Revista UNEMAT de Contabilidade

Vol. 14, nº 28, Ano 2025

FRAMEWORK DE RISCOS NA LGPD: IMPACTOS PARA A INOVAÇÃO CONTÁBIL EM MATO GROSSO

LGPD RISK FRAMEWORK: IMPACTS ON ACCOUNTING INNOVATION IN MATO GROSSO

Clayton Ferreira Leão
Mestrando em Propriedade Intelectual e Transferência de Tecnologia para Inovação(UNEMAT)
Universidade Federal de Mato Grosso (UFMT)
e-mail: professor.leao@yahoo.com.br

Ivor Prolo
Doutor em administração (ESPM)
Universidade do Estado de Mato Grosso(UNEMAT)
e-mail: ivorprolo@unemat.br

Joaquim Manoel da Silva
Doutor em Genética e Biologia Molecular(UNICAMP)
Universidade do Estado de Mato Grosso (UNEMAT)
e-mail: joaquimmanoel@unemat.br

RESUMO: A presente pesquisa tem o propósito principal de analisar como a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD), impacta os escritórios de contabilidade em Mato Grosso, com ênfase na adoção de mecanismos de *compliance* orientados por análises de riscos e na promoção da inovação na prestação de serviços contábeis. Para alcançar tal propósito a metodologia utilizada caracteriza-se por uma abordagem quanti-qualitativa, transversal, com natureza metodológica explicativa e descritiva. Utilizou-se as técnicas de coleta de dados bibliográfica e documental (normas diversas) e uma pesquisa *survey* com questionário on-line encaminhado aos profissionais de contabilidade que atuam nos escritórios de contabilidade no estado de Mato Grosso. Ao final da pesquisa totalizou 41 respondentes. A análise dos dados foi alcançada por meio da utilização do modelo desenvolvido por Mendes (2018), ferramenta que permite analisar em que nível está o risco de segurança e privacidade e segurança dos escritórios de contabilidade. Foi detectado que, o controle de segurança física, lógica e documentação, estão "Bem definidos" dentro dos escritórios de contabilidade. Já as categorias: coleta e gestão da informação, transferência de dados e consentimento, assim como direito dos titulares, carece de melhorias nos controles, processos e pessoas.
Palavras-chave: Lei Geral de Proteção de Dados (LGPD), *Compliance*, Análise de Riscos, Inovação.

ABSTRACT: The main purpose of this research is to analyze how the implementation of the General Law on the Protection of Personal Data (LGPD) impacts accounting firms in Mato Grosso, with an emphasis on the adoption of compliance mechanisms

guided by risk analysis and the promotion of innovation in the provision of accounting services. To achieve this, the methodology used is characterized by a quantitative-qualitative, cross-sectional approach, with an explanatory and descriptive methodological nature. It used bibliographic and documentary data collection techniques (various standards) and a survey with an online questionnaire sent to accounting professionals working in accounting offices in the state of Mato Grosso. At the end of the survey, there were 41 respondents. The data was analyzed using the model developed by Mendes (2018), a tool that makes it possible to analyze the level of security and privacy risk in accounting firms. It was found that physical, logical and documentation security controls are "well defined" within accounting firms. On the other hand, the categories of information collection and management, data transfer and consent, as well as the rights of data subjects, need to be improved in terms of controls, processes and people.

Keywords: General Data Protection Law (GDPR), Compliance, Risk Analysis, Innovation.

1 - INTRODUÇÃO

A proteção de dados pessoais tronou-se um conceito central no contexto jurídico e tecnológico atual, pois, para diminuir as ameaças presentes quanto a proteção de dados pessoais, é necessária uma regulamentação que defina as ações a serem tomadas na coleta, processamento, armazenamento, descarte, e transferência dos mesmos (dados pessoais), o que impactou na reformulação da estrutura operacional dos escritórios de contabilidade.

Para os profissionais da contabilidade que atuam nos escritórios de contabilidade, a tecnologia trouxe à tona questões relevantes no que tange à segurança das informações (Ribeiro, Krüger, Michelin e Raddatz, 2020), frente a responsabilidade, seja objetiva ou subjetiva, obrigando-os a adotar estrutura e métodos para salvaguardar os dados de seus clientes e o seu correto tratamento e descarte.

Neste sentido, para assegurar a proteção necessária as pessoas, foi aprovado no Brasil, a Lei Geral de Proteção de Dados - LGPD (Lei n° 13.709/18), sancionada em 2018 no Brasil, que estabelece regras claras sobre a coleta, tratamento, armazenamento, descarte e compartilhamento de dados pessoais, com o objetivo de garantir a privacidade e os direitos dos indivíduos.

A norma se alinha com os princípios da CF - Constituição da República Federativa do Brasil (Brasil, [2016-EC]), que assegura o direito à intimidade e à privacidade (artigo 5º, X) e ao Código Civil (Lei n° 10.406/02) que em seus artigos, regula aspectos do direito à personalidade, como o direito à imagem e à honra, impactados pela coleta e uso de dados pessoais. Esses fundamentos buscam criar um equilíbrio entre a inovação tecnológica e a proteção dos direitos fundamentais dos cidadãos.

Moraes (2024) evidencia que, a identificação de critérios objetivos para a avaliação de riscos de privacidade traz diversos benefícios para os agentes regulados. Primeiramente, a otimização de recursos permite que as empresas concentrem seus esforços nas atividades que realmente demandam maior atenção, evitando o desperdício de tempo e recursos em atividades de baixo risco. Além disso, a identificação de atividades de alto risco facilita a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais

(RIPDs) mais completos e detalhados. Ao focar nos casos mais críticos, os agentes de tratamento podem fornecer informações mais relevantes às autoridades de proteção de dados, demonstrando seu compromisso com a conformidade e a transparência.

No Estado de Mato Grosso, dados de março de 2024 possuía 465.246 empresas ativas para um universo de 9.761 profissionais da contabilidade que atuam nos escritórios de contabilidade (CFC-2024) atuando de forma autônoma ou inserido em escritórios de contabilidade (1.996 escritórios), ou contratado no regime CLT em outras entidades jurídicas. O Estado possui uma população total de 3.567.234 de habitantes conforme dados divulgados pelo IBGE (2022).

Torchia (2020) destaca que, a implementação da norma é complexa, demanda de esforço financeiro e mecanismos de *compliance* como ferramenta de avaliação de riscos internos, voltados para a segurança jurídica. Trazendo como consequências para a organização e aos profissionais que não se adequarem a norma impositiva, as punições regulatórias que vão desde uma advertência até multa pecuniária. A implementação da LGPD, em uma organização contábil deve ter uma interseção com a prática contábil, destacando as obrigações dos profissionais contábeis no tratamento de informações pessoais, e os mecanismos de *compliance* para assegurar a conformidade com a norma.

Krüger et al. (2021), aponta a importância de estudar a LGPD na área contábil de forma contínua, pois, o escritório de contabilidade é um reservatório de dados pessoais sensíveis, com o poder de impactar não somente o ciclo operacional dos profissionais, mas também prejuízos incalculáveis aos proprietários dos dados.

Brilhante (2022) destaca que, a Lei Geral de Proteção de Dados Pessoais (LGPD), ampliou os fundamentos outrora elencados no Marco Civil da Internet, trazendo em seu Art. 2º. e incisos, e devido a sua relevância ao estudo aqui demostrado, cabe o destaque: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A legislação ampliou também a aplicabilidade, tanto para pessoas naturais quanto para pessoas jurídicas, e mais, estabeleceu, ainda, os agentes de atuação entre as trocas de informações: quem coleta dados, quais dados coleta, por que coleta, quem efetua o tratamento desses dados coletados, e todas essas informações devem ser controladas por um Encarregado dos Dados ou Data Protection Officer (DPO).

O CFC – Conselho Federal de Contabilidade, publicou a Resolução 1.626/21 que, institui a Política Interna de Proteção de Dados Pessoais do Conselho Federal de Contabilidade, normatizando os processos e procedimento para melhor atender as obrigações taxativas da LGPD, trazendo segurança jurídica enquanto Conselho representativo.

Diante do exposto, questiona-se: Quais fatores influenciam a adoção de mecanismos de *compliance* com foco em análise de riscos por escritórios de contabilidade em Mato Grosso, visando à conformidade com a LGPD (Lei nº 13.709/18) e à promoção da inovação na prestação de serviços contábeis?

Para esclarecer tal problemática, esse estudo teve como objetivo principal analisar como

a implementação da LGPD impacta os escritórios de contabilidade em Mato Grosso, com ênfase na adoção de mecanismos de compliance orientados por análises de riscos e na promoção da inovação na prestação de serviços contábeis.

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018, representa um novo marco regulatório foi instituído no país, exigindo das organizações a adoção de mecanismos efetivos de *compliance* e proteção de dados é alto. A LGPD exige, entre outras obrigações, a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais, conforme o artigo 5º, XVII e artigo 38 da Lei, os quais descrevem o ciclo de tratamento dos dados e as estratégias de mitigação de riscos adotadas. A Autoridade Nacional de Proteção de Dados (ANPD) pode, inclusive, exigir a apresentação desses documentos a qualquer momento, sob risco de penalidades severas.

Além do impacto regulatório, há também um forte apelo à inovação. O cumprimento da LGPD exige investimentos em processos, tecnologia e capacitação, impulsionando transformações na forma como os serviços contábeis são prestados. As sanções previstas no artigo 52 da Lei, que incluem multas de até R$ 50 milhões por infração, reforçam a urgência de adequação. Nesse contexto, a Avaliação de Impacto à Proteção de Dados (AIPD) torna-se uma ferramenta estratégica, não apenas para garantir a conformidade legal, mas também para promover segurança, confiança e diferenciação competitiva no mercado.

A pesquisa traz uma proposta inovadora ao criar um espaço de discussão e desenvolvimento de políticas de educação continuada para a classe contábil, promovendo o acesso a informações e conhecimentos essenciais sobre a LGPD.

A pesquisa apresenta como sugestão de um modelo para avaliar a maturidade dos processos organizacionais que envolvem o tratamento de dados pessoais, possibilitando a execução de análises de riscos nestes processos, em conformidade com o LGPD, e será útil de maneira imediata para auxiliar as empresas atingirem a conformidade com o Artigo 5, XVII e outros dispositivos, que trata das Análises de Impacto de Proteção de Dados (AIPD), garantindo assim os direitos e liberdades dos titulares.

Portanto, esta pesquisa se justifica pela necessidade de compreender como a LGPD está sendo implementada no âmbito da contabilidade em Mato Grosso, identificando os desafios enfrentados pelos profissionais e propondo caminhos para fortalecer a gestão de riscos e o *compliance*.

2 - REFERENCIAL TEÓRICO

Neste capítulo, apresenta-se uma introdução à legislação brasileira de proteção de dados, abordando seus conceitos fundamentais, suas implicações para o tratamento de dados pessoais e os referenciais teóricos que sustentam a discussão. Para facilitar o entendimento, o conteúdo é organizado em seções específicas.

Segundo Carvalho (2021), a LGPD (Lei nº 13.709/18) representa a consolidação de diretrizes já presentes em legislações anteriores, como a Lei de Acesso à Informação (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014). Além disso, a LGPD é fortemente influenciada pelo Regulamento Geral de Proteção de Dados da União Europeia (GDPR – *General Data Protection Regulation*), de 2016, considerado um marco internacional na proteção da privacidade dos titulares de dados pessoais (DP).

A LGPD define com clareza, em seu artigo 5º, incisos I e II, os conceitos de dado pessoal e dado pessoal sensível, os quais exigem atenção redobrada por parte de empresas e profissionais autônomos, dado o impacto jurídico e financeiro decorrente de seu uso indevido: I – Dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II – Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Essa proteção é respaldada constitucionalmente no artigo 5º da Constituição Federal de 1988, em seu inciso LXXIX (incluído pela Emenda Constitucional nº 115, de 2022), que assegura o direito à proteção dos dados pessoais, inclusive nos meios digitais, e impõe obrigações quanto ao tratamento, armazenamento e descarte dessas informações (BRASIL, 2022).

Uma das principais preocupações da LGPD reside na preservação da privacidade dos indivíduos. O artigo 5º, XVII, da norma, reforça essa diretriz ao definir o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como a documentação do controlador que descreve os processos de tratamento de dados que possam representar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas e salvaguardas adotadas para mitigá-los.

Nesse sentido, torna-se essencial que as organizações desenvolvam e mantenham programas estruturados de *compliance*, com ênfase em análise de riscos. O artigo 50 da LGPD reforça essa exigência, ao estabelecer que controladores e operadores devem adotar mecanismos internos de supervisão e mitigação de riscos, garantindo o cumprimento das diretrizes legais no tratamento de dados.

De acordo com Burkart (2021), o conceito de compliance deriva do verbo inglês *to comply*, que significa obedecer, concordar ou estar em conformidade. No contexto organizacional, representa o conjunto de políticas e práticas que visam assegurar a adequação às normas legais e regulatórias. Assim, os programas de *compliance* constituem instrumentos fundamentais para orientar as ações institucionais frente às exigências legais, como as impostas pela LGPD.

Dessa forma, este capítulo apresenta os fundamentos teóricos que sustentam a pesquisa, abordando os temas de privacidade, dados pessoais, *compliance* e os riscos específicos à atuação contábil diante da LGPD, que constituem o alicerce para as análises desenvolvidas ao longo do trabalho.

2.1 LGPD - Lei Geral de Proteção de Dados Pessoais

Como limitações da pesquisa cita-se a escassez de estudos a respeito do tema, especialmente para a área contábil, justamente por se tratar de uma lei recente, o que dificultou a discussão dos resultados. Também corresponde a um fator limitador as variáveis e constructos desenvolvidos, visto que podem existir demais influenciadores para a conformidade com a LGPD, e que podem não ter sido considerados. Além disso, cita-se a dificuldade de estimar de maneira taxativa o tamanho da população de profissionais voltados à área contábil.

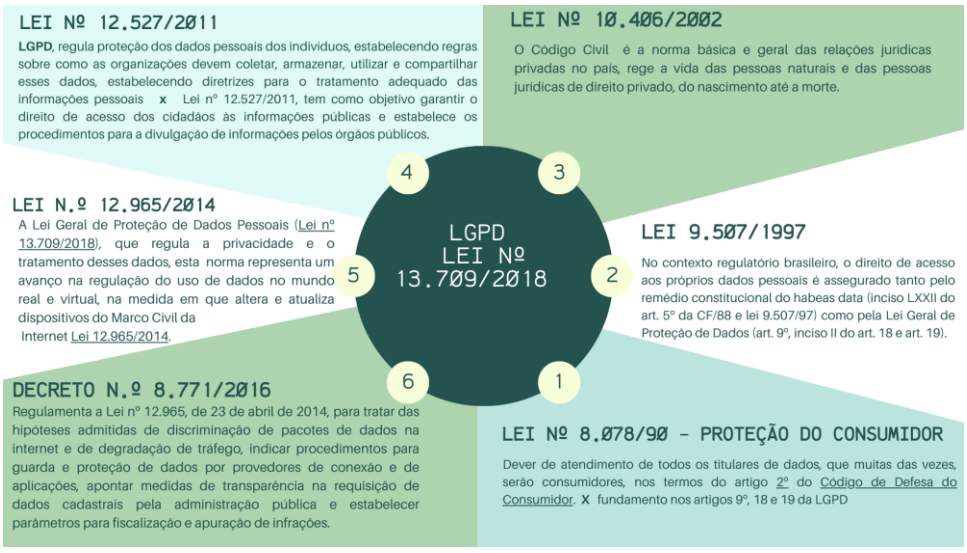
A nova lei sofreu nítidas influências do Regulamento Geral de Proteção de Dados Europeu - GDPR de maio de 2018, amparando sobremaneira a intimidade e a vida privada, em constantes ataques, principalmente no âmbito das redes sociais.

Tartuce (2021) em sua análise descreve que, a proteção dos dados pessoais acabou por ser regulada pela Lei 13.709, de 14 de agosto de 2018 (Lei de Proteção de Dados Pessoais – LGPD), norma que aborda o tema em sessenta e cinco artigos e que entrou em vigor no País em setembro de 2020 – com exceção dos seus arts. 52 a 54, que tratam de sanções administrativas, e que entrou em vigor em 1.º de agosto de 2021, por força do art. 20 da Lei 14.010/2020. O diploma tem incidência em qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de Direito Público ou Privado.

Caranti e Fukuhara (2021), traz uma reflexão normativa, destacando que, antes da LGPD, no Brasil à partir da década de 1990, iniciou-se a construção de normas legais que abraçaram a proteção da privacidade e a salvaguarda dos dados pessoais, incluindo: a) Lei 8.078/1990 - O Código de Defesa do Consumidor; b) Lei 9.507/1997 - Que regulamenta o direito de acesso à informação e estabelece o procedimento do habeas data; c) Lei 10.406/2002 - O Código Civil Brasileiro; d) Lei 12.527/2011 - Que regula o acesso à informação; e) Lei n.º 12.965/2014 - Que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil; f) Decreto n.º 8.771/2016 - Que aborda as circunstâncias permitidas de discriminação de pacotes de dados na internet e de degradação do tráfego.

É possível citar como exemplo o artigo 43 do Código de Defesa do Consumidor que cuidou dos bancos de dados e cadastros dos consumidores. Neste caso, o legislador buscou abarcar todo e qualquer banco de dados que atingisse o livre desenvolvimento do consumidor, não apenas aqueles que apresentem informações negativas dos indivíduos. A Figura 1 – "Conexões Normativas", apresenta um resumo referente as principias conexões das normas ao tema central LGPD.

Figura 1 - Conexões Normativas

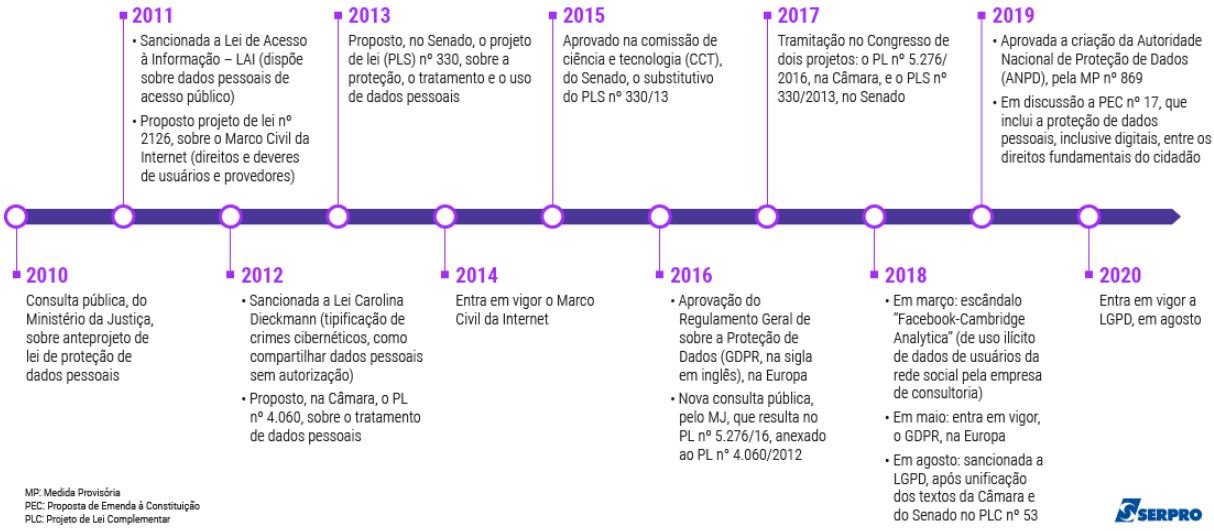


Fonte: Elaborado pelo autor, 2025.

A coleta, armazenamento e descarte de dados, independentemente de serem sensíveis ou não, agora estão amparados por legislação no Brasil, afetando significativamente a vida de cidadãos, consumidores, empresas e governo que é a Lei n° 13.709/18 (BRASIL, 2018). A LGPD, fortemente influenciada pelo GDPR europeu, foi promulgada para estabelecer um quadro regulatório mais sólido no Brasil. A lei destaca o consentimento como um dos fundamentos legais para o tratamento de dados pessoais, embora o Código Civil já tenha tratado da anulação de negócios jurídicos baseados em erro substancial.

Brilhante (2022), analisa a linha temporal da norma, com os debates no continente europeu. Nesse mesmo sentido, é interessante perceber como as mesmas iniciativas com relação à proteção de dados são tratadas nos demais países, principalmente com relação a maior ou menor força de regulamentação e de punição. A LGPD vigente no Brasil é considerada com nível moderado em termos de regulamentação e de sanção pelo descumprimento. A *Timeline* a seguir demonstra esta evolução histórica normativa (Figura 2):

Figura – 2 - Linha do Tempo do processo de regulação da LGPD no Brasil



Fonte: SERPRO (2021, n.p.)

As principais diferenças entre a LGPD e o GDPR, aborda aspectos como o escopo territorial, o tratamento de dados sensíveis, o tratamento de dados de menores, a formalização do vínculo entre controlador e operador, relatórios de impacto, notificações de violações de dados e sanções administrativas.

Assim, também se destaca a importância do *compliance* nas organizações contábeis, abordando a necessidade de adaptação interna das entidades às normas que impactam suas operações, a fim de reduzir riscos legais e de imagem. Para tanto, aplica-se ao estudo diversos conceitos extraídos da ISO 37301:2021 *Compliance management systems — Requirements with guidance for use* (Sistemas de gestão de conformidade - Requisitos com orientação para uso) assim como, a ISO 31000 que trata da norma geral de gestão de riscos, e a ISO 27001 e 27701, normas específicas para segurança e privacidade da informação.

Portanto, a LGDP obriga os profissionais da contabilidade que atuam nos escritórios de contabilidade ao tratamento de dados pessoais, inclusive nos meios digitais, por pessoa

natural ou por pessoa jurídica de direito público ou privado, a proteção: a) aos direitos fundamentais de liberdade e de privacidade; b) o livre desenvolvimento da personalidade da pessoa natural.

A própria norma determina que a proteção de dados pessoais deve ter, entre outros fundamentos: a) o respeito à privacidade e à dignidade; b) a inviolabilidade da intimidade, da honra e da imagem; c) o desenvolvimento econômico e tecnológico e a inovação; d) a livre iniciativa, a livre concorrência e a defesa do consumidor; e) o exercício da cidadania pelas pessoas naturais, Lei n° 13.709/18 (Brasil, 2018).

Implementar (no ciclo operacional dos profissionais da contabilidade que atuam nos escritórios de contabilidade) a LGPD contribui para proteger os dados pessoais, garantir a conformidade legal, evitar multas, promover confiança dos clientes, fortalecer a reputação da empresa. Proteger a privacidade é um direito humano fundamental, garantindo o uso ético de dados pessoais e fortalecendo a dignidade da pessoa humana conforme a CF/88 (BRASIL), e Tratados Internacionais na qual o Brasil é signatário.

Dentre os Tratados tem-se a Declaração Universal dos Direitos Humanos adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948, em seu artigo 12 que diz: “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques”.

2.2 Dados Pessoais – Tipos e Tratamento

Na Lei Geral de Proteção de Dados Pessoais (LGPD), dados pessoais são definidos como qualquer informação relacionada a uma pessoa natural identificada ou identificável. Em outras palavras, são dados que podem ser usados, sozinhos ou em combinação com outras informações, para identificar uma pessoa.

Os dados pessoais se dividem em três tipos fundamentais sendo: a) pessoal que é a informação relacionada à pessoa natural identificada ou identificável, tais como: nome, RG, CPF, endereço, e-mail etc.; b) pessoal sensível, é neste item que devem redobrar os cuidados. Trata-se de dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural LGPD (Lei n° 13.709/18).

Para Lima, e Garrido (2022), considera-se como tratamento de dados pessoais as seguintes ações: acesso, armazenamento, arquivamento, avaliação, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização. Ainda podem ser interpretados como tratamento de dados os processos organizacionais que realizem análises de caráter qualitativo e/ou qualitativo, cópias de segurança (backup), estruturação e indexação de dados.

A LGPD abraçou diversos dispositivos normativos que já garantiam uma certa proteção ao indivíduo como a Lei nº 14.289/2022, que determina a vedação a divulgação (sigilo), pelos agentes públicos ou privados, de informações que permitam a identificação da condição de pessoa com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose, nos

seguintes âmbitos: a) serviços de saúde; b) estabelecimentos de ensino; c) locais de trabalho; d) administração pública; e) segurança pública; f) processos judiciais; g) mídia escrita e audiovisual. Dados estes altamente sensíveis e devem ser protegidos.

Complementa o debate, os artigos 46 e seguintes, da LGPD, que tratam da segurança de dados, governança e sanções administrativas adequadas em caso de incidentes de segurança. Reconhece este artigo, portanto, as boas práticas aplicáveis ao tratamento de dados pessoais, indicando a necessidade de adoção de medidas que previnam e evitem danos aos titulares de dados, dando assim um caráter subjetivo.

Lima e Filho (20149), reforça a importância sobremaneira a implementação de programas de *compliance* no âmbito das empresas, bem como análise de riscos.

2.3 O *Compliane* e a Análise de Risco frente a implementação da LGPD

O termo *compliance* é polissêmico, trazido à doutrina brasileira sobremaneira pela influência do direito americano. O seu espectro de sentido compreende originalmente o controle de condutas corporativas, visando, sobretudo, à superação da influência de interesses pessoais ou de um grupo em prol dos interesses da companhia e seus acionistas. Essa compreensão original é bem mais ampla do que aquela que tende a prevalecer no Brasil (Lima e Filho, 2019).

Para atender as determinações da LGPD, os escritórios e os profissionais da contabilidade que atuam nos escritórios de contabilidade devem: a) desenvolver/manter processos e procedimentos atualizados; b) adotar regras de boas práticas de *compliance* (gestão de riscos); c) não coletar dados que não tenham relação com o contrato de trabalho ou dados sensíveis; d) ter procedimentos administrativos para proteger os dados pessoais de seus colaboradores e clientes; e, e) capacitar os colaboradores que lidam com estes dados, especialmente os das áreas de recursos humanos (RH) e do departamento de pessoal (DP), para que observem as determinações legais atinentes ao assunto.

Ribeiro, Krüger, Michelin e Raddatz (2020) descreve que, há uma relação que pode ser estabelecida entre a LGPD e as políticas de *compliance* que se apresentam de forma distribuída em diversos pontos da legislação sobre proteção de dados pessoais e dados sensíveis.

Neste sentido, Pinheiro (2021) destaca que, existe uma relação direita entre LGPD e a proteção aos direitos fundamentais poderá ser observada na análise do art. 2º da LGPD, no qual são mencionados princípios encontrados no texto constitucional brasileiro como cerne do desenvolvimento de todo e qualquer tratamento de dados pessoais. Dentre os artigos constitucionais que podem ser relacionados com os princípios apontados no art. 2º da LGPD destacam-se os art. 3º, I, II; art. 4º, II; art. 5º, X, XII; art. 7º, XXVII; art. 2198.

Conforme estabelecido na Lei nº 13.709/2018 (LGPD) na comunicação entre operador dos dados e a ANPD deverá constar, no mínimo: a) a descrição da natureza dos dados pessoais afetados; b) as informações sobre os titulares envolvidos; c) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; d) os riscos relacionados ao incidente; e) os motivos da demora, no caso de a comunicação não ter sido imediata; e f) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. A ANPD verificará a

gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de outras providências.

Ribeiro, Krüger, Michelin e Raddatz (2020), enfatiza que, a LGPD traz uma proteção ampla ao tratamento de dados pessoais, seja esse tratamento realizado de maneira analógica ou digital. Para ambas as hipóteses, é necessário um completo redesenho das políticas de *compliance* empregadas pelas organizações.

Neste sentido, um programa estabelecido de *compliance* (análise de risco), identifica e trata a subjetividade a que uma análise de risco de um processo de tratamento de dados está sujeito pode ser reduzida significativamente com uma metodologia que permita avaliar o risco com base no contexto, propósitos do tratamento de dados, criticidade dos dados pessoais e das aplicações envolvidas no tratamento, sendo assim mais fácil e direto propor soluções para mitigar os riscos associados, esta foi análise conduzida por Mendes (2018) no trabalho título “Análise de risco no GDPR” pela Universidade de Lisboa.

2.4 Infrações - Penalidades

A Lei nº 13.709/2018 (LGPD), também define um sistema de infrações e penalidades para garantir sua eficácia. As infrações podem ocorrer quando há descumprimento das normas relativas ao tratamento de dados pessoais, como o uso inadequado, o vazamento ou a falta de transparência com os titulares. As penalidades podem variar desde advertências e multas até sanções mais severas, como a suspensão do tratamento de dados ou a proibição parcial ou total das atividades de processamento de dados.

Esse sistema de penalidades tem o objetivo de incentivar a conformidade com a lei, garantindo que as organizações adotem práticas adequadas de proteção de dados e oferecendo uma resposta eficaz às violações. O *enforcement* da LGPD é conduzido pela Autoridade Nacional de Proteção de Dados (ANPD), que é responsável por fiscalizar, aplicar as penalidades e promover a educação sobre o tema.

As infrações às determinações da LGPD são passíveis das seguintes sanções administrativas, aplicáveis pela ANPD:

a) advertência, com indicação de prazo para adoção de medidas corretivas; b) multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 por infração; c) multa diária, observado o limite total mencionado na letra "b"; d) publicização da infração após devidamente apurada e confirmada a sua ocorrência; e) bloqueio dos dados pessoais a que se refere a infração até a sua regularização; f) eliminação dos dados pessoais a que se refere a infração; g) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

Neste sentido, esta pesquisa busca compreender como a implementação da LGPD impacta na atuação, *compliance* (identificação e gestão de riscos), inovação e práticas dos profissionais de contabilidade no Estado de Mato Grosso.

3 - METODOLOGIA

O presente estudo busca resumidamente, compreender as principais barreiras para implementação da LGPD em escritórios de contabilidade localizados em Mato Grosso, os

procedimentos legais de tratamento de dados pessoais, avaliar o nível de aplicação desses conceitos pelos profissionais contábeis que representam os escritórios de contabilidade no estado de Mato Grosso, analisando os riscos dessa aplicação (*compliance*).

Neste capítulo serão apresentados os principais procedimentos metodológicos adotados, como as técnicas para coleta dos dados bibliográficas, e estratégia para aplicar o questionário e análise dos resultados.

Para Krüger et al. (2021), que também investigou a aplicação da LGPD no *laboro* dos profissionais de contabilidade, este destacou como limitação em sua pesquisa a escassez de estudos a respeito do tema, especialmente para a área contábil, justamente por se tratar de uma lei recente, o que dificultou a discussão dos resultados. Também corresponde a um fator limitador as variáveis e constructos desenvolvidos, visto que podem existir demais influenciadores para a conformidade com a LGPD, e que podem não ter sido considerados.

Para compreender os impactos da LGPD nos escritórios de contabilidade localizados em Mato Grosso, optou-se por realizar uma análise de riscos na implementação da LGPD (*compliance*) cuja origem em termos gerais está alicerçada na ISO 27001 e 27701, que poderão ser vistas como uma aplicação da gestão de riscos da ISO 31000, especificamente no contexto da segurança e privacidade da informação. Já a ISO 27701 é uma extensão da ISO 27001 e complementa-a com requisitos específicos para privacidade da informação.

Neste sentido, e após analisar diversas publicações sobre o tema, foi escolhido um desenvolvido por Mendes (2018) e aplicado no contexto deste trabalho com algumas adaptações à LGPD. Com o foco de atingir os objetivos propostos nesta dissertação, serão aplicados os procedimentos metodológicos apresentados neste capítulo, o qual apresenta a caracterização o público-alvo, o método de coleta e da análise de dados, especificando as estratégias e as técnicas adotadas.

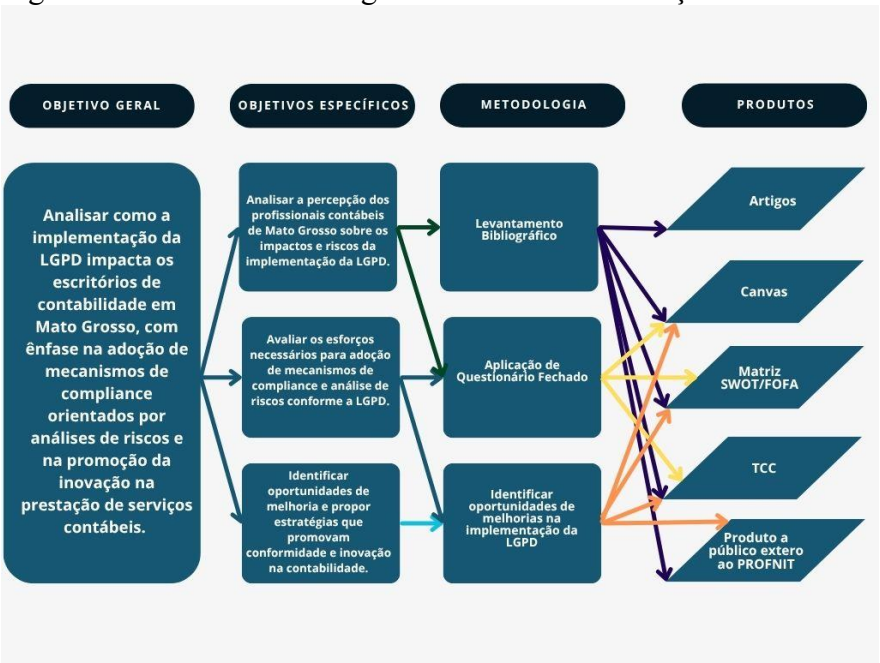
3.1 Caracterização da Pesquisa

Para alcançar tal propósito a metodologia utilizada caracteriza-se por uma abordagem quanti-qualitativa, transversal, com natureza metodológica explicativa e descritiva. Utilizou-se as técnicas de coleta de dados bibliográfica e documental (normas diversas) e uma pesquisa *survey* com questionário on-line encaminhado aos profissionais de contabilidade que atuam nos escritórios de contabilidade no estado de Mato Grosso.

Desta forma, partindo da problemática proposta que buscou diagnosticar a compreensão da aplicabilidade da LGPD no *laboro* dos profissionais da contabilidade que atuam nos escritórios de contabilidade no estado de Mato Grosso, e seu impacto na política de *compliance* em especial análise de riscos.

A pesquisa utilizou como ponto de partida as pesquisas bibliográfica e normativa, que foram o alicerce para a elaboração do questionário aplicado a coleta de dados (BERTASSI, 2016). A seguir a Figura -3 “Síntese Metodológica e Matriz de Amarração” ilustra a intersecção entre objetivo geral, objetivos específicos, metodologia e produtos.

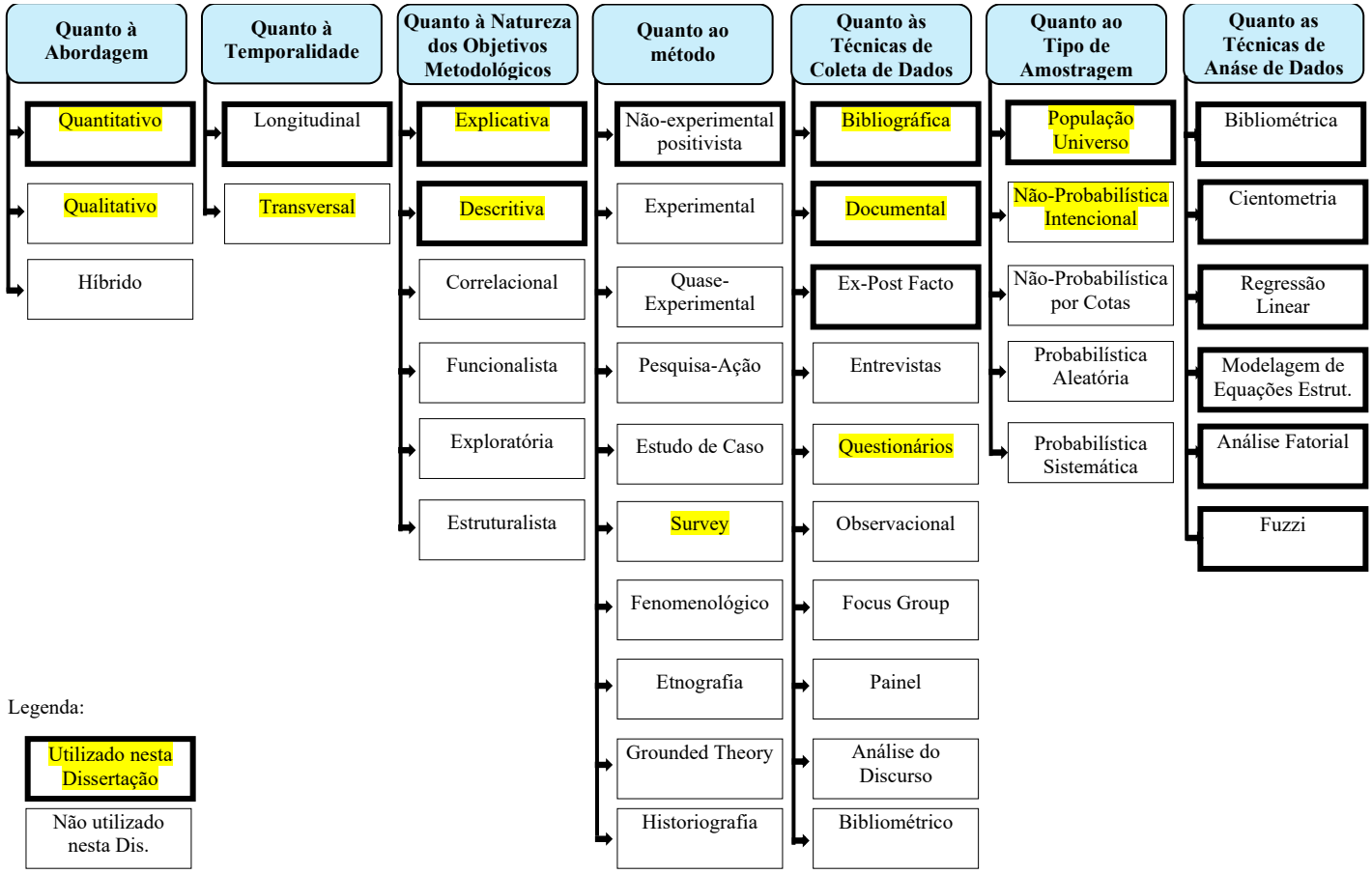
Figura -3. Síntese Metodológica e Matriz de Amarração



Fonte: Elaborado pelo autor, 2025.

Já a Figura 4 ilustra um diagrama de fluxo metodológico que visa proporcionar uma compreensão abrangente da abordagem proposta, com o objetivo de alcançar as metas estabelecidas para esta investigação. Em seguida à Figura 4 – Fluxograma Metodológico base, serão detalhadas as particularidades e os passos metodológicos adotados.

Figura 4 – Fluxograma Metodológico base



Fonte: Elaborado de Bertassi (2016, p. 51) e Do Prado (2019).

As metodologias destacadas na Figura 2 podem ser entendidas conforme as explanações a seguir. No que diz respeito à abordagem, este estudo pode ser descrito como híbrido, o que significa que integra aspectos qualitativos e quantitativos.

Quanto à abordagem para Gil (2002, p. 134) nas pesquisas quantitativas, as categorias são freqüentemente estabelecidas a priori, o que simplifica sobremaneira o trabalho analítico. Já nas pesquisas qualitativas, o conjunto inicial de categorias em geral é reexaminado e modificado sucessivamente, com vista em obter ideais mais abrangentes e significativos. Por outro lado, nessas pesquisas os dados costumam ser organizados em tabelas, enquanto, nas pesquisas qualitativas, necessita-se valer de textos narrativos, matrizes, esquemas etc.

Quanto à temporalidade conforme Oliveira (2019) a presente proposta de pesquisa tem características transversal pois é aplicado um questionário fechado que procura evidenciar a aplicabilidade da LGPD nos escritórios de contabilidade em um determinado momento no tempo, pois muitas alterações de procedimentos e legislação e jurisprudência ocorrem frequentemente.

Quanto à Natureza dos Objetivos Metodológicos, este estudo pode ser classificado como explicativo e descritivo. O estudo explicativo visa esclarecer os fatores que determinam ou que contribuem para a ocorrência dos fenômenos. Esse é o tipo de

pesquisa que mais aprofunda o conhecimento da realidade. O estudo descritivo tem como preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos. Esse é o tipo de pesquisa que mais aprofunda o conhecimento da realidade, porque explica a razão, o porquê das coisas. Por isso mesmo, é o tipo mais complexo e delicado, já que o risco de cometer erros aumenta consideravelmente (GIL, 2002, p. 42).

Quanto às Técnicas de Coleta de Dados, foram utilizadas as pesquisas bibliográfica, documental e questionário. Para Gil (2002), a pesquisa bibliográfica assim como qualquer outra modalidade de pesquisa, desenvolve-se ao longo de uma série de etapas. Portanto, pode ser entendida como um processo que envolve: a) escolha do tema; b) levantamento bibliográfico preliminar; c) formulação do problema; d) elaboração do plano provisório de assunto; e) busca das fontes; f) leitura do material; g) fichamento; h) organização lógica do assunto; e i) redação do texto. Já a pesquisa documental pode exigir a consulta aos mais diversos tipos de arquivos públicos e particulares. Já o questionário entende-se por um conjunto de questões que são respondidas por escrito pelo pesquisado.

A pesquisa bibliográfica foi conduzida com base em livros, artigos científicos, teses e dissertações que abordaram os aspectos normativos relacionados à aplicabilidade da Lei Geral de Proteção de Dados Pessoais (LGPD) no campo da contabilidade.

O recorte temporal adotado compreendeu o período de 2018 a 2023, justificado por corresponder ao momento de maior impacto e mobilização prática e teórica em torno da implementação da LGPD, instituída pela Lei nº 13.709/2018. As buscas foram realizadas nas bases de dados Web of Science e Scopus, por meio de combinações de palavras-chave como "Lei Geral de Proteção de Dados", "LGPD", "*Compliance*", "Contabilidade" e "General Data Protection Regulation", incluindo suas respectivas traduções para o inglês, conectadas pelo operador booleano “AND”.

Na base Web of Science, utilizou-se o campo de busca “All Fields”, enquanto na base Scopus foi selecionada a opção “Article Title, Abstract, Keywords”. Os dados foram submetidos a uma triagem, com exclusão de duplicatas e análise dos resumos, a fim de verificar a pertinência dos documentos ao escopo da pesquisa e ao público-alvo.

A análise revelou um número reduzido de publicações no período selecionado que tratassem da LGPD em articulação com a atividade contábil. A combinação entre as palavras-chave “*Compliance*” e “LGPD” resultou em 19 publicações na Web of Science e 20 na Scopus. Além da LGPD, a pesquisa considerou normativos que, de forma indireta, abordam a proteção de dados pessoais, como o Código de Defesa do Consumidor (Lei nº 8.078/1990) e a Lei do Habeas Data (Lei nº 9.507/1997).

A inclusão da palavra-chave *compliance* se justificou pelo fato de que, mesmo antes da LGPD, já existiam dispositivos legais que exigiam o tratamento adequado de dados sensíveis, especialmente no ambiente digital. Além disso, o tratamento de dados pessoais já era objeto de normatização internacional, como a ISO 37301, que estabelece diretrizes para sistemas de gestão de *compliance*, incluindo a prevenção e correção de não conformidades legais. Com a entrada em vigor da LGPD, essa exigência se intensificou, tornando-se mais uma obrigação a ser incorporada pelos escritórios contábeis.

Verificou-se que as áreas do conhecimento com maior volume de publicações no período foram Direito e Computação/Informática, sem destaque expressivo para a área

da Contabilidade, evidenciando uma lacuna na literatura científica quanto à abordagem prática da LGPD nesse setor.

Nesse contexto, compreender como os escritórios de contabilidade têm interpretado e implementado a LGPD é essencial para o aprimoramento da atuação profissional. A adequação à norma tornou-se parte integrante dos processos de *compliance* dessas entidades, exigindo atualização técnica e reorganização procedimental.

Diante disso, esta pesquisa justifica-se também por seu caráter aplicado, ao direcionar-se especificamente ao público-alvo formado por profissionais da contabilidade atuantes em escritórios contábeis. Para tanto, aplicou-se um questionário estruturado junto a esses profissionais, com o objetivo de identificar suas percepções quanto à implementação da LGPD e os impactos decorrentes sobre práticas inovadoras no exercício da profissão no estado de Mato Grosso.

A amostragem adotada foi do tipo não-probabilística, intencional, tanto nas buscas bibliográficas quanto na coleta de dados empíricos, conforme defendido por Oliveira (2019), por basear-se no julgamento criterioso do pesquisador em vez da aplicação de técnicas estatísticas.

A população-alvo da pesquisa compreendeu os profissionais com registro ativo no Conselho Regional de Contabilidade de Mato Grosso (CRC-MT). De acordo com dados do Conselho Federal de Contabilidade (CFC), o estado contava, no período analisado, com 4.239 contadores (bacharéis) e 1.116 técnicos em contabilidade do gênero masculino, e 4.020 contadoras (bacharéis) e 386 técnicas em contabilidade do gênero feminino, totalizando 9.761 profissionais.

Embora esta pesquisa não exigisse um número mínimo de respondentes, buscou-se obter o maior número possível de respostas de contadores atuantes em escritórios de contabilidade, com o objetivo de ampliar a representatividade do grupo analisado. Durante o período em que o questionário on-line disponível de 03-06-2025 a 18-06-2025, foram obtidas 41 respostas válidas. A divulgação e coleta das respostas ocorreram por meio de diferentes canais de comunicação, incluindo e-mail, WhatsApp e redes sociais (Instagram), com apoio efetivo do Sindicato das Empresas de Serviços Contábeis do Estado de Mato Grosso SESCON que colaborou na mobilização dos profissionais da categoria.

A análise dos dados foi orientada pelo modelo proposto por Mendes (2018), cuja aplicação será detalhada nas próximas secções deste trabalho.

3.2 Modelo para análise de risco

No âmbito desta dissertação foi realizado uma pesquisa sobre publicações quanto ao tema central LGPD e seus impactos na atividade laboral dos profissionais de contabilidade. Todavia, há poucas publicações no período de 2018 a 2023.

Neste contexto, foi identificado como ponto de partida um documento público de autoria da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, contendo referências a publicações e a outros documentos técnicos, com destaque para aqueles do Center for Internet Security (CIS), do *National Institute of Standards and Technology* (NIST), da *International Standardization Organization/Eletrotechnical Commission* (ISO/IEC) e da Associação Brasileira de Normas Técnicas (ABNT NBR).

Uma análise mais profunda do Guia, identificou-se que o foco é realizar uma análise risco nos órgãos públicos vinculados quanto a LGPD, gerenciamento e controle destes riscos (*compliance*). Neste sentido, o TCU – Tribunal de Contas da União também elaborou em 2018 o Referencial Básico de Gestão de Riscos.

A Gestão de riscos (TCU-2018) consiste em um conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos. Este Guia utilizou dos conceitos prescritos na própria norma e em diversos dispositivos elencado na ISO (*the International Organization for Standardization*) utilizada e padronizado em todo o mundo.

Neste sentido, foram analisados os preceitos contidos na ISO 37301:2021 que é um padrão internacional que fornece um guia para as organizações que desejam implementar e manter um sistema de gestão eficaz dos riscos de conformidade e o cumprimento das obrigações legais e regulamentares. Já a ISO 31000 fornece o marco geral para a gestão de riscos, enquanto a ISO 27001 e a ISO 27701 aplicam esse marco à segurança e privacidade da informação, respectivamente.

Assim a ISO 37301:2021 que trata dos Sistemas de Gestão de Conformidade (*compliance*) - Requisitos com orientação para uso (*Compliance management systems — Requirements with guidance for use*) no item 4.6 – descreve a avaliação de risco de conformidade, indicando que, a organização deve identificar, analisar e avaliar seus riscos de conformidade com base em uma avaliação de risco de conformidade periodicamente e sempre que houver mudanças materiais nas circunstâncias ou no contexto organizacional. A organização deve reter informações documentadas sobre a avaliação de risco de conformidade e sobre as ações para tratar de seus riscos de conformidade.

Desta forma, um “Framework” conceitua a Estrutura Básica de Segurança. Trata-se de um conjunto de atividades de segurança que visam a produzir resultados desejados e referências aplicáveis que são comuns em setores de infraestrutura crítica, seja lógica ou física. NIST (2018)

Diante do exposto, encontrou-se um trabalho publicado pelo mestre Pedro A. B. Mendes (2018), pela Universidade de ULisboa, que aplicou método de *compliance* (análise de risco) similar ao utilizado pelos diversos agentes públicos, todavia, em replicável que foi utilizado para avaliar ao *General Data Protection Regulation* – GDPR-UE. Tal modelo foi adaptado para análise da LGPD.

3.2.1 Avaliações de Risco e DPIAs no âmbito do RGPD-LGPD

O modelo desenvolvido por Mendes (2018), cita que, no final de 2016, a CIPL (*Centre for Information Policy Leadership*) que é um think tank global de política de privacidade e dados, sediado em Washington, D.C., Bruxelas e Londres, publicou um artigo que interpretava o conceito de risco e das Avaliações de Impacto de Proteção de Dados, com base nos artigos e implicações do RGPD, e os correlacionava com a sua própria abordagem ao risco.

Dessa forma, os “Riscos relacionados com tratamento dos dados pessoais”, Mendes (2018) sugeriu uma série de riscos que devem ser considerados relacionados à privacidade dos dados, além de uma proposta de abordagem para a elaboração dos

Relatórios de Impacto à Proteção de Dados Pessoais ou *Data Protection Impact Assessment* (DPIA).

Para facilitar o controle e operação matemática utilizou-se um padrão racional para identificar resumidamente os riscos – "id" R. Este trabalho aplicou um modelo utilizado para avaliar os impactos e risco quanto a GDPR, adaptando-o a LGPD.

4. APRESENTAÇÃO DOS RESULTADOS

Neste capítulo, as figuras apresentadas demonstram os resultados alcançados. O modelo aplicado é uma adaptação de um framework desenvolvido e publicado por Mendes (2018) utilizando o software Excel, que aplicou o modelo para avaliar os riscos nas empresas referente a GDPR (UE). Neste sentido, a mesma ferramenta foi adaptada para ser aplicada na análise do questionário enviado nos escritórios de contabilidade em Mato Grosso, devidamente adequada a LGPD.

O modelo é composto por 14 folhas (planilha em *excel*), cada uma com uma finalidade diferente. Resumidamente, as questões do questionário são preposicionadas para que todas as análises sejam agrupadas no sentido de atender os requisitos da LGPD, divididos nas seguintes fases:

- Avaliação de criticidade: Esta fase está contemplada na folha "04 Criticidade";
- Avaliação de maturidade: Esta fase é realizada na folha "05 Maturidade", onde é classificada cada uma das questões descritas (em Anexo) que por sua vez estão associadas a artigos do LGPD. Os resultados desta fase são apresentados na folha seguinte;
- Identificação de potenciais riscos: Para esta fase não existe necessidade de interação. Os riscos já foram identificados previamente e mapeados com as questões de maturidade no desenvolvimento do modelo, e inseridos no protótipo. Como tal pode-se observar os riscos presentes associados a cada questão na folha "08 Riscos";
- Avaliação dos riscos: Esta fase acontece também na folha "08 Riscos", onde para cada questão da avaliação de maturidade, que já tem os riscos mapeados, pode-se classificar a probabilidade de ocorrência e impacto dos mesmos;
- Validação do risco aceitável: Esta fase é ser realizada através da observação dos resultados da fase anterior, na folha "09 Resumo riscos";
- Mitigação dos riscos: Nesta fase são escolhidas as estratégias face ao risco de cada questão da avaliação de maturidade, que decorre na folha "10 Mitigação";
- Revisão: Esta fase passa por rever algumas das fases anteriores, e deve basear-se nos resultados da fase anterior disponíveis na folha "11 Resumo mitigação".

A redução de riscos deve ser baseada nos resultados da aplicação do modelo. Durante a fase de mitigação de risco, a planilha "10 Mitigação" descreve possíveis soluções que podem ser usadas para mitigar o risco. Após esta etapa, o processo pode ser revisto.

Assim, devido ao modelo metodológico aplicado não há a necessidade de pelo comitê de ética de pesquisa. A subjetividade inerente a uma avaliação de risco de um

procedimento de tratamento de dados pode ser drasticamente diminuída com uma metodologia que possibilite avaliar o risco considerando o contexto, os objetivos do processamento de dados, a sensibilidade dos dados pessoais e as aplicações envolvidas. Dessa forma, torna-se mais simples e direto sugerir soluções para minimizar os riscos relacionados.

Inicialmente, é preciso realizar uma avaliação de maturidade dos processos para compreender a sua situação em relação à conformidade com as normas e os controles e medidas de segurança em vigor. Assim, poderemos calcular os riscos (*compliance*) relacionados ao LGPD e à segurança dos dados, tornando mais fácil sugerir medidas de segurança (mitigação) a serem implementadas (inovação - processos) em diversas circunstâncias, pela maioria das organizações.

Inicialmente o questionário objetivava identificar o perfil do escritório contábil. Nisto, o levantamento sobre a localização dos escritórios de contabilidade que participaram deste estudo revelou que 58,5% situam-se na mesorregião Centro-Sul Mato-Grossense (região de Cuiabá e entorno), 14,6% no Sudoeste Mato-Grossense (região de Tangará da Serra e entorno), outros 14,6% no Norte Mato-Grossense (região de Sinop e entorno) e 7,3% no Nordeste Mato-Grossense (região de Canarana e entorno). Além disso, 4,9% dos escritórios participantes não estão localizados em Mato Grosso.

Na sequência utilizou-se a classificação – SEBRAE para identificar o porte do escritório de contabilidade. Esta classificação está interligada a quantidade de colaboradores definidos pelo SEBRAE e não pela LC 123/2006. Sendo assim, o resultado foi: 58,5% Microempresa (até 9 colaboradores), 36,6% Empresa de pequeno porte (de 10 a 49 colaboradores), 2,4% Empresa de médio porte (de 50 a 99 colaboradores), 2,4% Empresa de grande porte (100 ou mais colaboradores).

Para melhor identificar quem está a responder o questionário, ficou evidenciado que, 56,1% trata-se de Proprietário(a) / Sócio(a), 14,6% Contador(a) Responsável Técnico, 4,9% Analista Contábil, 7,3% Analista Fiscal, 4,9% Analista Trabalhista / Departamento Pessoal, 7,3% Assistente / Auxiliar, 2,4% Administrativo / Financeiro, 2,4% Estagiário. Apesar de que foram respondidos por diversos atores dentro da organização, devido ao baixo número de respostas e entendendo que, todos, independentemente do nível hierárquico ou responsabilidade técnica, devem ter o conhecimento sobre LGPD caso a entidade tenha uma política estruturada, pois todos são responsáveis pela manutenção seja direita ou indiretamente.

Quanto aos serviços que os escritórios de contabilidade oferecem, observa-se que, em sua maioria desenvolvem atividades básicas como, escrituração contábil, fiscal e departamento de pessoal, veja a Figura 12 – Fases da mitigação de risco abaixo:

4.1 – Avaliação da Maturidade

Como já descrito no item 5.3.2 Critério de Maturidade, (extrai-se os dados do questionário por indicativo da maioria, alimenta-se a ferramenta em Excel) sua avaliação (Figura 5 – Extrato da avalição de maturidade) é segmentada em seis áreas principais, todas diretamente ligadas aos artigos extraídos da LGPD. Cada uma dessas áreas apresenta um conjunto de questões, indicando o artigo ou artigos relacionados a cada uma delas (adaptado da análise da GDPR), juntamente com uma explicação sucinta sobre a necessidade de um controle para assegurar a aderência a essa questão.

Apenas a coluna "Maturidade" deve ser preenchida nesta folha, conforme o estado atual do processo, para confirmar a conformidade com a questão a ser preenchida.

Figura 5 – Extrato da avalição de maturidade

Avaliação de maturidade						
Área	GPDR Artigo	LGPD Artigo	Justificação	Id	Questão	Maturidade
Coleta e informação	7	6,9,14	Os titulares devem ser informados do propósito do tratamento dos seus dados, do período durante o qual os seus dados irão ser armazenados, dos seus direitos, e caso aplicável, se os dados serão transferidos para outros países ou instituições.	1.1	5. Até que ponto seu escritório adota um processo que assegura que, antes da coleta de dados, os titulares sejam devidamente informados, sobre a finalidade da coleta e sobre as etapas do tratamento dos seus dados pessoais?	Não implementado
	6, 7	8	Os titulares devem dar o consentimento para o processamento dos seus dados e deve ser possível demonstrar que os titulares deram o consentimento para o tratamento dos seus dados, excetuando quando o processamento for necessário para garantir conformidade com uma obrigação legal.	1.2	6. Existe uma forma definida de registar, armazenar e disponibilizar (dados) quando requisitado o consentimento para o processamento ?	Bem definido
	5	6	Devem ser coletados apenas os dados necessários para os tratamentos identificados.	1.3	7. Existe um processo para garantir que são coletados apenas os dados necessários para cada procedimento?	Bem definido
	5	6	Apenas devem ser realizados os tratamentos aos dados pessoais que foram identificados para os titulares na recolha dos dados.	1.4	8. Existe um processo para garantir que apenas são realizados os tratamentos que foram propostos aos titulares?	Bem definido
	5	16,5	Os dados pessoais devem apenas permitir identificar os titulares durante o propósito para o qual os dados foram recolhidos.	1.5	9. Existem medidas de minimização dos dados, como anonimização para garantir que os dados depois dos tratamentos não permitem a identificação dos titulares?	Não implementado

Fonte: Elaborado pelo autor, 2025 (resumo).

Observa-se que, para facilitar o controle das áreas utiliza-se a fator numérico “id” em que nas etapas seguintes é um norteador para equação matemática, identificando a área x questão. A coluna “maturidade” será preenchida conforme opção do profissional que irá responder o questionário. Observe as colunas iniciais que reverencia os artigos impactados por cada área, sua justificação e questão. Assim, cada questão foi pensada em atender aos quesitos específicos de cada norma.

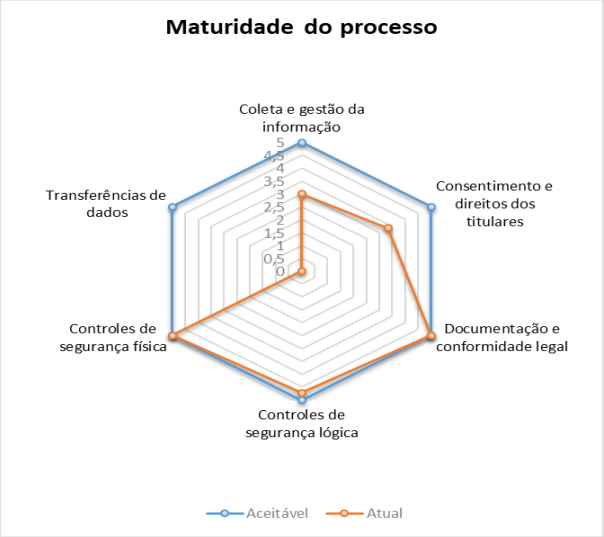
4.1.1 - Resumo da avaliação de maturidade – Radar de Criticidade

Depois de completar a avaliação de maturidade, tem-se um gráfico (Figura 6 – Resumo de maturidade do processo – Radar de Criticidade) que resume a conformidade do processo de tratamento de dados com a LGPD e as pontuações de maturidade atribuídas. A média da classificação por área é apresentada no resumo da avaliação de maturidade, e a classificação "Bem definido" é considerada aceitável para a área estar em conformidade conforme parâmetro já destacado por Mendes (2018).

Todos os resultados analisados específicos ao tema proposto, foram obtidos via questões de 5 a 39 aplicadas aos profissionais que atuam em escritórios de contabilidade divididos nas seguintes áreas: coleta de informações; consentimento e direitos dos titulares; documentação e requisitos legais; controles de segurança lógico; controles de segurança física e transferência de dados. Cada subárea possuí questões específicas.

O gráfico a seguir resume o nível de maturidade referente a LGPD obtido após a aplicação do questionário, sendo o ideal nota cinco.

Figura 6 – Resumo de maturidade do processo – Radar de Criticidade



Fonte: Elaborado pelo autor, 2025.

O Radar de Criticidade, é uma ferramenta que tem grande potencial para ajudar na análise e avaliação de projetos devido as suas características: flexibilidade para utilização em diversas áreas de negócio; alto grau de liberdade para melhorias e adaptações nas etapas propostas; utilização de uma ferramenta conhecida no mercado para seu desenvolvimento; facilidade de visualização do resultado por meio de um gráfico e uma nota, conforme destaca Ferrari e Louro (2016).

Este diagrama proporciona uma perspectiva geral do processo, possibilitando a identificação imediata das áreas onde será preciso um maior empenho para adequar o procedimento a LGPD, por consequente em paralelo com a análise de risco, proporciona uma visão ampla do processo conforme e não conforme.

No resultado obtido, observa-se que, o controle de segurança física, lógica, documentação, estão “Bem definidos” dentro das organizações, isto se dá devido ao fato de que, todos os escritórios possuem servidor e sistema de contabilidade que entrega uma segurança quanto a proteção de dedados através de senhas e banco de dados próprios, conforme destaco nas respostas abertas.

Já os itens coletam e gestão da informação, transferência de dados e consentimento e direito dos titulares, carece de melhorias nos controles, processos e mão-de-obra.

4.2 – Avaliação dos Riscos

Em seguida, abordaremos a parte de avaliação de riscos (Figura 7 – Classificação de riscos). Todavia, antes da avaliação propriamente dita, temos a folha "07 Classificação de Risco", já devidamente descrito no item 5.3.3 Avaliação dos Riscos, que detalha os impactos e probabilidades, além de fornecer a matriz de risco.

Segundo Mendes (2018) a folha "08 Riscos" apresenta a avaliação de riscos, são os riscos relacionados a cada questão da avaliação de maturidade. Para cada pergunta, a classificação de maturidade previamente preenchida, a questão em si, as

vulnerabilidades às quais a questão pode estar exposta e os perigos que podem surgir da exploração dessas vulnerabilidades.

Esses riscos estão organizados segundo a lista fornecida no item 5.2.1. Nas duas colunas seguintes, são registradas a probabilidade de ocorrência das vulnerabilidades e o impacto gerado pela exploração delas e pelo comprometimento dos sistemas. Após o preenchimento destes dois parâmetros a coluna do valor do risco será preenchida automaticamente. Para facilitar o controle e operação matemática utilizou-se um padrão racional para identificar resumidamente os riscos – "id" R.

Nas duas colunas seguintes preenche-se a probabilidade de ocorrência das vulnerabilidades e o impacto que a exploração das mesmas e o comprometimento dos dados pessoais podem ter nos titulares dos dados. Após o preenchimento destes dois parâmetros a coluna do risco deverá ficar preenchida.

Figura 7– Classificação de riscos

Id	Maturidade da questão	Questão	Vulnerabilidades	Riscos	Possíveis consequências	Probabilidade de ocorrência	Impacto	Valor do risco
1.1	Não implementado	5. Até que ponto seu escritório adota um processo que assegura que, antes da coleta de dados, os titulares sejam devidamente informados, sobre a finalidade da coleta e sobre as etapas do tratamento dos seus dados pessoais?	- Falta de informação aos titulares	- R01 - R08	- Podem ser realizados tratamentos aos dados pessoais que o titular não tenha autorizado e que não esteja de acordo	Significante	Significante	Alto
1.2	Bem definido	6. Existe uma forma definida de registar, armazenar e disponibilizar (dados) quando requisitado o consentimento para o processamento ?	- O consentimento não fica devidamente registado	- R08 - R10	- A organização não consegue validar que está a efetuar tratamentos apenas para titulares que autorizaram o tratamento dos seus dados - A organização não consegue demonstrar o consentimento dado caso requisitado	Insignificante	Limitado	Baixo

Fonte: Elaborado pelo autor, 2025.

Apresenta-se aqui a correlação entre "questão" x vulnerabilidade x riscos, assim como suas classificações. Auxiliando a empresa a compreender em que estágio está a análise do tema, sua implementação, seus impactos no ciclo operacional do escritório. Resultados que prepara a entidade a reflexão quanto a mitigação (diminuição ou eliminação) dos riscos frente ao atendimento dos requisitos da LGPD.

Nas questões marcadas como "Não aplicável", não será preciso avaliar o risco para esses itens, pois não se relacionam com o processo analisado, e o valor do risco já está preenchido como "n/a", que significa não aplicável.

Destaca-se nos resultados analisados neste item, a inexistência da figura do DPO (*Data Protection Officer*), assim como um sistema de compliance, identificado na análise de maturidade (Radar de Criticidade).

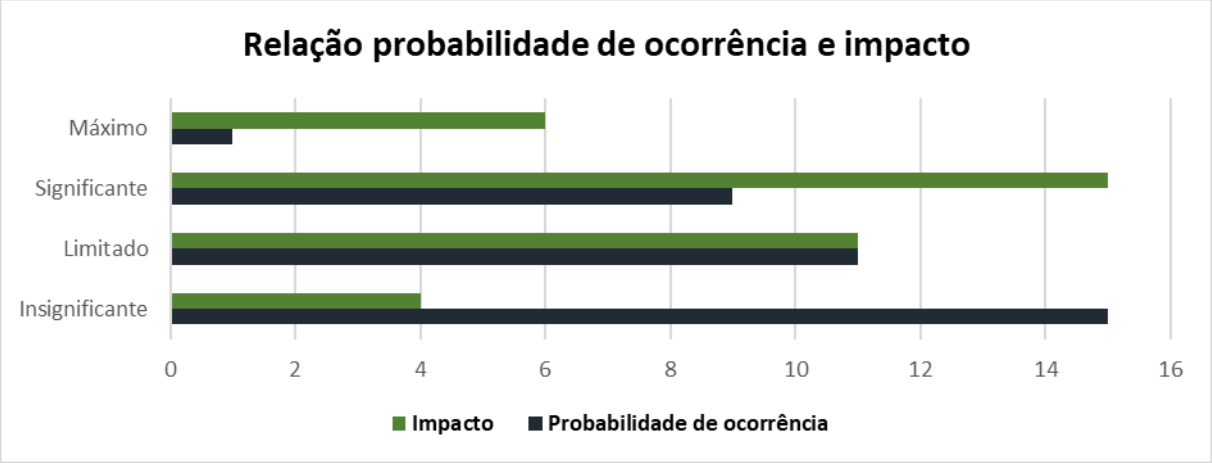
A falta de um Encarregado de Proteção de Dados (DPO) na organização contábil poderá resultar em várias consequências adversas, como multas, penalidades, prejuízos à imagem e desafios em auditorias. A LGPD (Lei Geral de Proteção de Dados) requer que as organizações designem um DPO para assegurar a aderência à lei. A ausência dessa designação pode resultar em penalidades severas.

A falta de *compliance* com a LGPD pode levar a consequências severas para as organizações em termos tanto financeiros quanto de reputação. As penalidades mais duras abrangem multas de até 2% da receita da empresa, limitadas a R$ 50 milhões por infração, bem como sanções como advertências, bloqueio de dados e suspensão ou proibição das atividades relacionadas ao processamento de dados.

4.2.1 – Resumo da avaliação dos riscos

A próxima aba da planilha de nome "09 Resumo Riscos", destacado na “Figura 8 – Relação probabilidade de ocorrência e impacto num processo” abaixo, apresenta um resumo da categorização dos riscos, permitindo uma visão geral do processo em relação aos riscos existentes e à sua categorização. É possível identificar a existência de riscos no processo de acordo com sua gravidade, o valor médio do risco por área de avaliação de maturidade, a relação entre a probabilidade de ocorrência e o impacto para as questões, além do *top* 7 de vulnerabilidades com o risco mais alto (selecionado 7 tópicos que mais tem probabilidade de ocorrer um alto impacto, conforme respostas colhidas dos respondentes), juntamente com os controles de mitigação propostos e os níveis de risco vinculados a cada a cada vulnerabilidade.

Figura 8 – Relação probabilidade de ocorrência e impacto num processo



Fonte: Elaborado pelo autor, 2025.

Conforme explicação evidenciada no Item 5.3.3 e tabela 10 e 11, observa-se que após aplicar o questionário e validar os dados no item 6.2 (Avaliação dos Riscos), tem-se a correlação entre impacto x probabilidade de ocorrência, por questão respondia devidamente agrupada em sua área (soma-se cada item: insignificante 15; limitado 11; significante 9; máximo 1.) formando assim o gráfico acima.

Já o *top* 7 (evidenciado na Figura 9 Indicativo de vulnerabilidade – top 7) de vulnerabilidades com o risco mais alto, juntamente com os controles de mitigação propostos e os níveis de risco vinculados a cada a cada vulnerabilidade identificados pós aplicação do questionário são:

Figura 9 – Indicativo de vulnerabilidadade – Top 7

Top 7 vulnerabilidades			
Questão	Vulnerabilidade	Controle de mitigação	Nível de risco
4.13	Uso não controlado dos sistemas	Implementação de um mecanismo de verificação de integridade no registo de ações	Elevado
1.3	Coleta de dados desnecessários	Identificação dos dados pessoais a recolher	Alto
4.10	Falhas conhecidas nas aplicações	Definição e execução de um plano de testes de segurança periódico	Alto
4.11	Uso não controlado dos sistemas	Implementação de um mecanismo de registo de ações	Alto
4.14	Canais de comunicação inseguros	Implementação de mecanismos de cifra para transferências entre aplicações	Alto
6.1	Processamentos realizados por entidade em não conformidade	Validação de contratos com entidade externa e de cláusulas referentes ao RGPD	Alto
1.1	Falta de informação aos titulares	Documento onde estejam descritos os motivos e finalidades da recolha dos dados pessoais	Alto

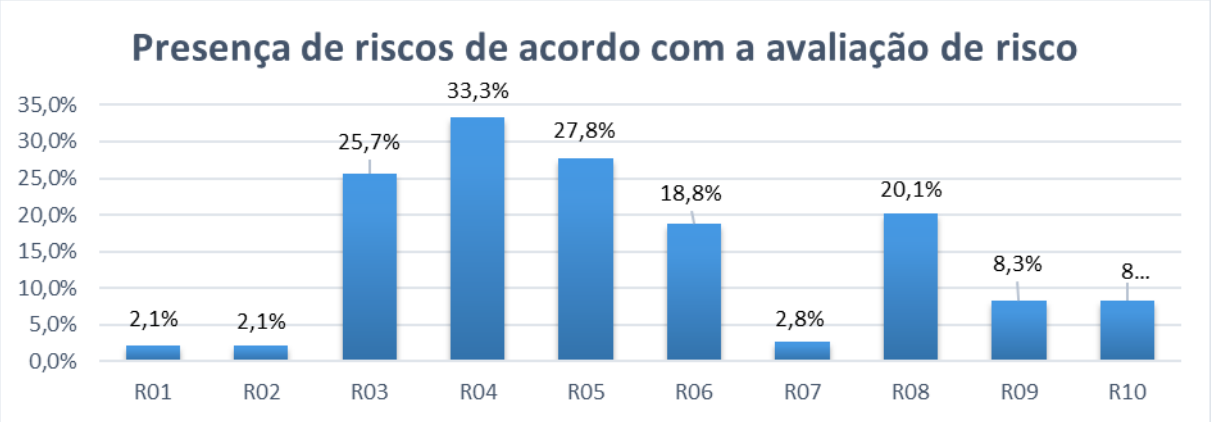
Fonte: Elaborado pelo autor,2025.

A questão de ID 4.13 que representa no questionário correspondente a de número 32, refere-se a implementação de mecanismos técnicos para garantir a integridade dos backups bem como seu acesso. Portanto, ter um processo que garanta os backups e seu acesso é questão *sine qua non* a um processo de mitigação de riscos, nisto a sua importância no top 7 subitens vulnerabilidade. Nota-se que, o status "bem definido" corresponde a resposta dos entrevistados em sua totalidade.

4.2.2 – Validação do risco aceitável

Conforme mencionado anteriormente, no resumo da avaliação de riscos é possível identificar a existência de riscos no processo, conforme ilustrado na Figura 10 (Presença dos riscos em um processo) abaixo. A partir da porcentagem de riscos presentes no processo, pode-se avaliar se essa percentagem excede o que se espera aceitar, e assim decidir se é necessário tomar alguma ação em relação a cada vulnerabilidade.

Figura 10 – Presença dos riscos em um processo



Fonte: Elaborado pelo autor, 2025.

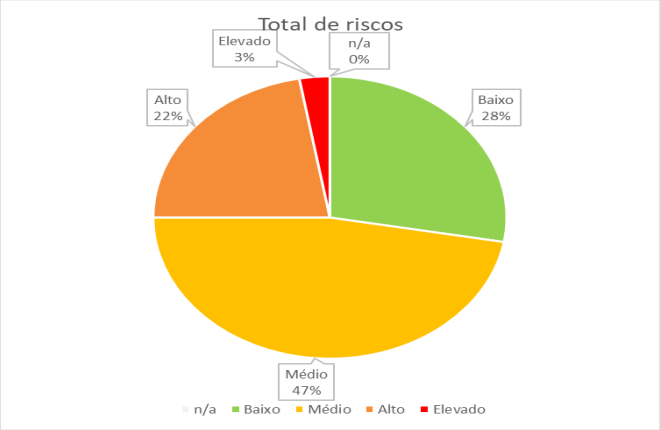
A classificação de risco foi devidamente definida no item "5.2.1 Avaliações de Risco e DPIAs no âmbito do RGPD-LGPD". Dessa forma, sugeriu uma série de riscos que

devem ser considerados relacionados à privacidade dos dados, além de uma proposta de abordagem para a elaboração dos Relatórios de Impacto à Proteção de Dados Pessoais ou *Data Protection Impact Assessment* (DPIA) utilizado no continente europeu e adaptado pelo autor a LGPD.

Após aplicar o questionário e analisar os resultados, deve-se ter bastante atenção aos itens: R03 referente ao acesso não autorizado aos dados que, conforme respostas colhidas representa uma presença de risco de 25,7% versando mais especificamente sobre a má gestão de *passwords* (questão 23 ou ID 4.4). Já o item R04 possui uma presença de risco de 33,3% referente a destruição ou alteração acidental/ilegal de dados, assim como o R05 em 27,8% referente a divulgação não autorizada de dados. Diante do exposto, recomenda-se confrontar o resultado do gráfico com seus respectivos R0's e a qual questão ou questões correlacionam no questionário.

De todas as questões respondidas, o nível de risco aceitável em uma área, seja, baixo, médio ou alto, basta observar o gráfico abaixo que traz uma visão mais ampla de todas as questões. Neste diagrama, todos os riscos das áreas estão representados, inclusive os que não são aplicáveis. Deve-se tomar uma decisão, ao menos, em relação a riscos elevados, altos e médios analisando a questão correspondente, conforme figura 11 abaixo - Riscos subsistentes num processo.

Figura 11 – Riscos subsistentes num processo



Fonte: Elaborado pelo autor,2025

Segundo Mendes (2018), se a intenção é mitigar alguns dos riscos identificados, deve-se seguir a seguinte folha/planilha "10 Mitigação" para determinar a estratégia a ser adotada em relação aos riscos. Caso se considere que os riscos detectados são toleráveis, o procedimento de avaliação de risco pode ser encerrado nesta etapa.

4.3 – Mitigação dos Risco

No sentido de, não somente coletar as informações e apresentar os resultados frente a implementação da LGPD versus seus impactos no ciclo operacional dos profissionais da contabilidade que atuam nos escritórios de contabilidade, mas, tendo em mãos tais resultados, poderá utilizá-los como ferramenta de gestão via de "Mitigação dos Risco",

ou seja, identificando o risco, seu impacto será apresentado possíveis consequências e estratégias para mitigá-los.

Assim, após aplicar as perguntas relacionadas à avaliação de maturidade, incluindo a classificação de maturidade e risco, bem como as possíveis repercussões da exploração de vulnerabilidades, na planilha – 10 "mitigação de riscos", tem-se uma relação de questões da avaliação de maturidade, com suas respectivas classificações de maturidade e risco, além das potenciais repercussões da exploração das vulnerabilidades identificadas na mesma folha/planilha. Adicionou-se uma coluna para identificar a estratégia de gestão de risco para cada questão, onde se pode optar por uma de duas alternativas, conforme Mendes (2018):

- Proteger: Decisão de mitigar o risco, através da implementação de políticas/procedimentos ou medidas tecnológicas;
- Aceitar: Decisão de aceitar o risco e não fazer nada em relação ao mesmo.

Para os riscos que requerem uma decisão de proteção, são apresentadas sugestões de medidas sugeridas para diminuir os riscos, mediante adaptação do modelo aplicado por Mendes (2018) juntamente com as tecnologias associadas, e uma data estimada para a execução das recomendações. Assim como as tecnologias e as estimativas, as sugestões são apenas alicerces para a tomada de decisões, cabe ao gestor aplicá-las ou não. Contudo, elas podem e devem ser alteradas sempre que uma entidade tomar uma decisão diferente, para registrar sua atitude em relação ao risco. Adicionalmente, existe uma área para comentários, onde se podem inserir observações que possam ser pertinentes na redução dos riscos. Neste sentido a figura 12 a seguir demonstra a fase de mitigação dos riscos.

Figura 12 – Fase de mitigação dos riscos

Id	Maturidade da questão	Risco da questão	Questão	Possíveis consequências	Estratégia de mitigação do risco	Medidas recomendadas	Tecnologias	Comentários	Esforço
1.1	Não implementado	Alto	5. Até que ponto seu escritório adota um processo que assegura que, antes da coleta de dados, os titulares sejam devidamente informados, sobre a finalidade da coleta e sobre as etapas do tratamento dos seus dados pessoais?	- Podem ser realizados tratamentos aos dados pessoais que o titular não tenha autorizado e que não esteja de acordo	Proteger	Criar um documento onde estejam descritos os motivos e finalidades da recolha dos dados pessoais, ou seja o propósito do processo identificado na aba "Processo", e os tratamentos a que os dados vão ser sujeitos. Este documento deve ser claro e de fácil leitura, e sempre disponibilizado aos titulares previamente à recolha de dados. Esta documentação deve ser revista sempre que se efetuarem alterações no processo de tratamento de dados.	Ferramenta de processamento de texto, ex: Word.		1 semana
1.2	Bem definido	Baixo	6. Existe uma forma definida de registar, armazenar e disponibilizar (dados) quando requisitado o consentimento para o processamento ?	- A organização não consegue validar que está a efetuar tratamentos apenas para titulares que autorizaram o tratamento dos seus dados - A organização não consegue demonstrar o consentimento dado caso requisitado	Proteger	Definir um procedimento de gestão de consentimentos onde esteja definido que deve ficar registado, previamente à recolha dos dados do titular, algo que torne possível a verificação do consentimento do utilizador, seja o registo de uma ação efetuada numa página web, um documento assinado digitalmente ou presencialmente, ou um email recebido pelo titular, e ter um sistema que permita à organização pesquisar pelo consentimento quando necessário, seja uma base de dados, um sistema de ficheiros ou um arquivo onde estejam implementadas medidas para garantir a integridade do consentimento.	Sistema onde seja possível armazenar documentos digitais e pesquisar pelos mesmos: - Base de dados; - Sistema de gestão de ficheiros.		2 a 3 semanas

Fonte: Elaborado pelo autor,2025 (resumo)

Dois momentos críticos analisados após aplicação do questionário foi identificar que nos escritórios de contabilidade entrevistados, ainda não está definido o DPO – *Data Protection Officer* ou Encarregado de Proteção de Dados, o relatório acima (em resumo) objetiva a ajudar ao entrevistado a entender as possíveis consequências quanto a este grave risco ou seja, as empresas podem não ter implementadas medidas para garantir que os dados não são perdidos ou alvo de fugas de informação, assim, a medida recomendada seria "Previamente ao se transferir os dados para uma entidade (terceiro), deve-se garantir que essa entidade cumpre com os requisitos da LGPD e esta validação deve ser feita periodicamente, sugerindo uma prazo para solução em definitivo da não conformidade.

Outro ponto importante é a falta de um processo definido de *complicance* também identificado após aplicar o questionário, em que os escritórios declaram não haver uma política definida, assim, frente ao foco central "risco" na planilha acima tem-se a reflexão quanto as possíveis conseqüências: Contas de utilizador privilegiadas podem ser comprometidas mais facilmente; Acesso a dados pessoais por utilizadores não autorizados; Fuga de informação dos dados acedidos; Destruição e/ou modificação indevida dos dados.

Nisto tem-se as seguintes medidas recomendadas: deve existir um meio adicional de autenticação para além de uma *password* para acessos privilegiados a funcionalidades mais críticas para reduzir os riscos no caso de comprometimento destes *passwords*.

Diante do exposto, trata-se aqui de não apenas apresentar resultados frente ao questionário aplicado, mas propor medidas de melhorias continuadas.

4.3.1 – Resumo da mitigação dos riscos

Permite reconhecer os riscos por categoria (planilha – 11), isto após a fase "mitigação de riscos", que continuarão existindo mesmo após a implementação de medidas de mitigação. Ademais, disponibiliza uma relação de riscos que foram aceitos ou atenuados. Também, disponibiliza uma tabela que sintetiza a aderência do processo aos artigos da LGPD, baseada nos resultados da avaliação de maturidade, da avaliação de risco e das escolhas feitas em relação ao risco.

Nela, o valor da terceira coluna é calculado com base na avaliação de maturidade preenchida inicialmente, sendo feita uma média da conformidade das várias questões em que o artigo pode estar presente, e em que se consideram os seguintes valores para cada classificação:

- Não implementado: 0%;
- Executado informalmente: 50%;
- Bem definido ou superior: 100%.

Nesta esteira, o valor da quarta coluna muda de acordo com a decisão tomada em relação ao risco nas questões onde o artigo é mencionado. Em outras palavras, se uma questão for categorizada como "Não implementada" e existir um risco que, se mitigado, irá alinhar a conformidade da questão com os artigos relacionados, com base no valor da coluna de estratégia de mitigação na folha anterior, o valor será "Sim" ou "Não", dependendo da escolha de mitigar, ou aceitar o risco.

Neste sentido, apresenta-se a figura abaixo (Figura 13 - Resumo da conformidade do processo) indicando o estado de não conformidade sem que ocorre-se alguma ação sugerida no item anterior, (pois não foi realizada a devolutiva ao escritório para devidos ajustes nas não conformidades), ou seja, a figura a seguir trata-se de uma fotografia após planilhamento e análise dos dados coletados nas questões aplicadas aos profissionais de contabilidade referente aos seus respectivos escritórios de contabilidade.

Figura 13 – Resumo da conformidade do processo

LGPD	GDPR	Estado de conformidade dos artigos relacionados com o processo			
		Artigo	Questões de maturidade - ID	Conformidade	Vai ficar em conformidade?
5,6,7,16	5	Princípios relativos ao tratamento de dados pessoais	1.1, 1.3, 1.4, 1.5	50%	Sim
8	6	Licitude do tratamento	1.2	Em conformidade	Não aplicável
6,8,9,14	7	Condições aplicáveis ao consentimento	1.2, 2.1	Em conformidade	Não aplicável
5,11	9	Tratamento de categorias especiais de dados pessoais	3.2	Em conformidade	Não aplicável
6,9,14	13	Informações a facultar quando os dados pessoais são recolhidos junto do titular	1.1	0%	Sim
6,9,14	14	Informações a facultar quando os dados pessoais não são recolhidos junto do titular	1.1	0%	Sim
6,18,19	15	Direito de acesso do titular dos dados	2.2	Em conformidade	Não aplicável
11,14,15,18	16	Direito de retificação	2.3	Em conformidade	Não aplicável
18	17	Direito ao apagamento dos dados («direito a ser	2.4, 3.4	Em conformidade	Não aplicável
8,18,20	18	Direito à limitação do tratamento	2.6	0%	Não
18	19	Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento	2.3, 2.4	Em conformidade	Não aplicável
18	20	Direito de portabilidade dos dados	2.5	0%	Não
8,18,20	21	Direito de oposição	2.6	0%	Não
38,46,50	25	Proteção de dados desde a conceção e por defeito	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18, 5.1	95%	Não
16,39	28	Subcontratante	3.3	Em conformidade	Não aplicável
37	30	Registos das atividades de tratamento	3.1	Em conformidade	Não aplicável
38,46,50	32	Segurança do tratamento	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18, 5.1	95%	Não
33	44	Princípio geral das transferências	6.1, 6.2	0%	Sim
33	45	Transferências com base numa decisão de adequação	6.1, 6.2	0%	Sim
33	46	Transferências sujeitas a garantias adequadas	6.1, 6.2	0%	Sim

Fonte: Elaborado pelo autor, 2025

Observa-se na planilha acima, como é completa no sentido de apresentar o item não conforme, ou seja, qual item deve o escritório resolver com prioridade já indicando o "id" por consequência qual questão na qual respondeu no questionário e o artigo atingido na LGPD. Portanto, uma ferramenta de gestão imprescindível ao DPO e qual operador dos dados pessoais na entidade.

5. DISCUSSÃO DOS RESULTADOS

É importante resgatar que, para compreender a aplicabilidade da LGPD nos escritórios de contabilidade localizados em Mato Grosso, fez-se necessário à utilização de uma conjunto de conhecimentos específicos referente as ferramentas disponíveis e seus impactos na análise de risco (*compliance*) pois, existe uma interdisciplinaridade entre informações diversa tais como: normas legais, gestão de processos e riscos bem como a aplicabilidade de normas ISO. Formando um conjunto de conhecimentos que se convergem com o propósito desta pesquisa.

Para ter dados analisáveis quanto ao tema proposto, estes foram coletados por meio de um questionário baseado no referencial teórico abordado na revisão bibliográfica e metodologia, com ênfase na Lei n. 13.709 (2018). O questionário, criado na plataforma *Google Forms*, continha 39 perguntas fechadas (resposta obrigatória) e 3 abertas (descrever opinião – não obrigatório) organizadas em seis áreas principais, a saber: coleta e gestão da informação; consentimento e direitos dos titulares; documentação e requisitos legais; controles de segurança lógico; controles de segurança física e transferência de dados.

O *framework* proposto alcançou o objetivo central que é analisar como a implementação da LGPD impacta os escritórios de contabilidade em Mato Grosso, com ênfase na adoção de mecanismos de *compliance* orientados por análises de riscos e na promoção da inovação na prestação de serviços contábeis.

Inicialmente o questionário identificou o perfil do escritório contábil. Nisto, o levantamento sobre a localização dos escritórios de contabilidade que participaram deste estudo revelou que 58,5% situam-se na mesorregião Centro-Sul Mato-Grossense (região de Cuiabá e entorno), totalmente compreensível, tendo a capital maior quantidade de faculdades em ciências contábeis, assim como, maior quantidade de empresas constituídas e população (consumidor).

Quanto ao porte, foi utilizado como parâmetro dados do SEBRAE (2022) com métrica em quantidade de colaboradores e não de faturamento (indicador fiscal). Sendo assim, o resultado foi: 58,5% Microempresa (até 9 colaboradores), 36,6% Empresa de pequeno porte (de 10 a 49 colaboradores). Seguindo a lógica da utilização de inteligência artificial na rotina dos escritórios de contabilidade, executa-se mais serviços com menos colaboradores. IA que importa automaticamente informações fiscais que alimenta a escrita fiscal e folha de pagãmente, bem como conciliação automática.

O *framework* aplicado tem o potencial de contribuir com os profissionais de contabilidade que atual nos escritórios contábeis, empresas, universidades. Estes profissionais têm um campo profícuo de atuação no sentido de que ainda há muito trabalho a ser feito para a real inclusão do país na economia 4.0, ou seja, em um mundo cheio de normas, controles e ágil traves de novas tecnologias (CHAGAS,2021).

Já os respondentes, identificados via questionário ficou evidenciado que, 56,1% trata-se de Proprietário(a) / Sócio(a), 14,6% Contador(a) Responsável Técnico. Porém, referente ao tema estudado independentemente do nível hierárquico ou responsabilidade técnica, devem ter o conhecimento sobre LGPD caso a entidade tenha uma política estruturada, pois todos são responsáveis pela manutenção seja direita ou indiretamente da aplicabilidade da norma.

No tocante a análise da percepção dos profissionais contábeis de Mato Grosso identificados via *framework* aplicado, referente os impactos e riscos da implementação da LGPD, devem avaliar os esforços necessários para adoção de mecanismos de *compliance* e análise de riscos conforme a LGPD, bem como identificar oportunidades de melhoria e propor estratégias que promovam conformidade e inovação na contabilidade, também foram atendidas em duas entregas:

a) Na tabela onze, onde demonstra a mitigação aos efeitos dos resultados frentes as questões postas, o risco, a maturidade tabela seis, possíveis consequências e medidas recomendadas;

b) Envio a todos os profissionais de contabilidade do estado de Mato Grosso, um Guia Framework de Avaliação de Riscos de Segurança e Privacidade na Implementação da LGPD e seus Impactos para a Inovação, encaminhada via SESCON-MT e CRC-MT. Objetivo também alcançado.

Quanto a avalição dos esforços exigidos para a adoção da LGPD, na implementação de mecanismos de *compliance* (análise de riscos) pelos profissionais de contabilidade, ficou demonstrado na pesquisa que, 43,9% dos entrevistados não implementaram uma estrutura (física, pessoas) de *compliance* nos escritórios, tão somente, conforme relato descrito, utilizam o software de contabilidade como ferramenta mínima de controle e mitigação de riscos.

Neste sentido, o *framework* proposto também entrega sugestões de implementação de medidas de mitigação de risco, referente a ausência de uma política estruturada de

compliance, (esta é uma inovação importante da ferramenta) que por consequência coloca em risco a sustentabilidade financeira do escritório, com valores pecuniários de até 50 milhões de reais por infração.

Portanto, na esteira da interdisciplinaridade, saber utilizar ferramentas como o Ciclo PDCA (Plan-Do-Check-Act), na busca por sua melhoria contínua dentro dos processos é fundamental para compreender os pontos de melhorias e mitigação de riscos, nos seus processos internos, eliminando não conformidades.

Albuquerque (2015) descreve que, um dos objetivos da utilização do PDCA no processo decisório é que o mesmo pode otimizar os resultados operacionais, reduzindo os custos e melhorando a qualidade dos produtos ou serviços prestados. Na perspectiva organizacional, o enfoque na qualidade tem um caráter essencialmente econômico, pois isso significa aumento de produtividade e redução de custos operacionais.

Alinhado ao PDCA, o *framework* proposto aplicado a análise dados, "conecta" diversas possibilidades de análise em uma única ferramenta (em *excel* que será disponibilizado).

Na mesma esteira, está inserido no *framework* proposto, se conecta com a ISO 37301:2021, assim como a ISO 31000:2018 que trata da Gestão de Riscos — Diretrizes (*Risk management — Guidelines*), que traz na sua essência que, gerenciar riscos é iterativo e auxilia as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas. Portanto no processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos.

Assim, convém que o processo de gestão de riscos seja parte integrante da gestão e da tomada de decisão, e seja integrado na estrutura, operações e processos da organização. Pode ser aplicado nos níveis estratégico, operacional, de programas ou de projetos.

O *framework* proposto absorve o tripé referente a norma ISO e ao tema estudado (LGPD) vinculado ao *Compliance* (análise de risco) tem-se a ISO 27701:2019, referente a "Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes (*Security techniques — Extension to ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for privacy information management — Requirements and guidelines*).

Que procura proteger os Dados Pessoais pois, quase todas as organizações tratam de dados pessoais (DP). Além disso, a quantidade e os tipos de DP tratados estão aumentando, assim como o número de situações em que uma organização precisa cooperar com outras organizações em relação ao tratamento de DP. A proteção da privacidade no contexto do tratamento de DP é uma necessidade da sociedade, bem como um tópico de legislação e/ou regulamentação dedicada em todo o mundo.

O Sistema de Gestão de Segurança da Informação (SGSI), definido na ABNT NBR ISO/IEC 27001, é projetado para permitir a adição de requisitos específicos setoriais, sem a necessidade de desenvolver um novo Sistema de Gestão. As Normas de Sistemas de Gestão ISO, incluindo as específicas por setor, são projetadas para poderem ser implementadas separadamente ou como um Sistema de Gestão combinado.

Portanto, aplica-se o *framework* proposto também como ferramentas de controle, gestão e mitigação de riscos (compliance) é obrigatório e taxativo, conforme a norma determina.

Em análise das demais questões aplicadas em relação as seis áreas abordadas, tudo se resume a não conformidades pela falta de conhecimento interdisciplinar, como: normas legais, ISO, gestão (PDCA), utilizando-se do software contábil como ferramenta de controle (mínimo) dos dados, seu manejo e descarte.

Fator evidenciado nas questões abertas em que, a maioria relata como fato impeditivo de ter e manter m sistema de *compliance*: custo elevado de implementação, falta de mão de obra. Bem como, o que traz uma relativa segurança é a utilização de software específico para escritórios contábeis, nele possui ferramentas de comunicação segura com os clientes, bem como manejo e descarte dos dados sensíveis.

Se comparamos o modelo (Mendes, 2018) aplicado devidamente equiparado os artigos da GDPR com a LGPD guardado as devidas proporções (pois o modelo foi aplicado no continente europeu e a empresas diversas não somente aos escritórios de contabilidade) o *framework* proposto identificou há presença dos riscos elevados nos mesmos processos ou seja, nas empresas estudadas por Mendes (2018) e as estudadas nesta pesquisa mesmo sendo segmentos diferentes com normas similares, a saber: a) Acesso não autorizado aos dados (R03); b) Destruição ou alteração acidental/ilegal de dados (R04); c) Divulgação não autorizada de dados (R05). Isto demostra as mesmas dificuldades em continentes distintos e normas similares.

Por fim, com os objetivos alcançados, o *framework* proposto superou as expectativas, pois além de coletar e analisar os dados, consegue entregar uma análise de mitigação dos riscos encontrados, trazendo a inovação que os escritórios necessitam no quesito LGPD.

Por outro lado, é preciso traçar as limitações e os desafios verificados neste trabalho. A principal limitação diz respeito à aplicação do *framework* restritamente aos itens previamente selecionados, ou seja, poderá ter elementos dentro da norma (LGPD) que não foram explorados nesta pesquisa.

6. CONSIDERAÇÕES FINAIS

O propósito deste capítulo é detalhar as conclusões finais que este estudo chegou, bem como apontar alguns potenciais pontos de aprimoramento que podem ser incorporados ao modelo no futuro.

Na busca pela excelência acadêmica, esta pesquisa através do *framework* aplicado, alinha-se a técnica de análise utilizada por grandes organizações de controle (TCU – Tribunal de Contas da União, dentre outros) evidenciando o grau de conformidade quanto a aplicação e gestão da LGPD no clico operacional das entidades.

Veja que, no Art. 5º, XVII, LGPD, é taxativo na determinação em ter e manter relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Assim como no Art. 50 do mesmo diploma que define “Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança,

os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Portanto, para assegurar a qualidade do *framework* sugerido e adaptado ao caso concreto (planilha em Excel), além de avaliar o benefício que efetivamente proporcionarão às organizações contábeis ao analisá-las em alguns quesitos quanto ao cumprir da LGPD, este *framework* foi utilizado por Mendes (2018) no continente europeu em sua dissertação de mestrado em Segurança Informática, na faculdade ULisboa, em análise quanto à adequação e utilização da GPDR. Portanto, modelo conforme próprio auto narra validado através de uma pesquisa de satisfação realizada junto aos entrevistados, com ótimas avaliações tais como:

- O fato de permitir centralizar todo o ciclo de vida de gestão de maturidade e dos riscos do processo é um ponto bastante positivo, facilitando a organização e gestão do ciclo de vida dos processos;
- Ainda devido a estar tudo centrado num ficheiro de *Excel*, pode-se evitar custos, sendo necessária apenas uma primeira formação com os responsáveis dos processos, permitindo entregar depois o modelo aos clientes que poderão de forma autónoma classificar os processos com mais calma e detalhe, evitando a necessidade de várias entrevistas.

Este Autor adaptou o *framework* para atender aos requisitos (artigos) da LGPD e aplicou junto aos profissionais de contabilidade, divulgando em redes sociais (WhatsApp, Instagram), além de grupos de discussão dedicados à contabilidade no estado de Mato Grosso. Adicionalmente, o questionário foi enviado por e-mail e WhatsApp, vinculados ao demandante O SESCON-MT (entidade representativa da classe empresarial que abrange as empresas de prestação de serviços contábeis, de assessoramento, perícias, informações e pesquisas sediadas no Estado de Mato Grosso), assim como, ao CRC-MT na presença do Presidente que gentilmente encaminhou a todos os profissionais cadastrados na entidade (ativos).

No início foram identificados os pontos conformes, que interliga a GDPR e a LGPD. Em seguida foi adaptado a gramática, as questões em conformidades com os artigos dispostos na norma, ajustado a nomenclatura e estrutura (não muito) do modelo para atender as especificações de nosso país.

Neste sentido, foi construído um questionário baseado no referencial teórico abordado na revisão bibliográfica e modelo, com ênfase na Lei n. 13.709 (2018). O questionário, criado na plataforma *Google Forms*, continha 39 perguntas fechadas (resposta obrigatória e 3 abertas (colocar opinião – não obrigatório) organizadas em oito seções principais.

Ao planejar este trabalho, foram estabelecidos diversos objetivos a serem atingidos para analisar como a implementação da LGPD impacta os escritórios de contabilidade em Mato Grosso, com ênfase na adoção de mecanismos de *compliance* orientados por análises de riscos e na promoção da inovação na prestação de serviços contábeis. Para tanto, não somente foi aplicado um questionário “qualquer”, mas um modelo validado que proporcionou a vinculação da “questão” ao artigo específico da LGPD em comparação a GPDR, entregando ao final não somente a análise, mas, um relatório de risco e impacto com recomendações. Portanto, totalmente atendido este objetivo principal.

Diante do exposto, o *framework* utilizado apesar de carecer sempre de revisão, conforme relato de Mendes (2018) que narra em suas conclusões finais em que conseguiu auxiliar as empresas analisadas no continente europeu (diversas).

Nisto, foi realizado uma adaptação frente a nossa legislação (LGPD) e ao público alvo, todavia, em ambas as análises ficou demonstrado que não basta avaliar somente a aplicabilidade na norma, mas principalmente compreender seus riscos ao negócio, mitigando-os com ações precisas conforme cada artigo, ou seja, ter e manter um sistema de *compliance* é fundamental para a saúde operacional e por consequente financeira da entidade, garantido assim, a inovação seja em processos, negócios, tornando-a mais forte dentro do seu segmento, em resumo sendo sustentável em todas as formas, ambiental e financeiro.

Para trabalhos futuros, poderá ser incrementado mais questões abordando outros artigos da norma que também trazem consequências gravíssimas a exemplo das penalidades, alinhando assim com a responsabilização dos sócios quotistas e o Encarregado de Proteção de Dados.

Este *framework* futuramente poderia ser desenvolvido um *App* (ao invés de planilha em excel) para facilitar a análise para um maior grupo de pessoas, pesquisadores e empresas, através do modelo aqui utilizado.

Por fim, através do *framework*, conseguiu-se atender os objetivos desta pesquisa. Concluí-se que, além de ser um recurso valioso para apoiar a conformidade com o regulamento, também é uma contribuição para analisar a aplicabilidade prática da LGPD.

A gestão de Riscos é condição de sobrevivência dos escritórios de contabilidade frente a aplicação completa da LGPD em seu ciclo operacional.

As inovações que que poderão ser implementadas através das análises que foram realizadas, estão além de aspectos físicos (estrutura, hardware) mas também em processos e pessoas.

Demonstra em definitivo a importância desta pesquisa para classe acadêmica e empresarial.

7 - REFERÊNCIAS

ANDRADE, Marcelo Henrique Lapolla. LAMBOY, Christian Karl de. LEITE, Luciano Vasconcelos. **Manual de implementação da Lei Geral de Proteção de Dados**. 1. ed. São Paulo: Via Ética, 2019.

ALEXANDRE, P. **Análise de risco no GDPR**. Repositorio.ul.pt, 2018. Universidade de Lisboa, https://repositorio.ulisboa.pt/handle/10451/35494. Acessado em: 7 maio de 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Diário Oficial da União, Brasília, DF, 15 ago. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 09/03/2024.

BRASIL. Lei nº 10.406/02. **Código Civil Brasileiro**. Diário Oficial da União, Brasília, DF, 10 de janeiro de 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 09/03/2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível:https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 09/03/2024.
BRASIL. DL 4295/45. Cria o Conselho Federal de Contabilidade. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del9295.htm. Acessado em 16/06/2023.
BRASIL. **Resolução CFC Nº 1.640/21**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cfc-n-1.640-de-18-de-novembro-de-2021-367541982. Acessado em 16/06/2023.
BRASIL. **Organização Mundial de Propriedade Intelectual** (OMPI). https://www.gov.br/mre/pt-br/delbrasomc/brasil-e-ompi/brasil-e-ompi. Acessado em 13/11/2024.
BRASIL. **Programa de Governança em Privacidade**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acessado em 09/09/2024.
BRASIL. DIA DO EMPRESÁRIO CONTÁBIL. CFC - Conselho Federal de Contabilidade: Disponível em: https://cfc.org.br/noticias/dia-do-empresario-contabil-a-importancia-das-empresas-de-contabilidade-para-o-crescimento-dos-negocios-no-pais/#:~:text=Segundo%20levantamento%20recente%20do%20CFC,(26.438)%20em%20S%C3%A3o%20Paulo. Acessado em 09/09/2024.
BRASIL. **Profissionais Ativos Nos Conselhos Regionais De Contabilidade**. CFC - Conselho Federal de Contabilidade:Disponível:https://www3.cfc.org.br/spw/crcs/ConselhoRegionalAtivo.aspx?_gl=1*180fbb3*_ga*NTI2MzQ1OTQwLjE3MjU5MTYzNzM.*_ga_38VHCFH9HD*MTcyNzAxNDMzMy4yLjEuMTcyNzAxNTE1NC4wLjAuMA. Acessado em 10/06/2023.
BRASIL. **Emprego, ocupações, empresas, dados demográficos e educação | Observatório Data MPE Brasil.** SEBRAE, Data MPE (2024); acessado em: 10/11/2024. Disponível em: https://datampe.sebrae.com.br/profile/geo/brasil. Acessado em 10/06/2023.
BRASIL. **Resolução CFC N.º 1.626, de 19 de Agosto de 2021**. Disponível em: https://www1.cfc.org.br/sisweb/SRE/docs/RES_1626(1).pdf. Acessado em 10/06/2023.
BRASIL. CFC – **CONSELHO FEDERAL DE CONTABILIDADE**. Organizações Contábeis -2025. Disponível: https://www3.cfc.org.br/spw/crcs/ConselhoRegionalAtivo.aspx?_gl=1*crat52*_ga*MTM5Nzc4MDY2NS4xNzQ2MTI3NDIy*_ga_38VHCFH9HD*MTc0NjEyNzQyMS4xLjAuMTc0NjEyNzQyMS4wLjAuMA. Acessado em 01/05/2025.

BRASIL. DE, F. **Linha do tempo da proteção de dados pessoais e da Lei Geral de Proteção de Dados Pessoais, no Brasil — LGPD - Lei Geral de Proteção de Dados Pessoais** | Serpro. Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/linha-do-tempo-1/view. Acesso em: 6 de maio de 2025.
BRASIL, N. ABNT NBR ISO Gestão de riscos -Diretrizes Risk management - Guidelines. [s.l: s.n.]. Disponível em: https://dintegcgcin.saude.gov.br/attachments/download/23/2018%20-%20Diretrizes%20-%20Gest%C3%A3o%20de%20Riscos_ABNT%20NBR%20ISO%2031000.pdf. Acessado em: 12 maio de 2025.

BRILHANTE , Sibeli Moraes Oliveira. **Barreiras no Projeto de Implementação da LGPD em uma Empresa Brasileira de Médio Porte** http://mestradoprofissional.fipecafi.org/wp-content/uploads/2022/11/Disserta%C3%A7%C3%A3o-Sibeli-Moraes-Oliveira-Brilhante.pdf>. Acesso em: 6 maio. 2025c

BERTASSI, A. L. **Controladoria estratégica governamental aplicada ao poder executivo: uma contribuição teórica.** 2016. 232 p. Tese (Doutorado em Administração) – Universidade Metodista de Piracicaba, São Paulo, 2016.

CHAGAS, M.; SCHWINDT, S.; ALVES COSTA, S. **Os Principais Impactos da Inteligência Artificial na Contabilidade Gerencial.** [s.l: s.n.]. Disponível em: https://congressousp.fipecafi.org/anais/21UspInternational/ArtigosDownload/3172.pdf Acessado em 17/06/2025.

CORREIA, Henrique. **Compliance e sua aplicação no direito do trabalho**. Revista Eletrônica do Tribunal Regional do Trabalho da 9ª Região, Brasília, DF, ano IX, n. 91, ago./2020. https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/151250/2020_correia_henrique_compliance_aplicacao.pdf?sequence=1&isAllowed=yhttps://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/151250/2020_correia_henrique_compliance_aplicacao.pdf?sequence=1&isAllowed=y.Acessado em 16/06/2023.

CRUZ, Uniran Lemos da; PASSAROTO, Matheus; NAURO, JÚNIOR; Thomaz. **O Impacto da Lei Geral de Proteção de Dados Pessoais (LGPD) nos escritórios de contabilidade**. 2021. Contabilidade em texto, PPGCONT – UFRGS, Porto Alegre, v. 21, n. 49, p. 30-39, set./dez. 2021. Disponível em: https://seer.ufrgs.br/index.php/ConTexto/article/view/112561/pdf. Acesso em: 20 ago. 2022

CARVALHO, A. dissertação de mestrado profissional **Proposta de um Framework de Compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): Um estudo de caso para prevenção a fraude no contexto de Big Data UNIVERSIDADE DE BRASÍLIA FACULDADE DE TECNOLOGIA**. [s.l: s.n.]. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/01/PPEE.MP_.012-1.pdf. Acessado em 01-05-2025.

CARANTI, Larissa Mônaco e Tatiana Lie Fukuhara: **Vista do Responsabilização de Empresas à luz da Lei Geral de Proteção de Dados**. Revista de Direito PUCSP - 2021. Disponível em: https://revistas.pucsp.br/index.php/DIGE/article/view/56260/38291. Acessado em 01-05-2025.

CLEDISON, Carlos De Oliveira. **Relação Entre Intangibilidade E Desempenho Econômico De Empresas De Capital Aberto Lavras** -MG 2019. [s.l: s.n.]. Disponível em: http://repositorio.ufla.br/jspui/bitstream/1/33449/2/DISSERTA%C3%87%C3%83O_Rela%C3%A7%C3%A3o%20entre%20intangibilidade%20e%20desempenho%20econ%C3%B4mico%20de%20empresas%20de%20capital%20aberto.pdf. Acesso em: 11 maio. 2025.

CRISTIANO, C.; ERNANI, P.; DE FREITAS, C. Capa Associação Pró-Ensino Superior em Novo Hamburgo -ASPEUR Universidade Feevale mEtodologia do trabalho CiEntíFiCo: **Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico 2a edição**. [s.l: s.n.]. Disponível em: https://www.feevale.br/Comum/midias/0163c988-1f5d-496f-b118-a6e009a7a2f9/E-

book%20Metodologia%20do%20Trabalho%20Cientifico.pdf. Acesso em: 12 maio. 2024.
DA SILVA, G. A. S. **Desafios das empresas de serviços contábeis frente a lei geral de proteção de dados pessoais (lgpd) lei 13.709/2018.** Disponível em: https://engemausp.submissao.com.br/25/anais/arquivos/17.pdf?v=1733596420 Acesso em: 7 dez. 2024.
DE, D.; FLÁVIO, M.; FERNANDES VOLPON, H. UNIVERSIDADE DE SÃO PAULO ESCOLA DE ENGENHARIA DE SÃO CARLOS **Simulação do Fluxo de Peças Durante a Operação de Torneamento em Sistemas Flexíveis de Fabricação Baseado em Framework Orientado a Objetos.** [s.l: s.n.]. Disponível em: https://teses.usp.br/teses/disponiveis/18/18145/tde-31052012-234109/publico/Dissertacao_Flavio_Volpon.pdf. Acesso em: 6 março de 2025.
DE PEQUENO PORTE, A. 9. E. A. 19 E. E. et al. Porte Comércio e Serviços Indústria. Disponível: https://sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/SP/Pesquisas/MPE_conceito_empregados.pdf. Acessado em 25 jun. de 2024.
DE DADOS, A. DE G. DE C. P. E. P. **Lgpd Acadêmico - Comparativo**. Disponível em:https://observatoriolgpd.com/wp-content/uploads/2020/02/Comparativo-17022020.pdf.pdf.pdf. Acessado em 12 maio de 2025.
DO PRADO, J.W., de Castro Alcântara, V., de Melo Carvalho, F. et al. **Multivariate analysis of credit risk and bankruptcy research data: a bibliometric study involving different knowledge fields (1968–2014).** Scientometrics 106, 1007–1029 (2016). https://doi.org/10.1007/s11192-015-1829-6. Acessado em: 7 maio de 2025.
EWEN, Macaskill, G. D. (1 de Novembro de 2013). NSA Files: Decoded. **Obtido de The Guardian:** https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/4. acessado em 17/06/2025.
EUA. UNITED STATES DEPARTMENT OF JUSTICE. **Overview of the Privacy Act of 1974 - 2020 Edition.** Disponível em: https://www.justice.gov/opcl/privacy-act-1974. Acesso em 15 de abril de 2025.
FACHINETTI, A. F.; CAMARGO, G. Opinião: **A Convenção 108+ e a relevância da proteção de dados.** Disponível em: https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados/. Acessado em: 6 de maio de 2025.
FERREIRA, L. P. (2017). **Cloud Security Risk and Readiness**. Em Dissertação de Mestrado em Segurança Informática. Faculdade de Ciências da Universidade de Lisboa. Obtido em Dezembro de 2017, de http://repositorio.ul.pt/handle/10451/31251. Acessado em 17/11/2024.
FERRARI, A. M. **Radar de Criticidade: Ferramenta e metodologia de avaliação de projetos correntes com múltiplas variáveis**. Disponível em: https://www.singep.org.br/5singep/resultado/372.pdf. Acesso em: 22 jun. 2025.
FOR, O. ISO 37301:2021. Disponível em: https://www.iso.org/standard/75080.html#lifecycle. Acessado em: 12 maio de 2025.
FOR, O. ISO - 37301:2021 Compliance management systems — **Requirements with guidance for use** (Sistemas de gestão de conformidade - Requisitos com orientação para uso)
GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002.. — Maurício Façanha. Disponível em: https://docente.ifrn.edu.br/mauriciofacanha/ensino-superior/redacao-cientifica/livros/gil-a.-c.-como-elaborar-projetos-de-pesquisa.-sao-paulo-atlas-2002./view. Acessado em 09/09/2024.

HERMES, Pedro Henrique **proteção de dados pessoais na sociedade de risco; : limites e possibilidades à liberdade no ambiente digital** https://repositorio.unisc.br/jspui/handle/11624/3559?mode=full>. Acessado em: 6 maio. 2025.

IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. Brasília, DF: IBGE, 2013. https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/36371-pib-cresce-2-9-em-2022-e-fecha-o-ano-em-r-9-9-trilhoes. Acessado em: 31/05/2024.

INNOVACIÓN, Tecnología | AEPD. Disponível em: https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia. Acessado em 25 jun. 2024.

INTERPRETATION, C. G. **Risk, high risk, risk assessments and data protection impact assessments under the GDPR**. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf. Acessado em: 7 maio de 2025.

JURÍDICA, B. PROTEÇÃO DOS DADOS PESSOAIS. [s.l: s.n.]. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acessado em 10/06/2023.

KRÜGER, C et al. (2021). **Lei Geral de Proteção de Dados Pessoais: uma análise dos determinantes junto aos profissionais de Contabilidade**. Revista Catarinense Da Ciência Contábil, 20, e3220. Recuperado de https://doi.org/10.16930/2237-766220213220. Acessado em 09/09/2024.

KRÜGER, C et al. (2021). **Lei Geral de Proteção de Dados Pessoais: uma análise dos determinantes junto aos profissionais de Contabilidade**. Revista Catarinense da Ciência Contábil, vol. 20, pp. 1-19, 2021. Recuperado de https://www.redalyc.org/journal/4775/477565816021/html/. Acessado em 09/09/2024.

KRÜGER, C., Baldassari, A.C.C., Lopes, LF.D & Silva, L.I. (2021). **Vista do Lei Geral de Proteção de Dados Pessoais.** Disponível em: https://revista.crcsc.org.br/index.php/CRCSC/article/view/3220/2323. Acesso em: 7 dez. 2024.

LIMA, R. A. de; GARRIDO, G. L. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) **E Compliance: Um Panorama Da Adequação Normativa Para Organizações Contemporâneas**. Revista Eletrônica do Curso de Direito da UFSM, [S. l.], v. 17, n. 1, p. e68680 , 2022. DOI: 10.5902/1981369468680. Disponível: https://periodicos.ufsm.br/revistadireito/article/view/68680. Acesso em: 1 maio. 2025.

LIMA, Ricardo Alves de, e Filho, Marco Aurélio Pinto Florêncio: **Compliance And Succession Planning: Family Corporate Governance.** Lima. Revista da Faculdade de Direito do Sul de Minas, Pouso Alegre, v. 35, n. 2: 91-103, jul./dez. 2019 Disponível em: https://www.fdsm.edu.br/conteudo/artigos/74f5c82a4554a10faf90a7159fe89a47.pdf. Acessado em: 7 maio de 2025.

MACFARLAND, K.; MACFARLAND, D. Re: **Developing a Privacy Framework** (Docket No. 181101997-8997-01). [s.l: s.n.].Disponível: https://www.nist.gov/system/files/documents/2019/02/04/nymity_terry_mcquay_teresa_troester-falk_002.pdf. Acesso em: 25 jun. 2024

MULHOLLAND, Caitlin. **Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018).** Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acessado em 09/09/2024.

MORAES, H. F. (2024, December 17). **Critérios para análise de risco às liberdades e garantias fundamentais de titulares de dados pessoais.** Disponível em: https://repositorio.fgv.br/items/c598cf79-ddba-4d6a-8f85-62264873a6e5. Acessado em 01-05-2025.

NIST. Framework Documents. 2018. Disponível: https://www.nist.gov/cyberframework/framework.
Acessado em: 6 de março de 2025.

NOGUEIRA, Fernanda Araújo Couto e Melo; FONSECA, Maurício Leopoldino da. "**O consentimento na Lei Geral de Proteção de Dados: autonomia privada e o consentimento livre, informado, específico e expresso".** In Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] Org. Bernardo Menicucci Grossi. Porto Alegre/ RS: Editora Fi, 2020, pp. 15-35. P. 22. Disponível em: https://www.researchgate.net/profile/Bernardo-Grossi-2/publication/345774449_Lei_Geral_de_Protecao_de_Dados_uma_analise_preliminar_da_Lei_1370918_e_da_experiencia_de_sua_implantacao_no_contexto_empresarial/links/5fad7a6aa6fdcc9389acd493/Lei-Geral-de-Protecao-de-Dados-uma-analise-preliminar-da-Lei-13709-18-e-da-experiencia-de-sua-implantacao-no-contexto-empresarial.pdf.
Acessado em 10/06/2023.

ONU. **Declaração Universal dos Direitos Humanos**. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acessado: 09/09/2024.

PINHEIRO, P. P. **Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas.** Revista eletrônica [do] Tribunal Regional do Trabalho da 9ª Região, Curitiba, v. 10, n. 97, p. 75- 87, 2021. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/186011. Acessado em 09/08/2023.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais : comentários à Lei n. 13.709/2018** (LGPD) / Patrícia Peck Pinheiro. – São Paulo: Saraiva Educação, 2018.

PRODANOV, C. C.; FREITAS, E. C. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho**. 2. ed. Novo Hamburgo. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/49435/1/METODOLOGIA%20DO%20TRABALHO%20CIENT%C3%8DFICO.pdf. Acesso em: 25 jun. 2024.

RIBEIRO, R., Krüger, C., Michelin, C. de F., & Raddatz, J. C. (2020). **Cibersegurança e segurança da informação contábil: uma análise da percepção do profissional contábil.RAGC: Revista de Auditoria, Governança e Contabilidade**,8(32), 71-85. Disponível em: https://revistas.fucamp.edu.br/index.php/ragc/article/view/2007. Acesso em: 13/11/2024

RIBEIRO, R. et al. **Cibersegurança E Segurança Da Informação Contábil: Uma Análise Da Percepção Do Profissional Contábil**. RAGC, v. 8, n. 32, 20 abr. 2020. Disponível em: https://revistas.fucamp.edu.br/index.php/ragc/article/view/2007. Acessado em: 13/11/2024.

RINGLE, C. M., Silva, D., & Bido, D. S. (2014). **Modelagem de equações estruturais com utilização do SmartPLS. REMark-** Revista Brasileira de Marketing, 13(2), 56-73. https://periodicos.uninove.br/remark/article/view/12032/5665. Acesso em: 25 jun. 2024

ROSA, Bárbara Madalena Heck da; BERTONCINI, Mateus Eduardo Siqueira Nunes. **Intervenção Do Estado Em Matéria Consumerista E A Lgpd**. Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo, Florianopolis, Brasil, v. 8, n. 1, 2022. DOI: 10.26668/IndexLawJournals/2526-0030/2022.v8i1.8794.Disponível:

https://www.indexlaw.org/index.php/revistadgrc/article/view/8794. Acesso em: 1 maio. 2025.

SAMUEL D. WARREN AND LOUIS D. BRANDEIS. **The Right to Privacy**. Disponível em: https://www.jstor.org/stable/pdf/1321160.pdf?refreqid=excelsior%3A1fedf03570729dd6edc074d98a2ae08e&ab_segments=&origin=&initiator=&acceptTC=1. Acessado em 10/06/2023.

SAMUEL D. Warren and Louis D. **Brandeis Harvard Law Review** , Dec. 15, 1890, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220 Published by: The Harvard Law Review Association. 1890. Disponível em: https://www.jstor.org/stable/pdf/1321160.pdf?refreqid=excelsior%3A1fedf03570729dd6edc074d98a2ae08e&ab_segments=&origin=&initiator=&acceptTC=1. Acessado em 10/06/2023.

SILVA, R. O. DA et al. **O ciclo PDCA como proposta para uma gestão escolar eficiente. Revista de Gestão e Avaliação Educacional**, v. 1, n. 1, p. 1–13, 6 jan. 2019. Disponível em: https://periodicos.ufsm.br/regae/article/view/36102. Acessado em 12 maio de 2025.

SILVA, C. L.; GONZALEZ, M. C.; MARANGONI, M. M. Bibliometria e Cientometria. Disponível em: https://www.pucsp.br/sites/default/files/download/posgraduacao/programas/administracao/bibliometria-e-cientometria.pdf. Acesso em: 12 de maio de 2025.

TAKAHASHI, Adriana Roseli; Fischer, André Luiz. Revista de Administração – RAUSP - 2009 . **Aprendizagem e competências organizacionais em instituições de educação tecnológica: estudos de casos.** Disponível em: https://www.redalyc.org/articulo.oa?id=223417460004. Acessado em 09/09/2024.

TARTUCE, Flávio. **Manual de Direito Civil: volume único** / Flávio Tartuce. – 11. ed. – Rio de Janeiro, Forense; METODO, 2021, p. 225.

TORCHIA, B. (2020). **Como o compliance pode ser um diferencial na gestão das organizações.** Entrevistadora: Fernanda Maria Pereira. Revista Científica Faculdade Unimed, 1(3), 1-4. Disponível em: https://revista.faculdadeunimed.edu.br/index.php/RCFU1/article/view/83. Acessado em 09/09/2024.

UE. **Recommendations for a methodology of the assessment of severity of personal data breaches.** Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity>. Acesso em: 15 maio de 2025.

VIEIRA, A. K. M.; DALMORO, M. **Dilemas na Construção de Escalas Tipo Likert: o Número de Itens e a Disposição Influenciam nos Resultados?** Disponível em: https://arquivo.anpad.org.br/abrir_pdf.php?e=OTQ1MA. Acesso em: 25 jun. 2024.

ZAGANELLI, Margareth Vetis. FILHO, **Douglas Luis. Revista de Bioética y Derecho, Universitat de Barcelona. La Llei General de Protecció de Dades i les seves implicacions per a la salut: Avaluacions d'Impacte sobre el tractament de dades en el context clínic i hospitalari**. Disponível: https://revistes.ub.edu/index.php/RBD/article/view/36005/37126. Acessado em 10/06/2023.