (Rocha; Zabeu; Machado, 2018).

Dentre os diversos modelos de processos disponíveis, adotou-se o CMMI pela sua ampla aplicação na Engenharia de Software. Este modelo oferece boas práticas organizadas em áreas de atividade e níveis de maturidade, sendo recomendado para organizações que buscam melhorar seus processos de desenvolvimento e manutenção de software (Chrissis; Konrad; Shrum, 2003; Morgado *et al*., 2007).

3. Trabalhos relacionados

Nesta seção, apresentam-se estudos relacionados ao tema desta pesquisa, com destaque para as contribuições relevantes desses estudos em relação à abordagem aqui adotada.

A pesquisa realizada por Ferreira e Okano (2021) avaliou o uso de um recurso visual que enfatiza as principais questões ligadas à privacidade, proteção e conformidade com a LGPD. Como resultado, foi proposto o LGPD Model Canvas, uma ferramenta desenvolvida para auxiliar organizações na formulação de estratégias de adequação à LGPD.

Outro estudo sugere um *framework* chamado LGPD4BP, que consiste em um método para avaliar e modelar processos de negócio conforme a LGPD, empregando a notação de BPMN. A modelagem do estudo inclui um questionário para avaliar a conformidade dos processos com a LGPD, um catálogo de padrões e modelagens criado para estruturar requisitos específicos da lei e, finalmente, um método de modelagem que orienta o modelador de negócios a criar ou ajustar processos para garantir a compatibilidade com a LGPD (Araújo *et al*., 2021).

No contexto da Regulamentação Geral de Proteção de Dados (GDPR) da União Europeia, Labadie e Legner (2019) desenvolveram um modelo de capacidades com base em um processo iterativo de design científico interativo. Esse modelo integra tanto a interpretação de textos legais quanto percepções práticas obtidas de grupos focais com mais de 30 especialistas, além de três projetos da GDPR na União Europeia. O principal objetivo desse modelo é orientar as organizações na implementação dos requisitos da GDPR nas suas práticas organizacionais.

Outro estudo relevante é o de Cortina et al. (2019), que descreve o desenvolvimento de um modelo de avaliação de processos de *Privileged Access Management* (PAM) baseado na GDPR. Neste

trabalho, os requisitos legais foram organizados em tópicos e convertidos em processos candidatos, seguindo os componentes da norma ISO/IEC 33004. A partir disso, foram estabelecidos modelos de referência e avaliação de processos baseados no COBIT (*Control Objectives for Information and Related Technology*) PAM.

O estudo de Zitoun *et al*. (2021) apresenta um modelo de avaliação de maturidade, voltado para diagnosticar o nível atual de maturidade de uma empresa em termos de gestão de dados e informações. O foco deste artigo está na criação de um conjunto de ferramentas que não apenas simplifique a aplicação do modelo, mas também ofereça um roteiro evolutivo fundamentado em evidências. O *Data Management Maturity Model* (DMMM) proposto foi concebido para apoiar a transformação digital desde os estágios iniciais até a otimização plena, abordando aspectos como a estrutura organizacional, os sistemas de informação, as dimensões dos dados e as operações.

Estes trabalhos propõem ferramentas como canvas, *frameworks* e modelos para apoiar organizações na conformidade com os requisitos da LGPD. No entanto, não avaliam o amadurecimento dessas organizações por meio de processos iterativos que visem atender integralmente à legislação. Os estudos que fazem referência ao Modelo de Maturidade de Gestão de Dados (DMM) abordam a gestão de dados de forma ampla, sem se concentrar especificamente na maturação de processos voltados para a adequação à LGPD.

4. Proposta do trabalho

Conforme a motivação descrita na Seção 1, o crescimento acelerado do acesso à internet, embora tenha promovido avanços econômicos e sociais por meio das Tecnologias da Informação e Comunicação (TIC), também ampliou os riscos associados à coleta e uso de dados pessoais. Esse cenário, no qual informações pessoais são frequentemente obtidas sem consentimento, expõe os consumidores a vulnerabilidades, como roubo de identidade e discriminação. A LGPD foi, então, estabelecida para formalizar, no âmbito legal, a necessidade de proteger esses dados, exigindo estratégias de conformidade e implementação eficazes. A adoção de um modelo de processo para a implementação da LGPD nas organizações é, portanto, essencial, fornecendo uma estrutura que orienta desde o mapeamento de dados até a implementação de políticas e práticas de proteção, garantindo o cumprimento das exigências legais.

Dada a variedade de modelos de processos disponíveis, optou-se pelo modelo CMMI, amplamente utilizado e aceito na Engenharia de Software, o que o torna uma escolha atraente devido à sua consolidação nessa área. Além disso, o modelo CMMI foi adaptado para o domínio da lei, onde foi utilizado como referência para avaliar e aprimorar a maturidade dos processos, promovendo a padronização e a melhoria contínua conforme os requisitos legais. Esses níveis de maturidade são aplicados a processos de conformidade derivados da norma.

O modelo resultante, denominado CMM-PC, segue uma abordagem em três fases, semelhante ao trabalho de Cortina *et al*. (2019), mencionado na Seção 3. Primeiramente, a lei foi analisada e seus requisitos extraídos; em seguida, esses requisitos foram agrupados em temas ou assuntos semelhantes. Finalmente, para cada requisito, foram modelados ou adequados os processos organizacionais de proteção de dados correspondentes. Após a elaboração dos processos, propôs-se a associação com os níveis de maturidade do modelo CMMI.

Nas próximas subseções, detalham-se os níveis de maturidade (Subseção 4.1) e a relação dos processos do modelo CMM-PC (Subseção 4.2).

4.1. Níveis de maturidade

O modelo possui cinco níveis de maturidade, refletindo a evolução das capacidades organizacionais de privacidade, desde a conformidade inicial até a excelência em proteção de dados, organizando processos conforme os requisitos da LGPD.

Os níveis de maturidade foram definidos com base em documentos e recomendações de melhores práticas, como os descritos por Paulk *et al.* (1993) e Knoke e Nwankwo (2022), conforme listado a seguir:

- Nível 1 (informal): as atividades são realizadas de forma assistemática, baseando-se em práticas habituais e sem a devida documentação;

- Nível 2 (estruturado): neste nível, existe uma estrutura mínima de gestão dos processos, conduzida por indivíduos com conhecimento sobre proteção de dados, com algumas práticas estruturadas e formalizadas;
- Nível 3 (formalizado): as ações são realizadas de acordo com um processo definido, padronizado, formalizado e documentado;
- Nível 4 (gerenciado): os processos neste nível são bem definidos, consistentes e monitorados, com metas qualitativas e quantitativas estabelecidas;
- Nível 5 (optimizado): o nível final caracteriza uma organização inteira comprometida com a melhoria contínua de seus processos.

4.2. Processos do modelo CMM-PC

Os artigos da LGPD foram inicialmente mapeados e agrupados por temas correlatos, visando associá-los a processos organizacionais específicos. Cada artigo da lei foi analisado para identificar seu conteúdo e sua relação com as operações das organizações. Esse mapeamento resultou na derivação de 27 processos específicos, organizados em cinco grupos temáticos, detalhados para tornar a legislação mais acessível e aplicável ao contexto organizacional.

Cada processo corresponde a um conjunto de atributos, atividades e/ou ações que devem ser incorporados às rotinas da organização, conforme discutido por Araújo et al. (2021). Esses elementos definem as áreas da LGPD nas quais a organização necessita se adequar para estar em conformidade. Os processos são independentes entre si, cada um com níveis de maturidade distintos, focando nas características específicas e nas exigências particulares de cada requisito da Lei.

Os processos descritos no modelo CMM-PC, foram estruturados em cinco grupos temáticos e distribuídos nas Tabelas de 1 a 5. A Tabela 1 reúne todos os processos sobre tratamento de dados Pessoais, a Tabela 2, sobre os direitos do titular dos dados; processos de transferência internacional de dados estão na Tabela 3, governança e segurança da informação na Tabela 4 e por fim processos sobre sanções administrativas, na Tabela 5. Abaixo estão detalhados os processos de cada grupo temático:

Os processos descritos no modelo CMM-PC foram organizados em cinco grupos temáticos, apresentados nas Tabelas 1 a 5. A Tabela 1 reúne os processos relacionados ao tratamento de dados pessoais, enquanto a Tabela 2 aborda os direitos do titular dos dados; a Tabela 3 apresenta os processos de transferência internacional de dados; a Tabela 4 trata da governança e segurança da informação; e, por fim, a Tabela 5 abrange processos sobre sanções administrativas.

Tabela 1 – Processos sobre tratamento dados pessoais

Código	Processo	Descrição
P01	Consentimento de dados ao titular	Formalização para consentimento de uso de dados do titular
P02	Revogação do consentimento de dados ao titular	Formalização para a revogação do consentimento de uso de dados do titular
P03	Acesso aos dados do titular	Fornecer ao titular o acesso às informações sobre o tratamento de seus dados
P04	Tratamento de dados sensíveis	Tratar de forma explícita e transparente as finalidades do uso de dados pessoais sensíveis
P05	Consentimento para dados sensíveis	Estabelecer processos para o consentimento no tratamento de dados pessoais sensíveis, por pais ou responsáveis
P06	Publicização dos tipos de dados	Estabelecer processos para divulgação dos tipos de dados coletados, e eliminação dos mesmos, após o término do tratamento
P07	Tratamento de dados pessoais pelo poder público	Tratar as ações de execução de competências legais ou atribuições legais do serviço público, incluindo compartilhamento e divulgação de dados coletados

Fonte: dados da pesquisa

Tabela 2 – Processos sobre direitos do titular dos dados

Código	Processo	Descrição
P08	Confirmação sobre existência de tratamento	Confirmação de que a organização realiza o tratamento adequado dos dados do titular, em conformidade com os requisitos legais
P09	Acesso aos dados	Processo que permite ao titular solicitar acesso aos dados pessoais mantidos pela organização
P10	Retificação e exclusão de dados	Processo para solicitar a alteração, correção ou exclusão dos dados do titular de maneira formal e documentada
P11	Portabilidade dos dados	Processo para possibilitar a portabilidade dos dados do titular a outro fornecedor de serviço ou produto, respeitando os requisitos legais
P12	Informações sobre compartilhamento de dados	Processo que permite ao titular solicitar a relação das organizações com as quais seus dados foram compartilhados

Fonte: dados da pesquisa

Tabela 3 – Processo de transferência internacional de dados

Código	Processo	Descrição
P13	Transferência internacionais de dados	Procedimentos para realizar a transferência de dados pessoais para país estrangeiro ou organismo internacional ao qual o Brasil esteja vinculado

Fonte: dados da pesquisa

Tabela 4 – Processos de governança e segurança da informação

Código	Processo	Descrição
P14	Gestão em segurança da informação	Processo para estabelecer e manter um programa em gestão da segurança da informação, incluindo a proteção os dados pessoais
P15	Políticas de proteção e privacidade de dados	Processo para desenvolver e atualizar políticas de proteção e privacidade de dados, conforme exigências legais
P16	Treinamento e conscientização	Realização periódica de treinamentos e atividades de conscientização para colaboradores envolvidos no tratamento de dados pessoais
P17	Auditorias internas	Processo para conduzir auditorias internas regulares, com o objetivo de verificar a conformidade com a LGPD
P18	Operações de tratamento de dados pessoais	Registro atualizado das operações de tratamento de dados pessoais realizadas pela organização
P19	Plano de resposta a incidentes	Desenvolvimento e implementação de um plano para resposta a incidentes de segurança da informação
P20	Relatório de Impacto à Proteção de Dados Pessoais (RIDP)	Procedimentos para elaboração do RIDP referentes às operações de tratamento de dados
P21	Encarregado de dados pessoais	Processo para nomeação, treinamento e avaliação do encarregado de dados pessoais
P22	Padrões de interoperabilidade	Normas de interoperabilidade, estabelecidas pela ANPD, para facilitar a portabilidade, segurança e o livre acesso aos dados

Fonte: dados da pesquisa

Tabela 5 – Processos de sanções administrativas

Código	Processo	Descrição
P23	Comunicação de não conformidade	Identificação, documentação e notificação de infrações cometidas pelos agentes de tratamento de dados;
P24	Notificação e aplicação de sanções	Processo que envolve a avaliação e o cálculo de multas, tanto simples quanto diárias, com base na infração e no faturamento da organização
P25	Publicidade e transparência de infrações	Divulgação de infrações confirmadas, visando à transparência; Estabelecimento e publicação de metodologias para o cálculo de multas
P26	Bloqueio, eliminação e suspensão de dados	Procedimentos para bloquear e eliminar dados pessoais em caso de infração, bem como para suspender temporariamente o tratamento de dados
P27	Proibição de tratamento de dados	Proibição das atividades de tratamento de dados em situações graves de não conformidade

Fonte: dados da pesquisa

Estes processos foram desenvolvidos com base nas diretrizes da LGPD, promulgada em 2018. É importante destacar que eventuais alterações na legislação podem demandar uma reavaliação do modelo proposto para identificar possíveis adaptações necessárias. Na sequência, será apresentada uma representação quantitativa dos processos avaliados, visando fornecer uma medida do grau de conformidade da organização em relação ao modelo proposto.

4.3. Metodologia para avaliação processos e níveis de maturidade

Nesta subseção, apresenta-se a metodologia para a aplicação do modelo CMM-PC. Na subseção 4.2, foram descritos os processos organizacionais relacionados ao CMM-PC, que foram extraídos dos requisitos da LGPD, bem como os respectivos níveis de maturidade. A aplicação do modelo resulta da combinação desses dois elementos, como exemplificado na Tabela 6.

Tabela 6 – Matriz de maturidade

Processo	Níveis de maturidade				
	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
Processo 1 (P01)					
Processo 2 (P02)					
...					
Processo N (P0N)					

Fonte: dados da pesquisa

A Tabela 6 exibe os processos organizacionais distribuídos em diferentes níveis de maturidade, configurando o que denominamos de matriz de maturidade. Esses processos podem operar de forma independente, possibilitando que cada um se situe em um nível de maturidade distinto em relação aos demais processos. Essa característica assegura flexibilidade e adaptabilidade, permitindo ajustes específicos conforme o nível de maturidade atribuído a cada processo.

Cada matriz corresponde a um grupo de processos de uma área específica, facilitando a organização e a gestão das atividades dentro de cada setor. Essa abordagem estruturada e focada visa garantir que os processos, ainda que não relacionados entre si, estejam adequadamente alinhados com os objetivos e necessidades de cada área.

Para ilustrar o modelo descrito, apresenta-se na Tabela 7 um exemplo hipotético de como os processos podem ser distribuídos em diferentes níveis de maturidade, de modo a visualizar a aplicação específica de cada processo em sua respectiva área.

Tabela 7 – Processos e níveis de maturidade

Processo	Níveis de maturidade				
	Nível 1	**Nível 2**	**Nível 3**	**Nível 4**	**Nível 5**
P01	X				
P02			X		
P03		X			

Fonte: dados da pesquisa

Para alcançar esses resultados, cada processo foi analisado de acordo com as características dos níveis de maturidade descritos na subseção 4.1, a fim de determinar o nível em que se enquadra. Com o processo identificado, inicia-se pelo primeiro nível, comparando-se o estado atual do processo com as práticas exigidas pelo CMM-PC para esse nível. Cada nível possui um conjunto específico de práticas que a organização precisa adotar. Caso o nível analisado seja atendido e suas práticas estejam devidamente estabilizadas, procede-se ao próximo nível, repetindo o procedimento até atingir o último nível do CMM-PC, o Nível 5.

Por exemplo, o processo P01 de Consentimento de Dados ao Titular está em seu estágio inicial de maturidade, classificado no Nível 1, pois se verificou que as atividades referentes ao processo são executadas de maneira assistemática, sem documentação formal, baseando-se em práticas já estabelecidas pela área. Seguindo esse critério, o processo P02 encontra-se em um estágio mais avançado, no Nível 3, enquanto o P03 está classificado no Nível 2, indicando um estágio intermediário de maturidade.

Ao aplicar os critérios estabelecidos para cada nível, obtém-se uma matriz de maturidade. A partir dessa matriz, podem-se derivar diversas perspectivas, incluindo uma visão de valor numérico condensado em um índice de maturidade, bem como uma visão espacial representada por um gráfico, os quais serão apresentados a seguir.

4.3.1 Indicador de conformidade

Para proporcionar maior clareza e objetividade, optou-se pela implementação de uma metodologia de quantificação simplificada na aplicação do modelo CMM-PC. A quantificação permite uma avaliação precisa dos processos organizacionais, fornecendo métricas claras e dados concretos. Essa abordagem facilita a identificação de pontos fortes e áreas de melhoria, possibilitando um diagnóstico detalhado do estado atual dos processos. Adicionalmente, a quantificação estabelece padrões de desempenho e benchmarks, que servem como referências para comparações internas e externas.

4.3.2 Cálculo do indicador

Para a avaliação completa do modelo CMM-PC, adotou-se uma abordagem baseada em pontuação. O modelo é composto por cinco grupos de processos organizacionais, cada um com igual importância. Assim, a pontuação total é distribuída uniformemente entre esses grupos.

Cada processo dentro dos grupos pode alcançar até o quinto nível de maturidade. Dessa forma, as pontuações, referentes a este processo, variam de 1 (menos maduro) a 5 (mais maduro), refletindo o grau de maturidade do processo. A pontuação de cada grupo é a soma dessas pontuações dos processos pertencentes a ele. Se um grupo possui *n* processos, e cada processo está em um nível de maturidade m_i, então a pontuação do grupo G_j é dada por:

$$G_j = \sum_{i=1}^{n} m_i \tag{1}$$

onde G_j é a pontuação do grupo *j*.

De forma semelhante, a pontuação geral da organização corresponde à soma das pontuações dos cinco grupos:

$$\text{Pontuação total} = \sum_{j=1}^{5} G_j \quad (2)$$

Por fim, a maturidade total, em valores percentuais (ou indicador de maturidade), é calculada conforme a Equação 3:

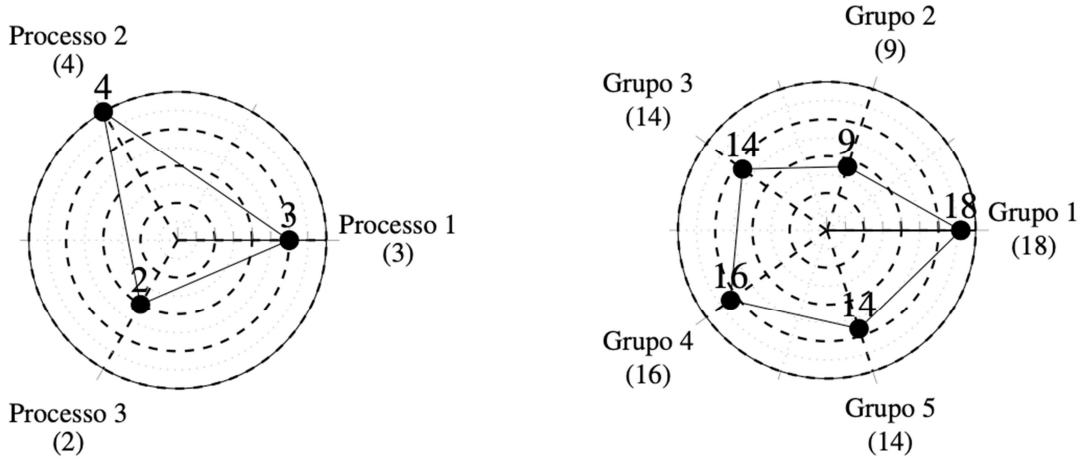
$$\text{Maturidade total} = \left(\frac{\text{Pontuação total}}{\text{Pontuação máxima}} \right) \times 100\% \quad (3)$$

Quanto maior o indicador de maturidade total calculado, mais elevado será o nível de conformidade da organização com a LGPD e, consequentemente, o seu nível de maturidade. A pontuação máxima corresponde ao somatório de todos os processos aplicáveis na avaliação da organização, multiplicado pelo valor máximo de maturidade, que é 5. Em algumas organizações, determinados tipos de tratamento de dados podem não ser relevantes; nesses casos, os grupos de processos correspondentes não serão incluídos no cálculo da pontuação máxima. Por exemplo, em uma organização que não mantém relações com empresas ou instituições internacionais, o grupo de processos relacionado ao tratamento de dados internacionais será excluído do cálculo do total máximo.

4.3.3 Representação gráfica

Além da análise numérica, é possível obter uma visão gráfica da maturidade organizacional por meio do gráfico radar. O gráfico radar, também conhecido como gráfico de aranha ou teia, é uma ferramenta visual que permite a representação de múltiplas variáveis em um único gráfico. Esse tipo de gráfico possibilita múltiplas visualizações, como ilustrado na Figura 1a, que apresenta uma visão por processo, e na Figura 1b, que demonstra a visão por grupo de processos.

Figura 1 – Exemplo de gráfico radar por processo (a) e todo os grupos (b)



(a) (b)

Fonte: dados da pesquisa

Nesse tipo de gráfico, cada variável é representada por um eixo que se estende a partir de um ponto central, formando um formato de estrela ou teia. A pontuação de cada variável é então plotada ao longo desses eixos e conectada, formando uma área poligonal. No contexto do CMM-PC, quanto mais próximo o valor estiver do centro do gráfico, menor será a maturidade da organização ou do grupo de processos; valores mais afastados do centro indicam maior maturidade. Esse formato facilita a comparação visual de diferentes áreas e a identificação rápida de pontos fortes e de áreas que necessitam de aprimoramento.

5 Estudo de caso

Esta seção apresenta os resultados da aplicação do modelo CMM-PC em duas avaliações distintas realizadas em uma instituição federal de ensino com mais de 20.000 alunos nos níveis médio e superior. As avaliações focaram nos processos de tratamento de dados pessoais e nos processos de governança e segurança da informação. Esses dois grupos foram selecionados por possuírem a maior quantidade de processos, o que proporciona um volume significativo de dados para a análise do modelo CMM-PC.

A coleta de dados foi realizada exclusivamente através de pesquisas no site oficial da instituição e da análise de documentos públicos disponíveis, em conformidade com a Lei de Acesso à Informação (LAI), a qual determina que órgãos e entidades públicas devem divulgar informações sobre sua estrutura organizacional, legislações, programas, ações, projetos e obras em seus sites (Brasil, 2011). Foram coletadas evidências relacionadas aos processos mencionados, com o uso de palavras-chave como LGPD, tratamento de dados, Política de Segurança e POSIN (Política de Segurança da Informação). Com os dados obtidos, foi determinado o nível de maturidade de cada processo.

O resultado da análise resultou em uma matriz de maturidade, que permitiu a derivação de dois indicadores: o indicador de maturidade e o gráfico radar, que fornece uma visão espacial dos grupos de processos.

Para cada processo na matriz, foi indicado o nível de maturidade atingido ou a ausência dele, bem como a indicação de sua aplicabilidade na organização, conforme a legenda a seguir:

- "X": possui o nível indicado;
- "–": não possui o nível indicado;
- "N.A.": não aplicável.

Na Tabela 8 apresenta o resultado da avaliação.

Tabela 8 – Matriz de maturidade – Tratamento de dados pessoais

Processo	**Níveis de maturidade**				
	Nível 1	**Nível 2**	**Nível 3**	**Nível 4**	**Nível 5**
P01	X				
P02	X				
P03	X				
P04	X				
P05	X				
P06	–				
P07		X			

Fonte: dados da pesquisa

Na Política de Proteção de Dados Pessoais, foram identificadas referências ao tratamento de dados do titular, abrangendo os processos P01, P02 e P03. Em relação aos procedimentos específicos para consentimento, revogação e acesso aos dados do titular, a política menciona que tais solicitações devem ser encaminhadas ao encarregado de dados, sem fornecer detalhes adicionais. Para o processo P04, foram identificadas evidências apenas em estágio inicial. Observa-se, nos documentos analisados, que o tratamento de dados sensíveis é reconhecido como um procedimento de risco maior para o titular, motivo pelo qual a organização se compromete a adotar medidas de proteção adicionais.

No caso dos processos P05 e P06, foram encontradas evidências somente para o primeiro, relacionado ao consentimento para uso de dados de crianças e adolescentes. No entanto, não foram encontradas referências adicionais quanto ao tratamento específico desses dados e aos tipos de dados coletados. Para o processo P07, há evidências da existência de um Comitê Gestor de Dados Pessoais, responsável por avaliar e propor estratégias de proteção de dados conforme as exigências da LGPD, assegurando o alinhamento da organização com as regulamentações legais.

No cenário geral, considera-se que esses processos atingiram o nível de maturidade 2 (dois), indicando um mínimo de gerência.

Nesse contexto, foi encontrada evidência apenas no processo P05. A legislação referente à proteção de dados de menores de idade exige o consentimento explícito, específico e destacado, fornecido por um dos pais ou pelo responsável legal. Além disso, a lei determina que sejam tornados públicos os tipos de dados coletados, conforme previsto no processo P06, assim como a forma de utilização desses dados e os procedimentos para solicitar acesso, correção, eliminação ou portabilidade. No entanto, para este processo, não foram encontradas evidências documentais que comprovem o cumprimento dessas exigências.

Na segunda avaliação, voltada ao grupo de Governança e Segurança da Informação, foi identificado um nível baixo de maturidade nos processos, com a ausência de alguns deles. A Tabela 9 ilustra esse cenário.

Tabela 9 – Matriz de maturidade – Governança e segurança da informação

Processo	**Níveis de maturidade**				
	Nível 1	**Nível 2**	**Nível 3**	**Nível 4**	**Nível 5**
P14		X			
P15	X				
P16	–				
P17	–				
P18	–				
P19	–				
P20	–				

Fonte: dados da pesquisa

Na avaliação, foram observados elementos de conformidade nos processos P14, evidenciando a atuação de um comitê de segurança da informação, e no processo P15, com normas e procedimentos disponíveis no portal institucional. Nos demais processos (P16 a P20), não foram identificadas evidências de implementação. A ausência de processos, como treinamento e conscientização (P16), auditorias internas (P17), procedimentos para registro de tratamento de dados (P18) e plano de resposta a incidentes (P19), compromete a capacidade da instituição em gerenciar e monitorar incidentes e se adequar às exigências da ANPD. A elaboração de um relatório de impacto à proteção de dados pessoais (P20) também é essencial, pois descreve os processos que podem representar riscos e pode ser solicitado pela ANPD a qualquer momento. A falta desses processos eleva o risco de sanções regulatórias e compromete a conformidade da instituição.

5.1. Indicador de maturidade do estudo de caso

Dois grupos distintos foram analisados: tratamento de dados pessoais e governança e segurança da informação. A seguir, é apresentado o indicador de maturidade para cada grupo, avaliando o estágio de desenvolvimento e a eficácia dos processos.

A Tabela 10a representa o primeiro grupo de processos, enquanto a Tabela 10b representa o segundo.

Tabela 10 – Pontuação dos processos (a) Tratamento dados pessoais. (b) Governança e segurança da informação

Processo	**Nível**
P01	1
P02	1
P03	1
P04	1
P05	1
P06	0
P07	2

Processo	**Nível**
P14	2
P15	1
P16	0
P17	0
P18	0
P19	0
P20	0

Total	7

(a)

P21	0
P22	0
Total	3

(b)

Fonte: dados da pesquisa

Os processos P06 e P16 a P22 não receberam pontuação, sendo considerados com valor zero. No cálculo do indicador, foram incluídos apenas os processos avaliados, pois valores zero anulariam o total. Com isso, usando a Equação 2, obteve-se:

$$\text{Pontuação total} = \sum_{j=1}^{5} G_j = 10 \tag{4}$$

Considerando a avaliação de 16 processos (7 do grupo de tratamento de dados e 9 do grupo de governança e segurança da informação), a pontuação máxima deste estudo de caso é:

$$\text{Pontuação máxima} = (7 + 9) \times 5 = 80 \tag{5}$$

Assim, calculando o indicador de maturidade conforme a Equação 3, em valores percentuais, tem-se:

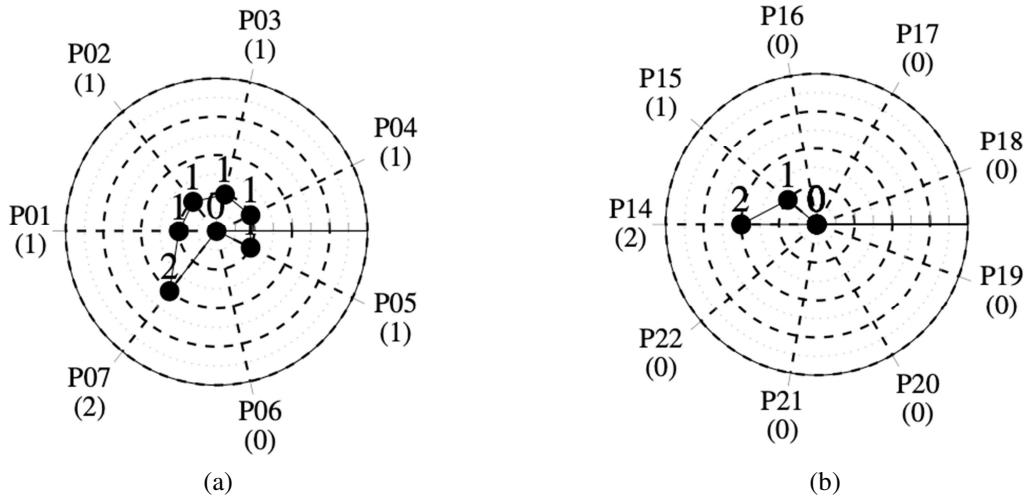
$$\text{Maturidade total } = \left(\frac{100}{80}\right) \times 100\% = 12{,}5\% \tag{6}$$

Conclui-se que, com base nos processos avaliados, a organização atingiu um indicador de maturidade de 12,5%. Ressalta-se que esta é uma avaliação parcial, visto que alguns processos não foram avaliados. Somente após uma avaliação completa será possível obter uma visão abrangente.

5.2. Gráfico de maturidade do estudo de caso

As Figuras 2a e 2b representam graficamente os dados apresentados na análise do estudo de caso.

Figura 2 – Gráfico de maturidade dos grupos de processo. (a) Tratamento de dados pessoais. (b) Governança e segurança da informação



(a) (b)

Fonte: dados da pesquisa

Quanto mais próximo do centro do gráfico, maior a evidência de imaturidade nos processos organizacionais. A Figura 2b, ao exibir apenas três pontos, pode inicialmente sugerir uma situação atípica. Contudo, ao se consultar a tabela de avaliação, observa-se que apenas 2 dos 9 processos obtiveram uma pontuação acima de zero. Os outros 7 processos receberam nota zero, justificando a ausência de pontos no gráfico para esses casos.

6 Conclusões

Este trabalho apresentou um modelo de maturidade de processo para aplicação de conformidade com a LGPD. O modelo CMM-PC foi aplicado em duas avaliações distintas, realizadas em uma instituição federal de ensino. As avaliações abrangeram tanto os processos de tratamento de dados pessoais quanto os de governança e segurança da informação. A análise deste estudo de caso foi realizada com base em documentos públicos disponíveis no portal institucional da organização. Como a Lei de Acesso à Informação (LAI) determina que os órgãos e entidades públicas devem, independentemente de solicitações, divulgar em seus sites da internet informações de interesse coletivo ou geral, como estrutura organizacional, legislações pertinentes, dados sobre programas, ações, projetos e obras, entre outras (Brasil, 2011). Além da própria LGPD que destaca o princípio da transparência e publicização em vários pontos da lei, exigindo que os agentes de tratamento de dados forneçam informações claras, precisas e facilmente acessíveis sobre o tratamento de dados pessoais, garantindo que os titulares compreendam como seus dados estão sendo utilizados (BRASIL, 2018). Alguns dos processos avaliados não foram encontradas evidências de sua existência. Entende-se que a ausência de informações públicas pode indicar que tais processos não existem, não foram formalizados ou não estão sendo gerenciados.

O modelo foi projetado para ser um instrumento que permita às organizações avaliar e

melhorar continuamente seus processos relacionados à proteção de dados, reduzindo os riscos legais e aumentando a confiança de seu público-alvo. Assim, foi possível identificar os níveis de maturidade dos processos organizacionais, fundamentais para estabelecer a conformidade da organização avaliada com a LGPD. A estrutura organizada do modelo, com processos independentes, permite destacar áreas que requerem maior atenção e cuidado. Além disso, o indicador e o gráfico de maturidade oferecem uma perspectiva adicional, fornecendo alternativas para a adequação da organização às exigências de conformidade.

As principais contribuições deste estudo consistem em analisar e interpretar a Lei Geral de Proteção de Dados (LGPD), mapeando seus requisitos em processos organizacionais. Dessa forma, organizações que enfrentam dificuldades para se adequar à conformidade legal poderão utilizar o modelo proposto como um instrumento-guia para atender aos requisitos estabelecidos pela LGPD. Além disso, o estudo propõe níveis de maturidade para os processos organizacionais, permitindo que as instituições avaliem e aprimorem suas práticas de forma independente, concentrando os esforços nas áreas onde houver maior necessidade de evolução.

Uma limitação do estudo foi a falta de aprofundamento, devido à escassez de evidências de conformidade com a LGPD na organização avaliada. Entrevistas *in loco* com profissionais de áreas específicas poderiam ter enriquecido a análise. No entanto, o foco principal foi a análise de documentos públicos disponíveis no portal institucional, conforme a LAI.

Para as próximas etapas deste trabalho em andamento, propõe-se desenvolver métodos para quantificar a avaliação realizada em uma organização, podendo ser tanto geral quanto individualizada por grupo de processo. Estão previstos também estudos de caso mais aprofundados em etapas específicas, como a inscrição e a matrícula de candidatos, visando avaliar mais profundamente a aplicabilidade e a eficácia do modelo proposto. Essa abordagem ofereceria uma visão integrada da aderência da organização aos requisitos da LGPD, facilitando assim a identificação de áreas que demandam atenção prioritária.

Em relação aos trabalhos presentes na literatura, (Ferreira; Okano, 2021) propõe o LGPD *Model Canvas*, uma ferramenta visual destinada a orientar as organizações a desenvolver estratégias para conformidade com a Lei Geral de Proteção de Dados no Brasil. Outro trabalho, de (Araújo *et al*., 2021), apresenta um método para avaliar e modelar processos de negócios segundo a LGPD. Embora ambos enfoquem processos, nenhum aborda a evolução dos mesmos ou a avaliação em níveis de maturidade.

O modelo CMM-PC concentra-se na evolução contínua dos processos, tratando-os como elementos independentes. Cada processo, estruturado e alinhado com requisitos similares, pode progredir em sua própria trajetória de maturidade. Essa abordagem proporciona flexibilidade essencial, permitindo que as organizações se ajustem às demandas dinâmicas e variadas da LGPD.

Em conclusão, a experiência preliminar positiva com o modelo CMM-PC aponta para uma eficácia como instrumento para avaliar a conformidade com a LGPD e fortalecer as boas práticas de proteção de dados nas organizações. O CMM-PC poderá auxiliar as organizações a evoluírem de práticas básicas de privacidade para uma excelência em proteção de dados. Espera-se que, com a contínua evolução e adaptação do modelo, ocorra a diminuição de riscos legais e o fortalecimento da confiança dos clientes, tornando-o uma referência importante para organizações que buscam aprimorar suas práticas de privacidade e segurança.

Financiamento
Esta pesquisa não recebeu financiamento

Conflito de interesses
Os autores declaram não haver conflito de interesses

Nota

Os resultados deste trabalho são decorrentes na dissertação de Mestrado de Jonas Pereira de Andrade Filho, disponível em: https://repositorio.ufpb.br/jspui/handle/tede/5439.

Contribuições ao artigo

ARAUJO FILHO, J. P.; MOTTA, G. H. M. B.: concepção do estudo/pesquisa; análise e/ou interpretação dos dados; revisão final com participação crítica e intelectual no manuscrito. Todos os autores participaram da escrita, discussão, leitura e aprovação da versão final do artigo.

Referências

ARAÚJO, E. F. M.; VILELA, J.; SILVA, C. T. L. L.; ALVES, C. F. Are my business process models compliant with LGPD? the LGPD4BP method to evaluate and to model LGPD aware business processes. *In*: BRAZILIAN SYMPOSIUM ON INFORMATION SYSTEMS, 12. 2021, Uberlândia. **Proceedings […].** New York: ACM, 2021. DOI: https://doi.org/10.1145/3466933.3466982.

BARBOSA, T. S.; LOPES, J. M.; PIAU, D. D. N. D.; SILVA, M. S.;TELES, E. O. A Lei Geral de Proteção de Dados (LGPD) nas instituições públicas de ensino: possíveis impactos e desafios. *In*: ENCONTRO NACIONAL DE PROPRIEDADE INTELECTUAL (ENPI), 7., 2021, on-line.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no [...]. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 29 jul. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para uso da internet no Brasil. **Diário Oficial da União,** Brasília, DF, 2014. Disponível em: https://www.in.gov.br/web/dou/-/lei-n-12-965-de-23-de-abril-de-2014-30054600. Acesso em: 14 nov. 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 nov. 2024.

CGU – Controladoria Geral da União. BRASIL, C.-G. d. U. **Acesso à informação pública**: uma introdução à Lei nº 12.527, de 18 de novembro de 2011. Brasília: CGU, 2011. Disponível em: https://www.gov.br/acessoainformacao/pt-br/central-de-conteudo/publicacoes/arquivos/cartilhaacessoainformacao-1.pdf. Acesso em: 29 nov. 2024.

CHRISSIS, M. B.; KONRAD, M.; SHRUM, S. **CMMI**: guidelines for process integration and product improvement. Boston: Addison-Wesley, 2003.

CMMI Institute. **CMMI Institute**. 2024. Disponível em: https://www.cmmiinstitute.com/cmmi. Acesso em: 14 nov. 2024.

CORTINA, S.; VALOGGIA, P.; BARAFORT, B.; RENAULT, A. Designing a data protection process assessment model based on the GPDR. *In*: WALKER, A.; O'CONNOR, R.; MESSNARZ, R. (ed.) **Systems, softwares and services process improvement**. EuroSPI 2019. Communications in Computer and Infofrmation Science, v. 1060. Charm: Springer, 2019. p. 136-148. DOI: https://doi.org/10.1007/978-3-030-28005-5_11.

COTS, M.; OLIVEIRA, R. **Lei geral de proteção de dados pessoais**: comentada. 2. ed. São Paulo: Revista dos Tribunais, 2019.

CRESPO, M. Proteção de dados pessoais e o poder público: noções essenciais. *In*: CRAVO, D. C.; CUNDA, D. Z. G.; RAMOS, R. (org.). **Lei Geral de Proteção de Dados e o Poder Público**. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021. p. 16-28. Disponível em: https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf. Acesso em: 14 nov. 2024.

CUNHA, B. Q. **O vazamento de dados do *e-commerce* Netshoes**: implicações da Lei Geral de Proteção de Dados (LGPD). 2022. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal Rural do Semiário, Mossoró, 2022. Disponível em: https://repositorio.ufersa.edu.br/handle/prefix/8898. Acesso em: 29 nov. 2024.

DANIEL, M. A. **A evolução e aplicação da segurança da informação por meio da Lei Geral de Proteção de Dados pessoais (LGPD)**: um estudo de caso em uma instituição financeira.2022 Trabalho de Conclusão de Curso (Bacharelado em Tecnologias da Informação e Comunicação) – Universidade Federal de Santa Catarina, Araranguá, 2022. Disponível em: https://repositorio.ufsc.br/handle/123456789/233375. Acesso em: 14 nov. 2024.

FAYAYOLA, O. A.; OLORUNFEMI, O. L.; SHOETAN, P. O. Data privacy and security in it: a review of techniques and challenges. **Computer Science & IT Research Journal**, v. 5, n. 3, p. 606-615, 2024. DOI: https://doi.org/10.51594/csitrj.v5i3.909.

FERREIRA, L.; OKANO, M. T. Um panorama da implementação da LGPD no Brasil: uma pesquisa exploratória com 216 profissionais. *In*: XVI Simpósio dos Programas de Mestrado Profissional (SIMPROFI), 16., 2021, São Paulo. **Anais [...]**, São Paulo: CPS, 2021. Disponível em: http://www.pos.cps.sp.gov.br/files/artigo/file/1156/bccaf2858e19a55702075c3afbfee4be.pdf. Acesso em: 14 nov. 2024.

FINKELSTEIN, M. E.; FINKELSTEIN, C. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira (RDB)**, v. 23, n. 9, p. 284-381, 2020. DOI: https://doi.org/10.26668/IndexLawJournals/2358-1352/2019.v23i9.5343.

KALINOWSKI, T. B. Business process maturity assessment: concept, methods and tools. Acta Universitatis Lodziensis, v. 257, p. 229-240, 2011. Disponível em: https://dspace.uni.lodz.pl:8443/xmlui/handle/11089/744. Acesso em: 14 nov. 2024.

KNOKE, F.; NWANKWO, I. Practitioner's corner managing data protection compliance through maturity models: a primer. **European Data Protection Law Review**, v. 8, n. 4, p. 536-543, 2022. DOI: https://doi.org/10.21552/edpl/2022/4/14.

LABADIE, C.; LEGNER, C. Understanding data protection regulations from a data management perspective: a capability-based approach to EU-GDPR. *In*: INTERNATIONAL CONFERENCE ON WIRTSCHAFTSINFORMATIK, 14., 2019, Siegen. **Proceedings [...]**, Siegen, 2019. Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1261&context=wi2019. Acesso em: 14 nov. 2024.

LEE, J.; LEE, D.; KANG, S. An overview of the Business Process Maturity Model (BPMM). *In*: CHANG, K. C.-C.; WANG, W. CHEN, L.; ELLIS, C. A.; HSU, C.-H.; TSOI, A. C.; WANG, H. (eds). **Advances in web and network technologies (APWeb WAIM 2007)**. Lecture Notes in Computer Science, v. 4537. Berlin: Springer, 2007. p. 384-395. DOI: https://doi.org/10.1007/978-3-540-72909-9_42.

MORGADO, G. P.; MORGADO, G. P.; GESSER, I.; SILVEIRA, D. S.; MANSO, F. S.; LIMA, P.; SCHMITZ, E. A. . Práticas do CMMI® como regras de negócio. **Produção**, v. 17, n. 2, p. 383-394, 2007. DOI: https://doi.org/10.1590/S0103-65132007000200013.

MPDFT – Ministério Público do Distrito Federal e Territórios. **MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados**. 2024. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-dedanos-morais-coletivos-apos-vazamento-de-dados. Acesso em: 2 set. 2024.

PAULK, M. C.; CURTIS, B.; CHRISSIS, M. B.; WEBER, C. V. Capability maturity model, version 1.1. **IEEE Software**, v. 10, n. 4, p. 18-27, 1993. DOI: https://doi.org/10.1109/52.219617.

PEREIRA, R.; SILVA, M. M. ITIL maturity model. *In*: IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES, 5., 2010. Santiago de Compostela. **Proceedings [...]**. IEEE: Santiago de Compostela, 2010. p. 1-6. Disponível em: https://ieeexplore.ieee.org/document/5556698. Acesso em: 14 nov. 2024.

PINHEIRO, P. P. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020.

RNP – Rede Nacional de Ensino e Pesquisa.**LGPD**: tudo o que você precisa para se adequar. Brasília: RNP, 2022. Disponível em: https://www.rnp.br/sistema-rnp/adeque-se-a-lgpd. Acesso em: 14 nov. 2024.

ROCHA, A. R.; ZABEU, A. C.; MACHADO, C. F. MR-MPS-SW:2016 and CMMI-DEV v2.0: an initial experience of harmonization. *In*: BRAZILIAN SYMPOSIUM ON SOFTWARE QUALITY (SBQS '18), 12., 2018, Curitiba. **Proceedings [...]**. New York: ACM, 2018. p. 287-295. DOI: https://doi.org/10.1145/3275245.3275285.

SANTOS, R. G. T. **A Lei Geral de Proteção de Dados Brasileira**: uma política pública regulatória. 2020. Monografia (Especialização) – Instituto Serzedello Corrêa Brasília, 2020. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/a-lei-geral-de-protecao-de-dados-brasileira-uma-politica-publica-regulatoria.htm. Acesso em: 14 nov. 2024.

SARASWAT, A. K.; MEEL, V. Protecting data in the 21st century: challenges, strategies and future prospects. **Information Technology in Industry**, v. 10, n. 2, p. 26-35, 2022. Disponível em: http://www.it-in-industry.org/index.php/itii/article/view/854. Acesso em: 14 nov. 2024.

VASCONCELOS, C. R.; SALIB, M. L. L. **Lei geral de proteção de dados pessoais**: desafios e impactos para o Poder Público. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade Católica de Rondônia, Porto Velho, 2021. Disponível em: https://lgpd.tcero.tc.br/wp-content/uploads/2021/07/TCC-Charles-Roge%CC%81rio-Vasconcelos_TCE-RO.pdf. Acesso em: 19 out. 2024.

WARREN, S.; BRANDEIS, L. The right to privacy. Harvard Law Review, v. IV, n. 5, p. 193-220, 1890. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 14 nov. 2024.

ZITOUN, C; BELGHITH, O. FERJAOUI, S.; GABOUJE, S. S. D. DMMM: Data management maturity model. *In*: INTERNATIONAL CONFERENCE ON ADVANED ENTERPRISE INFORMATION SYSTEM (AEIS), 2021, St. Petersburg. **Proceedings […].** St. Petersburg: IEEE, 2021. p. 33-39. DOI: https://doi.org/10.1109/AEIS53850.2021.00013.