UNIVERSIDADE DE CAXIAS DO SUL
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO – PPGA
CURSO DE MESTRADO

ANDRÉA CASARIN ZEN

INOVAÇÃO NA GESTÃO DE MICRO E PEQUENAS EMPRESAS: ASSESSORIA DE ORGANIZAÇÕES CONTÁBEIS NA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

CAXIAS DO SUL
2024

ANDREA CASARIN ZEN

INOVAÇÃO NA GESTÃO DE MICRO E PEQUENAS EMPRESAS: ASSESSORIA DE ORGANIZAÇÕES CONTÁBEIS NA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Dissertação de Mestrado submetido à Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em Administração da Universidade de Caxias do Sul, como parte dos requisitos necessários para obtenção do título de Mestre (a) em Administração.

Orientador: Prof. Dra. Cíntia Paese Giacomello.

CAXIAS DO SUL
2024

Dados Internacionais de Catalogação na Publicação (CIP)
Universidade de Caxias do Sul
Sistema de Bibliotecas UCS - Processamento Técnico

Z54i Zen, Andrea Casarin
Inovação na gestão de micro e pequenas empresas [recurso eletrônico] : assessoria de organizações contábeis na adequação à Lei Geral de Proteção de Dados – LGPD / Andrea Casarin Zen. – 2024.
Dados eletrônicos.

Dissertação (Mestrado) - Universidade de Caxias do Sul, Programa de Pós-Graduação em Administração, 2024.
Orientação: Cíntia Paese Giacomello.
Modo de acesso: World Wide Web
Disponível em: https://repositorio.ucs.br

1. Administração de empresas. 2. Pequenas e médias empresas - Administração. 3. Brasil. Lei n. 13.853, de 08 de julho de 2019. 4. Desenvolvimento organizacional. I. Giacomello, Cíntia Paese, orient. II. Título.

CDU 2. ed.: 005

Catalogação na fonte elaborada pela(o) bibliotecária(o)
Carolina Machado Quadros - CRB 10/2236

ANDREA CASARIN ZEN

INOVAÇÃO NA GESTÃO DE MICRO E PEQUENAS EMPRESAS: ASSESSORIA DE ORGANIZAÇÕES CONTÁBEIS NA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Dissertação de mestrado submetido à Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em Administração da Universidade de Caxias do Sul, como parte dos requisitos necessários para obtenção do título de Mestre em Administração.

Orientadora: Prof. Dra. Cíntia Paese Giacomello

Aprovada em: / /2024.

Banca Examinadora

_____
Prof. Dra. Cíntia Paese Giacomello
Universidade de Caxias do Sul – UCS

_____
Prof. Dr. Alex Eckert
Universidade de Caxias do Sul – UCS

_____
Prof. Dra. Marlei Salete Mecca
Universidade de Caxias do Sul – UCS

_____
Prof. Dr. Guilherme Costa Wiedenhõft
Universidade Federal do Rio Grande – FURG

Dedico este trabalho a todos que me apoiaram nesta jornada acadêmica: minha família, amigos, colegas de trabalho, professores, orientadora e colaboradores. Que este trabalho contribua para o avanço do conhecimento em minha área e inspire outros em suas trajetórias acadêmicas.

AGRADECIMENTOS

Gostaria de aproveitar este momento para expressar minha sincera gratidão a todas as pessoas e instituições que contribuíram para o desenvolvimento e conclusão deste trabalho.

Em primeiro lugar, gostaria de agradecer minha família, que tem sido meu alicerce e apoio incondicional em todos os momentos. Seu amor, encorajamento e paciência foram fundamentais para minha trajetória acadêmica.

À minha orientadora e professores, expresso minha profunda gratidão. Sua orientação, conhecimento e sabedoria foram essenciais para a realização deste trabalho. Sou grata pela paciência demonstrada ao longo das discussões, pelos valiosos ensinamentos e pela dedicação em me ajudar a aprimorar minhas habilidades de pesquisa.

Aos meus amigos, que compreenderam minha prioridade e que não pouparam esforços para me apoiar e ouvir minhas lamentações quando algo não saía conforme o planejado. Compartilharam risos, conselhos e momentos preciosos ao longo dessa jornada, meu mais sincero agradecimento. Sua presença e apoio foram essenciais para manter minha motivação e sanidade durante os períodos desafiadores.

Gostaria de agradecer também aos colaboradores que contribuíram com ideias, sugestões e discussões enriquecedoras. Elas foram valiosas para o desenvolvimento deste trabalho e para minha formação como pesquisadora.

Não posso deixar de agradecer aos colegas de curso, cuja amizade e camaradagem tornaram essa jornada acadêmica muito mais prazerosa e memorável. Nossas discussões e trocas de ideias foram enriquecedoras, e a colaboração entre nós foi primordial para o crescimento mútuo. Seus estímulos e apoio foram uma fonte constante de motivação e inspiração.

Por fim, gostaria de expressar minha gratidão a mim mesma. Este trabalho é um testemunho do meu esforço, perseverança e dedicação em alcançar meus objetivos acadêmicos. Agradeço por nunca desistir, mesmo diante dos desafios e obstáculos encontrados ao longo do caminho.

Que este trabalho possa contribuir para o avanço do conhecimento em minha área de estudo e inspirar outros pesquisadores a seguirem seus próprios caminhos acadêmicos.

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes.”

Marthin Luther King

RESUMO

A Lei Geral de Proteção de Dados (LGPD) foi promulgada no Brasil em 2018, com o objetivo proteger os direitos fundamentais de privacidade e liberdade dos cidadãos em relação aos seus dados pessoais. Inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece princípios e regras que devem ser seguidos por empresas e instituições que coletam, armazenam, processam, compartilham e eliminam dados pessoais em atividade no Brasil, independente do seu porte. No contexto específico das micro e pequenas empresas, é comum que recorram às organizações contábeis para auxílio em suas rotinas. Assim, este trabalho propõe um artefato para ajudar esses profissionais a contribuírem para a conformidade com a LGPD neste segmento empresarial. A metodologia aplicada para o desenvolvimento desse artefato foi a *Design Science Research*, que consiste em projetar artefatos para solucionar problemas. O artefato desenvolvido consiste em um roteiro de fácil operação, composto por campos extraídos da própria lei, orientações da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e de pesquisas realizadas por meio de pesquisas bibliográficas. Essa ferramenta foi validada por profissionais de organizações contábeis através de consultas e entrevistas, os quais forneceram sugestões para seu aprimoramento, tornando viável sua aplicação em micro e pequenas empresas. Além disso, foram estabelecidos protocolos de governança corporativa e de segurança da informação para orientar sua implementação. Este artefato é um uma solução inovadora ao permitir que as organizações contábeis se aproximem dos seus clientes auxiliando-os na compreensão dos processos e na adequação à LGPD, melhoria da eficiência, segurança e conformidade com a legislação. A tecnologia adotada é simples e de baixo custo, o que permite maior acessibilidade. Ao repensar suas práticas de coleta de dados, essas organizações encontram maneiras de respeitar a privacidade dos titulares dos dados. Também contribui como um recurso inovador para a pesquisa acadêmica, fornecendo um modelo replicável e adaptável para estudos futuros sobre a conformidade com a LGPD e a interseção entre a contabilidade, a governança corporativa e a segurança da informação.

Palavras-chave: LGPD; organizações contábeis; inovação; micro e pequenas empresas.

ABSTRACT

The General Data Protection Law (LGPD) was enacted in Brazil in 2018, to protect the fundamental rights of privacy and freedom of citizens to their personal data. Inspired by the General Data Protection Regulation (GDPR) of the European Union, the LGPD establishes principles and rules that must be followed by companies and institutions that collect, store, process, share, and eliminate personal data operating in Brazil, regardless of their size. In the specific context of micro and small businesses, they commonly turn to accounting organizations for assistance in their routines. Therefore, this work proposes an artifact to help these professionals contribute to compliance with the LGPD in this business segment. The methodology applied to develop this artifact was Design Science Research, which consists of designing artifacts to solve problems. The developed artifact consists of an easy-to-operate script, composed of fields extracted from the law, guidelines from the National Personal Data Protection Authority (ANPD), and research carried out through bibliographic research. This tool was validated by professionals from accounting organizations through consultations and interviews, who provided constructive suggestions for its improvement, making its application viable in micro and small companies. In addition, corporate governance and information security protocols were established to guide its implementation. This artifact is an innovative solution that allows accounting organizations to get closer to their clients, helping them understand processes and adapt to LGPD, improving efficiency, security, and compliance with the legislation. The technology adopted is simple and low-cost, which allows for greater accessibility. By rethinking their data collection practices, these organizations are finding ways to respect the privacy of data subjects. It also contributes as an innovative resource for academic research, providing a replicable and adaptable model for future studies on GDPR compliance and the intersection between accounting, corporate governance, and information security.

Keywords: LGPD; accounting organization; innovation; micro and small companies.

LISTA DE FIGURAS

Figura 1 - Quantidade de artigos publicados com os termos “LGPD” e “Implementação” 2015 a 2022 – Google Acadêmico 25
Figura 2 - Quantidade de artigos publicados com os termos “LGPD” e “implementação” comparado aos termos “GDPR” e “implementation” 2015 a 2022 – Google Acadêmico 26
Figura 3 - Quantidade de artigos por autor com o termo LGPD (2018 – 2022).....27
Figura 4 - Quantidade de artigos por autor com o termo GDPR (2018 – 2022).....27
Figura 5 - Quantidade e Palavras-chave em artigos por termo GDPR e LGPD (2018-2022) 29
Figura 6 - Ciclo da administração de pessoas.....51
Figura 7 - Etapas da pesquisa Design Science Research e o movimento do ciclo do artefato. 63
Figura 8 - Artefato: Sobre a LGPD 74
Figura 9 - Artefato: Início 75
Figura 10 - Artefato: Diretório com arquivos para auxiliar na adequação à LGPD....76
Figura 11 - Artefato: Início - Indicador 76
Figura 12 - Artefato: Levantamento inicial 1 77
Figura 13 - Artefato: Levantamento inicial 2 78
Figura 14 - Artefato: Levantamento inicial 2 – indicador 79
Figura 15 - Artefato: Fornecedores 80
Figura 16 - Artefato: Ativos de informações 81
Figura 17 - Artefato: TI inventário 82
Figura 18 - Artefato: Atribuições da área de tecnologia da informação.....82
Figura 19 - Artefato: Identificação dos processos (incluso exemplo) 83
Figura 20 - Artefato: Mapeamento e RIPD 84
Figura 21 - Artefato: Plano de Ação (incluso exemplo) 85
Figura 22 - Artefato: Sobre a LGPD – Dicas de Governança Corporativa e de Segurança da Informação 92

LISTA DE TABELAS

Tabela 1 - Quantidade de artigos publicados de 2018 a 2022 – Termos: “LGPD” e “Adequação” 24
Tabela 2 - Quantidade de artigos publicados de 2018 a 2022 – Termos: “LGPD” e “Implementação” 24
Tabela 3 - Quantidade de periódicos por termo LGPD (2018-2022) 28
Tabela 4 - Quantidade de periódicos por termo GDPR (2018 – 2022) 29
Tabela 5 - Quantidade de empresas por natureza jurídica (out/2022) 31

LISTA DE QUADROS

Quadro 1 - Princípios da LGPD - Tratamento de dados pessoais.....37
Quadro 2 - Termos utilizados na LGPD 41
Quadro 3 - Classificação das empresas por receita.....48
Quadro 4 - Classificação tributária das empresas.....49
Quadro 5 - Os princípios da governança corporativa.....56

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPAD	Associação Nacional de Pós-graduação e Pesquisa em Administração
ANPD	Autoridade Nacional de Proteção de Dados
Art.	Artigo de lei
BDTD	Biblioteca Digital Brasileira de Teses e Dissertações
CFC	Conselho Federal de Contabilidade
COFINS	Contribuição para o Financiamento da Seguridade Social
CRC	Conselho Regional de Contabilidade
CSLL	Contribuição Social sobre o Lucro Líquido
DPO	*Data Protection Officer* ou Encarregado de Dados
DSR	*Design Science Research*
e-Social	Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas
GDPR	*General Data Protection Regulation*
ICMS	Imposto sobre Circulação de Mercadorias e Serviços
IPI	Imposto sobre Produtos Industrializados
IRPJ	Imposto sobre a Renda das Pessoas Jurídicas
ISSQN	Imposto sobre Serviços de Qualquer Natureza
LGPD	Lei Geral de Proteção de Dados, Lei nº 13.709 de 14 de agosto de 2018
MEI	Microempreendedor Individual
OCDE	Organização para Cooperação e Desenvolvimento Econômico
PIB	Produto Interno Bruto
PIS/PASEP	Programa de Integração Social e o Programa de Formação do Patrimônio do Servidor Público
PNAD	Pesquisa Nacional por Amostra de Domicílios
PPGA	Programa de Pós-graduação em Administração
RIPD	Relatório de Impacto à Proteção de Dados
SEBRAE	Serviço Brasileiro de Apoio às Micro e Pequenas Empresas
SNTD	Sistema Nacional para Transformação Digital

SUMÁRIO

1 INTRODUÇÃO 12
1.1 TEMA E PROBLEMA 18
1.2 OBJETIVOS 21
1.2.1 Objetivo geral 21
1.2.2 Objetivos específicos 21
1.3 JUSTIFICATIVA DO ESTUDO 22
1.4 ADERÊNCIA DO PROJETO À LINHA DE PESQUISA 33
2 REFERENCIAL TEÓRICO 35
2.1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS 35
2.1.1 Termos utilizados na LGPD 41
2.1.2 Relatório de Impacto à Proteção de Dados 44
2.1.3 Autoridade Nacional de Proteção de Dados (ANPD) 46
2.2 CLASSIFICAÇÃO DAS EMPRESAS 47
2.3 LGPD EM MICRO E PEQUENAS EMPRESAS 49
2.4 PAPEL DAS ORGANIZAÇÕES CONTÁBEIS NA GESTÃO DE MICRO E PEQUENAS EMPRESAS 50
2.5 INOVAÇÃO E A LGPD 52
2.6 GOVERNANÇA CORPORATIVA E A LGPD 55
2.7 SEGURANÇA DA INFORMAÇÃO E A LGPD 59
3 PROCEDIMENTOS METODOLÓGICOS 61
3.1 ETAPA 1: CONSCIENTIZAÇÃO 64
3.2 ETAPA 2: SUGESTÃO 64
3.3 ETAPA 3: DESENVOLVIMENTO 66
3.4 ETAPA 4: AVALIAÇÃO 69
3.5 ETAPA 5: CONCLUSÃO 71
4 RESULTADOS 73
4.1 CONSTRUÇÃO DO ARTEFATO 73
4.2 APLICAÇÃO DO ARTEFATO 86
4.3 GOVERNANÇA CORPORATIVA E DE SEGURANÇA DA INFORMAÇÃO 90
4.3.1 Política de Segurança 92
4.3.2 Política de Privacidade 93
5 CONCLUSÃO 95
5.1 ALCANCE DOS OBJETIVOS 96
5.2 CONTRIBUIÇÕES PRÁTICAS 97

5.3 CONTRIBUIÇÕES TEÓRICAS 98
5.4 RECOMENDAÇÕES E PESQUISAS FUTURAS 98
REFERÊNCIAS 100
GLOSSÁRIO 111
APÊNDICE A – ARTIGOS MAIS CITADOS NA PLATAFORMA SCOPUS COM O TERMO LGPD (2018-2022) 116
APÊNDICE B – ARTIGOS MAIS CITADOS NA PLATAFORMA SCOPUS COM O TERMO GDPR (2018-2022) 119
APÊNDICE C – EMBASAMENTO DA CONSTRUÇÃO DO ARTEFATO 121
APÊNDICE D – ROTEIRO DE ADEQUAÇÃO À LGPD - ARTEFATO 128
APÊNDICE E – COMPARAÇÃO DOS TIPOS DE INOVAÇÃO DAS 3ª E 4ª EDIÇÕES DO MANUAL DE OSLO 133

1 INTRODUÇÃO

Na conjuntura contemporânea, observa-se a ubiquidade de dados pessoais em diversos meios digitais, incluindo, mas não se limitando a, redes sociais, internet, sistemas corporativos, instituições bancárias e entidades governamentais, bem como em suportes físicos de armazenamento. A fim de assegurar a proteção e a privacidade dessas informações, foi instituída a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018. Esta legislação tem como propósito estipular diretrizes e normativas que norteiam suas operações diárias, sejam elas relativas a dados pessoais de colaboradores, clientes, fornecedores ou terceiros.

Nesse cenário, as empresas, classificadas como controladoras segundo a LGPD, ao acessarem os dados pessoais, assumem a responsabilidade de garantir que o armazenamento, processamento ou transferência dessas informações sejam realizadas mediante a autorização do proprietário dos dados, identificado na LGPD como titular (BRASIL, 2018). Tal medida tem como objetivo salvaguardar a privacidade e a autonomia dos indivíduos em relação às suas informações pessoais, enfatizando a necessidade de obtenção de consentimento prévio e o informando que, para a coleta, armazenamento e uso desses dados, é utilizada a fundamentação do Art. 2º da LGPD (BRASIL, 2018). Assim, a LGPD visa fomentar uma cultura de proteção e conscientização acerca da segurança dos dados pessoais, estabelecendo direitos e responsabilidades claros para as organizações que operam nesse contexto.

O dado pessoal, conforme definido pelo Art. 5º da LGPD (BRASIL, 2018), refere-se a qualquer informação relacionada a uma pessoa natural que possa ser identificada ou identificável, como uma fotografia, nome ou endereço. A LGPD também aborda o conceito de dado pessoal sensível, que engloba informações sobre a saúde, vida sexual, dado genético, biométrico, opção religiosa, ou seja, algum dado que possa discriminar um indivíduo. Esses dados são essenciais para a estruturação e proteção da identidade de um indivíduo (ECHTTERHOFF, 2010). Dessa forma, a LGPD busca assegurar a proteção dos dados estabelecendo diretrizes e regulamentações claras sobre a coleta, o armazenamento e o tratamento dessas informações, que é reforçada pela norma ABNT NBR ISO/IEC 27002 (ABNT, 2013), que trata das técnicas de segurança e prática para controles de segurança da informação. No contexto deste trabalho acadêmico, está focado no tratamento dos

dados pessoais coletados pelas empresas, especificamente abordando o papel desempenhado por essas organizações enquanto controladoras dos referidos dados.

A LGPD impõe às empresas uma maior responsabilidade no que diz respeito à coleta de dados pessoais, com o objetivo de minimizar a ocorrência de vazamentos de dados. Tais vazamentos podem ocorrer tanto de forma física quanto de forma digital. No contexto físico, um exemplo seria uma situação na qual um funcionário do departamento de Recursos Humanos deixa os holerites de todos os funcionários da empresa à vista em sua mesa e se ausenta do seu local de trabalho, deixando informações sensíveis e sigilosas expostas. No âmbito digital, um vazamento de dados é categorizado como um delito cibernético, uma vez que dados pessoais podem ser comprometidos por meio de uma invasão a um sistema ou rede de uma empresa cujos controles de acesso se encontram vulneráveis (CRUZ, 2021). Tal ataque pode resultar na exposição de informações confidenciais de clientes, fornecedores, colaboradores e parceiros.

Em 2018, a Revista Exame divulgou um incidente de vazamento de dados digitais que envolveu a rede social Facebook. Essa plataforma revelou que, a maioria dos seus quase dois bilhões de usuários podem ter tido dados acessados indevidamente. Em uma ocorrência separada, em 2015, Isaak e Hanna (2018) relataram que a empresa de consultoria Cambridge Analytica acessou 87 milhões de dados pessoais dos usuários do Facebook com a intenção de analisar e influenciar o comportamento dos eleitores americanos. No Brasil, Zanatta (2015) menciona um exemplo de uma decisão da Secretaria Nacional do Consumidor, na qual a empresa Oi S/A foi multada em 3,5 milhões de reais. Essa penalidade foi aplicada devido a identificação do uso de um software que criava, ilegalmente, um banco de dados pessoais dos seus clientes e o revendia a terceiros. Esses exemplos destacam a relevância da proteção de dados e as consequências de sua violação.

Com base nesses exemplos, torna-se imprescindível que as empresas adotem medidas de segurança robustas em suas plataformas de sistemas, redes, aplicativos, bem como em ambientes físicos onde os dados pessoais estão armazenados. O objetivo dessas medidas é assegurar a proteção eficaz dessas informações. As práticas de proteção podem incluir o uso de programas antivírus e *firewalls* atualizados, a criação de senhas virtuais complexas e a alteração periódica dessas senhas, conforme destacado por Pimenta e Quaresma (2016). Além disso, a implementação de sistemas de segurança físicos, como salas e armários trancados

com acesso restrito, também é uma estratégia importante para a proteção de dados. Essas medidas coletivas podem ajudar a prevenir vazamentos de dados e garantir a privacidade e a segurança das informações pessoais.

Essas medidas de proteção são necessárias para atenuar os riscos associados ao acesso não autorizado, divulgação indevida ou manipulação inadequada de dados pessoais. Essas proteções garantem a conformidade com a legislação vigente e as políticas corporativas, caracterizando a *compliance* e orientando as práticas de boa governança (QUEIROZ, 2019). Além disso, é imperativo que essas práticas sejam devidamente documentadas e evidenciadas. Isso serve para demonstrar o comprometimento da organização com a segurança dos dados e a aderência às disposições da LGPD. A documentação adequada dessas medidas reforça a transparência, integridade e a responsabilidade da empresa com elementos-chave para a construção de uma cultura de proteção de dados eficaz (ABNT NBR ISO/IEC 37301, 2021).

Ao implementar tais medidas de segurança, as empresas estão contribuindo para o fortalecimento da proteção dos dados pessoais, garantindo a privacidade e a integridade das informações de seus titulares. Essa ação demonstra o compromisso legal e a responsabilidade na gestão adequada dos dados pessoais sob a custódia da empresa (ABNT NBR ISO/IEC 27002, 2013).

No entanto, um estudo realizado (FEBRABAN, 2022) revelou que cerca de 80% das empresas brasileiras ainda não se adequaram às exigências da LGPD. No contexto desse estudo, observou-se que as empresas de médio e grande porte possuem departamentos internos que possivelmente auxiliam na condução dos processos de adequação à LGPD. Por outro lado, ao analisar as micro e pequenas empresas, constatou-se que essas organizações não possuem áreas internas específicas dedicadas à orientação e implementação da referida legislação. Isso ressalta a necessidade de um maior esforço para garantir a conformidade com a LGPD em todos os níveis do ecossistema empresarial.

A partir deste enfoque, a presente análise evidencia uma lacuna na implementação de estratégias básicas para a conformidade com LGPD, particularmente no contexto das micro e pequenas empresas. A falta de recursos internos alocados especificamente para esta finalidade, pode constituir um obstáculo adicional para estas organizações, que frequentemente se deparam com restrições de recursos e falta de *expertise* especializada no domínio da proteção de dados

(SEBRAE, 2022). Dentro deste cenário, as micro e pequenas empresas, que não dispõem de infraestruturas internas dedicadas, podem encontrar dificuldades em cumprir com as obrigações legais e, muitas vezes, não estão cientes dos requisitos estipulados pela LGPD.

Diante dessa realidade, torna-se essencial a busca por estratégias e soluções para auxiliar as micro e pequenas empresas na sua jornada de adequação à LGPD. Isso pode incluir a disponibilização de recursos educacionais, treinamentos específicos e o compartilhamento de boas práticas, a fim de promover a conscientização e a implementação das medidas necessárias para a proteção dos dados pessoais nessas empresas de menor porte (ABNT NBR ISO/IEC 27701, 2019).

No entanto, as micro e pequenas empresas são, em geral, constituídas por uma equipe limitada, tanto em termos de quantidade de pessoas quanto de qualidade. Como não tem condições de contratar especialistas para atender às necessidades da empresa, o empresário assume múltiplas funções, abrangendo áreas como produção, compras, marketing, vendas e recursos humanos (MARTENS, 2001). As micro e pequenas empresas possuem um papel econômico-social relevante no ambiente em que estão inseridas, como a geração de emprego e renda e como pólo de criação e distribuição de riqueza (SANTOS; SILVA; NEVES, 2011).

Dessa forma, Beuren, Barp e Filipin (2013) afirmam que, para apoio nos negócios e criação de forças competitivas, as micro e pequenas empresas precisam de auxílio gerencial, e grande parte dessas organizações utilizam-se de instrumentos fornecidos por serviços contábeis para a tomada de decisões que, em sua maioria, são terceirizados. As atribuições dos profissionais contábeis são associadas ao cumprimento de obrigações fiscais e legais, porém Zarowin (1997) enfatiza que esses profissionais devem ser agentes de mudança e podem aprender novas habilidades. Ressalta ainda que, melhorar a qualidade dos produtos e serviços, e aumentar a produtividade, terá um resultado, aumentando sua vantagem competitiva à sua capacidade de aprender e de continuar a aprender.

Entre vários pontos do aprendizado, Zarowin (1997) destaca o papel de um contador no desenvolvimento de uma compreensão profunda de todos os aspectos de um negócio. Dessa forma, o contador, como conhecedor da empresa do seu cliente, pode ramificar sua operação incluindo a adequação à LGPD em suas atividades, fornecendo um diferencial em seu portfólio de serviços.

As organizações contábeis desempenham um papel fundamental no suporte às empresas, por meio de profissionais qualificados e atualizados, que têm a responsabilidade de se manterem informados sobre leis e obrigações e de garantir a conformidade de seus clientes com tais requisitos. Essa relação estabelecida entre o contador e seus clientes é pautada na confiança, uma vez que todas as operações empresariais, sejam elas de natureza fiscal, contábil, patrimonial ou relacionadas ao departamento de pessoal, são registradas e analisadas por esses profissionais contratados (ECKERT *et al*., 2020).

A relação de confiança estabelecida entre a organização contábil e o cliente é essencial, pois permite que esta empresa terceirizada tenha acesso a informações sensíveis e confidenciais do seu cliente, possibilitando um trabalho minucioso e preciso. Além disso, essa parceria permite uma análise aprofundada das informações contábeis, auxiliando na tomada de decisões estratégicas e contribuindo para o sucesso organizacional (ECKERT *et al*., 2020).

Diante desse contexto, o presente estudo apresenta uma proposta direcionada às organizações contábeis, por meio de seus profissionais, com o intuito de orientar seus clientes acerca da LGPD e propor medidas de adequação visando evitar possíveis penalidades. Essas penalidades podem surgir da não conformidade com a LGPD, principalmente em casos de vazamento de dados pessoais e podem ser desde uma advertência até multas monetárias significativas, que podem chegar a 2% do faturamento, com um limite de R$ 50.000.000,00 por infração, conforme o Art. 52 da LGPD (BRASIL, 2018).

Considerando a importância das organizações contábeis como facilitadores e assessores das empresas, esses profissionais possuem conhecimentos técnicos e especializados para oferecer suporte na compreensão e implementação das diretrizes legais pertinentes. Dessa forma, eles podem desempenhar um papel relevante ao fornecer informações claras e atualizadas sobre a LGPD, bem como orientar seus clientes sobre as ações básicas para garantir a conformidade com a referida lei.

Esta proposta busca conscientizar as organizações contábeis sobre seu potencial papel na disseminação do conhecimento acerca da LGPD, bem como na sugestão de medidas de adequação que podem ser adotadas pelas empresas. Essas medidas podem incluir a implementação de políticas internas de proteção de dados, revisão dos processos de coleta, armazenamento, processamento, compartilhamento e eliminação de informações pessoais, realização de treinamentos para os

colaboradores e a adoção de medidas técnicas de segurança, visando garantir a privacidade e a integridade dos dados dos clientes, colaboradores, fornecedores e terceiros (ABNT NBR ISO/IEC 27002, 2013).

Ao desempenhar essa função orientadora, as organizações contábeis podem contribuir para a prevenção de penalidades decorrentes do descumprimento à LGPD, além de promover a conscientização dos seus clientes sobre a importância da proteção de dados pessoais. Essa abordagem pró-ativa e de suporte pode estabelecer uma relação de confiança mais sólida entre o contador e o cliente, resultando em uma parceria estratégica para o alcance da conformidade e para a mitigação de riscos relacionados ao tratamento inadequado dos dados.

A partir dessa diretriz, pode-se oportunizar às micro e pequenas empresas a inserção da boa governança, utilizando-se de padrões éticos e comunitários geralmente aceitos para o alinhamento da conformidade das pessoas que trabalham para a organização, bem como o reconhecimento e implantação de medidas para promover o comportamento uniforme (ABNT NBR ISO/IEC 37301, 2021).

Dessa forma, a elaboração de um artefato, que, segundo Lacerda *et al*. (2013, p. 748), “representa um conjunto de passos que devem ser obedecidos para que um resultado seja produzido em determinado ambiente externo”. A *Design Science Research* estuda a criação de artefatos, que dentro de um contexto, cumprem um propósito ou adaptação de um objetivo, ou seja, um ciclo regulador que envolve a investigação do problema (REIS, 2019).

Assim, um artefato que viabilize a adequação à LGPD e à política de boa governança contribui para o fortalecimento e desenvolvimento do relacionamento da empresa com os seus clientes internos e externos, o que é o princípio da inovação definido por Paredes, Santana e Fell (2014). Auxiliar os clientes das organizações contábeis na adequação à LGPD, conscientização dos funcionários sobre os aspectos da lei, utilizando uma tecnologia simples e de baixo custo, poderá melhorar a eficiência e a segurança dos dados pessoais, bem como, das informações da própria empresa, termos destacados nas normas técnicas (ABNT NBR ISO/IEC 27002, 2013) e no Manual de Oslo (OCDE/Eurostat, 2018) como uma ferramenta inovadora.

1.1 TEMA E PROBLEMA

Os dados pessoais desempenham papel relevante em diferentes esferas. Abrangem desde a esfera comercial, onde são utilizados para fins de venda de produtos, até a esfera de cumprimento de obrigações legais por parte das empresas, como, por exemplo, o compartilhamento de informações de funcionários com o governo federal para a atualização do sistema e-Social.

O Art. 5º da LGPD (BRASIL, 2018, p.5) define o dado pessoal como sendo informação relacionada à “pessoa natural identificada ou identificável”. Ainda define o que considera dado pessoal sensível, caracterizado como informação que pode vir a ser discriminatório, como “origem racial ou étnica, religião, convicção política, filiação a sindicato, ou a organização de caráter filosófico, político, ou dado referente à saúde”, como, por exemplo, um exame laboratorial, “à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

Essa pesquisa visa compreender a coleta desses dados pessoais pelas empresas e seus propósitos específicos, pois conforme a LGPD, deve ser devidamente comunicado ao titular dos dados a finalidade dessa coleta, sendo que, após o uso, a empresa é responsável pelo devido descarte dessas informações (BRASIL, 2018). No processo de coleta, armazenamento, tratamento e descarte de dados sensíveis, podem surgir questões relevantes que variam de acordo com o tipo de organização, e esses dados são armazenados em diferentes locais, como servidores internos, serviços em nuvem ou mesmo em arquivos físicos (ABNT NBR ISO/IEC 27701, 2019). Dessa forma, em todo esse fluxo, avaliar a segurança na proteção e cuidado dessas informações pessoais que são utilizadas pelas empresas.

A identificação dos indivíduos que são responsáveis pelo armazenamento dos dados é necessária para verificação de alçadas, pois utilizam redes e sistemas pertencentes a uma determinada empresa. Convém que esta organização “assegure que as pessoas sob seu controle estejam conscientes da definição de dados pessoais e que saibam como reconhecer uma informação que é um dado pessoal” (ABNT NBR ISO/IEC 27701, 2019, p. 24). Essas pessoas devem ter autorização para utilização desses dados e a empresa deve assegurar que o acesso não esteja disponível para qualquer outro indivíduo não autorizado. E assim avaliar as permissões de acesso dos usuários se são controlados por senhas e permissões de forma documentada.

Compreender se, no contexto empresarial, as organizações contratam parceiros externos para fornecer produtos e serviços essenciais para o funcionamento de seus negócios. Nesse sentido, é relevante verificar quais acessos físicos e virtuais são concedidos a esses fornecedores dentro e fora das instalações da empresa e se são formalizados e regulamentados em contrato, principalmente se houver compartilhamento de dados pessoais. O parceiro da empresa controladora é denominado operador mediante o Art. 5º da LGPD (BRASIL, 2018).

Conforme observado pelo SEBRAE (2022), existem empresas que possuem departamentos internos, tais como Jurídico e de Tecnologia da Informação (TI) ou que dispõem de recursos financeiros para contratação de consultorias especializadas que auxiliam na adequação a LGPD. No entanto, algumas empresas, embora estejam cientes da LGPD, optam por dar prioridade às suas atividades comerciais, adiando assim sua adequação. Adicionalmente, há organizações que não estão familiarizadas com o conteúdo e o escopo da LGPD, principalmente micro e pequenas empresas.

A falta de conformidade com a LGPD pode resultar em sanções que vão de suspensão de atividades pertinentes a dados pessoais até penalidades monetárias. O Art. 52º da LGPD (BRASIL, 2018) apresenta as sanções que, para determinadas empresas, podem ser cruciais para o andamento de suas atividades. Diante disso, surge a questão de como conscientizar os empresários, gestores e colaboradores sobre a importância de realizar a adequação à LGPD. Uma das abordagens para operacionalizar essa adequação em empresas que não possuem uma estrutura interna consciente e capacitada para implementar as diretrizes da LGPD é por meio da colaboração das organizações contábeis.

As organizações contábeis terceirizadas, quando contratadas, desempenham papéis vitais para as empresas, particularmente para as micro e pequenas empresas. Para este segmento empresarial, as organizações contábeis são, frequentemente, o único meio de se atualizar sobre quaisquer alterações na legislação brasileira. Beuren, Barp e Filipin (2013) destacam que existe um desafio significativo para as empresas de serviços contábeis em fornecer suporte informacional robusto e eficaz ao processo de gestão das empresas de pequeno porte. Esse desafio é amplificado pela necessidade do contador de atuar como um agente transformador e gerador de informações. Através de suas habilidades especializadas e conhecimento aprofundado, o contador tem a capacidade de desenvolver e implementar atividades de contabilidade de gestão eficazes, que podem ter um impacto substancial na

operação e sucesso da empresa. Esta é uma área de oportunidade para as empresas de serviços contábeis, que podem se posicionar como parceiros estratégicos para as empresas de pequeno porte, fornecendo *insights* e orientações relevantes para ajudá-las a navegar no complexo ambiente de negócios e estarem adequadas à legislação (BEUREN; BARP; FILIPIN, 2013). Diante desse contexto, abre-se a oportunidade de diversificação do papel da organização contábil.

> A contabilidade é o principal núcleo de registros de quase todas as informações da empresa. São poucos os eventos ocorridos em uma organização que não implicam registro na contabilidade.[…] a contabilidade passa a ter outro papel na organização que é de gerenciar o conjunto de informações que são geradas em diversas áreas da empresa (OLIVEIRA, 2014, p.10).

De acordo com a Lei Complementar nº 128 (BRASIL, 2008), apenas os Microempreendedores Individuais (MEI) estão isentos de contratar os serviços de um profissional de contabilidade. No entanto, em certas situações, pode ser indispensável recorrer a um contador, inclusive com vantagens fiscais para o próprio microempreendedor ao contratar uma entidade contábil. A contabilidade desempenha um papel imprescindível no apoio às decisões estratégicas de uma empresa e na garantia do cumprimento de obrigações fiscais e legais (ECKERT *et al*., 2020), seja a contabilidade realizada internamente ou por meio de terceirização.

As organizações contábeis desempenham diversas atividades. Thomé (2001, p. 21) define os serviços contábeis na seguinte ordem: “consultoria, contabilidade, administração de pessoal, escrituração fiscal, expediente (ou serviços comerciais), auditoria, perícia e assessoria”. Wrubel, Toigo e Lavarda (2015, p. 1179) complementam que “o contador desempenha papel de destaque na gestão e controle dos recursos financeiros da empresa, na medida em que estes influenciam a tomada de decisão, uma vez que o gestor inteligente busca se basear em informações contábeis para tomar suas decisões”.

Nesse contexto, o papel do profissional contábil remete à confiança, sigilo, ética e buscam, constantemente, por atualização, pois se empenham para fazer o melhor para os seus clientes (NICOLAU; COUTO, 2018). Utilizando-se dessa *expertise*, este profissional pode contribuir ainda mais com o trabalho e sucesso do seu cliente, inserindo como um serviço diferencial, a adequação à LGPD, e com isso implementar um “programa de privacidade e governança da organização,

assegurando a *compliance* com as leis e regulamentações aplicáveis, relacionadas ao tratamento de dados pessoais", é o que reforça a ABNT NBR ISO/IEC 27701 (2019, p. 21) em consonância com o Código das Melhores Práticas de Governança Corporativa (IBGC, 2023).

Dessa forma, de que maneira as organizações contábeis podem auxiliar seus clientes, micro e pequenas empresas, na conscientização e na adequação aos requisitos estabelecidos pela LGPD e, ao mesmo tempo, promover as melhores práticas de governança corporativa?

1.2 OBJETIVOS

Na presente pesquisa, são estabelecidos um objetivo geral e objetivos específicos que orientam o desenvolvimento do estudo. O objetivo geral tem como propósito principal delinear a meta ampla que se pretende alcançar por meio da pesquisa. Por sua vez, os objetivos específicos têm o intuito de detalhar as etapas ou aspectos específicos que serão abordados para atingir o objetivo geral.

É importante ressaltar que os objetivos são elementos norteadores da pesquisa, fornecendo direcionamento para a coleta de dados, análise e interpretação dos resultados. Eles contribuem para a delimitação do escopo do estudo, auxiliando na organização e estruturação da pesquisa.

1.2.1 Objetivo geral

O objetivo geral desta pesquisa consiste em desenvolver um artefato inovador para organizações contábeis auxiliarem na implementação da Lei Geral de Proteção de Dados (LGPD) em micro e pequenas empresas e, em consonância, promover as melhores práticas de governança corporativa.

Entende-se que, por meio desse artefato, estas empresas serão beneficiadas ao incorporarem diretrizes estabelecidas pela LGPD em seus processos e a partir disso, adotarem boas práticas de governança corporativa.

1.2.2 Objetivos específicos

Os objetivos específicos desta pesquisa são os seguintes:

a) desenvolver uma proposta inovadora para que as organizações contábeis possam auxiliar no processo de adequação à LGPD em micro e pequenas empresas;

b) validar a proposta junto a organizações contábeis;

c) traçar práticas de boa governança corporativa.

Por meio desses objetivos específicos, pretende-se contribuir para a disseminação de conhecimentos e práticas que facilitem a adequação à LGPD nas micro e pequenas empresas, contando com a participação ativa das organizações contábeis na implementação dessas diretrizes de proteção de dados pessoais.

1.3 JUSTIFICATIVA DO ESTUDO

Na área de administração de empresas, a competitividade e a perpetuidade são fundamentais para estabelecer processos de qualidade e inovação. Oliveira *at al*. (2003) destaca que a responsabilidade pela liderança desses processos é percebida como complexa por parte dos seus gestores e a dificulade de gestão surgem devido à sua inexperiência e à dificuldade de tomada de decisões acertadas para determinar processos de qualidade.

Canedo *at al.* (2023, p.7), revela, em pesquisa com profissioais da área de tecnologia, que “há falta de comprometimento por parte de gestores e instituições” por não estarem em conformidade com a LGPD. Canedo *at al.* (2023) mostraram que há desconhecimento da legislação dos próprios profissionais de TI e das próprias regras de segurança e privacidade dos usuários que estão na Política de Segurança das empresas.

Silveira (2002) apresenta que há uma vantagem para as organizações que adotam boas práticas de governança corporativa. Essas vantagens podem ser classificadas como: facilidade na captação de recursos externos, atrair investidores externos e redudir o custo de capital. A adoção dessa prática pode resultar em crescimento e evolução constante da empresa, pois evita problemas futuros, melhora a gestão do empreendimento, homogeneidade dos processos e na própria perpetuidade do negócio. Além disso, o mercado brasileiro vem atraindo novos investidores globais que estão interessados na segurança da informação dentro das empresas brasileiras.

Dessa forma, conforme as empresas vão amadurecendo seus negócios, é necessário mesclar a segurança da informação (CANEDO *at al*., 2023) com a governança corporativa (SILVEIRA, 2002; IBGC, 2023) que é trabalhada a partir dos gestores das empresas. Dessa forma, os gestores são os responsáveis em adotar políticas de boa governança dentro de suas empresas. Essas políticas devem estar claras aos colaboradores das empresas (ABNT NBR ISO/IEC 27001), descritas em sua Política de Segurança e Privacidade, que também se referem à segurança dos dados pessoais que circulam dentro das empresas.

As boas práticas e políticas de governança estão descritas na LGPD (BRASIL, 2018), na seção II, que, de forma geral, se refere à proteção dos dados pessoais. O uso de dados pessoais desperta interesse em diversas áreas do conhecimento e transita de forma diversa dentro e fora do ramo empresarial. A partir do nascimento de uma pessoa até depois da sua morte os seus dados circulam nos mais variados meios, sejam em empresas privadas ou governamentais, através do registro do nascimento ou pelo registro de empregado na carteira de trabalho, que atualmente é digital, ou seja, para qualquer movimento de uma pessoa natural, há um movimento digital, com número de documento, fotos, vínculos familiares, exames médicos, entre outros dados.

Em conformidade com a LGPD, a entidade, responsável pela coleta de dados pessoais, está legalmente obrigada a garantir a segurança dessas informações. Essa segurança abrange servidores de dados em sua infraestrutura de Tecnologia da Informação (TI), serviços de armazenamento em nuvem ou por meio de medidas físicas, como acesso restrito a arquivos contendo dados pessoais, reservado apenas aos profissionais autorizados, com o propósito de coletar informações necessárias para a consecução de seus objetivos.

A preocupação em relação ao armazenamento, proteção e uso de dados pessoais foi inicialmente regulamentada na Europa pela *General Data Protection Regulation* (GDPR), exigindo que as empresas estivessem em conformidade com essa legislação ao lidarem com informações de cidadãos europeus, independentemente de sua localização geográfica. Posteriormente, em contrapartida à publicação da GDPR, o Brasil promulgou sua própria legislação específica sobre o tema, a Lei Geral de Proteção de Dados (LGPD), e como resultado as empresas brasileiras começaram a se adaptar para evitar prejuízos aos seus negócios (MACIEL, 2019).

Com o objetivo de aprofundar o tema, em fevereiro do ano de 2023, iniciou-se uma pesquisa nas bases de dados Scopus, *Web of Science*, Google Acadêmico, *Spell* e a Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), plataformas *online* que auxiliam as pesquisas acadêmicas. Dessa forma, foi realizada busca nessas plataformas pelos termos “LGPD”, “adequação” ou “implementação”, “contabilidade” e “clientes”, nos filtros de busca avançada. Optou-se buscar ambos os termos “adequação” e “implementação” pois dependendo da plataforma, o uso da expressão pode variar.

A Tabela 1 demonstra quantidade expressiva de artigos na plataforma do Google Acadêmico. Contudo, ao aprofundar leituras, observou-se que a adequação proposta era direcionada para organizações contábeis e não para a assistência na adequação de seus respectivos clientes.

Tabela 1 - Quantidade de artigos publicados de 2018 a 2022 – Termos: “LGPD” e “Adequação”

Pesquisas (termos)	SPELL	GOOGLE ACAD.	SCOPUS	BDTD	WEB OF SCIENCE
LGPD+ADEQUAÇÃO	2	3910	2	14	3
LGPD+ADEQUAÇÃO+CONTABILIDADE	2	576	0	1	0
LGPD+ADEQUAÇÃO+CONTABILIDADE+ CLIENTES	2	441	0	0	0

Fonte: Elaborado pela autora(2023).

A observação demonstrada na Tabela 1 também é corroborada pela Tabela 2, onde se emprega o termo “Implementação”.

Tabela 2 - Quantidade de artigos publicados de 2018 a 2022 – Termos: “LGPD” e “Implementação”

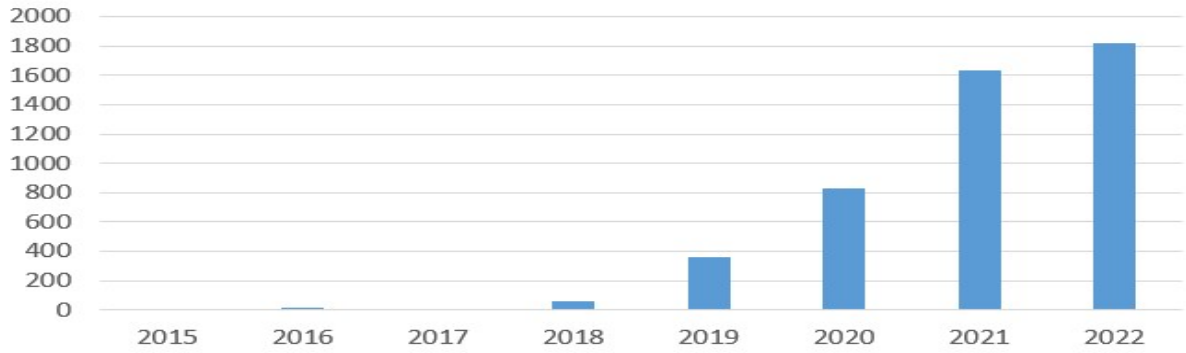
Pesquisas (termos)	SPELL	GOOGLE ACAD.	SCOPUS	BDTD	WEB OF SCIENCE
LGPD+IMPLEMENTAÇÃO	2	5140	0	14	11
LGPD+IMPLEMENTAÇÃO+ CONTABILIDADE	0	739	0	0	1
LGPD+IMPLEMENTAÇÃO+ CONTABILIDADE+ CLIENTES	0	564	0	0	0

Fonte: Elaborado pela autora(2023).

Comparando as tabelas Tabela 1 e Tabela 2, pode-se observar que, conforme se afunila a pesquisa, incluindo os termos “contabilidade” e “clientes” vai reduzindo a quantidade de artigos publicados. Ao investigar os títulos, demonstrou-se que, de fato, a adequação proposta era sobre as organizações contábeis e não mencionavam estas organizações no auxílio aos seus clientes na adequação ou implementação da LGPD. A análise da plataforma da BDTD demonstra que as publicações possuem a mesma quantidade para ambos os termos, porém os conteúdos são diferentes, o que justifica somar “adequação” e “implementação”. Diferente da plataforma Scopus, pois a quantidade apresentada no termo “adequação” está inclusa na pesquisa com o termo “implementação”.

A Figura 1 indica um aumento significativo de publicações com os termos “LGPD” e “implementação” na plataforma de pesquisa Google Acadêmico, passando de 57 publicações em 2018 para 1820 no ano de 2022. Esta crescente quantidade pode ter relação com a criação da LGPD em 2018.

Figura 1 - Quantidade de artigos publicados com os termos “LGPD” e “Implementação” 2015 a 2022 – Google Acadêmico



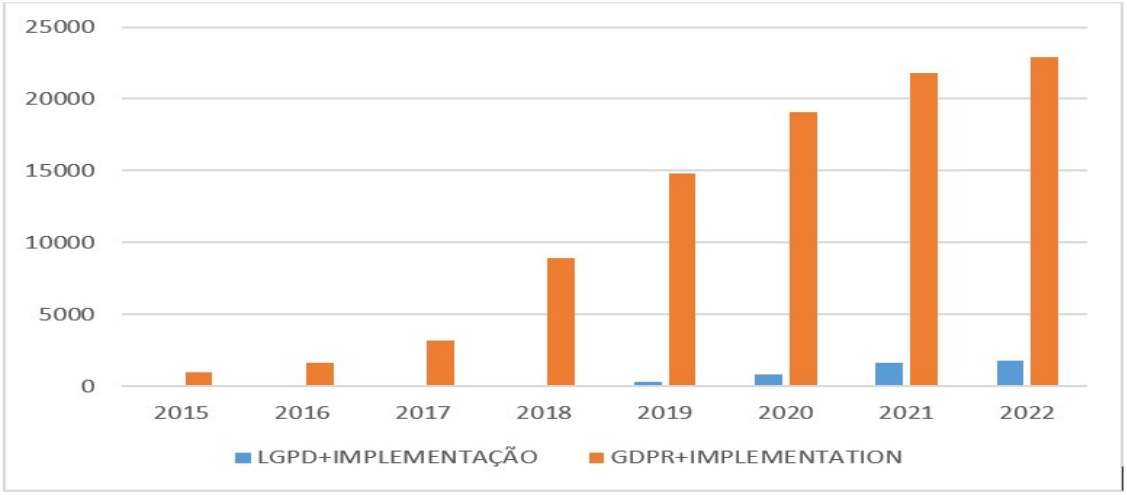
Fonte: Elaborado pela autora(2023).

A Europa é pioneira em publicar a *General Data Protection Regulation* (GDPR), que no Brasil foi reformulada para a LGPD. A publicação de artigos filtrando os termos “GDPR” e “*implementation*” foi muito maior em relação à LGPD, utilizando a mesma plataforma de pesquisa e o mesmo período de tempo.

A primeira proposta da GDPR ocorreu em janeiro de 2012 e a assinatura do regulamento ocorreu em 2016, porém sua vigência teve início somente em 2018 (CABRAL *et al*. 2023). Neste ano a LGPD foi publicada no Brasil, porém a vigência ocorreu em meados de 2020 (BRASIL, 2020). Assim, conforme demonstra a Figura 2,

a partir de 2020, alavancaram as publicações de artigos sobre a LGPD e sua aplicação nas empresas públicas e privadas brasileiras.

Figura 2 - Quantidade de artigos publicados com os termos “LGPD” e “implementação” comparado aos termos “GDPR” e “implementation” 2015 a 2022 – Google Acadêmico



Fonte: Elaborado pela autora(2023).

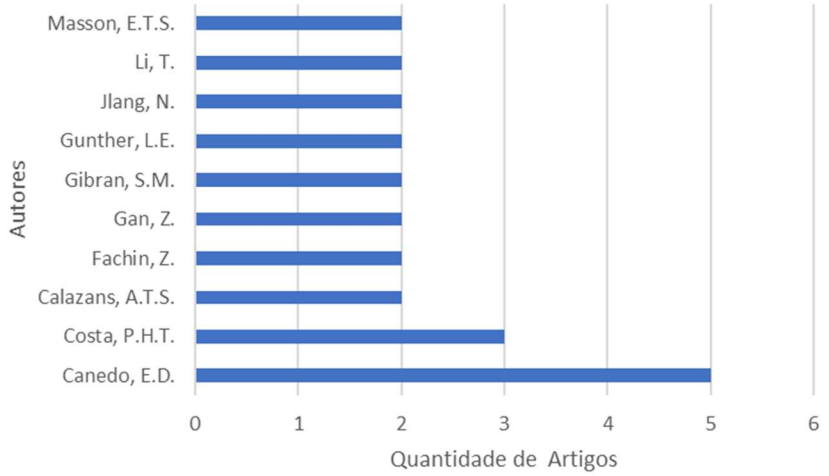
Analisando as plataformas de pesquisa: Scopus, *Web of Science*, Google Acadêmico, *Spell* e a Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), optou-se a análise deste trabalho na base Scopus, por ser reconhecida por sua extensa cobertura de periódicos científicos, conferências e literatura acadêmica, abrangendo várias disciplinas e oferecendo uma ampla gama de métricas e indicadores bibliométricos.

Ao realizar pesquisa na plataforma de pesquisa Scopus utilizando o termo “LGPD” e limitando os resultados aos artigos publicados entre os anos de 2018 e 2022, foi possível identificar, conforme ilustrado na Figura 3, os autores com maior produção científica na área. Entre esses autores, destacam-se Canedo E.D. e Costa, P.H.T, com seus respectivos índices H de 14 e 4. Além disso, observa-se que Canedo E.D. possui o maior número de citações, totalizando 627, o que demonstra grande contribuição para os estudos relacionados à LGPD.

Esses resultados indicam que a produção científica sobre o tema é concentrada em um número reduzido de autores, corroborando com a Lei de Lotka da bibliometria, formulada em 1926 (MACHADO *et al*., 2016). Essa lei estabelece que um

pequeno grupo de autores é responsável por uma parcela significativa da produção científica em determinada área de pesquisa.

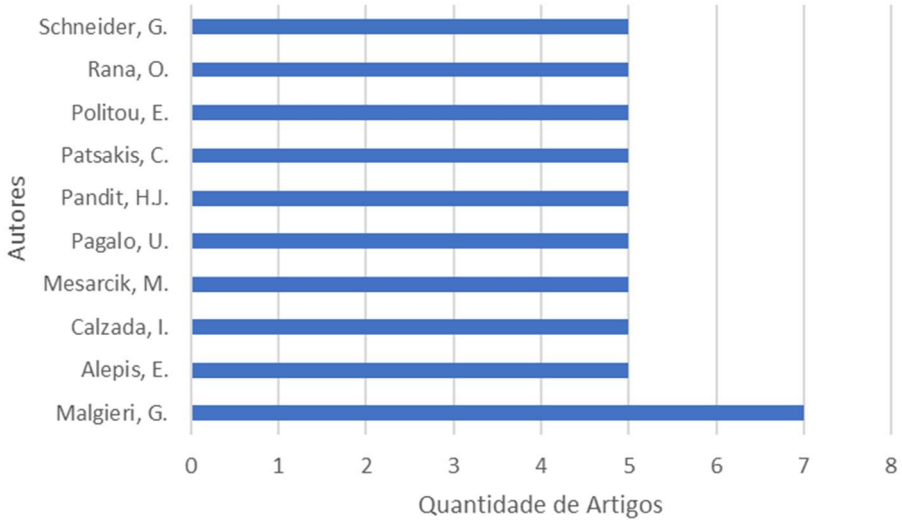
Figura 3 - Quantidade de artigos por autor com o termo LGPD (2018 – 2022)



Fonte: Base Scopus, elaborado pela autora (2023).

Ao comparar as Figura 3 e Figura 4, por meio da mesma plataforma de pesquisa, porém utilizando apenas o termo “GDPR”, pode-se observar uma maior quantidade de publicações por autor.

Figura 4 - Quantidade de artigos por autor com o termo GDPR (2018 – 2022)



Fonte: Base Scopus, elaborado pela autora (2023).

Na pesquisa relacionada ao termo “LGPD”, na Figura 3, o pesquisador com maior número de artigos publicados tinha 5, enquanto no contexto do GDPR, na Figura

4, esse número aumenta para 7. Além disso, os demais autores no âmbito da legislação europeia possuem 5 publicações cada, enquanto no contexto brasileiro esse número cai para 2 publicações.

Ao analisar o aspecto das citações na plataforma Scopus, observa-se que o autor Canedo E.D. possui 627 citações em seus artigos relacionados à LGPD. No entanto, o principal autor da lista referente ao GDPR apresenta 450 citações, e seu índice H é de 11, inferior ao do autor brasileiro.

Esses resultados sugerem que, em termos de quantidade de publicações, há uma maior produção científica sobre o GDPR em comparação com a LGPD. No entanto, mesmo com uma quantidade menor, o autor Canedo E.D. apresenta um número substancialmente maior de citações e um índice H mais elevado, indicando uma maior relevância e impacto de suas contribuições no contexto da LGPD.

Ao examinar a Tabela 3 é possível notar um número reduzido de publicações em periódicos relacionadas à LGPD. No contexto brasileiro, é evidente uma maior quantidade de publicações sobre essa lei em periódicos especializados na área jurídica. Ao analisar a Tabela 4, que apresenta as revistas que publicaram artigos relacionados à GDPR, observa-se uma predominância de periódicos voltados para a área de tecnologia da informação. Esta constatação indica uma forte associação entre a GDPR e temas relacionados à informática e a sistemas de informação.

Tabela 3 - Quantidade de periódicos por termo LGPD (2018-2022)

Revista	**LGPD**	**ISSN**
Civilistica Com	5	2316-8374
Risti Revista Ibérica de Sistemas eTecnologias de Informação	3	1646-9895
Revista de Direito e Desenvolvimento Sustentável	2	2526-0057
Relações Internacionais no Mundo Atual	2	2316-2880
Revista Jurídica	2	2316-753X

Fonte: Base Scopus, elaborado pela autora (2023).

A análise da Tabela 4 revela que o número de publicações em periódicos sobre a GDPR é significativamente maior em comparação com a LGPD. Além disso, verifica-se que, nos periódicos que abordam o termo “GDPR”, há uma ênfase notável nos conceitos de “segurança”, “proteção” e “privacidade”. Essa ênfase não foi identificada nas principais publicações sobre a LGPD, conforme demonstrado na Tabela 3.

Tabela 4 - Quantidade de periódicos por termo GDPR (2018 – 2022)

Revista	GDPR	ISSN
Revisão de leis e segurança de computadores	78	0267-3649
Jornal de proteção de dados e privacidade	72	2398-1679
Revisão da Lei Europeia de Proteção de Dados	65	2364-2831
Acesso IEEE	37	2169-3536
Lei Internacional de Privacidade de Dados	25	2044-3994

Fonte: Base Scopus, elaborado pela autora (2023).

Na Figura 5, foram extraídas as 20 palavras-chave mais utilizadas nos artigos pesquisados, observa-se termos na GDPR que na LGPD ainda não apresenta relevância, é o caso da "*Blockchain*", "Privacidade por *design*", "*Big data*" e "Segurança do computador". A quantidade das palavras-chave nos artigos sobre LGPD apresentam-se tímidos.

Figura 5 - Quantidade e Palavras-chave em artigos por termo GDPR e LGPD (2018-2022)

GDPR	LGPD
RGPD (608)	Proteção de dados (8)
Proteção de dados (279)	LGPD (7)
Privacidade (261)	Dados pessoais (6)
Dados privados (219)	Privacidade (6)
Regulamento Geral de Proteção de Dados (212)	Direitos de Personalidade (4)
Humano (167)	Decisões Automatizadas (3)
Artigo (146)	Dados privados (3)
Humanos (107)	Processamento de dados (3)
Regulamento Geral de Proteção de Dados (104)	Humano (3)
União Europeia (96)	Humanos (3)
Dados pessoais (90)	Lignina (3)
Blockchain (75)	Tecnologia (3)
Inteligência artificial (74)	Adequação (2)
Leis e Legislação (74)	Algoritmos (2)
Privacidade por design (73)	Artigo (2)
Adulto (63)	Inteligência artificial (2)
Segurança do computador (62)	Brasil (2)
Big Data (53)	Lei Geral de Proteção de Dados do Brasil (2)
Consentimento Informado (47)	Estudo controlado (2)
Internet das Coisas (46)	RGPD (2)

Fonte: Base Scopus, adaptado pela autora (2023).

Ao examinar trabalhos com essas expressões (APÊNDICE A – ARTIGOS MAIS CITADOS NA PLATAFORMA SCOPUS COM O TERMO LGPD (2018-2022)) identifica-se que a LGPD é mencionada em uma ampla variedade de setores de negócios, sendo mais proeminente nas áreas da saúde, direito e, também, em

tecnologia da informação. Foram apresentados oito títulos, pois somente estes incluíam citações com o termo “LGPD”. Entre esses títulos, destacam-se algumas palavras-chave de impacto que podem ser consideradas, com base na quantidade de ocorrências da Figura 5, tais como “privacidade do *software*”, “conformidade”, “proteção de dados”, “tratamento de dados pessoais” e “consentimento para tratamento dos dados pessoais”. Essas palavras-chave refletem aspectos base relacionados à LGPD e demonstram sua importância nos estudos e discussões acadêmicas.

Da mesma forma, relacionado à GDPR (APÊNDICE B – ARTIGOS MAIS CITADOS NA PLATAFORMA SCOPUS COM O TERMO GDPR (2018-2022)), verifica-se uma quantidade expressiva de citações para o título “Aprendizado de máquina federado: conceito e aplicações”, totalizando 1813 citações, o que é significativamente superior ao segundo título da lista, que possui 271 citações. Ao pesquisar sobre o primeiro da lista, constata-se que se refere a um artigo publicado em 2019, que propõe a construção de uma rede de dados por meio de inteligência artificial, permitindo o compartilhamento de conhecimento sem comprometer a privacidade do usuário.

A partir dos dados coletados, observa-se um aumento nos estudos relacionados à LGPD no Brasil e à GDPR na Europa, o que indica a relevância do tema. Esses estudos permitem à comunidade acadêmica obter uma compreensão mais abrangente das pesquisas realizadas em diversos cenários, considerando tanto dados pessoais quanto dados pessoais sensíveis. Além disso, é importante ressaltar que o tema possui publicações em diversas bases de dados, ampliando ainda mais o acesso e a disseminação do conhecimento acadêmico sobre o assunto.

Além do campo acadêmico, o tema LGPD é primordial para as operações de empresas públicas e privadas, pois conforme disponibilizado pelo governo federal, no Brasil há 20.191.290 empresas ativas e somente 20% destas empresas estão adequadas à LGPD, é o que mostra uma pesquisa publicada pela Febraban (2022).

Analisando a quantidade de empresas por natureza jurídica ativas no Brasil, conforme Tabela 5, observa-se que cerca de 70% são de empresários individuais e 30% de empresas de sociedade limitada, que alcançam diversas faixas de faturamento. O SEBRAE (2022) apontou que 72% dos empregos estão nas pequenas empresas e que estas são responsáveis por 30% do produto interno bruto (PIB) do Brasil. Empresas de grande porte geralmente têm diversas áreas alocadas

internamente, já empresas de pequeno porte contratam terceiros para execução de rotinas e processos.

Tabela 5 - Quantidade de empresas por natureza jurídica (out/2022)

Microempresas ativas	17.827.788	88,3%
Empresas de pequeno porte ativas	1.073.293	5,3%
Outras ativas	1.290.209	6,4%
Total de empresas ativas	**20.191.290**	**100%**
Empresário Individual	13.956.115	69,1%
Sociedade Limitada	5.935.609	29,4%
Sociedade Anônima	184.568	0,9%
Cooperativa	36.086	0,2%
Demais empresas	78.912	0,4%
Total de empresas ativas	**20.191.290**	**100%**

Fonte: Empresas & Negócios – Mapa de Empresas - Brasil (fev, 2023), adaptado pela autora (2023).

Em pesquisa realizada junto a PNAD (Pesquisa Nacional por Amostra de Domicílios) (IPEA, 2022), em 2022, o Brasil tinha 36,7 milhões de empregados com carteira assinada acima de 14 anos de idade, o que evidencia a existência de menores de idade e, portanto, as empresas que contratam menores de 18 anos respondem à LGPD no quesito dos dados sensíveis.

Estes empregados, tanto menores quanto maiores de 18 anos, possuem seus dados armazenados na empresa empregadora, seja de forma física ou virtual, contendo dados pessoais e dados pessoais sensíveis. As empresas, que não possuem um departamento de pessoal internamente, procuram organizações contábeis para que organizem, além de sua contabilidade, a área de pessoal, que abrange contratação de funcionários, armazenamento de dados pessoais para fins legais, folha de pagamento entre outras atividades, controles e encargos.

Dessa forma, incluiu-se na pesquisa na base Scopus o termo “Contábeis” e “Contabilidade”, com a finalidade de identificar a possibilidade desse segmento de empresa estar ou não contribuindo com a adequação à LGPD em seus clientes. A resposta obtida a partir dessa solicitação não produziu nenhum resultado. Não tendo resultado, a proposta das organizações contábeis contribuir para a adequação à

LGPD em seus clientes micro e pequenas empresas pode ser considerada como inovação.

Para identificar os profissionais contábeis no Brasil, conforme levantamento no Conselho Federal de Contabilidade (CFC, 2023), em janeiro de 2023 havia 526.627 profissionais da área da contabilidade, sendo 375.414 contadores e 151.213 técnicos. Neste mesmo período foram registradas 84.588 organizações contábeis que atendem clientes com diversas demandas. Nesse contexto, as organizações contábeis representam uma participação importante no cenário nacional e podem ser parceiros relevantes para as micro e pequenas empresas, um desses terceiros que são indispensáveis para a continuidade de um negócio, de diversos segmentos.

Esta pesquisa busca propor às organizações contábeis um trabalho que complemente o que já é realizado, além de suas atribuições normais. Eckert *et al*. (2020) enfatizam que o contador moderno pode ter mais possibilidades de serviço e assim expandir a visão operacional adquirida ao longo do processo de desenvolvimento da profissão, se tornando um profissional ativo e estratégico nas organizações, já que estão dentro do negócio do seu cliente.

Este estudo busca ampliar a participação de micro e pequenas empresas na adequação da LGPD e a importância é a segurança dos dados pessoais dos seus clientes, funcionários e terceiros, diminuido o risco de serem penalizadas financeiramente por quaisquer inconformidades. Cumprindo requisitos relulamentares e evidenciando sua preocupação com as informações que estão na empresa, demonstram compromisso com a proteção de dados pessoais gerando melhoria nos seus relacionamentos internos e externos, e assim ser mais competitiva (OCDE/EUROSTAT, 2018). Dessa forma, a proposta é caracterizada como inovadora e deve ser flexível para esse segmento de empresa, permitindo que se adequem à realidade da lei, ajustando à estrutura já existente a um custo baixo, permitindo melhoria de processos ou das condições de trabalho (OCDE/EUROSTAT, 2018), porém, dependendo do grau de ajuste, deve ser aprovado pelos seus gestores. Para isso, buscar uma ferramenta acadêmica que permita a classificação em etapas dessa aplicação, pois conforme busca bibliométrica, não há ferramentas que possibilitem essa adequação.

A presente pesquisa busca fundamentar a relevância das organizações contábeis no contexto da conformidade dos seus clientes com a LGPD. Considerando o conhecimento aprofundado que os profissionais da área contábil possuem acerca

das rotinas, negócios e processos das empresas, pretende-se destacar o papel essencial que desempenham na orientação e assistência aos seus clientes na adoção das medidas para adequação à LGPD e, assim, adotar boas práticas de governança. Nesse sentido, a pesquisa visa enfatizar a importância do tema da proteção de dados pessoais para evitar potenciais penalidades decorrentes do descumprimento da referida legislação, criando um artefato inovador para o cumprimento regulamentar.

1.4 ADERÊNCIA DO PROJETO À LINHA DE PESQUISA

Esta dissertação propõe uma abordagem para a conformidade com a Lei Geral de Proteção de Dados (LGPD) nas organizações, destacando a importância de cumprir as diretrizes estabelecidas. Considera-se que o não cumprimento dessas diretrizes pode resultar em multas substanciais, as quais variam de acordo com o faturamento da empresa. O estudo busca enfatizar a necessidade de implementar medidas adequadas para garantir a conformidade, segurança da informação e evitar as consequências financeiras decorrentes, se beneficiando com a boa governança.

Além dos riscos financeiros, as micro e pequenas empresas podem se beneficiar competitivamente, demonstrando sua preocupação com a segurança da informação e melhoria da qualidade no trabalho com dados pessoais coletados, tanto para clientes internos como externos. A busca bibliométrica demonstrou que não há trabalhos no qual as organizações contábeis estejam adequando à LGPD em seus clientes desse segmento, caracterizando esta proposta como inovadora.

Como se refere às empresas brasileiras e suas rotinas, esta pesquisa se insere na Área do Conhecimento de Ciências Sociais, desta forma, pertencendo ao Programa de Pós-graduação em Administração (PPGA) na linha de pesquisa de Inovação e Competitividade. Esta linha de pesquisa tem por objetivo estudar as dimensões relacionadas à inovação e à competitividade como fontes de crescimento, desenvolvimento e sustentabilidade das organizações. A dimensão Processos desta linha de pesquisa abrange os componentes e recursos relacionados com os processos organizacionais capazes de potencializar a capacidade inovadora das organizações, incluindo a geração e o fluxo de informações, os processos de aprendizagem e a gestão do conhecimento.

Este estudo apresenta uma contribuição específica ao propor uma abordagem que visa facilitar a compreensão e conformidade de um maior número de micro e

pequenas empresas em relação à LGPD, por meio da orientação fornecida pelas organizações contábeis. A proposta busca oferecer suporte e assistência especializada aos clientes das organizações contábeis, visando promover a conformidade com a LGPD. Essa abordagem tem o objetivo de ampliar o acesso e a compreensão da LGPD por parte das micro e pequenas empresas, auxiliando-as no processo de adaptação e cumprimento das disposições legais relativas à proteção de dados, e incorporando essa prática como uma política de boas práticas e de governança corporativa, caracterizando-se como inovadora para esse segmento empresarial.

Destaca-se, ainda, que o produto desta dissertação, o artefato, se caracteriza como uma produção técnica ou tecnológica (PTT), definida por um produto do eixo de produtos e processos que pode ser protegido gerando propriedade intelectual ao autor detalhado no Grupo de Trabalho da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) (BRASIL, 2019), pois assemelha-se a um manual de operação ou até ao desenvolvimento de um processo.

2 REFERENCIAL TEÓRICO

O referencial teórico está constituído por pesquisa em banco de dados de artigos científicos, buscando termos sobre a legislação de proteção de dados pessoais no âmbito brasileiro, propostas de adequação à LGPD nas empresas brasileiras e orientações da Autoridade Nacional de Proteção de Dados (ANPD), desta forma identificar práticas de boa governança. Com isso, apresentam-se conceitos e elementos que possam ser analisados para a formulação de proposta de adequação à LGPD em micro e pequenas empresas por meio das organizações contábeis. A partir da adequação à LGPD espera-se criar uma rotina de boas práticas de governança corporativa, incorporando a inovação como um elemento chave nesse processo.

Como a revisão bibliográfica não apresentou artigos sobre as organizações contábeis adequarem seus clientes à LGPD e também não apresentou propostas de adequação à micro e pequenas empresas e a própria legislação apresenta diferenciações nesse trabalho, buscou-se orientações na Associação Brasileira de Normas Técnicas (ABNT), em especial à NBR ISO/IEC 27001 e subsequentes, que remetem à Segurança da Informação. Essas normas são orientativas para o desenvolvimento da ferramenta proposta nesse trabalho, pois se vinculam à artigos da LGPD e às boas práticas e de governança. Dessa forma, a inovação mescla-se a esses conceitos e ao desenvolvimento do artefato.

2.1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), é uma legislação brasileira que estabelece diretrizes relacionadas ao processamento de dados pessoais, incluindo aqueles realizados em meios digitais, tanto por pessoas naturais como por pessoas jurídicas, sejam elas de natureza pública ou privada (BRASIL, 2018). O propósito essencial da LGPD é salvaguardar os direitos assegurados por lei.

A LGPD tem como fundamento a *General Data Protection Regulation* (GDPR), uma legislação europeia originada a partir de uma proposta legislativa da Comissão da União Europeia, com o objetivo de regulamentar a coleta e o processamento de dados pessoais de seus cidadãos (ZIMMERMANN GHISLENI, 2022). A LGPD foi

inspirada na GDPR e busca estabelecer um arcabouço legal semelhante no contexto brasileiro, com a finalidade de proteger os direitos dos indivíduos em relação aos seus dados pessoais. A referência à origem da GDPR destaca a influência internacional na concepção e implementação da LGPD, contribuindo para a adoção de práticas de proteção de dados em conformidade com os padrões globais.

A LGPD define o que são dados pessoais e dados pessoais sensíveis em seu Art. 5º (BRASIL, 2018), detalhados no subcapítulo 2.1.1. Em ambos dados pessoais, é imprescindível cuidados no tratamento. Havendo dados pessoais, sendo de brasileiros ou não, processados no Brasil, aplica-se a LGPD conforme seu Art. 33 (BRASIL, 2018). O mesmo ocorre se houver transferência de dados pessoais ao exterior.

Conforme determinado no Art. 42 (BRASIL, 2018), a responsabilidade pela proteção dos dados pessoais recai sobre a entidade que os recebe e os processa (controlador) e o operador, recebendo a informação do controlador também deve observar esta legislação.

O consentimento do titular dos dados é indispensável ao controlador e o operador para que haja a coleta da informação. Nesse termo deve constar os dados a serem coletados, a finalidade, o tempo de armazenamento e o prazo para a eliminação, observando o princípio da transparência da LGPD (Quadro 1).

Diversos tipos de dados digitais são gerados, transformados, transmitidos e armazenados em tempo real em todo o mundo (MACIEL, 2019). No contexto empresarial, esses dados podem abranger informações financeiras, indicadores de desempenho, balanços patrimoniais, bem como dados pessoais relacionados a funcionários e diretores. Maciel (2019), resguarda a essa lista, ainda, a proteção do segredo empresarial, que também está no Art. 6º da LGPD (BRASIL, 2018) no princípio da transparência (Quadro 1).

A LGPD reporta um capítulo sobre o tratamento de dados pessoais. A utilização desses dados pessoais deve ser direcionada para fins específicos conforme autorizado pelo titular no seu consentimento. Há alguns exemplos para demonstrar esses conceitos como: implementação de uma assinatura digital por parte de um diretor; atender a requisitos legais relacionados à contratação de um novo funcionário e ao departamento de recursos humanos. Portanto, a gestão eficaz desses dados é indispensável para a operação e conformidade legal de uma empresa.

Esses dados corporativos, de forma geral, são armazenados em um servidor conectado a uma rede, acessível internamente ou através da internet. As rotinas de uma empresa frequentemente requerem o acesso a outras redes, como, por exemplo, plataformas governamentais, como o e-Social, para cadastro de um funcionário, a plataforma de um fornecedor ou parceiro de negócios para inclusão de pedido de compra, e até mesmo para a reserva de um hotel. Todas essas situações envolvem a circulação de dados pessoais, seja no cadastro de um usuário ou transferência de uma informação. Desta forma, a entidade que recebe o dado pessoal tem a responsabilidade de garantir que esta informação esteja segura em sua infraestrutura de tecnologia da informação (CANEDO *at al*., 2023). No entanto, as organizações devem identificar onde estão suas vulnerabilidades para compreender as ameaças potenciais que estão sujeitas e assim implementar estratégias de proteção adequadas para diminuir riscos de invação ou vazamento de dados em sua infraestrutura armazenados (CANEDO *at al*., 2023). Nesse contexto, a LGPD surge como um regulamento para garantir a segurança desses dados.

Em seu Art. 6º, a LGPD (BRASIL, 2018), aponta 10 princípios sobre a atividade de tratamento de dados pessoais que o controlador deve observar. Esses princípios são para orientar boas práticas na conduta da rotina dos negócios, conforme apresentado no Quadro 1 .

Quadro 1 - Princípios da LGPD - Tratamento de dados pessoais (continua)

Princípio	Contextualização
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;	A partir da LGPD não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas. O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados. Ou seja, as empresas devem explicar para que usarão cada um dos dados pessoais. Essas finalidades também devem estar dentro dos limites da lei e devem vir expressamente acompanhadas de todas as informações relevantes para o titular. Além disso, a empresa não está autorizada a modificar a finalidade durante o tratamento. Se uma *startup* solicita o *e-mail* do cliente para a finalidade específica de *login* na plataforma, não pode automaticamente utilizar esse mesmo *e-mail* para enviar publicidade ou ofertas.

(continua)

Princípio	Contextualização
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;	Os dados pessoais tratados devem ser compatíveis com a finalidade informada pela empresa. Ou seja, sua justificativa deve fazer sentido com o caráter da informação que você pede. Por exemplo: se o negócio é um *e-commerce* de produtos eletrônicos, dificilmente será justificável pedir dados de saúde aos usuários. Então, se não é compatível, o tratamento se torna inadequado.
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;	As empresas em geral devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades. Procurar fazer uma ponderação entre o que é realmente essencial para o seu negócio e o que é apenas conveniente. Quanto mais dados forem coletados e tratados, maior será a responsabilidade do controlador, inclusive em casos de vazamentos e incidentes de segurança.
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;	A pessoa física, titular dos dados, tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito. Além disso, devem ser especificadas questões como: o que a empresa faz com as suas informações, de que forma o tratamento é realizado e por quanto tempo.
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;	Deve ser garantido aos titulares que as informações que a empresa tenha sobre eles sejam verdadeiras e atualizadas. É necessário ter atenção à exatidão, clareza e relevância dos dados, de acordo com a necessidade e com a finalidade de seu tratamento.

(continua)

Princípio	Contextualização
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;	Todas as informações passadas pela empresa, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras. Além disso, a empresa não pode compartilhar dados pessoais com outras pessoas de forma oculta. Se você repassa dados pessoais para terceiros, inclusive para operadores que sejam essenciais para a execução do serviço, o titular precisa saber.
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;	É responsabilidade das empresas buscar procedimentos, meios e tecnologias que garantam a proteção dos dados pessoais de acessos por terceiros, ainda que não sejam autorizados, como nos casos de invasões por *hackers*. Além disso, devem ser tomadas medidas para solucionar situações acidentais, como destruição, perda, alteração, comunicação ou difusão dos dados pessoais de suas bases.
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;	O princípio da prevenção objetiva que as empresas adotem medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados pessoais. Ou seja, as empresas devem agir antes dos problemas e não somente depois.
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;	Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares. A própria LGPD já criou regras específicas para o tratamento de dados que frequentemente são utilizados para discriminação, os chamados dados pessoais sensíveis, como os que tratam 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 e dado genético ou biométrico.

(conclusão)

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.	Além da preocupação em cumprir integralmente a Lei, as empresas devem ter provas e evidências de todas as medidas adotadas, para demonstrarem a sua boa-fé e a sua diligência. Alguns exemplos estão na comprovação que fizeram treinamentos de equipe, a contratação de consultorias especializadas, a utilização de protocolos e sistemas que garantam a segurança dos dados e o acesso facilitado do titular à empresa sempre que preciso.

Fonte: LGPD (BRASIL, 2018); Nunes(2019). Adaptado pela autora (2023).

Os princípios abordados no Quadro 1 fornecem diretrizes de como o controlador tem a obrigação da ciência da LGPD e todo o cuidado com os dados pessoais que for coletar. Nunes (2019) contextualiza cada princípio da LGPD e enfatiza que a empresa, através de seus profissionais, tem que compreender e internalizar a intenção da LGPD nos seus modelos de negócio e o tratamento de dados na prática.

A Constituição Federal (BRASIL, 1988) estabelece diretrizes para a proteção de dados pessoais, impondo restrições à liberdade de expressão e garantindo a proteção à imagem, à honra, à intimidade e à privacidade. Além disso, assegura o direito de resposta e indenização em casos de abuso. No entanto, a emergência da sociedade da informação transformou completamente os comportamentos, fundindo espaços públicos e privados, gerando uma sociedade confessional e criando danos colaterais da modernidade (BAUMAN, 2013). Nesse contexto, as redes sociais exemplificam a exposição da intimidade de um indivíduo. Portanto, é importante diferenciar entre uma informação que é pública e uma informação que foi publicizada.

O Sistema Nacional para Transformação Digital (SNTD) (BRASIL, 2018), por meio do decreto número 9.139, postula que o desenvolvimento econômico e social sustentável e inclusivo, impulsionado pela inovação, requer confiança no ambiente digital. Para isso, é forçoso uma ação governamental focada na proteção de direitos e privacidade, bem como na defesa e segurança no ambiente digital, abrangendo os dados pessoais e fortalecendo a segurança cibernética no país. Assim, a LGPD surge como uma resposta aos anseios elencados para a segurança jurídica no ambiente

digital brasileiro, estabelecendo a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2019), uma autarquia vinculada à Presidência da República, responsável por fiscalizar o cumprimento da LGPD.

A fiscalização e a aplicação de penalidades por descumprimento da LGPD é de responsabilidade da Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Esta entidade tem tarefas de orientar e regular a aplicação da LGPD, detalhado no subcapítulo 2.1.3.

2.1.1 Termos utilizados na LGPD

A LGPD emprega terminologia precisa visando promover um melhor entendimento e, consequentemente, uma melhor adequação das normas estabelecidas. Essa abordagem terminológica busca proporcionar clareza e precisão na definição dos direitos, deveres e responsabilidades relacionados à proteção de dados pessoais, contribuindo para uma interpretação mais precisa e uma implementação efetiva das disposições da lei. Maciel (2019) classifica esses termos e os define:

Quadro 2 - Termos utilizados na LGPD

(continua)

Termo	**Definição**
Banco de dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
Operador	(Processor): pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

(conclusão)

Encarregado	Também chamado de *Data Protection Officer* (DPO): pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados .
Agentes de tratamento	É o controlador e o operador.
Anonimização	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
Eliminação	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
Relatório de impacto à proteção de dados pessoais (RIPD)	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.
Autoridade Nacional	É o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei. (ANPD – Autoridade Nacional de Proteção de Dados)
Tratamento de dados	É toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Fonte: Maciel (2019, p.19) adaptado pela autora (2023).

Além desses termos, há outras terminologias que estão apresentadas no GLOSSÁRIO. Maciel (2019), fornece uma definição dos dados pessoais e apresenta critérios para sua identificação, conforme exposto a seguir:

> Dado pessoal é toda informação que pode identificar um indivíduo ainda que não diretamente. Portanto, incluem-se na referida definição, por exemplo, os números de *Internet Protocol* – IP, número de identificação de funcionário dentro de uma empresa, e até mesmo características físicas. Isso em razão da presença do léxico "identificável", que amplia a definição de dados pessoais (MACIEL, 2019, p.25).

A LGPD (BRASIL, 2018) também traz a definição do que é um dado pessoal: "informação relacionada a pessoa natural identificada ou identificável" portanto, qualquer informação que possa identificar um indivíduo.

De acordo com a LGPD (BRASIL, 2018), determinadas categorias de dados são consideradas sensíveis, tais como "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados relacionados à saúde ou vida sexual, dados genéticos ou biométricos". Esses dados sensíveis possuem um nível de proteção adicional devido à sua natureza particular. Conforme apontado por Maciel (2019), para o tratamento desses dados é imprescindível obter o consentimento específico do titular, conforme também estabelecido pela legislação, tanto para dados pessoais quanto para dados pessoais sensíveis.

Nesse contexto, o controlador de dados, ao realizar a coleta de informações pessoais, está obrigado a obter o consentimento do titular dos dados, detalhado na própria LGPD nos artigos 7º, 8º, 9º e 11º (BRASIL, 2018). Esse consentimento deve ser solicitado de maneira escrita, clara e específica. Na prática, pode-se utilizar um "Termo de Consentimento" para uso documental para assinatura. Em sites da internet observa-se a utilização de "*cookies*", definidos por Fontaínhas, Andrade e Almeida (2016) de "testemunhos de conexão", onde coletam dados de navegação e, também, dados pessoais, e, como praxe, se o usuário optar por permanecer no site, deve clicar em "aceitar *cookies*", mas antes deve-se ler a "Política de Privacidade" (SIEBRA; XAVIER, 2020) do site para verificação de quais informações coletam e para qual finalidade. Esse termo deve apresentar de forma transparente a finalidade da coleta dos dados, informando ao titular quais informações serão coletadas, como serão utilizadas e por quanto tempo serão retidas pelo controlador. Além disso, o termo deve permitir ao titular a possibilidade de solicitar a exclusão dos seus dados, conforme meios previamente estabelecidos e apresentados no documento.

2.1.2 Relatório de Impacto à Proteção de Dados

Com o objetivo de assegurar a conformidade do controlador com as diretrizes estabelecidas pela LGPD, esta legislação, no Art. 5, XVII, prevê a elaboração do Relatório de Impacto à Proteção de Dados (RIPD) (BRASIL, 2018). O RIPD é um documento que deve ser elaborado pelo controlador e tem como finalidade evidenciar as medidas e ações adotadas para proteger os dados pessoais em conformidade com as exigências da LGPD. Esse relatório visa identificar e avaliar possíveis riscos e impactos relacionados ao tratamento de dados pessoais, bem como propor medidas mitigadoras e de conformidade para proteger a privacidade e os direitos dos titulares de dados (MACIEL, 2019). A elaboração do RIPD é uma medida necessária para garantir a transparência e a responsabilidade no tratamento de dados, demonstrando o compromisso do controlador com a proteção de dados estabelecida pela LGPD.

> 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 (BRASIL, 2018, p. 3) (Art. 5 inciso XVII) […] o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (BRASIL, 2018, p. 13) (Art. 38 Parágrafo único).

O RIPD é um documento que pode ser requerido pela ANPD ao controlador (BRASIL, 2018). Esse relatório deve conter informações detalhadas sobre o tratamento de dados pessoais, inclusive aqueles considerados sensíveis, quando o tratamento é fundamentado no interesse legítimo do controlador, conforme Art. 10º da LGPD (BRASIL, 2018). O RIPD tem como objetivo evidenciar o ciclo de vida dos dados, ou seja, o trajeto percorrido pelos dados desde a sua coleta até a sua possível eliminação (ABNT NBR ISO/IEC 27000, 2013). Nesse relatório, devem ser apresentadas informações sobre as etapas do tratamento, as medidas de segurança adotadas, a finalidade do tratamento, bem como eventuais riscos e impactos identificados e as medidas de mitigação implementadas. O RIPD tem como propósito fornecer uma visão abrangente do processamento de dados realizado pelo controlador, com ênfase na transparência e na responsabilidade no tratamento de dados pessoais (MACIEL, 2019).

A LGPD estabelece que o controlador de dados deve implementar um programa de governança em privacidade, conforme disposto no artigo 50º, inciso I (BRASIL, 2018). Esse programa deve demonstrar o compromisso do controlador em adotar processos e políticas internas que garantam o cumprimento das normas e boas práticas relacionadas à proteção de dados pessoais (MACIEL, 2019). O programa de governança em privacidade pode ser estruturado de forma abrangente, levando em consideração as regulamentações aplicáveis e as melhores práticas no campo da proteção de dados. Através desse programa, o controlador pode estabelecer políticas e salvaguardas apropriadas, com o objetivo de promover a confiança do titular dos dados por meio de uma atuação transparente (BRASIL, 2018).

A documentação para a aplicação da LGPD não é explicitamente mencionada, entretanto, o Artigo 55-J desta lei, atribui responsabilidade à ANPD sobre a Política Nacional de Proteção de Dados Pessoais e Privacidade (BRASIL, 2018). Tal responsabilidade está ancorada na Constituição Federal Brasileira que assegura o direito humano à privacidade, à preservação da vida privada e da intimidade (BRASIL, 1988). A privacidade encontra-se ameaçada, especialmente em virtude dos meios digitais, o que dificulta cada vez mais a proteção das informações pessoais:

> Com o desenvolvimento da tecnologia e intensificação dos fluxos de informação, surgem novas possibilidades de armazenamento, utilização e manipulação de informações pessoais, refletindo em mudanças no conceito de direito à privacidade, de modo que a informação que antes era dispersa, torna-se organizada. Riscos que envolvem a violação à privacidade e à personalidade dos cidadãos na sociedade da informação crescem exponencialmente, como a possibilidade de uso indevido dos dados pessoais, cadastro e classificação dos indivíduos, propagandas de marketing invasivas, publicidade comportamental, vigilância estatal, utilização indevida da *Big Data*, coleta de dados através da Internet das coisas, entre outros (FINKELSTEIN; FINKELSTEIN, 2020, p.285).

A existência de uma legislação que busca proteger os dados pessoais confronta-se com a prática de coleta de informações das empresas para várias finalidades, conforme evidenciado por Finkelstein e Finkelstein (2020). Em um mundo cada vez mais digital, cabe ao controlador estabelecer políticas e termos de aceitação para que o titular possa decidir se deseja continuar a navegar em um determinado site ou fornecer seu currículo vitae para uma empresa, estipulando um prazo para a eliminação de seus dados, por exemplo.

A LGPD não estabelece um modelo específico de RIPD, porém indica os temas principais que devem ser abordados nesse documento. Cada empresa é

responsável por elaborar e organizar o RIPD de acordo com suas diretrizes cabendo cada empresa a montagem e organização desse documento de acordo com as diretrizes da legislação.

2.1.3 Autoridade Nacional de Proteção de Dados (ANPD)

A ANPD é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, é o que menciona o Art. 5º desta lei (BRASIL, 2018). Portanto, é o que orienta, fiscaliza e aplica sanções. Maciel complementa:

> […] a autoridade não teria apenas a função de aplicar as sanções – lembramos que não devem ser as sanções as únicas motivações para as organizações buscarem adequação – como também, e principalmente, a de regulamentar pontos fundamentais da lei, definindo padrões técnicos e procedimentos. A criação de uma autoridade de proteção de dados é, inclusive, um dos requisitos para considerar um país adequado para tratar dados sob o espeque da legislação europeia, que prevê além da existência de um sistema jurídico protetivo, também a existência de autoridades de controle (MACIEL, 2019, p.75).

Apesar do propósito de proteger os dados pessoais, a ausência de penalidades desencorajaria as empresas a investirem tempo e recursos na conformidade com a legislação (MACIEL, 2019). As sanções previstas em caso de não cumprimento da LGPD abrangem uma ampla gama de medidas punitivas, incluindo advertências com prazo para adoção de medidas corretivas e imposição de multas. O Art. 52 da LGPD detalha as sanções:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018, p. 16).

Essas sanções visam assegurar a aplicação efetiva da LGPD, incentivando as empresas a adotarem medidas de conformidade e garantindo a proteção dos direitos dos titulares de dados pessoais.

Dessa forma, a adoção de práticas de boa governança possibilita comprovar a boa fé do controlador, é o que apresenta o Art. 52 da LGPD (BRASIL, 2018). A implementação de medidas eficazes de governança em privacidade, em conformidade com as disposições da LGPD, demonstra o comprometimento do controlador em promover a proteção dos dados pessoais e o respeito aos direitos dos titulares (BRASIL, 2018). A boa governança engloba a adoção de políticas e processos internos adequados, a implementação de salvaguardas técnicas e organizacionais, a designação de responsáveis pela proteção de dados e a transparência nas práticas de tratamento de dados. Ao adotar tais práticas, o controlador pode estabelecer uma cultura de conformidade e demonstrar sua intenção de agir de acordo com os princípios e requisitos legais de proteção de dados, fortalecendo assim a confiança dos titulares e das autoridades reguladoras (MACIEL, 2019).

Conforme o Art. 44º da LGPD (BRASIL, 2018), a ANPD conta com o suporte técnico e administrativo da Casa Civil da Presidência da República no desempenho de suas atribuições. Essa disposição legal visa fornecer à ANPD o respaldo para o exercício de suas atividades, incluindo o desenvolvimento de regulamentos, diretrizes e orientações relacionadas à proteção de dados pessoais. A colaboração com a Casa Civil da Presidência da República proporciona à ANPD recursos e *expertise* adicionais para garantir a eficácia de suas ações e a implementação adequada da LGPD no contexto brasileiro.

2.2 CLASSIFICAÇÃO DAS EMPRESAS

No Brasil, a classificação fiscal de uma empresa é determinada pela Lei nº 123 de 2006 (BRASIL, 2006), que estabelece diretrizes específicas para as empresas de micro e pequeno porte. Entre outras atribuições, essa lei estabelece a apuração e recolhimento de impostos em regime único de arrecadação, além de facilitar o acesso

ao crédito e ao mercado. Para se enquadrar em uma das categorias definidas, existem limitações relativas ao faturamento e ao número de funcionários. A regulamentação, controle e fiscalização dessas empresas são realizadas por meio de comitês e representantes designados pelo governo federal, estadual e municipal (BRASIL, 2006).

Além de estarem cadastradas no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, são consideradas micro e pequenas empresas as que possuem sociedade empresária, sociedade simples e empresa individual de responsabilidade limitada (BRASIL, 2006).

O Quadro 3 demonstra a categorização da organização com base em sua receita operacional bruta anual, especificamente para micro e pequenas empresas. O tamanho da empresa é definido conforme o seu faturamento, tendo variações conforme o tipo de atividade do negócio da empresa. Em sua estrutura jurídica, na microempresa, há possibilidade do empresário possuir ou não sócios, aderindo a tipos jurídicos como sociedades limitadas. A legislação atual também inclui o regime de Microempreendedor Individual (MEI). Para efeitos de classificação, esse regime é considerado uma microempresa se a receita bruta anual não exceder a R$ 81.000,00 (BRASIL, 2006).

Quadro 3 - Classificação das empresas por receita

Classificação	Receita Bruta
Microempresa	Igual ou inferior a R$ 360.000,00
Empresa de Pequeno Porte	Entre R$ 360.001,00 a R$ 4.800.000,00

Fonte: SEBRAE (2023), adaptado pela autora.

As microempresas e empresas de pequeno porte estão sujeitas a opções de regimes tributários disponíveis no contexto brasileiro. Essas empresas podem optar pelo Simples Nacional, Lucro Presumido ou Lucro Real (Quadro 4), de acordo com as características específicas de suas atividades nos setores de serviços, comércio ou indústria (SEBRAE, 2023).

Quadro 4 - Classificação tributária das empresas

Simples Nacional	Lucro Presumido	Lucro Real
Unifica cálculo de tributos como: IRPJ, CSLL, PIS/PASEP, COFINS, IPI, ICMS, ISSQN e a Contribuição para a Seguridade Social destinada à Previdência Social a Cargo da Pessoa Jurídica	Se presume uma estimativa de lucro que variam de 1,6% a 32% da Receita Bruta.	Indicado para empresas de maior porte ou complexidade financeira maior.
O empresário paga uma única forma através do DAS (Documento de Arrecadação do Simples Nacional)	O pagamento é realizado trimestralmente.	A empresa paga impostos de acordo com o ganho efetivo, descontando as despesas e os custos do período.
É um regime tributário diferenciado para as Microempresas e Empresas de Pequeno Porte, previsto na Lei Complementar nº 123, de 14 de dezembro de 2006	É necessário verificar a atividade.	É necessário verificar a atividade.

Fonte: SEBRAE (2023) adaptado pela autora.

É de extrema importância exercer cautela na aplicação das regras tributárias, especialmente no que se refere aos limites de faturamento estabelecidos para cada regime. A escolha adequada do regime tributário e o monitoramento constante do faturamento são essenciais para garantir a conformidade fiscal e evitar eventuais penalidades ou sanções relacionadas ao não cumprimento das obrigações tributárias (SEBRAE, 2023). Portanto, é imprescindível que as microempresas e empresas de pequeno porte estejam atentas aos aspectos tributários e realizem uma análise criteriosa das opções disponíveis, de modo a se adequar à legislação fiscal vigente. Dessa forma, podem utilizar-se de benefícios da LGPD para a sua categoria.

2.3 LGPD EM MICRO E PEQUENAS EMPRESAS

Todas as organizações, sem distinção de porte, têm a capacidade de armazenar informações relacionadas a clientes, fornecedores e funcionários, o que inevitavelmente envolve o tratamento de dados pessoais de indivíduos (BRASIL, 2018). Essa realidade não é diferente para as microempresas e empresas de pequeno

porte. Para a Confederação Nacional da Indústria (CNI, 2020) , independentemente do tamanho da empresa, a coleta, o armazenamento e o processamento de dados pessoais são atividades comuns e necessárias para o funcionamento adequado de seus negócios. Ainda nesse segmento de empresa, também estão sujeitas às disposições legais relativas à proteção de dados pessoais, conforme estabelecido pela legislação vigente (BRASIL, 2018). Portanto, é imprescindível que essas empresas estejam cientes de suas obrigações legais e adotem medidas apropriadas para garantir a conformidade com as normas de proteção de dados, promovendo a privacidade e a segurança das informações pessoais de seus *stakeholders*.

Ao cadastrar um cliente pessoa física e obter o número de telefone, por exemplo, uma empresa já se sujeita à LGPD, uma vez que tal informação diz respeito a uma pessoa natural identificada ou identificável (BRASIL, 2018). Além disso, se a informação coletada envolver dados sensíveis, como o tipo sanguíneo de um funcionário, a empresa também estará sujeita às disposições da lei (BRASIL, 2018).

Apesar disso, as micro e pequenas empresas podem adotar uma política simplificada de segurança da informação, contanto que atendam a requisitos essenciais para o tratamento de dados pessoais (BRASIL, 2022), e podem ser dispensadas da indicação de um encarregado de dados (DPO), desde que disponibilizem um canal de comunicação com o titular dos dados. A designação de um DPO, no entanto, é considerada uma prática de boa governança pela ANPD. Em outras palavras, a dispensa de alguns dispositivos da LGPD para as micro e pequenas empresas não as exime das disposições legais, regulatórias e contratuais relacionadas à proteção de dados.

Portanto, as micro e pequenas empresas têm a obrigação de se adequar à LGPD, pois a coleta, armazenamento ou tratamento de qualquer dado pessoal está sujeita às disposições da lei.

2.4 PAPEL DAS ORGANIZAÇÕES CONTÁBEIS NA GESTÃO DE MICRO E PEQUENAS EMPRESAS

As organizações contábeis prestam uma série de serviços, que incluem escrituração contábil, conciliação de contas, elaboração de demonstrações financeiras, declarações fiscais, contabilidade gerencial, obrigações acessórias e eletrônicas, bem como a gestão do departamento fiscal, que é considerado um setor

de risco dentro dessas organizações, devido às elevadas penalidades impostas pelo poder público (WRUBEL; TOIGO; LAVARDA, 2015). Para realizar essas atividades, as organizações contábeis prestam serviços terceirizados que seguem as normas estabelecidas pelo Conselho Regional de Contabilidade (CRC) e pela legislação do Conselho Federal de Contabilidade (CFC).

Dentre as rotinas desempenhadas pelas organizações contábeis, destaca-se o serviço de departamento de pessoal, que deve estar em conformidade com as normas da Consolidação das Leis do Trabalho (CLT) (BRASIL, 1943). A CLT oferece diretrizes que vão desde a contratação até após o processo de desligamento de um funcionário. Ao longo desse ciclo, há diversas atividades a serem executadas, conforme destacado por Brogio e Mello (Figura 6).

Em contexto empresarial, as organizações contábeis têm a responsabilidade de orientar o seu cliente, e na sequência, realizar diversas rotinas, e as do departamento de pessoal estão representadas pela Figura 6. Além disso, o contador possui um papel vital na gestão de seus clientes, envolvendo o cuidado das finanças, conhecimento do negócio e transmissão de postura profissional e ética, com acesso às informações, rotinas e processos dos clientes (NICOLAU; COUTO, 2018).

Figura 6 - Ciclo da administração de pessoas

Fonte: BROGIO; MELLO (2016, p.4)

As organizações contábeis também devem se adequar à LGPD. Do ponto de vista desta lei, estas entidades detêm informações de suma importância sobre seus clientes e ainda tem que provar que estão operando no âmbito da legalidade (RIBEIRO; MOREIRA, 2020). Dessa forma, Ferreira (2019, p.2) contribui que “gerir adequadamente a documentação é fundamental para a comunicação entre o cliente e o escritório”, e ainda acrescenta “investir na segurança dos dados pessoais por meio de uma plataforma contábil, fazer uma boa gestão dos tributos e do financeiro, organizar e reter adequadamente estes arquivos pode ajudar na segurança e proteção dos dados”.

Desta forma, as organizações contábeis são reconhecidas como operadores de acordo com a LGPD (BRASIL, 2018). Estas entidades recebem dados dos clientes, que abrangem tanto o contexto corporativo quanto informações pessoais, incluindo dados pessoais sensíveis, uma vez que isso faz parte de suas responsabilidades. Uma vez que, muitos dos seus clientes, principalmente micro e pequenas empresas, tomam ciência da alteração de qualquer legislação, quase que exclusivamente, através do seu contador.

Além disso, a organização contábil, enquanto empresa, é também considerada controladora perante a LGPD. Como prestadora de serviços, pode ser classificada como micro ou pequena empresa, e eventualmente, como média ou grande empresa.

Portanto, a conduta ética e profissional do contador pode proporcionar uma orientação eficaz sobre a LGPD aos seus clientes, fornecendo diretrizes claras e práticas para a adequação à legislação. Isso por sua vez, pode reduzir o risco de aplicação de multas e penalidades, tanto para a organização contábil quanto ao seu cliente.

2.5 INOVAÇÃO E A LGPD

Paredes, Santana e Fell (2014) estabelecem que a inovação é um ativo multifacetado que contribui para o desenvolvimento e manutenção do relacionamento da organização com seus clientes. No Manual de Oslo (OCDE/Eurostat, 2018, p.22) o termo inovação pode significar “tanto uma atividade como o resultado de uma atividade”, podendo contemplar a criação de algo novo ou aprimorado, incluindo o

desenvolvimento de novos produtos, a implementação de processos mais eficientes ou a introdução de serviços inovadores.

A inovação desempenha uma orientação estratégica para superar desafios, permitindo às organizações entrarem em novos mercados, aumentando sua participação para obter uma vantagem competitiva (GUNDAY *at al*., 2011). Uma inovação empresarial "é um produto ou processo de negócio novo ou melhorado que difere significativamente dos produtos ou processos de negócios anteriores da empresa e que foi introduzido no mercado ou colocado em uso pela empresa" (OCDE/Eurostat, 2018, p.68).

No mínimo, as inovações devem incorporar características que não foram previamente disponibilizadas pela organização em questão aos seus usuários. Essas características podem ser novas ou não para a economia, a sociedade ou um mercado específico. Uma inovação pode ser fundamentada em produtos e processos que já foram utilizados em outros contextos, como em outros mercados geográficos ou de produtos. Nesse caso, a inovação representa um exemplo de difusão (OCDE/Eurostat, 2018), se espalhando por meio de uma cultura ou sociedade.

O Manual de Oslo considera quatro tipos de inovação: produto, processo, oganizacional e de marketing. Na última versão desse manual, reduz a complexidade do conceito de inovação para somente dois tipos principais, produtos ou processos de negócios (OCDE/Eurostat, 2018), conforme demonstrado no APÊNDICE E – COMPARAÇÃO DOS TIPOS DE INOVAÇÃO DAS 3ª E 4ª EDIÇÕES DO MANUAL DE OSLO.

Para Gunday *at al*. (2011, p.1), as "inovações de produtos e processos estão intimamente relacionadas ao conceito de desenvolvimento tecnológico". Uma inovação de produto refere-se à introdução no mercado de um serviço ou um bem que se apresenta como uma novidade ou com melhorias significativas em relação às suas características ou funcionalidades (OCDE/Eurostat, 2018).

Essa pesquisa se encaixa na inovação de produtos e processos, por se tratar da criação de um artefato que permite auxiliar às micro e pequenas empresas se adequarem à LGPD através de suas organizações contábeis terceirizadas. Isso porque oferece uma solução nova e melhorada para um desafio regulatório, ajudando esse segmento de empresas, além de se adequarem à legislação de proteção de dados, melhorar a eficiência e a segurança dos processos de gestão de dados. O artefato contribui também na gestão de projetos, pois pode incluir a implementação

de processos e sistemas que possam garantir a segurança da informação. Dessa forma, esses processos podem promover a melhora da organização e eficiência dos projetos adotando práticas de governança.

Ao integrar o conceito de inovação com a LGPD, torna-se evidente que a segurança dos dados dos clientes, especialmente no caso de indivíduos, é um elemento básico para fortalecer o relacionamento com os mesmos. Portanto, a inovação e a proteção de dados são componentes interdependentes na construção de relações sólidas e confiáveis com os clientes.

Assim, se categorizam como operação de apoio que gera vantagens competitivas, crescimento e desenvolvimento econômico das empresas (RUFFONI; REICHERT, 2018), pois o Brasil, tendo uma lei de proteção de dados e as empresas se adequando, pode abrir oportunidades em negócios nacionais e internacionais.

Além de atender as normas jurídicas brasileiras, a conformidade com a LGPD pode assegurar oportunidade ao buscar expandir negócios em outros países. As inovações, conforme o Manual de Oslo (OCDE/Eurostat, 2018, p. 46), “derivam de atividades baseadas no conhecimento que envolvem a aplicação prática de informações e conhecimentos existentes ou recentemente desenvolvidos”. As informações podem ser classificadas como o mapeamento dos processos na LGPD (BRASIL,2018), pois consistem em “dados organizados que podem ser produzidos e transferidos entre organizações a baixo custo” (OCDE/Eurostat, 2018, p. 46). E o conhecimento pode se referir à LGPD no que tange “à compreensão da informação e à capacidade de usá-la para diferentes propósitos”.

> O conhecimento é obtido através do esforço cognitivo e, consequentemente, novos conhecimentos são difíceis de transferir porque requerem aprendizagem por parte de quem os recebe. Tanto a informação como o conhecimento podem ser obtidos ou criados dentro ou fora de uma organização relevante (OCDE/Eurostat, 2018, p. 46).

Considerando a inovação como uma atividade econômica, ela requer recursos que poderiam ser alocados para outros propósitos. A presença de custos de oportunidade sugere a intenção subjacente de buscar alguma forma de criação ou preservação de valor por parte dos atores responsáveis pela inovação (OCDE/Eurostat, 2018). Assim, a inovação é, portanto, uma atividade orientada para a criação de valor (OCDE/Eurostat, 2018). Nesse contexto, a criação de valor está no

aprimoramento do conhecimento do negócio através do uso de um artefato, oportunizando conscientização e a governança corporativa.

O grau das inovações pode ser medido em termos de sua novidade ou do seu impacto econômico. O Manual de Oslo (OCDE/Eurostat, 2018, p.77) destaca que devem ser consideradas “se uma inovação é nova apenas para a empresa, nova para o mercado da empresa ou nova para o mundo; a expectativa da empresa quanto ao potencial para transformar o mercado que opera ou quanto ao potencial para melhorar a sua competitividade”.

Dessa forma, o artefato oferece uma solução única, pois nas pesquisas bibliográficas realizadas não foram identificados artigos ou trabalhos acadêmicos com o objetivo de auxiliar a adequação da LGPD em micro e pequenas empresas através das organizações contábeis, caracterizando sua originalidade. O impacto da aplicação do artefato é o aumento do nível de melhoria da eficiência, segurança e conformidade com a legislação. A tecnologia adotada no artefato é simples e de baixo custo, o que permite maior acessibilidade das empresas desse segmento. Assim, o artefato atende os requisitos de inovação de forma positiva e significativa, conforme definição no Manual de Oslo (OCDE/Eurostat, 2018).

Portanto, a empresa, ao iniciar o movimento de adequação à LGPD já está iniciando uma atividade inovadora, pois além da conscientização sobre a legislação e seus impactos, inicia-se uma revisão de processos e identifica-se caminho que um dado pessoal percorre na empresa. Criam-se documentos, revisam-se contratos, a área de TI é questionada sobre seus processos e a própria direção da empresa revisa suas autorizações, profissionalizando ainda mais a empresa.

2.6 GOVERNANÇA CORPORATIVA E A LGPD

O fundamento da governança corporativa é a ética, que “abrange um conjunto de valores e princípios que orienta a conduta e viabiliza o convívio e a evolução do ser humano em sociedades cada vez mais complexas”, é o que define o Código das Melhores Práticas de Governança Corporativa elaborado pelo Instituto Brasileiro de Governança Corporativa (IBGC) (IBGC, 2023, p.15). Dessa forma, o IBGC traz o seguinte conceito:

> Governança corporativa é um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral. Esse sistema baliza a atuação dos agentes de governança e demais indivíduos de uma organização na busca pelo equilíbrio entre os interesses de todas as partes, contribuindo positivamente para a sociedade e para o meio ambiente (IBGC, 2023, p.17).

Partindo desse conceito, pode-se fazer uma fusão entre a governança corporativa e a LGPD, pois a própria legislação remete a seção II que trata de boas práticas e de governança. Neste enfoque, pode-se trabalhar na conscientização e adequação à LGPD e fazer com que esta prática faça parte da governança da empresa. Zimmermann Ghisleni (2022, p.5) afirma que esta prática "pode ser usada para a prevenção de conflitos entre *stakeholders*, estruturas de poder desproporcionalmente concentradas, degeneração da imagem frente aos investidores e consumidores, tomada de decisões". Dessa forma, o IBGC (2023) recomenda cinco princípios para a aplicação da governança corporativa: integridade, transparência, equidade, responsabilização (*accountability*) e sustentabilidade (Quadro *5*).

Quadro 5 - Os princípios da governança corporativa (continua)

Integridade	Praticar e promover o contínuo aprimoramento da cultura ética na organização, evitando decisões sob a influência de conflitos de interesses, mantendo a coerência entre discurso e ação e preservando a lealdade à organização e o cuidado com suas partes interessadas, com a sociedade em geral e com o meio ambiente.
Transparência	Disponibilizar, para as partes interessadas, informações verdadeiras, tempestivas, coerentes, claras e relevantes, sejam elas positivas ou negativas, e não apenas aquelas exigidas por leis ou regulamentos. Essas informações não devem restringir-se ao desempenho econômico-financeiro, contemplando também os fatores ambiental, social e de governança. A promoção da transparência favorece o desenvolvimento dos negócios e estimula um ambiente de confiança para o relacionamento de todas as partes interessadas.

(conclusão)

Equidade	Tratar todos os sócios e demais partes interessadas de maneira justa, levando em consideração seus direitos, deveres, necessidades, interesses e expectativas, como indivíduos ou coletivamente. A equidade pressupõe uma abordagem diferenciada conforme as relações e demandas de cada parte interessada com a organização, motivada pelo senso de justiça, respeito, diversidade, inclusão, pluralismo e igualdade de direitos e oportunidades.
Responsabilização (Accountability)	Desempenhar suas funções com diligência, independência e com vistas à geração de valor sustentável no longo prazo, assumindo a responsabilidade pelas consequências de seus atos e omissões. Além disso, prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, cientes de que suas decisões podem não apenas responsabilizá-los individualmente, como impactar a organização, suas partes interessadas e o meio ambiente.
Sustentabilidade	Zelar pela viabilidade econômico-financeira da organização, reduzir as externalidades negativas de seus negócios e operações, e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, natural, reputacional) no curto, médio e longo prazos. Nessa perspectiva, compreender que as organizações atuam em uma relação de interdependência com os ecossistemas social, econômico e ambiental, fortalecendo seu protagonismo e suas responsabilidades perante a sociedade.

Fonte: IBGC (2023, p. 18), adaptado pela autora

Todos os princípios apresentados no Quadro 5 se confundem com a LGPD. Para Zimmermann Ghisleni (2022, p.6), um exemplo é a *accountability*, que para “empresas controladoras terão mais obstáculos se tentarem evadir sua responsabilidade jurídica” pois terão o dever de prestarem contas, em toda cadeia esclarecida na LGPD, na coleta, tratamento, compartilhamento, armazenamento e até exclusão dos dados pessoais. Diante disso, tem-se uma cadeia de gestão de responsabilidade pelo tratamento de dados (ZIMMERMANN GHISLENI, 2022).

A palavra integridade, apresentada como um princípio da governança corporativa, também é apresentada na própria LGPD no Art. 26 (BRASIL, 2018). Esta lei apresenta sobre resguardar a segurança e a integridade do titular dos dados, ou seja, como o controlador deve cuidar dos dados pessoais. Outro princípio que aparece, tanto na governança corporativa quanto na LGPD, é o da transparência. Este

princípio é enfatizado na LGPD como atividade do tratamento dos dados pessoais e boa-fé.

Desta forma, os princípios da governança corporativa se fundem à LGPD e é dever do controlador assegurar que a organização possua “políticas e processos claros, eficazes, implementados e devidamente disseminados” (IBGC, 2023, p. 21). Essas políticas e processos serão detalhadas no desenvolvimento do artefato proposto neste trabalho, no que tange à LGPD, principalmente na identificação de possíveis riscos na segurança dos dados pessoais.

Assim, no Código das Melhores Práticas de Governança Corporativa há o gerenciamento de riscos (IBGC, 2023, p. 63) “que se dá por meio de processos estruturados que auxiliem a identificação, o controle e a mitigação” e essa gestão de riscos “contribui para a continuidade e geração de valor da organização”. Dessa forma, a empresa controladora deve aplicar os princípios, políticas, normas, regulamentos e leis aplicáveis para a materializar a *compliance*, que é a “busca permanente da coerência entre aquilo que se espera de uma organização e o que ela, de fato, pratica no dia a dia” (IBGC, 2023, p. 65). Assim, a definição de programa de *compliance*:

> O programa de compliance de uma organização deve abranger um conjunto de mecanismos e procedimentos, políticas, diretrizes, código de conduta, canal de denúncias e demais instrumentos com o objetivo de prevenir, detectar e sanar desvios de conduta, fraudes, atos de corrupção, lavagem de dinheiro, atos ilícitos praticados contra a administração pública, dentre outras questões. Além disso, deve alinhar a atuação de todos na organização com os princípios, valores e propósito dela e promover uma cultura de integridade” (IBGC, 2023, p. 65).

Zimmermann Ghisleni (2022, p.14) destaca ainda que “o controlador possui papel significativo para assegurar o *accountability*, de modo que esteja em *compliance* com as medidas relativas aos demais princípios da lei”, esta lei que se refere, é a LGPD. Assim, pode-se constituir um ambiente que eleva o nível de confiança na organização, chegando no código de conduta ou código de ética, que é:

> “um conjunto de normas internas cujo objetivo principal é promover o propósito, os princípios e valores éticos; fomenta a transparência; disciplinar as relações internas e externas da organização […] e consolidar práticas de governança corporativa” (IBGC, 2023, p. 67).

Dessa forma, ao levar em consideração as práticas de governança corporativa, é imperativo também reconhecer as práticas de governança da segurança

da informação, cujas definições apresentam similaridades. A norma ABNT NBR ISO/IEC 27014 (2013, p. 2) estabelece que a governança da segurança da informação “necessita alinhar os objetivos e estratégias de segurança da informação com os objetivos e estratégias do negócio e requer a conformidade com as leis, regulamentos e contratos”. A gestão de risco deve ser avaliada, analisada e implementada. O corpo diretivo, como principal responsável pelas decisões da organização, deve assegurar a segurança das informações recebidas, armazenadas e transferidas, que, similarmente, é o que apresenta a LGPD.

2.7 SEGURANÇA DA INFORMAÇÃO E A LGPD

O princípio VII da LGPD reporta sobre segurança “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão”. Para Nunes (2019), as empresas têm responsabilidade em buscar ações que garantam a proteção dos dados pessoais coletados.

Canedo *at al.* (2021, p.5) descreve como requisitos prioritários para a segurança dos dados pessoais “o nível de proteção de dados, o risco de segurança, a gravidade do incidente e o risco de privacidade dos dados”. Ainda, para se adaptar à LGPD, uma empresa deve refletir sobre as mudanças na modelagem de processos de negócios como “ampla adaptação empresarial, investimento em TI e comunicação e recursos humanos para serem capazes de atender aos requisitos da privacidade de dados” (CANEDO *at al*., 2021, p.5).

A segurança da informação, nada mais é que à proteção de dados contra acessos não autorizados, alterações indevidas ou indisponibilidade (BARBOSA *at al*., 2021). Ainda, a segurança da informação protege informações que estão registradas, sem importar onde estejam situadas, como: discos rígidos dos computadores, impressões em papel e até mesmo na memória das pessoas (BARBOSA *at al*., 2021).

O espaço cibernético não é somente o ambiente de internet, mas também o que resulta da interação de pessoas, softwares, redes e dispositivos interconectados entre si (ABNT – NBR ISO/IEC 27032, 2012). Os ataques cibernéticos causam danos econômicos e de reputação significativos e podem ocorrer nas mais diversas formas, como: instalação de um programa ilícito como vírus, ataque de hacker, senhas frágeis e disponibiizadas à terceiros não autorizados, entre outros (BARBOSA *at al*., 2021).

Dessa forma, Barbosa *at al. (*2021, p.8) destaca que “a segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de *hardware* e *software”*.

Assim, a discussão sobre a LGPD está intrisecamente ligada à segurança da informação. Esses dois temas estão interconectados, uma vez que ambos se referem à proteção de dados, sejam eles de natureza empresarial ou pessoal.

3 PROCEDIMENTOS METODOLÓGICOS

A exposição dos procedimentos metodológicos tem por finalidade tornar explícita a estrutura sistemática utilizada para a realização do presente estudo, mediante a classificação da pesquisa em relação ao tema e às etapas que a compõem.

A proposta possui caráter qualitativo e aplicado. No que se refere à pesquisa qualitativa, se insere em um campo de investigação que abrange uma rede interconectada e complexa de termos, conceitos, pressupostos e estudos culturais e interpretativos (DENZIN; LINCOLN, 2008). Nesse contexto, em relação à proposta de pesquisa em questão, buscaram-se documentos e interpretações.

A pesquisa para desenvolver a proposta também se enquadra em estudos exploratório-descritivos por ter a possibilidade de desenvolver um estudo de caso para a aplicação do método a ser utilizado, acumulando informações para se obter as inter-relações entre o fato ou ambiente observado (LAKATOS, MARCONI, 2003).

A LGPD se refere à proteção dos dados pessoais e o artigo 5º detalha seus agentes. O enfoque é a proteção e a segurança desses dados pessoais. Dessa forma, buscou-se diretrizes padronizadas de segurança da informação. O caminho formalizado encontrado foram as normas técnicas da ISO (ABNT - Associação Brasileira de Normas Técnicas) no que tange a técnicas de segurança da informação. A ISO 27002 (ABNT, 2013) reporta uma relação de Códigos de Práticas para a Gestão de Segurança da Informação, e a partir da diretriz “Políticas para a segurança da informação”, a criação de etapas para o desenvolvimento de uma ferramenta que permita a adequação à LGPD.

Dessa forma, ao pesquisar sobre um método que se utiliza de etapas, foi identificado o denominado *Design Science Research*, que “se constitui em um processo rigoroso de projetar artefatos para resolver problemas, avaliar o que foi projetado ou o que está funcionando, e comunicar os resultados obtidos” (LACERDA *et al*., 2013, p.744). Carneiro e Almeida (2019, p.4) apresentam a *Design Science Research* como “metodologia que operacionaliza a base epistemológica da *Design Science* de uma maneira […] que auxilie a criação, a ação, em detrimento exclusivamente da observação do investigador sobre determinado fenômeno”. Portanto a *Design Science Research* “pode ser entendida como aquela que propicia a criação de novos conhecimentos através do *design* de artefatos” (p.4).

Nesse contexto, na perspectiva de um paradigma investigativo, a exploração detalhada de um problema envolve a identificação da necessidade, a avaliação da utilidade e a formulação de uma solução adequada. Assim, por meio da compreensão da resolução do problema em questão, busca-se a produção de conhecimento para a construção de um artefato que beneficie a adequação à LGPD em clientes, do segmento micro e pequenas empresas, de organizações contábeis.

O produto deste estudo é um artefato, na forma de um método que possa ser utilizado para adequação à LGPD, uma vez que a legislação atual torna o problema relevante, especialmente no que se refere aos dados pessoais e penalidades administrativas e monetárias.

O objeto em questão deve ser concebido de maneira a aliar praticidade e conformidade com as normativas ISO (ABNT) pertinentes à segurança da informação. Antes de se iniciar qualquer processo de adequação à LGPD, é imperativo que se tenha um profundo conhecimento acerca da organização e de suas operações, com especial atenção aos dados pessoais que são processados, transferidos e armazenados. Portanto, é crucial identificar os clientes, fornecedores e terceiros envolvidos, bem como os colaboradores que possuem autorização para executar ações que envolvam redes e sistemas computacionais internos. A discussão sobre a LGPD é indissociável da segurança e privacidade das informações referentes aos dados pessoais processados pela organização.

O artefato desenvolvido foi submetido à apreciação em clientes de organizações contábeis para avaliar a sua utilidade, qualidade e eficácia, e sua contribuição na adequação à legislação. A aplicação do artefato, conforme Carneiro e Almeida (2019, p.5), se classifica em “observacional, analítico, experimental e descritivo”.

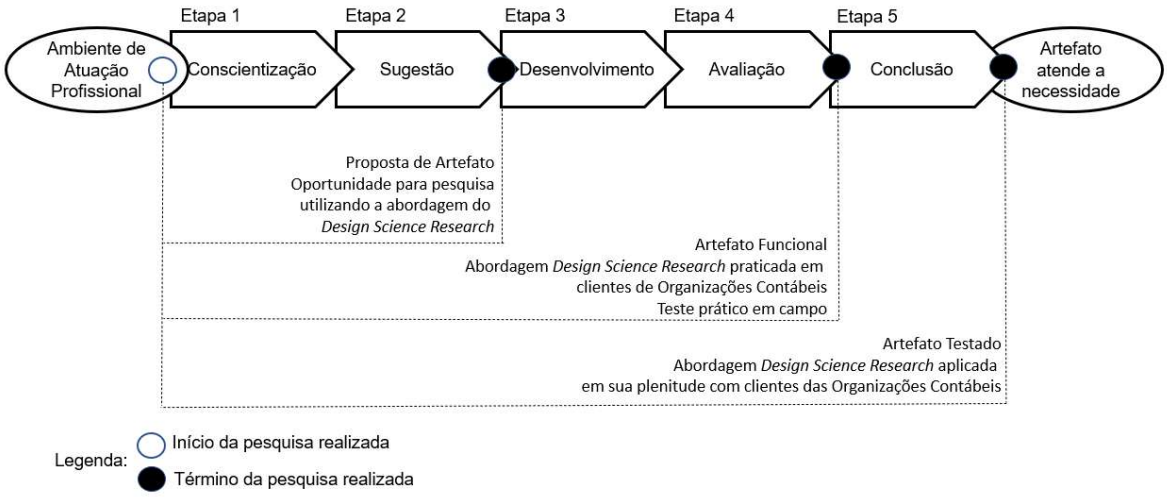
Dessa forma, o método utilizado consiste em um conjunto de etapas que abrangem constructos, principalmente a interpretação da legislação encaixando nas normas da ISO (ABNT), seguindo um modelo que apresenta detalhes da realidade com o objetivo de, posteriormente, adequá-los à linguagem da LGPD, visando solucionar o problema de adequação à essa legislação em micro e pequenas empresas por meio da utilização de um artefato. Para Lobato (2022, p.7), a *Design Science Research* “permite a construção de conhecimento antes, durante e após a construção do artefato, além de deixar claro os objetivos (utilidade) e desempenho (avaliação) dos constructos”.

O artefato utilizado para adequar micro e pequenas empresas à LGPD tem potencial para gerar conhecimento focado na solução de problemas específicos, o que pode estimular o desenvolvimento de novos artefatos (LOBATO, 2022). Dessa forma, há possibilidade de generalização e construção de um conhecimento útil que poderá ser avaliado, testado e aplicado em outras empresas.

Para o desenvolvimento do presente trabalho, os passos metodológicos da *Design Science Research* foram os propostos por Hevner, March e Park (2004, p.83) e adaptados por Lacerda *et al*. (2013, p.751) e compreendem a “conscientização, sugestão, desenvolvimento, avaliação e conclusão”. Cada uma dessas etapas está detalhada na sequência (Figura 7).

A Figura 7 descreve diferentes momentos do ciclo do desenvolvimento do artefato. Entre a avaliação e a conclusão, foi denominado “artefato funcional”, enquanto os testes para análise de utilidade estão descritos como “artefato testado”. A Figura 7 foi adaptada de Sordi, Azevedo e Meireles (2015) que estava no formato de *Design Science* ajustada para *Design Science Research*.

Figura 7 - Etapas da pesquisa *Design Science Research* e o movimento do ciclo do artefato.



Fonte: Sordi, Azevedo e Meireles (2015, p.8), adaptado pela autora.

A seguir a descrição das etapas da pesquisa *Design Science Research* aplicada no contexto da adequação com a LGPD em micro e pequenas empresas, através das organizações contábeis.

3.1 ETAPA 1: CONSCIENTIZAÇÃO

A presente etapa desenvolveu uma proposta para identificar o trajeto a ser percorrido a fim de solucionar o problema em questão. Lacerta *et al*. (2003) classificam essa etapa como conscientização, pois representa uma análise preliminar do problema.

Esta etapa foi construída a partir da revisão teórica e da experiência do pesquisador e de especialistas, utilizando para isso entrevistas não estruturadas. Estas entrevistas tiveram a participação de três especialistas na LGPD. Desses profissionais, um é advogado e dois são especialistas em tecnologia da informação. Essas entrevistas foram realizadas entre 05 de julho a 28 de julho de 2023. Dessa forma, houve uma produção de conhecimento, que conforme Bardin (2004), utilizando uma aplicação sistemática e objetiva dos procedimentos resulta na validade e confiabilidade dos resultados da pesquisa.

A partir desses resultados foram identificados que os aspectos que devem compor a estrutura do artefato estão nas normas técnicas da ISO (ABNT), no que tange à segurança da informação e assim estudada a melhor forma de apresentação. Entretanto, é necessário entender a técnica, compreender a aplicação e a interpretação dos resultados, uma vez que, conforme apontado por Bardin (2004), tem-se que revisar permanentemente, demandando um estudo contínuo, pois as leis sofrem alterações e as tecnologias estão em constante movimento.

3.2 ETAPA 2: SUGESTÃO

Segundo Manson (2006), o pesquisador cria um projeto provisório, e é nesta etapa que diferentes investigadores chegam a diferentes *designs* experimentais, ou seja, “diferentes pesquisadores podem chegar a diferentes teorias para explicar o mesmo conjunto de observações” (p.163). Portanto, este processo “pode ser considerado subjetivo e difícil de padronizar”. Nessa fase de proposição, conduziu-se uma análise abrangente de potenciais artefatos. Além disso, realizou-se um estudo da LGPD, integrando-a com medidas de salvaguarda da segurança dos dados. Consequentemente, foi desenvolvido um protótipo preliminar.

Com base nessa premissa, empreendeu-se um esforço para empregar uma linguagem compreensível, permitindo que os profissionais das organizações

contábeis executassem efetivamente o trabalho de adequação à LGPD em seus clientes. Assim, buscou-se um norteador da adequação, no quesito segurança e privacidade da informação. A ISO 27701 (ABNT NBR ISO/IEC 27701, 2019, p.3) fornece diretrizes para um roteiro:

a) políticas de segurança da informação;
b) organização da segurança da informação;
c) segurança em recursos humanos;
d) gestão de ativos;
e) criptografia;
f) controle de acesso;
g) segurança física e do ambiente;
h) segurança das operações;
i) segurança nas comunicações;
j) aquisição, desenvolvimento e manutenção de sistemas;
k) relacionamento da cadeia de suprimento;
l) gestão de incidentes da informação;
m) aspectos da segurança da informação na gestão da continuidade do negócio;
n) compliance.

O trabalho de adequação realizado pelas organizações contábeis, em conjunto com os clientes, consiste em apresentar a eles a situação atual da empresa em relação aos documentos pessoais que possuem, tanto em formato físico quanto virtual, e, principalmente, em relação aos locais onde esses documentos estão armazenados.

Cada organização empresarial é caracterizada por possuir suas próprias políticas internas, documentadas ou não, catálogo de produtos ou serviços, bem como uma equipe de trabalho composta por funcionários internos ou contratados externamente, além de estabelecer relações comerciais com fornecedores e clientes diversos. Nesse cenário, é imperativo realizar uma análise detalhada dos contratos celebrados, uma vez que há possibilidade de ocorrer a transferência de dados pessoais coletados para terceiros ao longo das atividades operacionais da empresa (ABNT NBR ISO/IEC 27701, 2019).

Canedo *et al.* (2023) apresenta uma lista de perguntas aplicadas no Survey cujos respondentes são funcionários de empresa pública e privada sobre o seu conhecimento sobre a LGPD e segurança das informações no quesito proteção de dados. Essas questões foram norteadoras para alavancagem do artefato.

Nesse sentido, foi elaborado um artefato que permite compreender a situação atual da empresa com base em sua estrutura interna e contratações, em relação aos dados pessoais coletados, transferidos e armazenados, bem como à segurança durante o cliclo de vida dessas informações, com o intuito de minimizar ao máximo a possibilidade de vazamentos de dados (ABNT NBR ISO/IEC 27701, 2019). Assim, caso seja identificado algum risco de vazamento de dados ou invasão, o mesmo será classificado e avaliado quanto ao seu impacto, e a empresa orientada a adotar medidas para mitigar tal risco, oportunizando melhorias nos processos.

Para a efetiva implementação do artefato em questão, é necessário que o profissional da organização contábil seja devidamente instruído e capacitado sobre os princípios e disposições da LGPD. Além disso, o profissional deve receber informações relevantes acerca de incidentes de vazamento de dados e invasões, permitindo-lhe compreender a seriedade dessas ocorrências e preparar-se para lidar com situações similares. Ademais, o profissional recebe orientações detalhadas sobre o funcionamento do referido artefato, visando a otimização de sua aplicação, sugestões de melhoria e a maximização dos resultados.

3.3 ETAPA 3: DESENVOLVIMENTO

Conforme Simon (1996, p.132), “resolver um problema significa simplesmente representá-lo de modo a tornar a solução transparente”. Adicionalmente, Simon (1996), argumenta que se busca soluções que sejam suficientemente adequadas para problemas cuja solução ótima seja inacessível ou cuja implementação seja inviável. A seção 2.5 evidencia um vínculo entre a inovação e a LGPD no que tange o relacionamento com o cliente e a segurança dos dados pessoais. Fundindo essa constatação com a argumentação de Simon (1996), pode-se chegar a uma solução simples que geram vantagens competitivas. Dessa forma, buscou-se estabelecer critérios de aceitação das soluções do artefato.

Nesse contexto, para o desenvolvimento do artefato em questão, foram consideradas ferramentas comumente utilizadas em organizações contábeis, tais

como planilhas eletrônicas ou ferramentas similares, além da possibilidade de desenvolvimento de um aplicativo ou sistema. No entanto, caso a escolha recaia sobre um aplicativo ou sistema, seria necessária uma ferramenta para uso padrão, requerendo a contratação de um especialista para desenvolvimento do *software,* o que pode acarretar ônus para as empresas.

Cabe ressaltar que cada empresa possui sua própria rotina, políticas e filosofias, influenciadas pelos seus administradores, que contribuem para seu diferencial competitivo. Portanto, o artefato em questão precisa ser adaptado de acordo com a organização específica de cada empresa. Nesse sentido, as planilhas eletrônicas representam uma opção viável, pois são amplamente acessíveis a qualquer usuário e permitem modificações de acordo com as necessidades da empresa. Isso vem ao encontro da seção 2.5, pois uma ferramenta de uso rotineiro pode ser utilizada para a adequação à LGPD, caracterizando o conceito da inovação (OCDE/Eurostat, 2018).

Por meio da utilização de planilhas eletrônicas, é viável realizar ajustes e formatar relatórios que preencham apenas os campos para compreensão do negócio e suas práticas, possibilitando comparações em cenários futuros. Ao adotar essa abordagem, o artefato desenvolvido em formato de planilha eletrônica pode ser estruturado em compartimentos, com o intuito de fornecer detalhes sobre a empresa tanto em seu aspecto físico quanto virtual, além de identificar os pontos em que dados pessoais estão sendo coletados, transformados, armazenados ou transferidos.

As questões que compõem o artefato são baseadas nas menções das normas da ISO que tratam sobre a segurança da informação e na experiência da autora sobre a LGPD. O APÊNDICE C – EMBASAMENTO DA CONSTRUÇÃO DO ARTEFATO apresenta uma tabela com o tema abordado e sua localização no artefato, a descrição desse vínculo e a fonte para melhor clareza da origem das questões. Os tipos de dados pessoais coletados entre um segmento de empresa e outro podem ser diferentes, dessa forma, o artefato permite fazer alterações conforme a identificação de um novo tema ou a sua própria exclusão.

A proposta do presente artefato consiste em realizar um detalhamento minucioso do negócio, visando identificar os fornecedores e clientes envolvidos, além de mapear o fluxo dos dados pessoais dentro de cada processo, em cada área interna da organização. E novamente, vem ao encontro da seção 2.5, pois a atividade orientada para a criação de valor está caracterizada como uma oportunidade

inovadora (OCDE/Eurostat, 2018). Essa criação de valor está vinculada à adequação à LGPD em consonância com a governança corporativa e segurança da informação, através da conscientização desses temas durante a conformidade, trazidas pelos profissionais das organizações contábeis. Adicionalmente, busca-se estabelecer a necessidade de designar um Encarregado de Proteção de Dados (DPO), em conformidade com a LGPD, a qual oferece flexibilidade quanto à obrigatoriedade dessa função com base no porte da empresa.

Durante elaboração do artefato, optou-se por dividir em etapas, essas detalhadas em planilhas, intituladas e esmiuçadas:

a) Orientações: breve apresentação sobre o artefato e seu preenchimento.
b) Sobre a LGPD: reporta sobre a LGPD e orientações sobre Governança Corporativa.
c) Início: é o roteiro de adequação à LGPD, neste estão todos os passos a serem sequidos, e deve-se colocar a posição do andamento do trabalho.
d) Levantamento inicial 1: trata-se de questões para conhecer a empresa e sua estrutura.
e) Levantamento inicial 2: trata-se de questões para conhecer o negócio da empresa.
f) Fornecedores: identificação dos fornecedores da empresa, principalmente de serviço, onde passam dados pessoais.
g) TI Ativos de informações: se identifica sistemas, portais, redes.
h) TI Inventário: para identificar computadores, servidores, celulares, sua localização e seus usuários.
i) TI Atribuições: refere-se sobre o responsável que realiza trabalhos de TI, ou seja, quem cadastra e-mails, quem faz o backup entre outras atribuições.
j) Identificação dos processos: detalha-se os processos de forma genérica, dentro de determinado departamento, com o foco de interpretar a possível passagem de dados pessoais.
k) Mapeamento – RIPD (em branco): detalha-se os processos de forma específica, identificando quais dados pessoais circulam nesse processo, questionando a finalidade da coleta dos dados pessoais (coleta, armazenamento, transferência, eliminação). Nessa etapa se analisa se há riscos de vazamento dos dados pessoais.

l) Plano de Ação: identificado algum risco de vazamento na etapa “Mapeamento – RIPD”, se detalha no Plano de Ação em que haverá um responsável para a execução de algum trabalho para mitigar riscos, sempre com a autorização da direção.
m) Cadastro no SEI: nesta planilha há o canal de comunicação da empresa com a ANPD, e orientação de cadastro.

Em consonância com o mencionado nas etapas acima, principalmente no “Mapeamento – RIPD”, buscou-se identificar possíveis riscos relacionados à segurança dos dados pessoais, estabelecendo prazos para a resolução de cada problema identificado. Esse processo é efetivado por meio da implementação de um Plano de Ação – 5w2h (NAKAGAWA, 2014), que visa controlar e monitorar as ações executadas para mitigar tais riscos, garantindo assim a conformidade com as normas de proteção de dados pessoais. Dessa forma, há vínculo de diversas ferramentas consolidadas em um instrumento.

Dessa forma, pode-se chegar na Análise de Conteúdo, segundo Bardin (2011), “é um conjunto de técnicas de análise das comunicações”. Busca compreender os discursos para além dos seus significados imediatos, construindo e apresentando concepções em torno de um objeto de estudo. É um método que segue um processo rigoroso, que inclui as seguintes fases: a pré-análise, a exploração do material e o tratamento dos resultados.

a) Pré-análise: é a preparação do material coletado, organizando-o e definindo o que vai para a análise. No artefato, é o preenchimento das informações necessárias para a adequação à LGPD.
b) Exploração do material: é a identificação de padrões e relação dos dados coletados no artefato.
c) Tratamento dos resultados: é a interpretação dos dados coletados no artefato, fazendo conclusões e apresentando concepções que foram construídas durante a análise.

3.4 ETAPA 4: AVALIAÇÃO

O artefato em questão foi submetido a testes por indivíduos que possuiam conhecimento em rotinas administrativas, financeiras, planilhas eletrônicas e,

particularmente, em tecnologia da informação. Segundo Lacerda *et al*. (2013, p.751) é nesta etapa, que pode ser aplicada a avaliação de validade de artefatos, para isso é necessário: “i) explicitar o ambiente interno, o ambiente externo e os objetivos clara e precisamente; ii) explicitar como o artefato pode ser testado; iii) descrever os mecanismos que medem os resultados”.

Dessa forma, Lacerda *et al.* (2013, p. 751) enfatizam que “o principal resultado do processo de avaliação são as descrições anteriores e as medidas de desempenho alcançadas como elemento último para comprovação da adequação do artefato”. Esse entendimento explica o desenvolvimento do artefato em questão, pois as descrições anteriores se enquadram no mapeamento dos processos e a sequência é a identificação dos riscos e como minimizá-los, classificados no Plano de Ação.

Assim, foi desenvolvido um roteiro de entrevista às micro e pequenas empresas, contendo questões específicas relacionadas ao negócio da empresa, bem como às ferramentas utilizadas para a execução de suas atividades e ao fluxo de dados pessoais envolvidos. No artefato, esse roteiro está apresentado como “Levantamento inicial 1” e “Levantamento inicial 2”. Conforme Lacerda *et al.* (2013) pode-se identificar esse processo com “descrições anteriores”. Essa abordagem evidencia se as organizações contábeis, enquanto prestadores de serviços contratados, detêm o conhecimento necessário para contribuir com a conformidade de seus clientes, especialmente aqueles classificados como micro e pequenas empresas, em relação às exigências estabelecidas.

Para a análise das informações inclusas no artefato, Canedo *et al*. (2023) mencionam tecnologias e metodologias que auxiliam a promover a proteção de dados, evitando ou minimizando os riscos:

> *Identity and Access Management (IAM)* - Solução de Gestão de Identidades e Acesso, ou seja, garantir que apenas as pessoas credenciadas e autorizadas irão acessar a informação de acordo com o grau de restrição, autorização essa que pode variar desde uma simples consulta até o backup e cópia de arquivos.
> *Master Data Management (MDM)*: Gestão dos dados utilizados como referência ou base para uma visão única, contendo todos os dados necessários para a gestão de negócios, infraestrutura, tecnologia, financeira, entre outras.
> *Privacy by Design e Privacy by Default*: Consiste na incorporação de salvaguardas de privacidade e dados pessoais em todos os projetos desenvolvidos, exatamente antes, ou seja, agindo como forma de prevenção e não de tratamento da ação de alguma falha. (Canedo *at al*. 2023, p.3)

Analisando as citações de proteção de dados de Canedo *at al.* (2023) pode-se aplicar essas referências no artefato, conforme mescladas as informações das normas da ISO (ABNT) e LGPD, adaptando a realidade de negócio das empresas.

O artefato foi aplicado em clientes de três organizações contábeis da cidade de Bento Gonçalves do estado do Rio Grande do Sul. A primeira organização contábil está em atividade há 43 anos, já possui adequação à LGPD e tem como diretores um Delegado e um Membro do Conselho Regional de Contabilidade. A segunda organização contábil está no mercado há 31 anos e participa de um grupo econômico onde há *expertise* em outras atividades de prestação de serviços. A terceira organização contábil está em atividade há 10 anos, porém a experiência dos sócios em outras entidades soma 25 anos no ramo.

Nas organizações contábeis que foram submetidas à avaliação do artefato, os colaboradores prestam assistência aos clientes de acordo com a sua carteira de clientes. Dessa forma, um profissional foi selecionado para receber um treinamento adequado, ministrado pela autora, sobre a LGPD e diretrizes do instrumento.

A etapa da avaliação reproduz subsídios para que o artefato seja melhorado (LACERDA *et al*., 2013). Uma vez feitas as modificações, podem ser necessárias outras avaliações pelas mesmas pessoas ou por outras pessoas designadas para aferição. Realizado o ciclo de avaliação, ajustes e novamente avaliação, foi possível partir para a etapa de conclusão.

Todas as etapas do ciclo bem como as modificações sugeridas por cada usuário foram registradas.

3.5 ETAPA 5: CONCLUSÃO

A partir dos resultados obtidos da fase anterior e das modificações sugeridas foi construída a versão final que pode ser apresentada como resultado do método de pesquisa em *Design Science Research*. Lacerda *et al.* (2013, p.751) reforçam que esta etapa “consiste na formalização geral do processo e sua comunicação às comunidades acadêmica e de profissionais”.

Nesta etapa, Vaishnavi e Kuechler (2009) apresentam os resultados obtidos, com a possibilidade de *design cycle*, ou seja, no caso de insucesso, poder começar novamente. Dessa forma, retornar à etapa 1 (seção 3.1 – Conscientização) e preencher as lacunas existentes (DRESCH, LACERDA, JÚNIOR, 2015).

É importante ressaltar que, como resultado desse método, é importante destacar o que funcionou conforme o planejado e quais modificações foram realizadas ao longo do processo. Isso permite uma análise reflexiva do desenvolvimento do artefato, evidenciando tanto os aspectos positivos quanto as adaptações necessárias para alcançar os objetivos propostos.

No capítulo seguinte estão apresentados os detalhamentos e resultados obtidos.

4 RESULTADOS

Esta pesquisa tem por objetivo a elaboração de um artefato que viabilize a conformidade com a Lei Geral de Proteção de Dados (LGPD) em micro e pequenas empresas, clientes de organizações contábeis. Entende-se que nessa adequação haverá conscientização dos administradores e colaboradores sobre a governança corporativa, principalmente, na questão de segurança da informação.

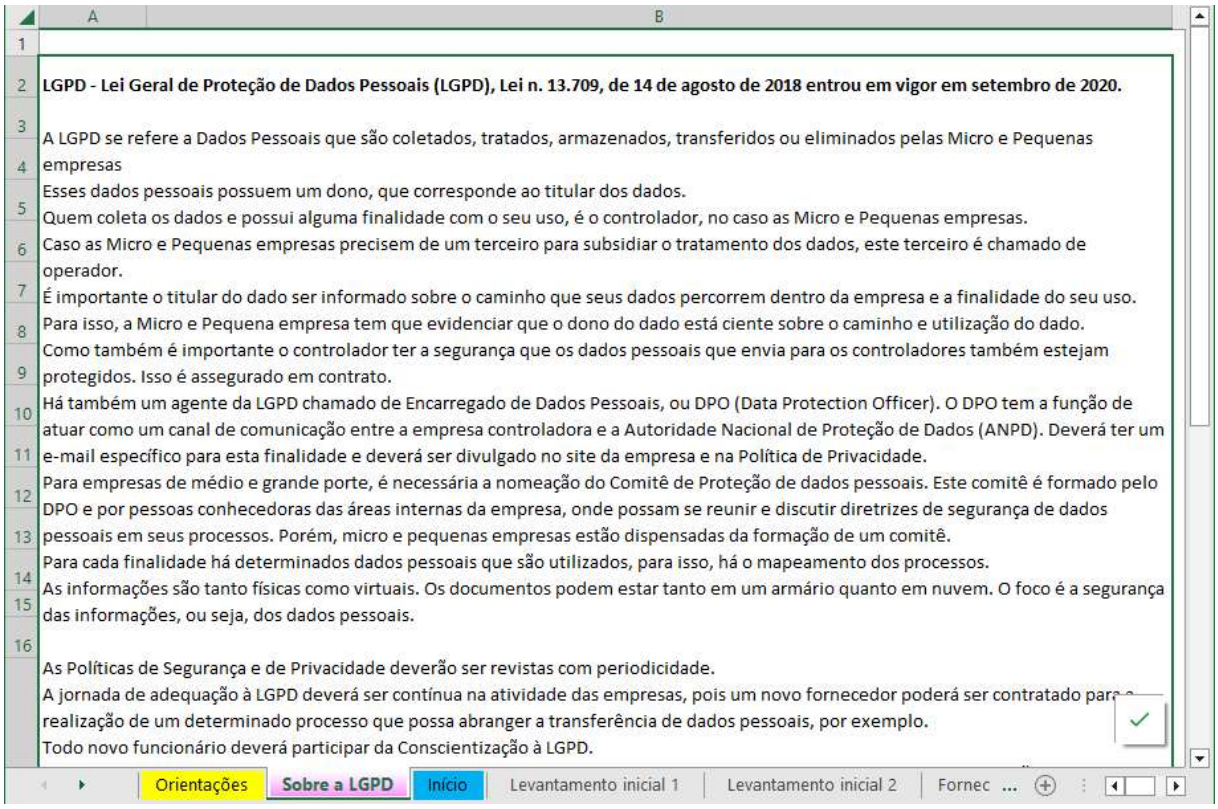
As propostas identificadas na revisão bibliográfica contribuíram na compreensão da LGPD, segregando os aspectos jurídicos, para concentrar-se na proteção dos dados pessoais que transitam na empresa, tanto no ambiente físico quanto virtual. Embora seja uma legislação, a LGPD configura orientações relacionadas à segurança da informação, seja no que tange à coleta, armazenamento, transferência, tratamento ou eliminação dessas informações.

4.1 CONSTRUÇÃO DO ARTEFATO

O resultado desta pesquisa, no caso o artefato produzido, está apresentado a seguir. Ele consiste em uma pasta de trabalho eletrônica (arquivo excel) composta por treze planilhas, que se vinculam a dezesseis arquivos para a sequência da adequação à LGPD. As organizações contábeis que desejam dispôr do artefato, poderão entrar em contato através do *e-mail* andreacasarinzen@gmail.com.

As três primeiras planilhas do artefato referem-se a esclarecimentos e orientações sobre como seguir os passos para a adequação à LGPD, conforme apresentado no item 3.3 ETAPA 3: DESENVOLVIMENTO. Para isso, criou-se uma planilha denominada “Orientações”. Nesta planilha há orientações sobre o funcionamento do artefato. Na sequência, uma planilha denominada “Sobre a LGPD” (Figura 8) apresenta a definição da lei, que estão relacionadas no item 2.1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS, em especial aos artigos 49 e 50 dessa referida lei e orientações sobre a adequação em micro e pequenas empresas. Ao final desta planilha há uma relação de boas práticas e governança a serem adotadas para minimizar riscos, principalmente no quesito da “segurança da informação” que se referem às instruções das Normas da ISO (ABNT NBR ISO/IEC 27701, 2019) e do Instituto Brasileiro de Governança Corporativa (IBGC).

Figura 8 - Artefato: Sobre a LGPD

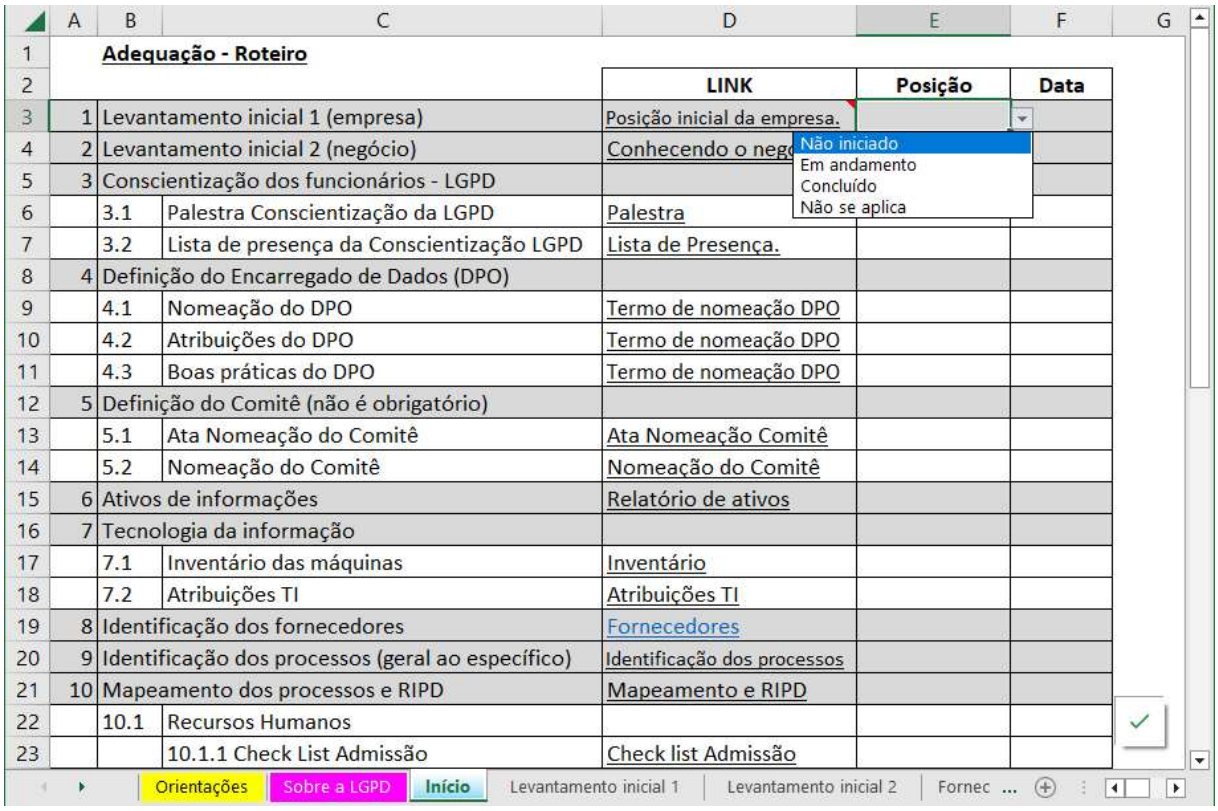


Fonte: Elaborado pela autora (2023).

Para organizar o conteúdo do artefato, criou-se uma planilha denominada “Início” (Figura 9). Esta planilha apresenta um roteiro para a adequação à LGPD em micro e pequenas empresas. A relação das etapas desse roteiro estão descritas no item 3.3 ETAPA 3: DESENVOLVIMENTO, dispostas nas recomendações da própria LGPD (BRASIL, 2018) e nas Normas da ISO que remetem a segurança da informação (ABNT NBR ISO/IEC). A descrição de cada etapa do roteiro está demonstrada no APÊNDICE D – ROTEIRO DE ADEQUAÇÃO À LGPD - ARTEFATO, inclusa a origem da etapa conforme a própria legislação.

Na coluna “posição” (Figura 9) da planilha intitulada “Início”, pode-se documentar a situação da empresa naquele momento, inclusive com a data. Esse roteiro está em ordem de adequação, ou seja, podendo facilitar ao profissional que irá aplicar o artefato no controle das informações.

Figura 9 - Artefato: Início

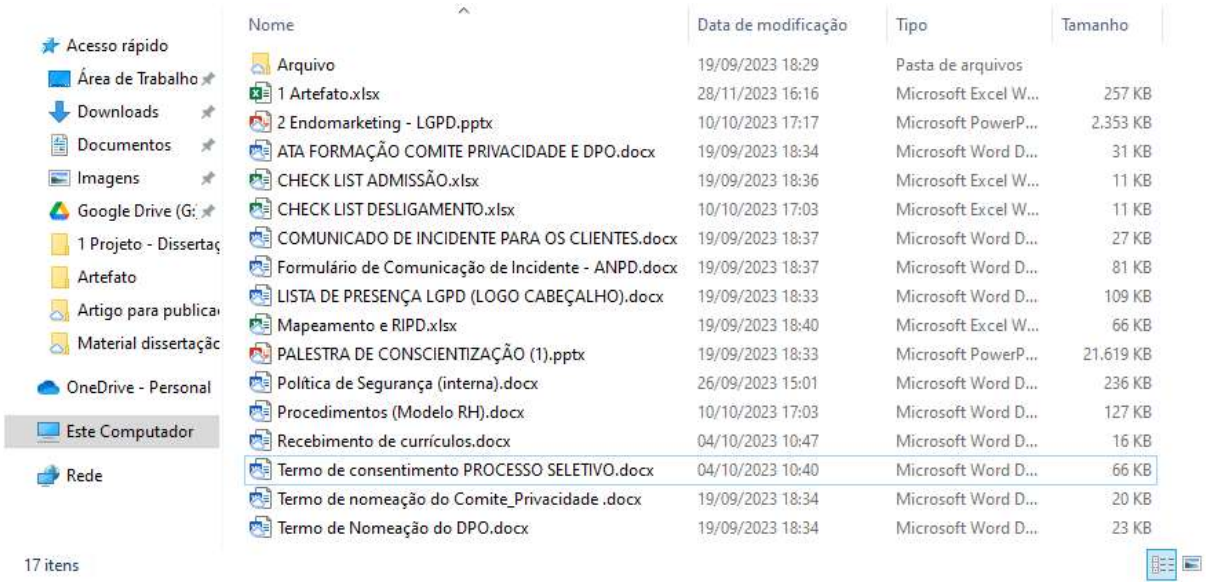


Fonte: Elaborado pela autora (2023).

A coluna “LINK” (Figura 9) remete a planilhas dentro da pasta ou de arquivos documentais que serão úteis durante a adequação à LGPD. Esses arquivos são sugestões que podem contribuir com a adequação, mas nada impede que cada empresas construa seus materiais de acordo com sua realidade. Os arquivos estão disponíveis em diretório disponibilizado aos usuários do artefato (Figura 10).

Esse diretório (Figura 10) é composto de arquivos documentais que irão auxiliar na adequação à LGPD em micro e pequenas empresas. Todos os documentos desse diretório possuem vínculo com a planilha do artefato intitulada “Início” (roteiro de adequação). Seguindo todos os passos, é possível realizar a adequação, porém, qualquer alteração em processo, criação de novo processo, contratação de novo fornecedor, admissão ou demissão de pessoal que em sua atividade está relacionada com acesso a sistemas e redes, mudança na legislação que envolva dados pessoais, entre outros, é indispensável repassar o roteiro do artefato. Recomenda-se, nesse caso, que seja criado novo diretório do artefato, com possibilidade de inclusão de versão dos documentos para manter um histórico.

Figura 10 - Artefato: Diretório com arquivos para auxiliar na adequação à LGPD

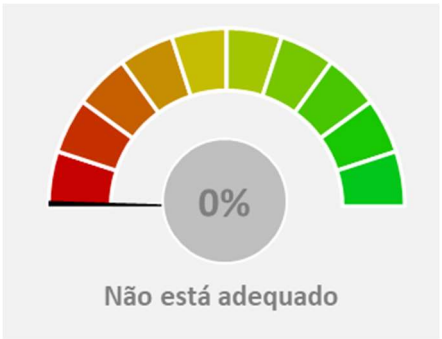


Fonte: Elaborado pela autora (2023).

Na planilha intitulada “Início” (Figura 9), identifica-se uma coluna denominada “Posição”. Esta coluna apresenta quatro possíveis estados para cada questão: “Não iniciado”, “Em andamento”, “Concluído” e “Não se aplica”. À medida que a adequação à LGPD progride, cada campo correspondende na coluna “Posição” deve ser atualizado. Esse procedimento permite que tanto o controlador quanto o profissional contábil, responsáveis pela execução do trabalho, acompanhem o progresso da adequação.

Ao preencher a planilha entitulada “Início” de acordo com o andamento da adequação, um indicador é exibido no final, quantificando a porcentagem do trabalho já realizado, conforme ilustrado na Figura 11.

Figura 11 - Artefato: Início - Indicador



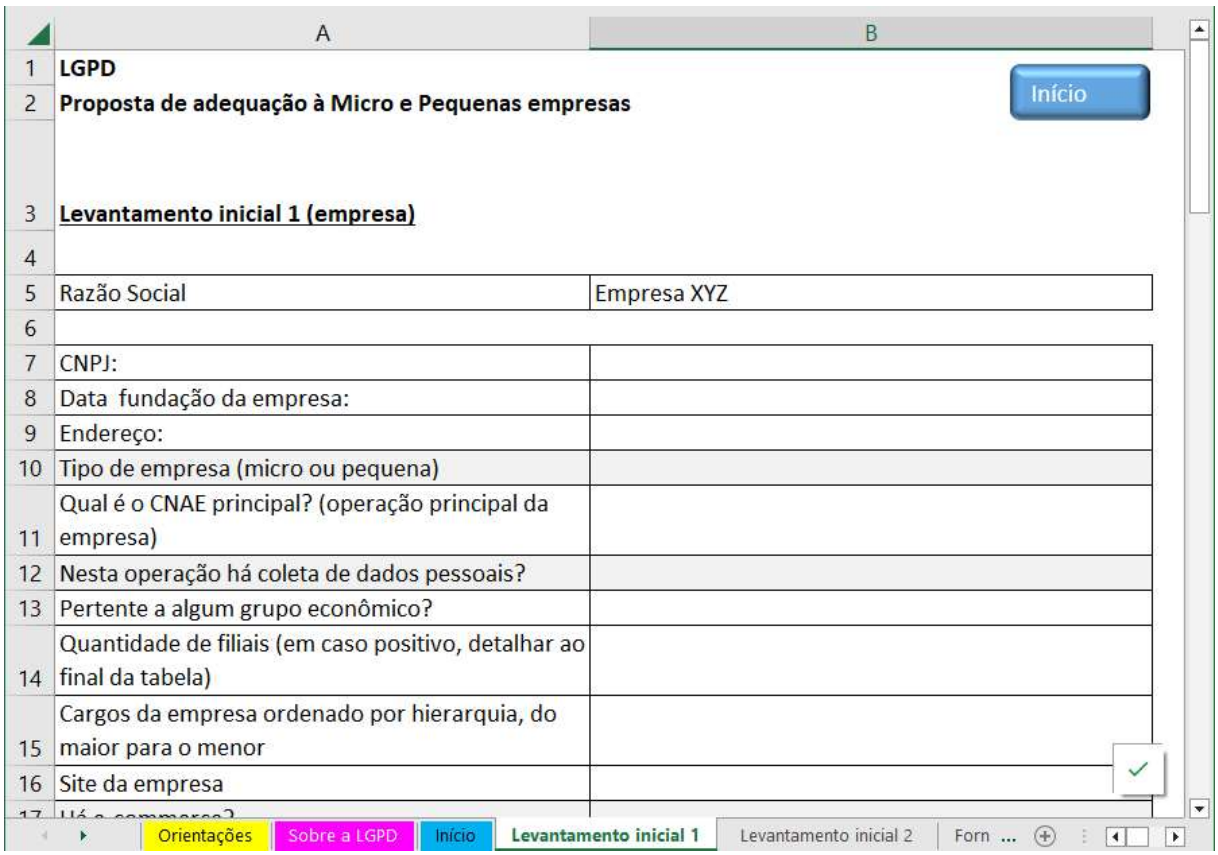
Fonte: Elaborado pela autora (2023).

Esse indicador (Figura 11) exibe uma entre quatro possíveis mensagens: “Adequado – Continue assim!”, “Precisa melhorar mais um pouco”, “É preciso se dedicar mais!” e “Não está adequado”. Essas mensagens têm o objetivo de oferecer um *feedback* instantâneo sobre o estado atual da adequação.

Da quarta planilha em diante são planilhas configuradas em campos que devem ser preenchidas em sequência. Mesmo a empresa optando por deixar campos em branco é importante que considere avaliar todos os campos sugeridos. Em cada planilha há um “botão” denominado “Início” que permite ao usuário retornar à planilha “Início”.

Compreender as características da empresa é muito importante. Essa ação foi definida na planilha denominada “Levantamento inicial 1” (Figura *12*). Um foco particular foi dado à determinação do enquadramento fiscal como micro ou pequena empresa, conforme os critérios legais discutidos na Seção 2.2 (Classificação das empresas). Caso a organização se enquadre em uma categoria diferente, ela não se adequaria aos critérios estabelecidos nesta pesquisa.

Figura 12 - Artefato: Levantamento inicial 1

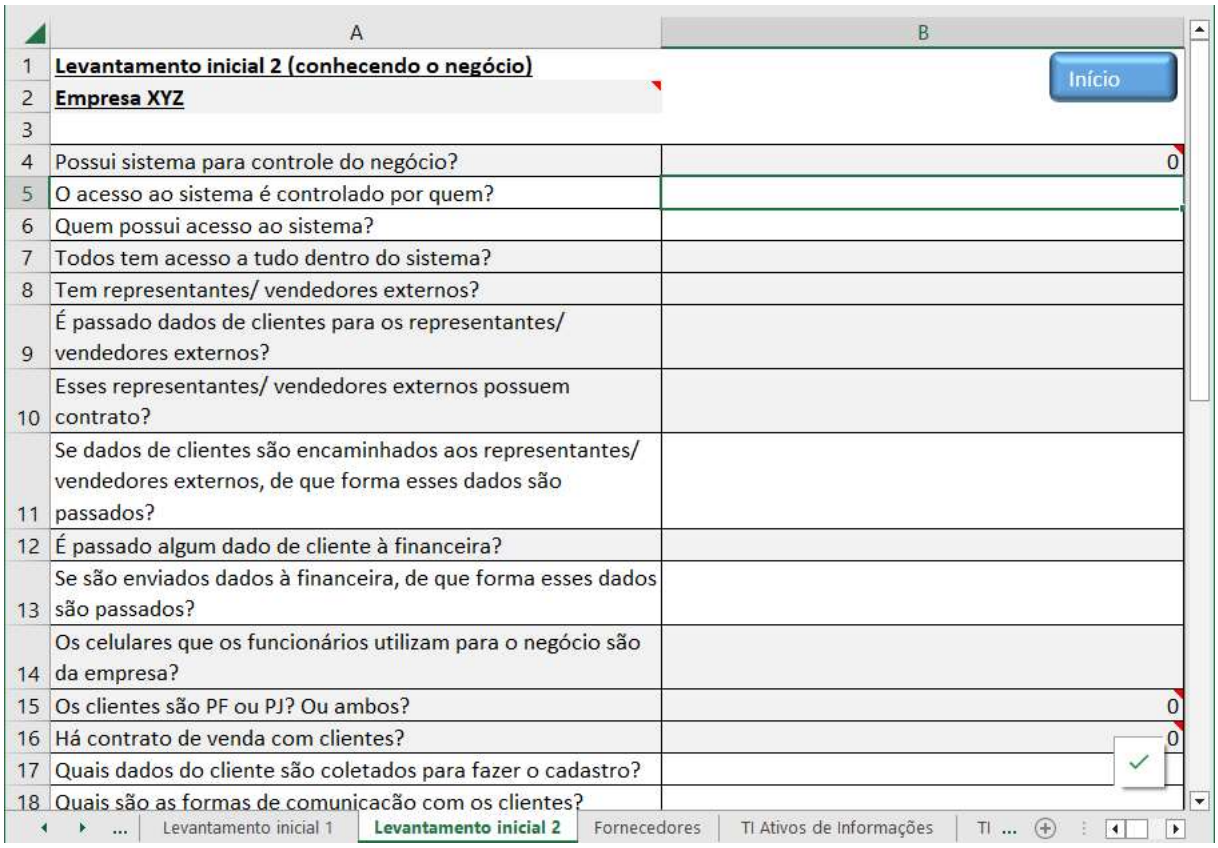


Fonte: Elaborado pela autora (2023)

No Levantamento inicial 1 (Figura 12), foi elaborado um conjunto de dados a serem coletados sobre a empresa. Esses incluem: atividade principal, se a área de TI é interna ou externa, se a empresa já sofreu ataques de vírus ou algum vazamento de dados, se há monitoramento por câmeras, entre outros aspectos relevantes para a adequação à LGPD.

Na Figura 12, “Levantamento inicial 1”, há 52 questões para preenchimento pelas organizações contábeis sobre seu cliente a ser adequado à LGPD. Estas questões abrangem dados sobre a empresa de forma geral. Na sequência, “Levantamento inicial 2” (Figura 13) abrange questões sobre o negócio da empresa, se ela tem *e-commerce*, se trabalham com financeiras terceirizadas, se possuem representantes comerciais, se os clientes são pessoa física ou jurídica, entre outros quesitos, totalizando 26 questões.

Figura 13 - Artefato: Levantamento inicial 2



	A	B
1	**Levantamento inicial 2 (conhecendo o negócio)**	Início
2	**Empresa XYZ**	
3		
4	Possui sistema para controle do negócio?	0
5	O acesso ao sistema é controlado por quem?	
6	Quem possui acesso ao sistema?	
7	Todos tem acesso a tudo dentro do sistema?	
8	Tem representantes/ vendedores externos?	
9	É passado dados de clientes para os representantes/ vendedores externos?	
10	Esses representantes/ vendedores externos possuem contrato?	
11	Se dados de clientes são encaminhados aos representantes/ vendedores externos, de que forma esses dados são passados?	
12	É passado algum dado de cliente à financeira?	
13	Se são enviados dados à financeira, de que forma esses dados são passados?	
14	Os celulares que os funcionários utilizam para o negócio são da empresa?	
15	Os clientes são PF ou PJ? Ou ambos?	0
16	Há contrato de venda com clientes?	0
17	Quais dados do cliente são coletados para fazer o cadastro?	
18	Quais são as formas de comunicação com os clientes?	

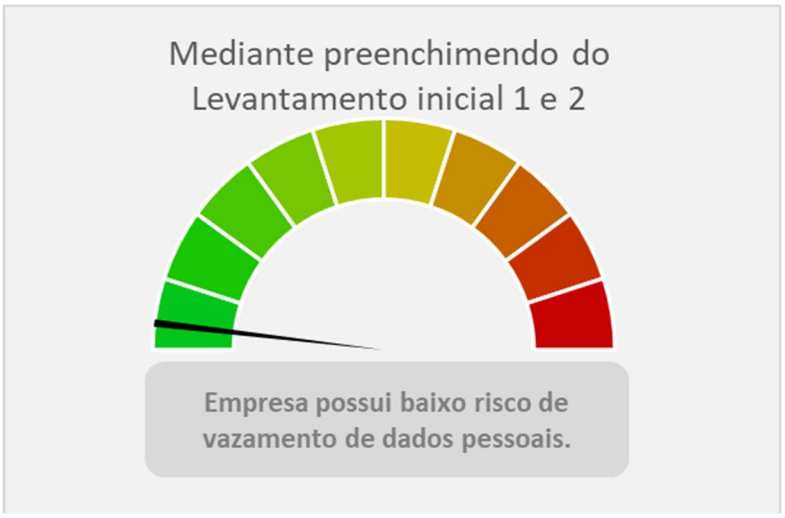
Fonte: Elaborado pela autora (2023).

Ao concluir o preenchimento das planilhas intituladas “Levantamento inicial 1” e “Levantamento inicial 2”, um indicador é apresentado ao final dessa segunda

planilha (Figura *14*). Esse indicador reflete a posição atual da empresa em relação à segurança dos dados pessoais em circulação na organização. Esse indicador pode exibir três possíveis mensagens, cujo objetivo é fornecer uma avaliação instantânea da situação atual da empresa em relação à proteção dos dados pessoais, categorizadas a seguir:

a) risco igual ou superior a 70%: “Empresa possui alto risco de vazamento de dados pessoais”;
b) risco igual ou superior a 30% até menor de 70%: “Empresa possui médio risco de vazamento de dados pessoais”;
c) risco menor de 30%: “Empresa possui baixo risco de vazamento de dados pessoais”.

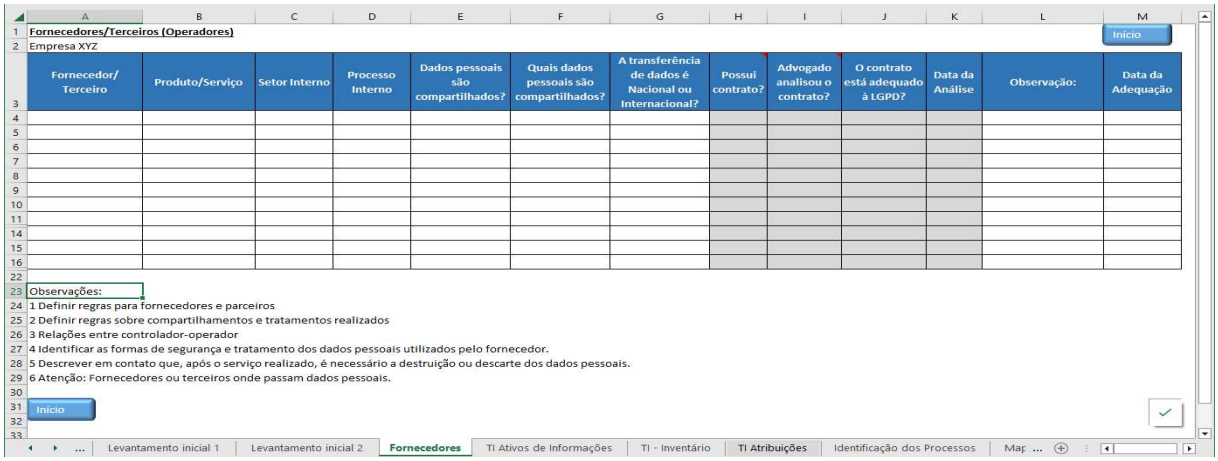
Figura 14 - Artefato: Levantamento inicial 2 – indicador



Fonte: Elaborado pela autora (2023).

Durante a aplicação do artefato, pode-se identificar algum compartilhamento de dados pessoais com fornecedores. Desta forma, há uma planilha no artefato que detalha o fornecedor (Figura 15) qual o serviço que presta ou produto, qual setor interno atende, entre outros quesitos, se há contrato e se está adequado à LGPD. Em cada título de coluna há um comentário com a orientação sobre o preenchimento.

Figura 15 - Artefato: Fornecedores



Fornecedores/Terceiros (Operadores)

Empresa XYZ

Início

Fornecedor/ Terceiro	Produto/Serviço	Setor Interno	Processo Interno	Dados pessoais são compartilhados?	Quais dados pessoais são compartilhados?	A transferência de dados é Nacional ou Internacional?	Possui contrato?	Advogado analisou o contrato?	O contrato está adequado à LGPD?	Data da Análise	Observação:	Data da Adequação

Observações:

1 Definir regras para fornecedores e parceiros

2 Definir regras sobre compartilhamentos e tratamentos realizados

3 Relações entre controlador-operador

4 Identificar as formas de segurança e tratamento dos dados pessoais utilizados pelo fornecedor.

5 Descrever em contato que, após o serviço realizado, é necessário a destruição ou descarte dos dados pessoais.

6 Atenção: Fornecedores ou terceiros onde passam dados pessoais.

Início

Levantamento inicial 1 | Levantamento inicial 2 | Fornecedores | TI Ativos de Informações | TI - Inventário | TI Atribuições | Identificação dos Processos | Map ...

Fonte: Elaborado pela autora (2023).

A norma ISO 27002 (ABNT NBR ISO/IEC 27002, 2013) apresenta a concepção de ativos e o valor da informação, destacando que a informação transcende as palavras escritas, números e imagens. Ela inclui conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis de informação. A norma enfatiza que, no processo de criação de um produto ou serviço, podem existir informações relevantes, que podem até constituir um segredo. Essas informações podem estar relacionadas a sistemas, redes e até mesmo às pessoas envolvidas nessas operações. Portanto, a gestão adequada desses ativos de informação é importante para a operação eficaz de uma organização.

> Ativos são objeto de ameaças, tanto acidentais como deliberadas, enquanto os processos,sistemas, redes e pessoas têm vulnerabilidades inerentes. Mudanças nos processos e sistemas do negócio ou outras mudanças externas (como novas leis e regulamentações), podem criar novos riscos de segurança da informação. Desta forma, em função das várias maneiras nas quais as ameaças podem se aproveitar das vulnerabilidades para causar dano à organização, os riscos de segurança da informação estão sempre presentes. Uma segurança da informação eficaz reduz estes riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos (ABNT NBR ISO/IEC 27002, 2013, p.x).

Para detalhar os ativos de informações da empresa, foi criada uma planilha com essa identificação no artefato. A Figura *16* apresenta uma forma de preenchimento, inclusive com orientações para caracterização de valores para cada tivo, como: confidencialidade, integridade e disponibilidade (ABNT NBR ISO/IEC

27001, 2013), com suas definições e orientações de preenchimento. Um ativo que, se por algum motivo faltar, impactará essas propriedades e o funcionamento da empresa.

Figura 16 - Artefato: Ativos de informações

Ativos da Informação	Quais a empresa possui? (descreva)	Determinação do Valor
Sistemas		
Portais		
Base de dados		
Equipamentos de comunicação		
Contratos		
Informação eletrônica		
Documentos em Papel		
Aplicativos		
Hardwares		
Instalações		
Pessoas		
Imagem e reputação da organização		
Serviços		

Fonte: Elaborado pela autora (2023).

Após a identificação dos ativos de informações, procurou-se identificar as vulnerabilidades de *hardware* e de *software*. A norma da ISO 27001 (ABNT NBR ISO/IEC 27001, 2013) reporta sobre as ameaças externas e do meio ambiente dos dispositivos móveis e equipamentos. Essa disposição trata de “impedir perdas, danos, roubo, ou comprometimento de ativos e interrupção das operações da organização” (p.19). A redução dos riscos de ameaças, dos perigos do meio ambiente, cabeamentos no quesito interceptação ou danos, manutenção contínua, backup, informações sobre os softwares instalados nos equipamentos e assegurar que os funcionários e terceiros estejam cientes da política de segurança da empresa, também estão alinhados no artefato.

No artefato, na planilha intitulada “TI-Inventário” (Figura 17), há questões sobre o inventário das máquinas e os softwares que a compõem. Devem ser incluídos a descrição dos dispositivos móveis e equipamentos diversos que necessitam de cabeamento em rede e a relação de softwares instalados, possuindo licença ou não, principalmente se há atualização de antivírus.

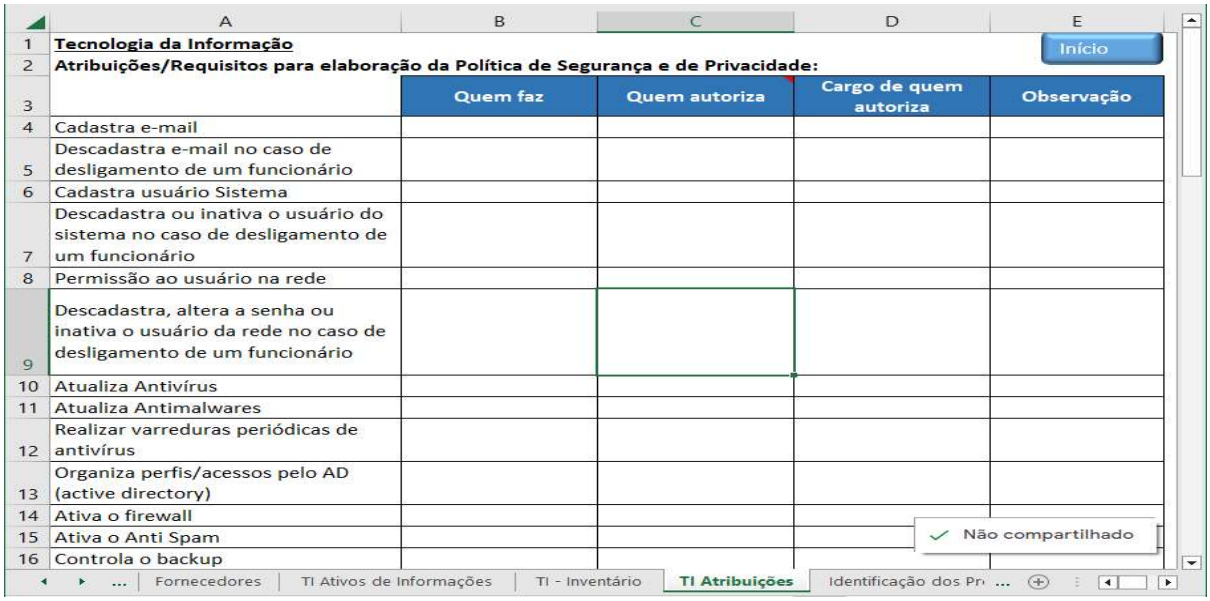
Para as questões relacionadas à TI, se espera que o respondente da empresa questione o profissional de TI e estime um prazo de resposta.

Figura 17 - Artefato: TI inventário

Fonte: Elaborado pela autora (2023).

Na sequência, revisou-se dados para montagem do artefato pelas Normas 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 (ABNT NBR ISO/IEC 27701, 2019). Foram identificados os temas que são correspondentes aos cuidados com os dados pessoais que abrangem a LGPD, assim, mesclaram-se com as necessidades de segurança das empresas, como: permissão do usuário à rede e sistemas, cadastramento de senhas, ativação ou desligamento de um usuário, atualização de antivírus, controle de *backup*. Essas questões estão apresentadas na Figura 18.

Figura 18 - Artefato: Atribuições da área de tecnologia da informação

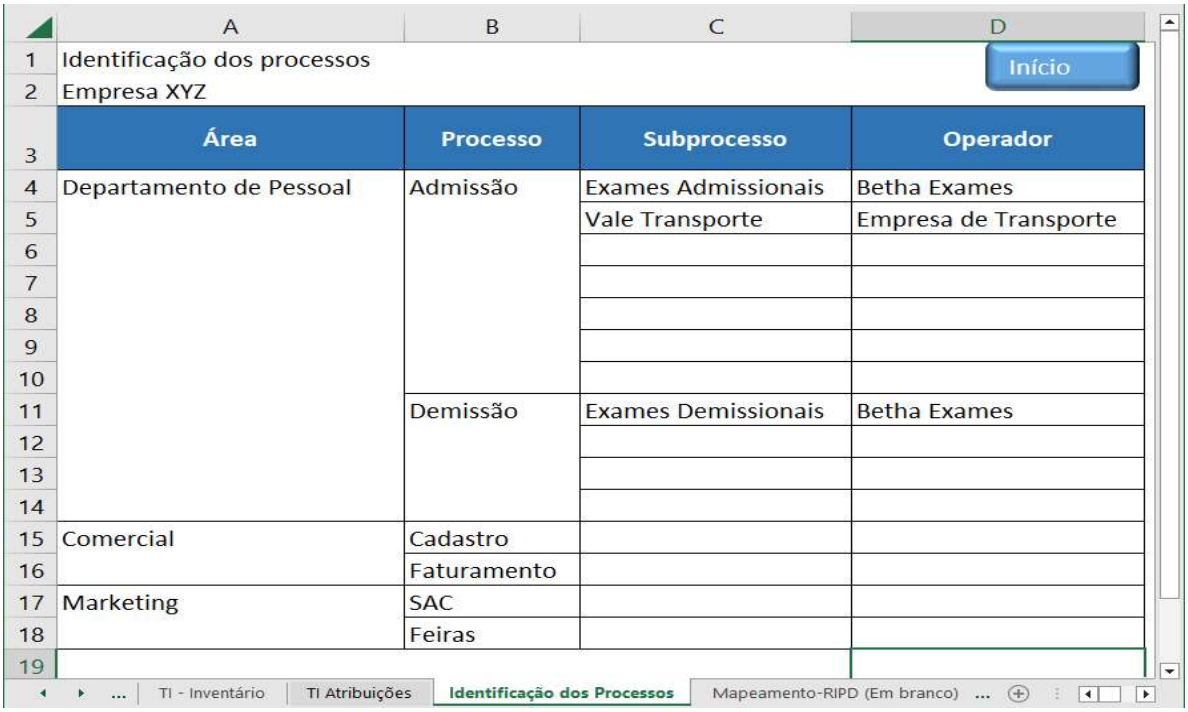


Fonte: Elaborado pela autora (2023).

As atribuições da área de TI (Figura 18) totalizam 36 questões para verificação com os clientes das organizações contábeis. Estas questões auxiliam na montagem da Política de Segurança da Informação, que é um dos norteadores especificados na seção 3.2 (Etapa: Sugestão).

A LGPD impõe o RIPD (Relatório de Impacto à Proteção de Dados) (BRASIL, 2018), documento que contém a descrição dos processos de tratamento dos dados pessoais, denominado em artigos pesquisados como “mapeamento”. No artefato, há a planilha “Identificação dos Processos” (Figura *19*), que é passo inicial do mapeamento, ou seja, identificação dos processos onde se coleta, armazena, transfere ou tratam dados pessoais de forma genérica. A norma da ISO 27701 (ABNT NBR ISO/IEC 27701, 2019, p. 78) apresenta que a “aplicação dos requisitos, diretrizes e controles podem ser relevantes para atender as obrigações da LGPD” e é “responsabilidade das organizações avaliarem suas obrigações legais e decidirem como estar em *compliance* com elas”.

Figura 19 - Artefato: Identificação dos processos (incluso exemplo)

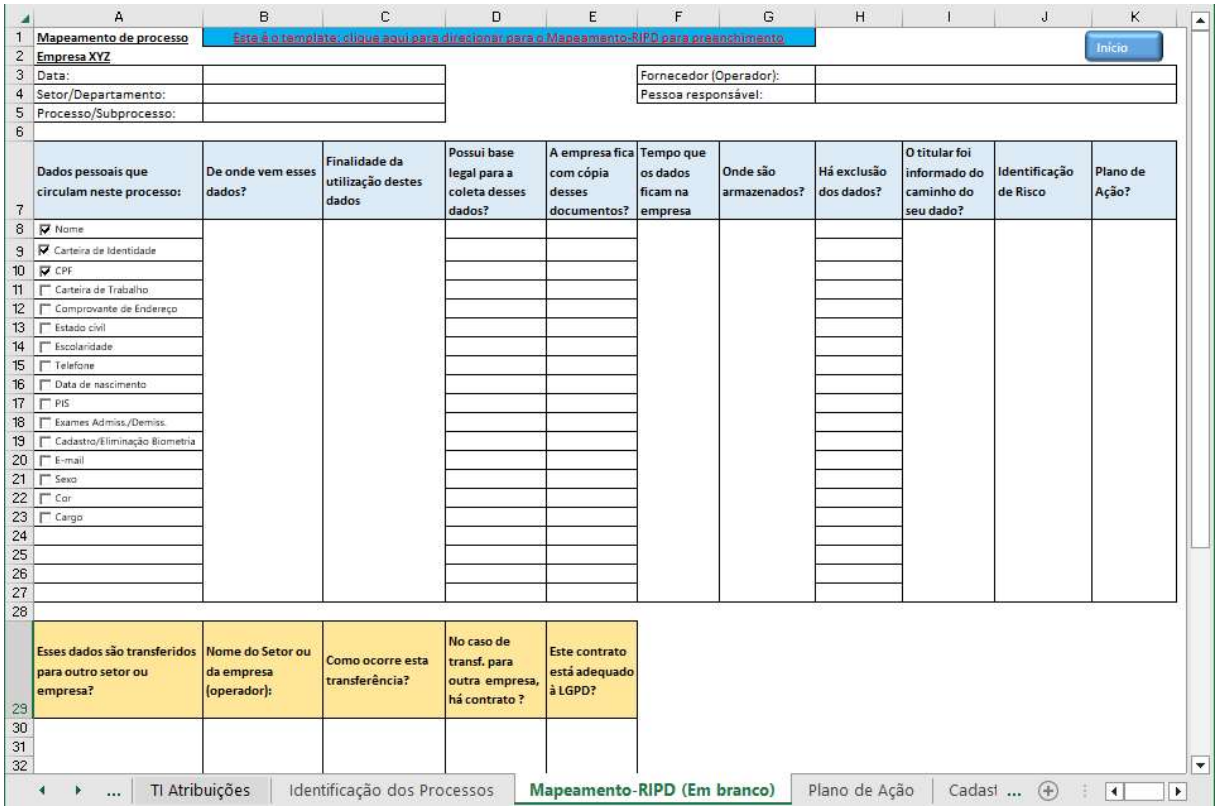


Fonte: Elaborado pela autora (2023).

Na sequência, o mapeamento dos processos deve ser realizado de forma mais detalhada, observando cada questão e preenchendo de forma minuciosa (Figura 20).

A relação de dados pessoais do “Mapeamento-RIPD” (Figura 20) foi extraída pela experiência da autora e das entrevistas não estruturadas e também durante a adequação à LGPD nos testes realizados em clientes das organizações contábeis. Cada dado pessoal será marcado conforme cada processo for mapeado, pois cada um possui uma finalidade. Nesse caso, se observa que a LGPD (BRASIL, 2018) determina através dos seus princípios (seção 2.1) em consonância à coleta, armazenamento, tratamento, transferência e eliminação dos dados pessoais. É nesse documento que se descreve a atividade, especificando os registros, se são armazenados na empresa, de forma física ou virtual, se são encaminhados aos operadores, enfim, a atividade em relação aos documentos pessoais coletados com o objetido de identificar alguma vulnerabilidade.

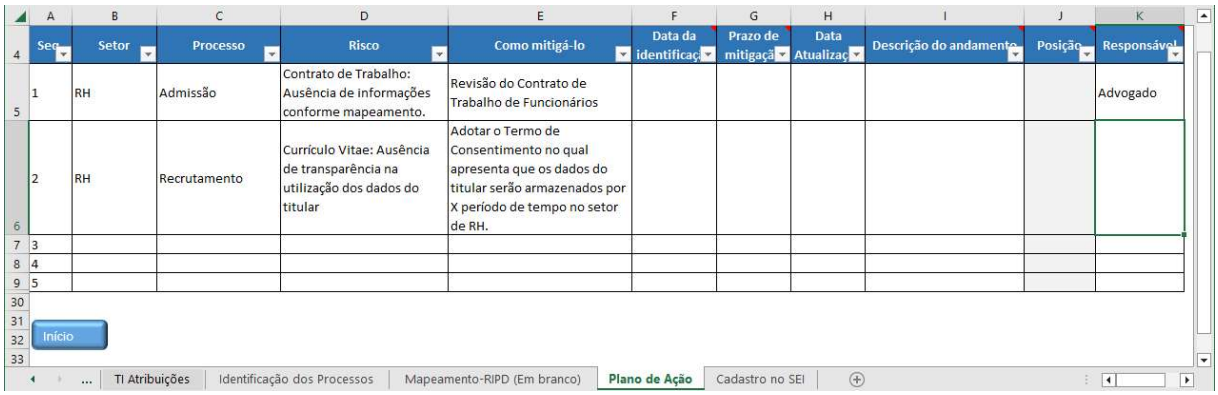
Figura 20 - Artefato: Mapeamento e RIPD



Fonte: Elaborado pela autora (2023).

A LGPD não determina como o RIPD deve ser elaborado, desde que contenha a “descrição dos processos de tratamento dos dados pessoais que podem gerar riscos […]” (BRASIL, 2018). Dessa forma, a autora desenvolveu, junto com o mapeamento dos processos, a adaptação do RIPD no mesmo documento, ou seja, que contenha a descrição dos riscos (Figura 20). Identificando alguma vulnerabilidade em algum processo, se avalia o encaminhamento ao Plano de Ação (Figura 21), cujas questões foram adaptadas pela autora.

Figura 21 - Artefato: Plano de Ação (incluso exemplo)



Seq	Setor	Processo	Risco	Como mitigá-lo	Data da identificaç	Prazo de mitigaçã	Data Atualizaç	Descrição do andamento	Posição	Responsável
1	RH	Admissão	Contrato de Trabalho: Ausência de informações conforme mapeamento.	Revisão do Contrato de Trabalho de Funcionários						Advogado
2	RH	Recrutamento	Currículo Vitae: Ausência de transparência na utilização dos dados do titular	Adotar o Termo de Consentimento no qual apresenta que os dados do titular serão armazenados por X período de tempo no setor de RH.						
3										
4										
5										

Início

TI Atribuições | Identificação dos Processos | Mapeamento-RIPD (Em branco) | Plano de Ação | Cadastro no SEI

Fonte: Elaborado pela autora (2023)

Na planilha “Plano de Ação” deve-se, necessariamente, anotar o risco igual ao identificado na planilha “Mapeamento-RIPD” e sugerir um plano para sua mitigação, definindo prazo e executor. Caso a empresa opte por não implementar a sugestão, é importante detalhar no Mapeamento-RIPD (Figura 20) e expor à organização o risco de autuação da ANPD no caso de algum vazamento de dados.

O artefato pode ser alterado conforme a necessidade da empresa. Cada empresa possui uma rotina. O objetivo do artefato não é alterar a rotina da empresa, mas sim, orientar para a segurança da informação dessas rotinas e verificar se o dado pessoal que a empresa coleta é realmente necessário (BRASIL, 2018) e se está seguro. Sendo necessário, busca-se o consentimento do titular do dado.

A ANPD recomenda o cadastro do controlador e do encarregado dos dados pessoais na sua plataforma, facilitando a comunicação entre os agentes. O *link* de acesso à plataforma está disponibilizado na planilha “Cadastro na ANPD” no artefato, onde há orientação de preenchimento. Esse é um canal de comunicação com a ANPD, pois no caso de algum incidente de vazamento de dados, esta entidade deverá ser

comunicada em até três dias úteis do conhecimento do fato pelo controlador (BRASIL, 2024).

Após a elaboração do artefato, três organizações contábeis avaliaram o material, o que está descrito na sequência.

4.2 APLICAÇÃO DO ARTEFATO

Primeiramente, houve o contato com os diretores das três organizações contábeis, já referidas na seção 3.4, que prontamente agendaram uma reunião. Nesse encontro foram esclarecidas as dúvidas dos diretores em relação à LGPD e apresentou-se o artefato. Nas três organizações houve o aceite para a testagem. Após o encontro, o artefato foi encaminhado por e-mail aos diretores para análise com sua equipe. Posteriormente, retornaram com sugestões para possível implementação.

A Organização Contábil 1 destacou as seguintes sugestões para o artefato, abaixo apresentadas:

a) incluir um *QR Code* na página inicial do artefato com informações sobre a LGPD;
b) incluir no “Levantamento inicial 1” uma questão sobre a empresa possuir o Seguro de Responsabilidade Civil;
c) incluir no “Levantamento inicial 2” uma questão sobre a empresa possuir um Termo de Confidencialidade assinado pelo funcionário e/ou terceiros;
d) incluir no “Levantamento inicial 2” uma questão sobre empresa possuir um controle/limite de horário de trabalho para atendimento ao cliente;
e) incluir no “Levantamento inicial 2” uma questão sobre a empresa possuir um bloqueador das informações internas fora do horário comercial, para que o funcionário não acesse fora do horário de expediente;
f) criar um “termômetro” para saber a situação da empresa em relação à LGPD;
g) houve uma sugestão que abrangia fornecedores onde não passam dados pessoais, dessa forma foi incluída uma observação no artefato, na planilha “Fornecedores” que se refere às empresas nas quais se envia ou recebe dados pessoais.

As sugestões dos itens foram devidamente aceitas e implementadas. Com relação ao item “a”, disponibilizou-se um *link* da lei para os usuários do artefato na planilha denominada “Sobre a LGPD”. Observa-se que, 80% das sugestões da Organização Contábil 1 referem-se à segurança, tanto corporativa quanto de informação.

Quando o artefato foi apresentado à Organização Contábil 2, as implementações da Organização Contábil 1 já haviam sido concluídas. Dessa forma, foram acrescentadas outras implementações, que são as descritas a seguir:

a) incluir no “Levantamento inicial 2” uma questão sobre a empresa possuir um documento de permissão do supervisor ao funcionário acessar o local de trabalho fora do horário de expediente;
b) incluir no “TI – Atribuições” uma questão sobre a empresa possuir algum controle de palavras-chave em sua área de TI de *e-mails* enviados pelos próprios funcionários, que a empresa poderia considerar suspeito.

Todos os itens sugeridos pela Organização Contábil 2 foram aceitos e implementados. Ressalta-se que suas sugestões foram especificamente no âmbito de segurança, tanto corporativa como de informação.

Após feitos os ajustes da Organização Contábil 2, o artefato foi enviado à Organização Contábil 3, que não apresentou sugestões.

Na Organização Contábil 1, optou-se por fazer um treinamento com um profissional cuja função é assistente contábil. Este profissional possui uma carteira de clientes sob sua alçada nas atribuições contábeis. O assistente contábil iniciou a aplicação do artefato em três clientes. Em relação a algumas questões do artefato, os diretores das empresas consultaram seus prestadores de serviços de TI. No entanto, estes não forneceram respostas imediatas, deixando tais questões pendentes. Em outras situações os riscos foram medidos e foram cadastrados no Plano de Ação, com prazo para execução.

A Organização Contábil 2 optou por fazer o treinamento com a Gerente Financeira, que recebeu orientações sobre a LGPD e o artefato. Este profissional não possui carteira de clientes, porém, como a Organização Contábil 2 possui outros segmentos de negócio, iniciou a adequação com o artefato nestas empresas. A área de TI é interna e atende seis empresas do grupo, inclusive da própria organização

contábil, dessa forma, agiliza nos retornos e andamento da documentação de adequação.

A Organização Contábil 3 iniciou a aplicação do artefato com três clientes. Teve dúvidas em questões pontuais, as quais foram esclarecidas assim que fizeram o contato com a autora.

Nos retornos das três organizações contábeis, observou-se que seus clientes desconheciam ou conheciam muito pouco sobre a LPGD, tampouco sobre segurança da informação. Em todas as empresas que iniciaram o processo de adequação a esta lei, o foco é a execução do seu negócio, não havendo preocupação com documentos, senhas, antivírus ou *backup*. A partir do momento em que os levantamentos foram realizados, os sócios começaram a "dar-se conta" da vulnerabilidade da documentação física e virtual das suas empresas, principalmente no despreparo de seus funcionários em segurança da informação.

Uma das empresas em que o artefato foi aplicado levantou uma indagação ao profissional da organização contábil, questionando a necessidade de adequação à LGPD, pois expressou dúvidas quanto à importância de tal conformidade. Então, a organização contábil reportou sobre o processo de mapeamento da área de recursos humanos, já que esta empresa possui aproximadamente 15 colaboradores registrados. Foram apresentados os documentos para fazer a admissão e a manutenção de um colaborador e por quem passam esses documentos e informações (seção 2.4). Dessa forma o empresário compreendeu que todos os passos da LGPD passam por esta área: coleta, tratamento, armazenamento, transferência e eliminação e, assim aplicados os princípios da LGPD (seção 2.1).

A Organização Contábil 3 reportou que, em uma das empresas que o artefato foi aplicado, "todos os funcionários sabiam o salário de todos", mas a gerência de recursos humanos não sabia como essa informação poderia ter sido vazada. Analisando o fato, identificaram um funcionário, com acesso à empresa para realização de suas atividades fora do horário normal, entrava na sala de recursos humanos, que não estava trancada, e mexia na papelada, que estava em armário sem chave. Prontamente, foi incluído no Plano de Ação a colocação de chave no armário, onde somente o profissional responsável tem acesso. Na sequência foi descrito este procedimento na área de recursos humanos.

O assistente contábil de outra empresa onde foi aplicado o artefato, observou que o servidor de dados de TI estava no refeitório desta empresa, onde todos os

funcionários passavam e até mesmo visitantes. Essa situação foi reportada como risco e cadastrada no Plano de Ação com o objetivo de rever o ambiente atual devido à sua vulnerabilidade em relação à segurança deste equipamento e dos dados nele armazenados.

Ainda nessa mesma empresa, foi constatado que na portaria era cadastrado o nome, CPF, placa do veículo de todos os visitantes em um computador que não tinha senha, *backup* e não estava logado em rede. Essa situação foi reportada como risco e sugerida no Plano de Ação para verificar a relevância da coleta desses dados. Se a coleta desses dados é relevantes para a empresa, é necessário informar ao titular do dado quanto tempo esses dados ficarão na empresa. Além disso, foi sugerido disponibilizar a estação de trabalho na rede da empresa, onde estaria coberta por antivírus, senhas e *backup*.

No roteiro do artefato, na planilha intitulada “Início”, há uma sequência de quesitos a seguir para o andamento da adequação à LGPD. Essa planilha foi enfatizada pelas três organizações contábeis como fundamental para a sequência e entendimento do processo, podendo ser considerada, dentro do conceito apresentado na seção 2.5, como um processo inovador.

Outro ponto enfatizado pelas organizações contábeis participantes foi a simplicidade do mapeamento dos processos que se combinam ao RIPD, sem a necessidade de elaboração de um relatório específico. Simplificando processos através da pesquisa e conhecimento, chega-se novamente ao conceito de inovação (seção 2.5) o que pode gerar um amadurecimento nos processos internos, proporcionando maior competitividade. Estas organizações entenderam o quesito “Mapeamento de Processos – RIPD” como ponto indispensável para a descrição dos processos e sequência da adequação à LGPD.

Um ponto observado pela pesquisadora é que os clientes das organizações contábeis não entendem a adequação à LGPD como prioridade. As empresas continuam dando foco às suas rotinas de negócio, ou seja, a adequação à LGPD fica em segundo plano. Dessa forma, as organizações contábeis devem periodicamente cobrar uma agenda para o andamento, enfatizando que a não adequação pode ocasionar sanções administrativas e perdas monetárias significativas e que a conformidade pode proporcionar uma melhoria nos seus processos de gestão.

4.3 GOVERNANÇA CORPORATIVA E DE SEGURANÇA DA INFORMAÇÃO

A adequação à LGPD implica em um compromisso contínuo. A adequação não é um processo estático que se encerra com o arquivamento de documentos, mas sim um processo dinâmico que requer atualizações constantes dentro das organizações. A LGPD, no Capítulo VII, Seção II, destaca especificamente “Das boas práticas e da governança” (BRASIL, 2018), reforçando a necessidade de uma abordagem proativa e contínua para a conformidade.

> 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 (BRASIL, 2018, p.19).

Dessa forma, para atender os princípios da LGPD, é necessária a implementação de política de governança e necessariamente a *compliance*. A governança tem como objetivo incorporar à organização, especialmente aos seus membros, o respeito às regras, a definição clara do propósito da empresa, seus valores e princípios que constituem sua identidade. Em outras palavras, a governança orienta o que a empresa espera que as pessoas pratiquem em suas rotinas diárias por meio de seus processos (IBGC, 2023). Esta diretriz conduz à definição de *compliance,* conforme descrito na seção 2.6. Assim, orienta-se para a elaboração da Política de Segurança da empresa, onde são descritas as diretrizes de segurança interna, e todos os funcionários são instruídos de forma documentada e assinada (ABNT NBR ISO/IEC 27001, 2013). Além disso, existe a Política de Privacidade, que é o documento pelo qual a empresa comunica aos visitantes de seu site se há coleta de dados pessoais (ABNT NBR ISO/IEC 27701, 2019).

Portanto, a governança e a conformidade são componentes essenciais na gestão eficaz de uma organização, requisitos básicos para alavancar a competitividade da empresa. A inovação, em particular, pode proporcionar uma vantagem competitiva, permitindo que a empresa se adapte e prospere em um ambiente de negócios em constante mudança (IBGC, 2023). Para que a política de

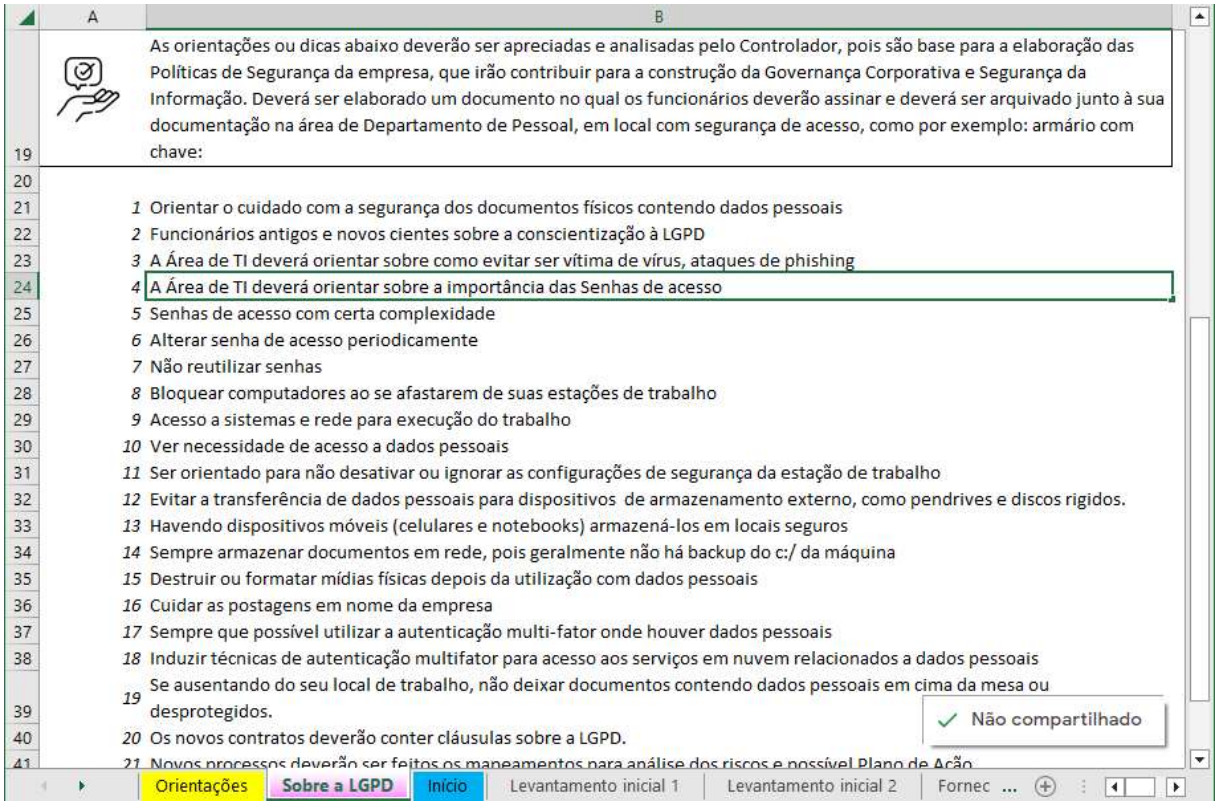
governança e *compliance* se efetivem, a organização deve estabelecer diretrizes no âmbito corporativo e de segurança da informação de forma documentada e preferencialmente assinada pelos colaboradores. No artefato, na planilha “Sobre a LGPD” há uma relação de dicas que contribuem para boas práticas, que podem ser transcritas para uma Política de Segurança Interna.

A empresa, sabendo do seu propósito, que é o que “direciona a estratégia e fundamenta a cultura da organização” (IBGC, 2023, p.15), através de sua equipe, deve adotar postura para contribuir positivamente para uma boa reputação da organização, fortalecendo a confiança de cliente internos e externos, e assim, o engajamento de todas as partes interessadas. Dessa forma, assumindo os princípios da governança corporativa mencionado na seção 2.6 (Governança corporativa e LGPD), Quadro *5*.

Da mesma forma, atribuindo a Governança de Segurança da Informação, que as normas da ISO (ABNT NBR ISO/IEC 27014, 2013; ABNT NBR ISO/IEC 31000, 2018; ABNT NBR ISO/IEC 27005, 2019) mencionam, não tem como tratar a Governança Corporativa de forma separada da Governança de Segurança da Informação. Assim, as orientações apresentadas na planilha intitulada “Sobre a LGPD” (Figura 22) contribuem na composição da Política de Segurança da empresa.

A integração da Governança Corporativa e da Governança de Segurança da Informação conduz ao que é enfatizado na Seção II do Capítulo VII da LGPD (BRASIL, 2018). Essa seção destaca a importância de definir a Política de Privacidade da empresa, esclarecer ao visitante do site da empresa quais dados são coletados e qual a finalidade dessa coleta. Além disso, é inevitável obter o consentimento do visitante para essa coleta, permitindo que ele decida se deseja ou não compartilhar o seu dado. Esse visitante é o titular, ou seja, o proprietário dos dados a serem coletados. Portanto, a conformidade com a LGPD requer uma abordagem holística que engloba tanto a governança corporativa quanto a segurança da informação.

Figura 22 - Artefato: Sobre a LGPD – Dicas de Governança Corporativa e de Segurança da Informação



Fonte: Elaborado pela autora (2023).

Essa combinação se mostra favorável ao comprometimento do controlador em assegurar o seu interesse em manter o dado do titular em seu ambiente, com segurança. Isso é demonstrado, no artefato, junto à planilha “TI-Atribuições”. Os princípios da Governança Corporativa devem estar vinculados nesse interesse do controlador. Todos esses quesitos têm que estar devidamente evidenciados pelo controlador, caso haja alguma fiscalização da ANPD, possui todas as questões documentadas.

4.3.1 Política de Segurança

Segundo Marcondes (2022, p. 1), uma política de segurança é o “conjunto de princípios, diretrizes e objetivos que condicionará a estratégia de segurança da organização, visando a preservação da incolumidade das pessoas, a proteção do patrimônio e missão da organização”. É um documento formal da empresa que deve

ser observado e aplicado por todos os colaboradores da organização (MARCONDES, 2022).

Desta forma, a Política de Segurança é responsável pelos procedimentos destinados a proteger os bens físicos e tecnológicos de uma organização. Através dessa política, é possível fornecer orientações claras aos funcionários quanto ao uso adequado de informações confidenciais da empresa (MARCONDES, 2022).

Marcondes (2022) e Paranhos (2023) condicionam a Política de Segurança com o planejamento de segurança da organização. Assim, busca preservar a segurança da empresa, da equipe, do patrimônio, das informações tanto pessoais quanto empresariais. Paranhos (2023, p. 5) ressalta que é necessário “ouvir os colaboradores” pois a segurança é uma via de mão dupla, e podem expor situações e sugerir prevenções para incluir na Política de Segurança da organização.

No artefato, na planilha intitulada “Início”, está apresentada no roteiro a demanda de Política de Segurança Interna, há um modelo desta política, mas em caráter orientativo (coluna intitulada “LINK”). A elaboração dessa política requer uma análise da gestão da empresa com a prática, dentro da infraestrutura e governança corporativa e de segurança.

4.3.2 Política de Privacidade

A Política de Privacidade é um documento que explica as práticas e processos adotados por um site, aplicativo ou provedor em relação à privacidade e segurança de seus usuários (BASTOS, 2021). Esta política está diretamente ligada à LGPD pois é nela que tem informações sobre coleta, armazenamento, tratamento, compartilhamento e eliminação de dados pessoais dos usuários.

É importante ressaltar que uma Política de Privacidade é um documento que o controlador explicita para o titular quais dados estão sendo coletados, porque esses dados estão sendo coletados, e como eles serão tratados, por quanto tempo eles serão tratados e qual a justificativa legal (também chamada de base legal) para o tratamento desses dados (BARTOLOMEO, 2023). Para citar um exemplo, a Política de Privacidade do Google explica que eles coletam informações para fornecer serviços melhores a todos os usuários, o que inclui descobrir coisas básicas, como idioma falado, até coisas mais complexas, como anúncios considerados mais úteis (GOOGLE, 2023).

Dessa forma, a Política de Privacidade desempenha papel relevante na transparência e na construção da confiança entre os usuários e provedores de serviços *online*. É importante que os usuários leiam e entendam essas políticas para proteger seus direitos de privacidade.

Operacionalmente, uma empresa que possui um site na internet precisa solicitar ao desenvolvedor do site informações sobre quais *cookies* são coletados e para qual finalidade, a fim de iniciar a construção de uma Política de Privacidade. É imperativo que a empresa detalhe essa coleta e finalidade, oferecendo ao usuário a opção de decidir se deseja ou não continuar acessando o site da empresa. Caso o usuário opte por não aceitar os *cookies*, a empresa deve esclarecer quais funcionalidades estarão disponíveis e quais estarão bloqueadas. Essas alternativas fazem parte de um detalhamento transparente que visa respeitar a privacidade do usuário e cumprir as regulamentações de proteção de dados.

A construção de uma Política de Privacidade depende de vários fatores, incluindo, mas não se limitando, à natureza do negócio da organização, ao tipo de dados pessoais coletados, à finalidade da coleta de dados e às medidas de segurança implementadas para proteger os dados. Todos esses fatores se moldam às exigências da LGPD. Além disso, é essencial considerar as expectativas e direitos dos titulares dos dados, bem como os princípios elencados nesta lei (seção 2.1). A inovação está presente nessa política, pois as organizações devem estar preparadas para adaptar suas políticas de privacidade às mudanças tecnológicas e regulatórias (seção 2.5).

5 CONCLUSÃO

Nos dias atuais, a informação circula de forma ordenada e desordenada em todos os aspectos. Não é diferente em relação aos dados pessoais. Plataformas digitais, incluindo as redes sociais, coletam, tratam, armazenam, compartilham esses dados, mas raramente observa-se a eliminação e nem o cuidado com essas informações. Os dados pessoais, muitas vezes, tornam-se o produto de uma transação, sem que haja qualquer comunicação ou consentimento do titular dos dados.

A LGPD foi promulgada para regular a proteção dos dados pessoais. Para qualquer ação que envolva essas informações, é necessária a autorização do titular, ou seja, o proprietário dos dados deve dar o seu consentimento. Nesta linha, a entidade que coleta os dados tem a obrigação de informar para qual finalidade eles serão utilizados. Assim, a LGPD imerge em conceitos de responsabilidade, ética, segurança da informação, boas práticas de governança e, em caso de fiscalização, possíveis sanções administrativas ou monetárias.

Embora as grandes e médias empresas possuam departamentos internos, contratem consultorias ou especialistas para garantir a conformidade, a realidade das micro e pequenas empresas está distante de estar em conformidade com esta legislação. Esse segmento de empresas de menor porte busca parceiros para o andamento dos negócios e obrigações fiscais, sendo as organizações contábeis um desses parceiros.

A segurança da informação é o fator mais relevante abordado na LGPD e a responsabilidade recai sobre o controlador. Associado a esse aspecto, a governança corporativa pode contribuir para que a adequação à lei se torne uma prática rotineira da empresa.

Assim iniciou-se a produção de um artefato, considerando a segurança das informações como um dos pilares para a sua construção. Além disso, buscou-se desenvolver um artefato simples para que este possa ser aplicado pelas organizações contábeis aos seus clientes, micro e pequenas empresas.

Considerando que esse é um estudo de administração de empresas, optou-se por empregar um método investigativo que refletisse a realidade das micro e pequenas empresas e das organizações contábeis, escolhendo a *Design Science Research*. Essa metodologia permitiu uma interação entre o ambiente acadêmico, a

LGPD e as empresas, conduzida através de etapas que possibilitaram a construção do artefato aplicável de forma prática nas empresas. Isso possibilita o desenvolvimento de novas estratégias e processos, caracterizando-se como inovavor para alavancar a competitividade no ambiente empresarial.

5.1 ALCANCE DOS OBJETIVOS

O objetivo geral desta pesquisa foi desenvolver um artefato que permitisse às organizações contábeis facilitarem a adequação à LGPD em seus clientes categorizados como micro e pequenas empresas. A construção do referido instrumento foi conduzida e as proposições estabelecidas foram cumpridas, demonstrando uma integração entre a LGPD, Governança Corporativa e Governança de Segurança da Informação.

O primeiro objetivo específico buscou formular uma proposta para que as organizações contábeis pudessem auxiliar no processo de adequação à LGPD em micro e pequenas empresas. Para a elaboração dessa proposta, empregou-se a metodologia da *Design Science Research* para a construção de um artefato. As fases dessa metodologia, que incluem conscientização, sugestão, desenvolvimento, avaliação e conclusão, foram seguidas na produção desse instrumento.

Através dessas etapas, foi possível compreender que tanto as organizações contábeis quanto as micro e pequenas empresas precisavam de uma ferramenta de fácil acesso e não onerosa. Assim, optou-se por uma planilha eletrônica para formalizar o referido artefato.

A elaboração do artefato demandou a compreensão da LGPD e da tecnologia da informação. O conhecimento básico em tecnologia da informação é necessário para entender sobre coleta, armazenamento, tratamento e possível exclusão do dado pessoal, pois impacta quase que diretamente o meio digital. Esse ciclo também abrange o meio físico, que pode ser compreendido e resolvido de forma física. Entretanto, tanto no aspecto físico como virtual, envolvem indivíduos em suas rotinas de trabalho, que devem ser conscientizados sobre a referida lei e processos internos onde circulam dados pessoais.

O segundo objetivo específico constituiu na validação desse artefato junto às organizações contábeis. Esse processo foi realizado, validado e as sugestões dos participantes foram acolhidas.

O terceiro objetivo específico envolveu o desenvolvimento e a implementação de práticas de boa governança corporativa em paralelo com a adequação à LGPD. Para alcançar este objetivo, buscou-se compreender o tema junto a entidades como o Instituto Brasileiro de Governança Corporativa. Através desse processo, chegou-se às normas técnicas da ISO, abrangendo categorias de Segurança da Informação até Governança de Segurança da Informação. Dessa forma, concluiu-se que a LGPD está intrinsecamente ligada à Governança Corporativa e à Governança de Segurança da Informação. Elementos extraídos desses documentos foram incorporados como orientações no artefato, contribuindo para a realização desse objetivo específico.

5.2 CONTRIBUIÇÕES PRÁTICAS

Este trabalho contribui para a capacitação das organizações contábeis na implementação da LGPD em seus clientes com perfil de micro e pequenas empresas. Isso se dá através de um processo de maturação profissional, tanto na compreensão aprofundada dos clientes, dos processos internos, quanto em relação à LGPD. Esse crescimento não se limita apenas à compreensão da referida legislação, mas também engloba a Governança Corporativa e a Segurança da Informação.

Essa abordagem oferece a oportunidade de aprofundar o conhecimento e esclarecer os processos organizacionais. Ao detalhar os procedimentos e identificar os fornecedores envolvidos, é possível realizar uma reavaliação crítica do que está funcionando bem e identificar processos que podem ser aprimorados. Além disso, essa análise permite questionar a necessidade de determinadas atividades, o que pode resultar economia de recursos.

A implementação do artefato proporciona uma reflexão sobre as atividades da empresa, principalmente na padronização de processos e comportamento uniforme, o que é observado através do mapeamento dos processos. Esse mapeamento proporciona a observação de lacunas quanto às políticas de boa governança estarem claras para toda a organização e se torna prática ao documentar Políticas de Segurança, Políticas de Privacidade e Práticas de Boa Governança, aprovadas pelo corpo diretivo e apresentada aos funcionários.

O mapeamento dos processos permite detalhar atividades e identificar o percurso do dado, ou o seu ciclo de vida, observando a segurança enquanto este dado estiver sob responsabilidade da empresa. Empresas terceirizadas também podem ser

responsáveis por esta segurança, e a verificação de contratos entre a empresa controladora e a operadora é indispensável para mitigação dos riscos de vazamento de dados.

O serviço de adequação à LGPD oferecido pela organização contábil pode ser um diferencial em seu portfólio, podendo gerar receitas adicionais e, principalmente, fidelizar ainda mais o seu cliente. Ao aplicar o artefato, o profissional contábil, que já tem o conhecimento de aspectos relacionados às rotinas contábeis, estará imergindo no negócio do cliente, o que pode gerar um maior entendimento de suas práticas, favorecendo uma relação de ganha-ganha.

5.3 CONTRIBUIÇÕES TEÓRICAS

Academicamente esta pesquisa contribui significativamente para preencher a lacuna teórica de aplicação da LGPD por organizações contábeis. A condução do método de *Design Science Research* para construção do artefato caracteriza-se uma aplicação inédita, pois interpretou-se a LGPD e outros documentos para gerar uma ferramenta prática. Este trabalho contribuiu com a aplicação do *Design Science Research* relacionado à LGPD, aplicação até então não localizada na literatura.

5.4 RECOMENDAÇÕES E PESQUISAS FUTURAS

O trabalho demonstrou a aplicação de um artefato construído através do método *Design Science Research*. Esse artefato foi desenvolvido através de planilha eletrônica, bem como *links* de documentos relacionados à adequação à LGPD, promovendo a construção de conhecimento dos profissionais das organizações contábeis. Por se tratar de um artefato produzido a partir da LGPD, qualquer atualização na lei demandará atualização do artefato, portanto, revisões periódicas são importantes.

O artefato em questão beneficia as empresas no aspecto financeiro, uma vez que planilhas eletrônicas são de fácil utilização e apresentam um custo relativamente acessível. Contudo, é possível ampliar esse artefato por meio do desenvolvimento de um sistema ou aplicativo, que facilitaria ainda mais sua utilização. Vale ressaltar que essa expansão implicaria em custos mais elevados, porém os benefícios em termos

de conformidade regulatória e eficiência operacional poderiam justificar esse investimento.

Este artefato foi desenvolvido especificamente para organizações contábeis auxiliarem na adequação à LGPD em micro e pequenas empresas, uma vez que a legislação favorece a simplificação do processo, como é o caso da figura do Encarregado de Proteção de Dados (DPO) ser opcional. No entanto, nada impede que o artefato seja aprimorado e adaptado para empresas de médio e grande porte, pois depende da realidade de cada organização.

Embora esse artefato seja destinado aos clientes do segmento micro e pequenas empresas das organizações contábeis, a própria organização contábil pode se beneficiar, realizando sua própria adequação e customização. Dessa forma, o artefato também pode ser aplicado em qualquer empresa de micro e pequeno porte por um profissional que tenha um grau básico de compreensão da tecnologia da informação e a percepção de melhorar seus processos, principalmente na segurança de documentos, tanto físicos como virtuais.

A organização contábil, ao implementar a adequação em seus clientes, pode ampliar seu portfólio de serviços incluindo o trabalho do Encarregado de Proteção de Dados (DPO) terceirizado, o que pode gerar mais receita para essa organização. Ampliando seu portfólio de serviços e estando ainda mais enraizado nos processos de seu cliente, estes tornam-se ainda mais próximos das organizações contábeis, fortalecendo a confiança entre o cliente e o prestador de serviços.

O processo de sensibilização em relação à LGPD para os funcionários é destinado à implementação dentro da organização. É plausível que indivíduos disseminem o assunto em seu círculo social, promovendo uma maior compreensão sobre a exposição de dados. Como resultado, eles podem exercer maior prudência ao acessar sites, redes sociais e ao expor seus dados pessoais, reduzindo probabilidade de se tornarem vítimas de golpes e fraudes.

REFERÊNCIAS

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27000**: Tecnologia da informação — Técnicas de segurança — Sistema de gestão da segurança da informação. Rio de Janeiro, 2013

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27001**: Tecnologia da informação — Técnicas de segurança — Sistema de gestão da segurança da informação – Requisitos. Rio de Janeiro, 2013.

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27002**: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27005**: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro, 2013.

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27014**: Tecnologia da informação — Técnicas de segurança — Governança da segurança da informação. Rio de Janeiro, 2013.

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27032**: Tecnologia da informação — Técnicas de segurança — *Guidelines for cybersecurity*. Geneva: ISO/IEC. 2012.

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27701**: 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. Rio de Janeiro, 2019.

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO 31000**: Gestão de riscos - Diretrizes. Rio de Janeiro, 2018.

ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO 37301**: Sistemas de gestão de compliance – Requisitos com orientação para uso. Rio de Janeiro, 2021.

BARBOSA, Juliana Souza; SILVA, Danihanne Borges; OLIVEIRA, Daniela Cabral de; JESUS, Dilça Cabral de; MIRANDA, Wesley Flávio. **A proteção de dados e segurança da informação na pandemia COVID-19**: contexto Nacional. Pesquisa, Sociedade e Desenvolvimento , [S. l.] , v. 2, pág. e40510212557, 2021. DOI: 10.33448/rsd-v10i2.12557. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/12557. Acesso em: 4 jun. 2024.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BARTOLOMEO, Felipe. **Política de privacidade: o que é, objetivo e caso do *threads***. Aurum. 2023.Disponível em: https://www.aurum.com.br/blog/politica-de-privacidade/. Acesso em: 01 nov. 2023.

BASTOS, Jader. **O que é política de privacidade, como fazer a sua relação com a LGPD**. Sólides. 2021. Disponível em: https://blog.solides.com.br/o-que-e-politica-de-privacidade/. Acesso em: 01 nov. 2023.

BAUMAN, Zygmunt. **Danos colaterais: desigualdades sociais numa era global**. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013. Título original: Collateral Damage: Social Inequalities in a Global Age. Disponível em: https://asdocs.net/L9rm?pt=L01BL1l4Z2ZxN0VnMGZ0d3lsNWtOV3RSTlZKRFZrUjBVM3BTTW5weWNXdFliREp4YmxFOVBRPT0%3D. Acesso em: 04 mai. 2023.

BEUREN, Ilse M.; BARP, Adriano D.; FILIPIN, Roselaine. **Barreiras e possibilidade de aplicação da contabilidade gerencial em micro e pequenas empresas por meio de empresas de serviços contábeis**. ConTexto - Contabilidade em Texto, Porto Alegre, v. 13, n. 24, p. 79–92, 2013. Disponível em: https://seer.ufrgs.br/index.php/ConTexto/article/view/32370. Acesso em: 12 nov. 2023.

BIBLIOTECA DIGITAL BRASILEIRA DE TESES E DISSERTAÇÕES. **Busca avançada**. Disponível em: http://bdtd.ibict.br/. Acesso em: 03 jan. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial [da] República Federativa do Brasil. Brasília, DF. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o regulamento de aplicação para agentes de tratamento de pequeno porte. Edição 20, seção 1, página 6. **Publicado em 28 jan. 2022**. Órgão: Presidência da República/Autoridade Nacional de Proteção de Dados. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 17 mar. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 mai. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Art. 6º e Art. 9º. **Diário Oficial República Federativa do Brasil**, Brasília, DF, 24 abr. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 05 mai. 2024.

BRASIL. Decreto nº 9.319, de 21 de março de 2018. Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. **Diário Oficial da União**, Brasília, DF, 22 mar. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm. Acesso em: 30 abr. 2023.

BRASIL. Lei Complementar nº 123, de 14 de dezembro de 2006. Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte. **Diário Oficial da**

República Federativa do Brasil. Brasília, DF, 15 dez. 2006. Seção 1, p. 12. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp123.htm. Acesso em: 04 mai. 2023.

BRASIL. Lei Complementar nº 128, de 19 de dezembro de 2008. Dispõe sobre a readmissão dos optantes pelo Simples Nacional excluídos desse regime de tributação. **Diário Oficial da União**, Brasília, DF, 22 dez. 2008. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp128.htm. Acesso em: 04 mai. 2023.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados. **Diário Oficial [da] República Federativa do Brasil**. Brasília, DF, 9 jul. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Lei/L13853.htm. Acesso em: 4 mai. 2023.

BRASIL. Lei nº 14.010, de 10 de junho de 2020. Dispõe sobre o vigor da Lei Geral de Proteção de Dados. **Diário Oficial [da] República Federativa do Brasil**. Brasília, DF, 11 jun. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm. Acesso em: 4 mai. 2023.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil**. Diário Oficial da União:** seção 1Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 27 mar. 2023.

BRASIL.[Consolidação das leis do trabalho (1943)]. Consolidação das leis do trabalho: Decreto-Lei nº 5.452. Rio de Janeiro, RJ: **Diário Oficial da União**, 1943. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del5452compilado.htm. Acesso em: 04 mai. 2023.

BRASIL. Empresas e Negócios. **Painel Mapa de Empresas**. 2023. Disponível em: https://www.gov.br/empresas-e-negocios/pt-br/mapa-de-empresas/painel-mapa-de-empresas. Acesso em: 06 fev. 2023.

BROGIO, Raíssa C.S.; MELLO, Ricardo B. **Importância do profissional de departamento pessoal e a relação com a contabilidade da empresa**. Varginha, MG: Fundação de Ensino e Pesquisa do Sul de Minas, 2016. II Congresso Internacional do Grupo Unis. Disponível em: http://repositorio.unis.edu.br/bitstream/prefix/502/1/IMPORT%C3%82NCIA%20DO%20PROFISSIONAL%20DE%20DEPARTAMENTO%20PESSOAL%20E%20A%20RELA%C3%87%C3%83O%20COM%20A%20CONTABILIDADE%20DA%20EMPRESA.pdf. Acesso em: 04 abr. 2023.

CABRAL, R. L. B.; VASCONCELOS, V. N.; LINS, F. A. A.; SANTOS, G. A. V.; LOSSE, M. A. P. F.; MEDEIROS, A. G. M.; SOUSA, E. T.; FELIX, M. S.. Transparência e Livre Acesso: **Uma Avaliação da Disponibilidade de Informações sobre a LGPD em Sites de Tribunais de Contas no Brasil**. In: workshop de computação aplicada em governo eletrônico (WCGE), 11. , 2023, João

Pessoa/PB. Porto Alegre: Sociedade Brasileira de Computação, 2023. p. ISSN 2763-8723. DOI. Disponível em: https://doi.org/10.5753/wcge.2023.230698. Acesso em: 15 out. 2023.

CANEDO, Edna Dias; FERNANDES, Marcio Aurélio de Souza; SANTOS, Rodrigo Marques dos; MENDONÇA, Fábio Lúcio Lopes de; SILVA, Daniel Alves da; SOUSA JR, Rafael Timóteo de. Universidade de Brasília – UNB, Campus Universitário Darcy Ribeiro, Brasília – DF, CEP 70910-900, Brasil. **Conferência Ibero-Americana de Computação Aplicada**, 2023, Madeira, Portugal. Disponível em: https://ciaca-conf.org/wp-content/uploads/2022/11/4_CIAWI2022_PT_F_031.pdf Acesso em: 20 mai.2024.

CANEDO, Edna Dias; CERQUEIRA, Anderson Jefferson; GRAVINA, Rogério Machado; RIBEIRO, Vanessa Coelho; CAMÕES, Renato; REIS, Vinicius Eloy dos; MENDONÇA, Fábio Lúcio Lopes; SOUSA JR, Rafael Timóteo de. Universidade de Brasília – UNB, Brasília – DF, CEP 70910-900, Brasil. ***Proposal of an Implementation Process for the Brazilian General Data Protection Law*** (LGPD), 2021. Disponível em: https://www.researchgate.net/publication/351340558 .Acesso em: 04 jun. 2024

CARNEIRO, Luciana E. dos S.; ALMEIDA, Maurício B. Design Science: Estudo de um campo teórico. **Brazilian Journal of Information Studies**. 2019.Disponível em: https://revistas.marilia.unesp.br/index.php/bjis/article/download/8796/5893/30207. Acesso em: 18 nov. 2023.

CFC – Conselho Federal de Contabilidade. **Quantidade de Contadores e Escritórios Contábeis no Brasil**. Brasília. 2023. Disponível em: https://www3.cfc.org.br/spw/crcs/ConselhoRegionalAtivo.aspx. Acesso em: 09 fev. 2023.

CNI – Confederação Nacional da Indústria. **LGPD: o que sua empresa precisa saber.** Brasília, 2020. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/d6/29/d6297686-923a-4f69-8d4b-ff81bb4e8eb8/lgpd_o_que_sua_empresa_precisa_saber.pdf Acesso em: 17 nov. 2023.

CRUZ, Alexa. **O que é vazamento de dados e como acontece**. Idwall. 2021. Disponível em: https://blog.idwall.co/o-que-e-vazamento-de-dados-e-como-acontece/. Acesso em: 04 nov. 2023.

DENZIN, Norman. K.; LINCOLN, Yvonna. S. Introdução: a disciplina e a prática da pesquisa qualitativa. **O planejamento da pesquisa qualitativa**: teorias e abordagens. 2. ed. Porto Alegre: Artmed, 2006.

DRESCH, Aline; LACERDA, Daniel P.; JÚNIOR, José A. V A. **Design science research: método de pesquisa para avanço da ciência e tecnologia** . Bookman: Grupo A, 2015. E-book. ISBN 9788582605530. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582605530/. Acesso em: 24 nov. 2023.

ECHTTERHOFF, Gisele. **Direito à privacidade dos dados genéticos**. Curitiba: Juruá, 2010.

ECKERT, Alex; MENEGUZZO, Ana P.; MECCA, Marlei S**.** Identificação e análise dos serviços prestados pelos profissionais contábeis aos clientes: uma pesquisa com micro e pequenas empresas metalúrgicas. Curitiba: **Administração de Empresas em Revista**, [S.l.], v. 2, n. 20, p. 174 - 198, set. 2020. ISSN 2316-7548. Disponível em: http://revista.unicuritiba.edu.br/index.php/admrevista/article/view/4314/371372592. Acesso em: 09 fev. 2023.

FEBRABAN (Febraban Tech). **LGPD está fora da realidade de 80% das empresas no Brasil**, diz estudo. 2022. Disponível em: https://febrabantech.febraban.org.br/blog/lgpd-esta-fora-da-realidade-de-80-das-empresas-no-brasil-diz-estudo. Acesso em: 09 fev. 2023.

FERREIRA, Adriano. **O impacto da LGPD nos escritórios de contabilidade**. 2019. Disponível em: https://www.dominiosistemas.com.br/blog/lgpd-nos-escritorios-de-contabilidade/. Acesso em: 31 out. 2023.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, Florianópolis, v. 23, n. 9, p. 284-301, fev. 2020. ISSN 2358-1352. doi:http://dx.doi.org/10.26668/IndexLawJournals/2358-1352/2019.v23i9.5343. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 26 abr. 2023.

FONTAINHAS, Emília Golim; ANDRADE, Francisco C.P.; ALMEIDA, José Bacelar. Do consentimento para a utilização de testemunhos de conexão (cookies). **Revista Scientia Ivridica**. Universidade do Minho. 2016. Disponível em: https://repositorium.uminho.pt/handle/1822/50509. Acesso em: 17 nov. 2023.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2010.

GOOGLE. 2023. **Política de Privacidade – Privacidade & Termos**. Disponível em: https://policies.google.com/privacy?hl=pt-BR. Acesso em: 01 nov. 2023.

GOOGLE ACADÊMICO. Busca avançada. Disponível em: https://scholar.google.com.br/?hl=pt. Acesso em: 05 fev. 2023.

GUNDAY, Gurhan; ULUSOY, Gunduz; KILIC, Kemal; ALPKAN, Lutfihak. *Effects of innovation types on firm performance. International Journal of Production Economics* (2011), 133(2), 662-676. Disponível em: https://doi.org/10.1016/j.ijpe.2011.05.014 . Acesso em: 07 jun.2024

HEVNER, Alan R.; MARCH, Salvatore T.; PARK, Jinsoo. Design Science in Information Systems Research. MIS Quaterly, v. 28, n. 1, p. 75-105, 2004. Disponível em:

https://www.researchgate.net/publication/201168946_Design_Science_in_Information_Systems_Research Acesso em 10 mar. 2023.

IBGC. Instituto Brasileiro de Governança Corporativa.**Código das melhores práticas de governança corporativa**. 2023. São Paulo: IBGC, 6º edição. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 16 nov. 2023.

IPEA – Instituto de Pesquisa Econômica Aplicada. Carta de Conjuntura – PNAD – **Pesquisa Nacional por Amostra de Domicílios** - Contínua. 2022. Disponível em: https://www.ipea.gov.br/cartadeconjuntura/index.php/tag/pnad-continua/. Acesso em: 02 mar. 2023.

ISAAK, Jim; HANNA, Mirna. J. **User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection**. Editora IEEE, Computer 51 (8), pp. 56-59 (doi: 10.1109/MC.2018.3191268. 2018. Disponível em: https://ieeexplore.ieee.org/document/8436400. Acesso em: 06 nov. 2023.

LACERDA, Daniel Pacheco; DRESCH, Aline; PROENÇA, Adriano; JÚNIOR, José Antonio Valle Antunes. ***Design Science Research*: método de pesquisa para a engenharia de produção**. São Carlos, SP: Gestão & Produção, São Carlos, v. 20, n. 4, p. 741-761, 2013. Disponível em: https://www.scielo.br/j/gp/a/3CZmL4JJxLmxCv6b3pnQ8pq/. Acesso em: 07 fev. 2023.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia científica**. 5º. ed. ver. ampl. São Paulo: Atlas, 2003.

LINKMEX Comércio Internacional. **Impactos da LGPD no comércio exterior e como proteger sua empresa**. 2022. Disponível em: https://www.linkmex.com.br/blog/comercio-exterior/impactos-da-lgpd-no-comercio-exterior-e-como-proteger-sua-empresa/. Acesso em: 16 nov. 2023.

LOBATO, Fábio M.F. **Proteção intelectual de obras produzidas por sistemas baseados em inteligência artificial:** uma visão tecnicista sobre o tema. Universidade Federal do Oeste do Pará. Instituto Observatório de Direito Autoral. 2022. Disponível em: 361161689_Proteccao_intelectual_de_obras_produzidas_por_sistemas_baseados_em_inteligencia_artificial_uma_visao_tecnicista_sobre_o_tema. Acesso em: 18 nov. 2023.

MACHADO, Celso Junior; SOUZA, Maria Tereza Saraiva de; PARISOTTO, Iara Regina dos Santos; PALMISANO, Angelo. As leis da bibliometria em diferentes bases de dados científicos. Santa Catarina: **Revista de Ciências da Administração**, v. 18, n. 44, p. 111-123. 2016. Disponível em: https://periodicos.ufsc.br/index.php/adm/article/view/2175-8077.2016v18n44p111. Acesso em: 08 fev. 2023.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. RM Digital Education. 1ª Edição. Goiânia – GO. 2019.

MANSON, N.J. Is operations research really research? **School of Information Technology**, Monash South Africa. 2006. Disponível em: https://orion.journals.ac.za/pub/article/view/40/40. Acesso em: 23 nov. 2023.

MARCONDES, José Sérgio. **Política de Segurança: O que é, Qual sua Importância, Como criar**. Blog Gestão de Segurança Privada. 2022. Disponível em: https://gestaodesegurancaprivada.com.br/politica-de-seguranca-o-que-e-qual-sua-importancia-como-criar/. Acesso em: 30 nov. 2023.

MARTENS, Cristina D.P. **A tecnologia de informação (TI) em pequenas empresas industriais do Vale do Taquari/RS**. Porto Alegre. 2001. Dissertação (Mestrado em Administração) - Universidade Federal do Rio Grande do Sul, Rio Grande do Sul. Disponível em: https://lume.ufrgs.br/handle/10183/2120. Acesso em: 12 nov. 2023.

MILFONT, Rejane F. de N**. Direito à privacidade e as melhores práticas das empresas na adequação à Lei Geral de Proteção de Dados – LGPD**. 2022. Dissertação (Mestrado em Administração) – Universidade de Caxias do Sul. Caxias do Sul, 2022.

NAKAGAWA, M. **Ferramenta: 5w2h** – Plano de Ação para empreendedores. São Paulo: Editora Globo, 2014. Disponível em: https://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/5W2H.pdf. Acesso em: 10 ago. 2023.

NICOLAU, Junia S.; COUTO, Pricila B. **A ética aplicada na rotina do profissional da contabilidade**. João Monlevade, MG: Instituto Ensinar Brasil, 2018. Disponível em: http://dspace.doctum.edu.br:8080/xmlui/handle/123456789/2122. Acesso em: 26 abr. 2023.

NUNES, Natália M. **10 princípios da LGPD para o tratamento dos dados pessoais.** NDM Nunes Duarte & Maganha Advogados. 2019. Disponível em: https://ndmadvogados.com.br/artigos/10-principios-da-lgpd-para-o-tratamento-de-dados-pessoais?gad_source=1&gclid=Cj0KCQiA35urBhDCARIsAOU7QwmwgWu8ACeJ-U2RhVTAravtZu41UDA3-SD3mAWeVsF__MrIPqAZdLAaAiwmEALw_wcB. Acesso em: 29 nov. 2023.

OCDE/Eurostat (2018), Manual de Oslo 2018: **Diretrizes para Coletar, Reportar e Usar Dados sobre Inovação**, 4ª Edição, A Medição de Atividades Científicas, Tecnológicas e de Inovação, OCDE Publishing, Paris/Eurostat, Luxemburgo. Disponível em: https://doi. org/10.1787/9789264304604-en. Acesso em: 16 nov. 2023.

OLIVEIRA, Edson. **Contabilidade Digital**. São Paulo: Atlas, 2014. E-book. ISBN 9788522491315. Disponível em:

https://integrada.minhabiblioteca.com.br/#/books/9788522491315/. Acesso em: 24 fev. 2023.

OLIVEIRA, Otávio J.; PALMISANO, Angelo; MAÑAS, Antonio V.; MODIA, Esther C.; MACHADO, Márcio C.; FABRÍCIO, Márcio M.; MARTINO, Mariluci A,; NASCIMENTO, Paulo T.de S.; PEREIRA, Raquel S.; SOUZA, Roberto de; BARROCO, Rosana; CALIXTO, Rosangela; SERRA, Sheyla M.P.; MELHADO, Silvio B.; CARVALHO, Valter R. de. **Gestão da qualidade: Tópicos avançados**. 1. Ed. [S.1.]: Editora: Cengage Learning, 2003.

PARANHOS, Carol F. **Modelo de política de segurança para as empresas.** Diego Castro Advogado. 2023. Disponível em: https://diegocastro.adv.br/modelo-de-politica-de-seguranca-para-empresas/. Acesso em: 30 nov. 2023.

PAREDES, Breno J.B.; SANTANA, Guilherme A.; FELL, André Felipe de A. Um estudo de aplicação do radar da inovação: o grau de inovação organizacional de uma empresa de pequeno porte no setor metal-mecânico**. Navus – Revista de Gestão e Tecnologia**. Florianópolis, SC. ISSN 2237-4558. 2014. Disponível em: https://www.redalyc.org/pdf/3504/350450613007.pdf. Acesso em: 13 nov. 2023.

PIMENTA, Alexandre M.S; QUARESMA, Rui F.C. A segurança dos sistemas de informação e o comportamento dos usuários. **JISTEM – Journal of Information Systems and Technology Management**, 13(3), 533-552. 2016. Disponível em: https://www.scielo.br/j/jistm/a/n6HBtP6htxYkTKKrjt9VsRz/?format=html#ModalTutors. Acesso em: 06.nov. 2023.

QUEIROZ, Rodrigo C. **Políticas de Governança e de Compliance – Objetivando mitigar os riscos das organizações.** Caderno de Pós-Graduação em Direito. Compliance e Relações Governamentais. Brasília. 2019. Disponível em: https://core.ac.uk/download/pdf/223118053.pdf#page=69. Acesso em: 05. nov. 2023

REIS, Paulo. **Ciência do Artificial e Design Science Research**. In: Coordenação de Desenvolvimento da Cultura da Inovação – CDCI. Artigos Técnicos – Ano 3, volume 22, 2019. Laboratório de Cenários - LabCen. Disponível em: https://inovacao.ufrj.br/images/vol_22_ciencia_artificial_design_science_research_2019.pdf. Acesso em: 05 nov. 2023.

REVISTA EXAME. São Paulo, SP. **O escândalo de vazamento de dados do Facebook é mito pior do que parecia**. 2018. Disponível em: https://exame.com/tecnologia/o-escandalo-de-vazamento-de-dados-do-facebook-e-muito-pior-do-que-parecia/. Acesso em: 03 nov. 2023.

RIBEIRO, Frank R. de P.; MOREIRA, Cristiano. A percepção dos profissionais da área contábil e dos gestores sobre os impactos da implementação da LGPD. **Revista de Auditoria, Governança e Contabilidade**. 2021. Disponível em: https://revistas.fucamp.edu.br/index.php/ragc/article/view/2431. Acesso em: 17 nov. 2023.

RUFFONI, Estêvão P.; REICHERT, Fernanda M. **Inovação em setores de baixa intensidade tecnológica: Uma análise das capacidades de inovação da**

indústria de calçados brasileira. 2018. Simpósio de gestão da Inovação Tecnológica. Porto Alegre/RS. Disponível em: https://www.researchgate.net/publication/339089010_Capacidades_de_Inovacao_na_Industria_Calcadista. Acesso em: 15 nov. 2023.

SANTOS, Lucas M. dos; SILVA, Gustavo M.; NEVES, Jorge A. B**.** Risco de sobrevivência de micro e pequenas empresas comerciais**. Revista de Contabilidade e Organizações**, [S. l.], v. 5, n. 11, p. 107-124, 2011. DOI: 10.11606/rco.v5i11.34788. Disponível em: https://www.revistas.usp.br/rco/article/view/34788. Acesso em: 12 nov. 2023.

SCOPUS. **Busca avançada**. Disponível em: https://www-scopus.ez314.periodicos.capes.gov.br/search/form.uri?display=basic#basic. Acesso em: 05 fev. 2023.

SEBRAE – Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. ANS Nacional. Brasil empreendedor. Dia da Micro e Pequena Empresa evidencia **a importância dos empreendedores para o Brasil**. 2022. Disponível em: https://agenciasebrae.com.br/brasil-empreendedor/dia-da-micro-e-pequena-empresa-evidencia-a-importancia-dos-empreendedores-para-o-brasil/#:~:text=Em%20mais%20um%20Dia%20Nacional,5%20milh%C3%B5es%20de%20pequenos%20neg%C3%B3cios. Acesso em: 28 mar. 2023.

SEBRAE – Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. **Tributos para as empresas: conheça as opções que estão disponíveis.** 2023. Disponível em: https://sebrae.com.br/sites/PortalSebrae/ufs/ap/artigos/conheca-os-tres-regimes-tributarios,1ddf8178de8c5610VgnVCM1000004c00210aRCRD. Acesso em: 17 nov. 2023.

SEBRAE – Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. **LGPD: qual o impacto nos pequenos negócios? Sua pequena empresa está preparada?** 2022. Disponível em: https://www.sebrae-sc.com.br/blog/lgpd-qual-o-impacto-nos-pequenosnegocios-sua-pequena-empresa-esta-preparada. Acesso em: 23 mai. 2022.

SEVERINO, Antonio J. **Metodologia do trabalho científico**. São Paulo: Cortez, 2016. Disponível em: https://www.ufrb.edu.br/ccaab/images/AEPE/Divulga%C3%A7%C3%A3o/LIVROS/Metodologia_do_Trabalho_Cient%C3%ADfico_-_1%C2%AA_Edi%C3%A7%C3%A3o_-_Antonio_Joaquim_Severino_-_2014.pdf. Acesso em: 19 abr. 2023.

SIEBRA, Sandra de A.; XAVIER, Gabriela A.C. **Políticas de privacidade da informação: caracterização e avaliação**. BIBLOS, [S. l.], v. 34, n. 2, 2020. DOI: 10.14295/biblos.v34i2.11870. Disponível em: https://periodicos.furg.br/biblos/article/view/11870. Acesso em: 17 nov. 2023.

SILVEIRA, Alexandre Di Miceli da. **Governança Corporativa, desempenho e valor da empresa no Brasil**. 2002. Dissertação (Mestrado em Administração) – Universidade de São Paulo. São Paulo, SP, 2002.

SIMON, Hebert A. The sciences of the artificial. 3 ed. Instituto de Tecnologia de Massachusetts.1996.

SORDI, José Osvaldo de.; AZEVEDO, Marcia Carvalho; MEIRELES, Manuel. A pesquisa design science no Brasil segundo as publicações em administração da informação. 2015. **JISTEM – Journal of Information Systems and Technology Management.** Disponível em: https://www.researchgate.net/figure/Figura-1-Fases-da-pesquisa-design-science-e-os-diferentes-momentos-do-ciclo-de_fig1_276486685. Acesso em: 18 nov. 2023.

SPELL – Scientific Periodicals Eletronic Library. **Busca avançada**. Disponível em: http://www.spell.org.br/. Acesso em: 05 fev. 2023.

TCW Comércio Exterior. **A importância da LGPD no comércio exterior**. 2022. Disponível em: https://tcwcomex.com.br/blog/artigos/a-importancia-da-lgpd-no-comercio-exterior/. Acesso em: 15 nov. 2023.

THOMÉ, Irineu. **Empresas de serviços contábeis: estrutura e funcionamento**. São Paulo: Atlas, 2001.

VAISHNAVI, Vijay; KUECHLER, Willian. **Design Research in Information Systems**. 2009. Disponível em: http:// desrist.org/design-research-in-information-systems. Acesso em: 18 nov. 2023.

WEB OF SCIENCE. **Busca avançada**. Disponível em: https://www-webofscience.ez314.periodicos.capes.gov.br/wos/woscc/basic-search. Acesso em: 05 jan. 2023.

WRUBEL, Franciele; TOIGO, Leandro A.; LAVARDA, Carlos Eduardo F. Mudanças nas rotinas contábeis: contradições institucionais e práxis humanas. Joaçaba, SC: **RACE - Revista de Administração, Contabilidade e Economia**, 2015. v. 14, n. 3, p. 1175-1204, set./dez. 2015. Disponível em: http://editora.unoesc.edu.br/index.php/race. Acesso em: 04 abr. 2023.

ZANATTA, Rafael A.F. **A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet**. São Paulo: Quartier Latin, p. 447-470. (2015). Disponível em: https://www.researchgate.net/profile/Rafael-Zanatta/publication/322581135_A_protecao_de_dados_pessoais_entre_leis_codigos_e_programacao_os_limites_do_Marco_Civil_da_Internet/links/5a60eef5aca272a1581742d4/A-protecao-de-dados-pessoais-entre-leis-codigos-e-programacao-os-limites-do-Marco-Civil-da-Internet.pdf. Acesso em: 04. nov. 2023.

ZAROWIN, Stanley. The new role faced by management accountants. **Journal of Accountancy**. 1997. Disponível em: https://www.journalofaccountancy.com/issues/1997/apr/bizind.html. Acesso em: 12 nov. 2023.

ZIMMERMANN GHISLENI, Júlia. A LGPD e a Risk-Based Approach da Governança Corporativa: A primeira medida para o controlador aplicar os princípios. Porto Alegre: **Revista de Economia, Empresas e Empreendedores** na CPLP 8, 2022: 103–126.

Disponível em: https://revistas.ponteditora.org/index.php/e3/article/view/618. Acesso em: 21 fev. 2023.

GLOSSÁRIO

Agentes de tratamento: Os agentes de tratamento são as empresas ou pessoas envolvidas no processo de tratamento dos dados pessoais. Neste caso, a lei define como agentes o controlador e o operador.

Antivírus: É um software que ajuda a proteger o computador contra a maior parte dos vírus que podem danificar os arquivos.

Aplicativo: É uma ferramenta virtual, que pode ser desenvolvida tanto para dispositivos móveis quanto para desktops e web.

Aprendizado de Máquina Federado: É uma técnica de *machine learning* que permite que vários dispositivos, ou clientes, treinem de forma colaborativa um modelo compartilhado, mantendo seus dados armazenados localmente e privados.

Autoridade Nacional de Proteção de Dados (ANPD): Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Banco de dados: É um conceito mais difundido, principalmente para quem é da área de tecnologia. Segundo a LGPD, banco de dados é o "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico". Vale lembrar que a LGPD se aplica a dados pessoais armazenados tanto de forma *online* quanto de forma física (papel).

Bases legais: As bases legais da LGPD são as justificativas e argumentos que legitimam o tratamento de dados pessoais. Pela lei, o tratamento só é considerado legal se atender a pelo menos uma base legal, também chamada de hipótese. A lei prevê dez bases legais, sendo que não há hierarquia entre elas. Uma das mais conhecidas é o consentimento do titular.

Big data: Em inglês significa "grande dado". Na prática ´uma ferramenta digical capaz de processar um enorme volume de dados de forma inteligente, rápida e eficaz. Sua tecnologia foi desenvolvida em torno de: volume, velocidade, variedade, veracidade e valor.

Blockchain: É um mecanismo de banco de dados avançado que permite o compartilhamento transparente de informações na rede de uma empresa. Um banco de dados blockchain armazena dados em blocos interligados em uma cadeia.

Compliance: Pode ser definido como "estar em conformidade".

Consentimento: O consentimento é um dos termos mais discutidos da LGPD e também uma das suas bases legais. Na prática, é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Cookies: Um cookie é uma pequena quantidade de dados gerada por um site e salva pelo seu navegador web. Seu propósito é lembrar informações sobre você, semelhante a um arquivo de preferências criado por um aplicativo de software. Enquanto os cookies servem muitas funções, seu propósito mais comum é armazenar informações de login para um site específico e melhorar a experiência de navegação na web.

Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Data mapping ou mapeamento de dados: Se refere ao processo de rastreamento e catalogação dos dados coletados e processados por determinada organização, identificando como estes são usados, onde e como são armazenados e como se propagam. Basicamente, consiste em um processo de realização de um inventário de todos os dados coletados e processados para mapear todo o ciclo de vida da informação.

Dado anonimizado: Sado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

DPO (Data Protection Officer): É o profissional que, dentro de uma organização, é encarregado de cuidar das questões referentes à proteção de dados pessoais da organização. Também chamado de Encarregado de dados.

Eliminação: O conceito de eliminação é claro: refere-se a “exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado”. Em geral, a eliminação entra dentro de um contexto de término do tratamento de dados. Aliás, é imprescindível que o tratamento tenha um começo e fim – por lei, em algum momento ele deve terminar.

Encarregado de dados: É o profissional que, dentro de uma organização, é encarregado de cuidar das questões referentes à proteção de dados pessoais da organização. Também chamado de Data Protection Officer (DPO).

Fake News: Notícias que são falsas.

Firewall: É um dispositivo de segurança da rede que monitora o tráfego de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto pré definido de regras de segurança.

Incidente de Segurança com Dados Pessoais: É qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais. Exemplo:

acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração ou vazamento.

Informação: É um conjunto de dados, podendo ser empresariais ou pessoais.

Informação pública: Refere-se a dados ou informações que são abertos ao público e podem ser acessados legalmente por qualquer pessoa.

Informação publicizada: Refere-se a informações privadas que foram divulgadas ao público, seja intencionalmente ou não. Essas informações podem ter sido originalmente privadas, mas foram tornadas públicas através de vários meios, como redes sociais, notícias ou vazamentos de dados. Embora estas informações estejam agora disponíveis publicamente, a sua divulgação pode levantar questões de privacidade e consentimento.

IP – Internet Protocol: É um dos principais protocolos utilizados na comunicação de dados na internet. É responsável pela identificação e endereçamento dos dispositivos conectados em uma rede, permitindo que eles se comuniquem entre si e compartilhem informações. Sem o IP, a internet como a conhecemos hoje não existiria.

Legítimo Interesse: É a base legal que justifica o tratamento de dados respeitando os direitos e liberdades fundamentais do titular que devem ter seus dados protegidos. É o que possibilita ao controlador a tratar dados pessoais sem o consentimento do titular. Porém essa base legal deve ser utilizada com cautela, notadamente pela sua grande possibilidade interpretativa.

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Plataforma digital: São ferramentas que funcionam por meio da tecnologia. São serviços ou aplicativos *online* que favorecem conteúdo, como notícias, música ou programas de televisão.

Princípios: Os princípios da LGPD são os pontos que devem nortear todo e qualquer tratamento de dados pessoais. Para que o tratamento seja considerado legal, todos os dez princípios da lei devem ser cumpridos. Dentre eles, o princípio da finalidade (os dados devem ser tratados apenas para uma finalidade específica informada ao titular) e o da segurança (os agentes envolvidos no tratamento devem adotar medidas para proteger os dados).

Privacidade: Direito de ser protegido de uma interferência em assuntos pessoais e familiares.

Privacy by design: Privacidade desde a concepção e longo do ciclo de vida de todo o projeto. Garantir que novos produtos e serviços, já nasçam com as questões de privacidade e proteção de dados contemplados.

Rede: É a combinação de dois ou mais computadores e seus elos de conexão.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): É um documento que deve ser elaborado pelo controlador sempre que o processo de tratamento de dados pessoais possa gerar riscos às liberdades civis e aos direitos fundamentais do titular. Basicamente, o RIPD cumpre a função de demonstrar que o controlador avaliou os riscos nas operações de tratamento de dados pessoais e adotou medidas para mitigá-los.

Segurança da informação: É a prática que mantém os dados empresariais, dados pessoais e dados pessoais sensíveis em sigilo, a defesa do que não é público. A segurança da informação se baseia em três pilares principais: confidencialidade, integridade e disponibilidade. Estes sustentam as práticas e políticas de proteção de dados nas empresas, servindo como parâmetros para guiar os processos.

Sistema de informação: É aplicável a todo mecanismo projetado com a finalidade de coletar, processar, armazenar e transmitir informações, de maneira a faciliar o acesso de usuários interessados, solucionando problemas e atendendo suas necessidades.

Stakeholders: São todos os grupos de pessoas ou organizações que podem ter algum tipo de ineresse pelas ações de uma determinada empresa. As partes interssadas podem ser desde colaboradores, considerados stakeholders internos, até investidoes, fornecedores, clientes e comunidade, chamados de externos.

Termo de confidencialidade: É um documento firmado entre duas ou mais partes com o objetivo de manter determinadas informações em sigilo.

Titular dos dados: O titular é o dono dos dados e das informações. É a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”. Ele está no centro da LGPD, que visa dar ao titular uma série de direitos e um controle maior sobre o que é feito com as suas informações.

Transferência internacional de dados: A lei define que a transferência internacional de dados é a “transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro”. Na prática, se a empresa opera no Brasil, trata dados pessoais e envia essas informações para fora do país, é preciso estar atento à lei porque existem situações em que a LGPD permite ou não a transferência.

Tratamento de dados: O conceito de tratamento de dados diz respeito a toda atividade feita com dados pessoais, como “coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”. A LGPD estabelece justamente as regras para o tratamento de dados nas empresas, definindo quando e sob quais critérios ele pode ocorrer.

Uso compartilhado de dados: Na própria lei, o uso compartilhado de dados é definido como a “comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais

modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados”.

Vazamento de dados: Ocorre quando informações confidenciais de pessoas são expostas por meios ilegais ou indevidos.

APÊNDICE A – ARTIGOS MAIS CITADOS NA PLATAFORMA SCOPUS COM O TERMO LGPD (2018-2022)

(continua)

Títulos dos Artigos	Ano Publ.	2018	2019	2020	2021	2022	Subtotal	>2022	Total
	Total	0	3	8	16	20	47	2	49
Filme estereocomplexo de poli(L-lactídeo)/lignina carregado com droga para aumentar a estabilidade e a liberação sustentada de trans-resveratrol Autor:LIU, Rui; DAI, Lin; ZOU, Zhufan; SI, Chuanling Periódico: Jornal Internacional de Macromoléculas Biológicas ISSN: 01418130	2018		3	6	6	4	**19**	1	**20**
Percepções de profissionais de TIC sobre privacidade de software Autor: CANEDO, Edna D.; CALAZANS, Angelica T.S.; MASSON, Eloisa T.S.; COSTA, Pedro H.T.; LIMA, Fernanda Periódico: Entropy - MDPI ISSN: 10994300	2020			2	6	7	**15**	1	**16**
Diagnóstico do processamento de dados por organizações brasileiras – um problema de baixa conformidade Autor: FERRÃO, Samara E.R.; CARVALHO, Artur P.; CANEDO, Edna D.; MOTA, Alana P.B.; COSTA, Pedro H. T.; CERQUEIRA, Anderson J. Periódico: Information - MDPI ISSN: 20782489	2021				1	6	**7**		**7**

(continua)

Resultados de desenvolvimento de crianças surdas e a autopercepção do papel parental de suas mães ouvintes Autor: KOBOSKO, Joana; GANC, Malgorzata; PALUCH, Paulina; JEDRZJCZAK, W. Wiktor; FLUDRA, Malgorzata; SKARZYNSKI, Henryk. Periódico:Revista Internacional de Otorrinolaringologia Pediátrica ISSN: 01655876	2021				2		**2**		**2**
Reforço de fusão e nucleação para cristalitos estereocomplexos em mistura de poli(L-lactídeo)/poli(D-lactídeo) enxertado com lignina Autor: ZHUANG, Zhuoxin; LI, Tiantian; NING, Zhen B.; JIANG, Ni; GAN, Zhihua Periódico:Jornal Europeu de Polímeros ISSN: 00143057	2022					1	**1**		**1**
Portabilidade e proteção de dados: tensões entre pessoa e mercado Autor:DE AVILA NEGRI, Sergio M.C.; KORKMAZ, Maria R.D.C.R.; FERNANDES, Elora R. Periódico: Civilística.com ISSN: 23168374	2021					1	**1**		**1**
Tratamento de dados pessoais de acordo com a lgpd: Um estudo sobre a base legal Autor:DE TEFFÉ, Chiara S.; VIOLA, Mário Periódico: Civilística.com ISSN: 23168374	2020					1	**1**		**1**

(conclusão)

Reflexões céticas, teóricas e econômicas sobre o consentimento necessário para o tratamento de dados Autor: DIVINO, Stéfano B.S. Periódico:Direito PUCCP ISSN: 02513420	2019				1		**1**		**1**

Fonte: Base Scopus elaborado pela autora (2023).

APÊNDICE B – ARTIGOS MAIS CITADOS NA PLATAFORMA SCOPUS COM O TERMO GDPR (2018-2022)

(continua)

Títulos dos Artigos	Ano Publ.	2018	2019	2020	2021	2022	Subtotal	>2022	Total
	Total	82	568	1680	3237	4572	10139	539	10679
Federated machine learning: Concept and applications	2019		37	280	614	795	1726	86	1813
Estimating the success of re-identifications in incomplete datasets using generative models	2019		10	76	87	88	261	10	271
EU General Data Protection Regulation: Changes and implications for personal data collecting companies	2018	12	32	33	25	37	139	1	140
The intuitive appeal of explainable machines	2018	1	24	36	27	43	131	2	133
PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities	2020			19	37	53	109	6	115
GDPR-Compliant Personal Data Management: A Blockchain-Based Solution	2020			9	47	50	106	4	110
The European Union general data protection regulation: What it is and what it means	2019		6	20	30	45	101	7	108
Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR	2018	3	16	38	26	22	105	3	108
The right to data portability in the GDPR: Towards user-centric interoperability of digital services	2018	7	15	28	24	23	97	2	99
Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor	2019		6	11	26	46	89	9	98
The law of everything. Broad concept of personal data and future of EU data protection law	2018	6	19	23	23	25	96	1	97
Deep learning in the construction industry: A review	2020				24	61	85	8	93

(conclusão)

of present status and future innovations									
MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption	2020			6	27	44	77	4	81
SecureBoost: A Lossless Federated Learning Framework	2021				9	57	66	11	77
COVID-19 mobile positioning data contact tracing and patient privacy regulations: Exploratory search of global response strategies and the use of digital tools in Nigeria	2020			17	32	14	63	2	65
Deconstructing datafication's brave new world	2018		8	25	17	13	63	1	64
Smart city IoT platform respecting GDPR privacy and security aspects	2020			11	28	23	62	1	63
(Smart) citizens from data providers to decision-makers? The case study of Barcelona	2018		6	18	24	13	61	2	63
Enslaving the Algorithm: From a "right to an Explanation" to a "right to Better Decisions"?	2018	1	8	14	19	20	62	1	63
COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes	2020			4	29	23	56	3	59

Fonte: Elaborado pela autora (2023).

APÊNDICE C – EMBASAMENTO DA CONSTRUÇÃO DO ARTEFATO

(continua)

Tema	Artefato	Descrição	Fonte
Estratégia do Negócio	Levantamento inicial 1 e 2	Identificação da empresa, relações, negócios, área de TI, controle. Identificar o quanto a empresa conhece sobre a LGPD e o quanto o negócio atua com a proteção de dados.	ABNT NBR ISO/IEC 27002:2013
Regulamentações, legislação e contratos	Fornecedores, Identificação dos Processos, Mapeamento - RIPD	Art. 7 da LGPD. Identificar fornecedores, se há contratos, políticas. Identificar os contratos, se estão adequados a LGPD. Termos e Conscentimentos.	ABNT NBR ISO/IEC 27002:2013
Ambiente de ameaça da segurança da informação, atual e futuro	Levantamento inicial 1 e 2, Fornecedores, TI Atribuições, Mapeamento - RIPD	Conhecer o ambiente da empresa e identificar permissões e controles de acesso.	ABNT NBR ISO/IEC 27002:2013
Atribuição de responsabilidades	Mapeamento - RIPD, TI Atribuições	Art. 5, inciso XVII e inciso X da LGPD Identificar o usuário e o responsável das permissões. Para analisar se há controle nas permissões de acesso ao sistema e redes.	ABNT NBR ISO/IEC 27002:2013

(continua)

Tema	Artefato	Descrição	Fonte
Mapeamento das atividades	Mapeamento - RIPD	Art. 5, inciso XVII da LGPD. Identificar o processo, principalmente onde passam dados pessoais.	ABNT NBR ISO/IEC 27002:2013
Controle de acesso	TI Atribuições	Art. 5, inciso X da LGPD reporta sobre os controles de acesso Identificar quem tem acesso ao quê dentro da empresa e quem permite o acesso.	ABNT NBR ISO/IEC 27002:2013
Classificação e tratamento da informação	Mapeamento - RIPD	Art. 5º inciso XVII da LGPD, reporta sobre descrição dos processos. Identificar de onde o dado vem, o que é feito com o dado e onde é armazenado.	ABNT NBR ISO/IEC 27002:2013
Segurança física e do ambiente	TI Atribuições	Art. 13 da LGPD reporta sore dados pessoais mantidos em ambiente controlado e seguro. Verificar se o ambiente dos servidores é seguro, se os documentos do RH (físicos) estão em armários com chave.	ABNT NBR ISO/IEC 27002:2013

(continua)

Tema	Artefato	Descrição	Fonte
Transferência de informações	Mapeamento - RIPD	No Art. 5, inciso X da LGPD, fala sobre o tratamento dos dados pessoais. Na transferência de dados pessoais, verificar se há contrato e se está com respaldo da LGPD.	ABNT NBR ISO/IEC 27002:2013
Dispositivos móveis	Ativos de Informações, TI Inventário	No Art. 5, inciso X da LGPD, fala sobre o tratamento dos dados pessoais. Verificar se os dispositivos móveis são da empresa, e se não são porque os usuários utilizam os seus particulares.	ABNT NBR ISO/IEC 27002:2013
Restrições sobre o uso e instalação de software	Ativos de Informações, TI Inventário	No Art. 5, inciso X da LGPD, fala sobre o tratamento dos dados pessoais, dessa forma, observa-se os acessos e permissões. No controle de acesso ter bloqueios de instalação de software não autorizado ou não seguro.	ABNT NBR ISO/IEC 27002:2013

(continua)

Tema	Artefato	Descrição	Fonte
Backup	Ativos de Informações, TI Inventário	Art. 5, inciso X da LGPD reporta sobre armazenamento e arquivamento das informações. Validar se há backup das informações da empresa, com que frequência, se se precisar voltar um backup, quanto tempo é necessário.	ABNT NBR ISO/IEC 27002:2013
Gestão de ativos	Ativos de Informações, TI Inventário	Fazer uma relação dos ativos da empresa, sejam de produção, máquina, software, se há licença e se estão atualizados. Art. 6º, inciso VI e VII da LGPD, observados os segredos comercial e industrial.	ABNT NBR ISO/IEC 27002:2013
Gerenciamento de vulnerabilidades	Mapeamento - RIPD, Plano de Ação	Mapeando o processo pode-se identificar vulnerabilidades na segurança dos dados pessoais, e havendo, analisar a possibilidade de mitigar esse risco.	ABNT NBR ISO/IEC 27002:2013
Proteção e privacidade da informação de identificação pessoal	Política de Segurança e Politica de Privacidade	Art. 50 da LGPD. Deixar claro para clientes internos e externos a política de segurança da empresa.	ABNT NBR ISO/IEC 27002:2013

(continua)

Tema	Artefato	Descrição	Fonte
Segurança nas comunicações	Mapeamento - RIPD, Plano de Ação, TI Atribuições	Art. 5º da LGPD, inciso XVII. Descrição dos processos. No controle dos acessos e mapeamento se verifica vulnerabilidades nos acessos às informações e comunicações da empresa, com possibilidade de mitigar repassado para o Plano de Ação.	ABNT NBR ISO/IEC 27002:2013
Assegurar o entendimento do ambiente de segurança da informação	Política de Segurança e Politica de Privacidade	Art. 50 da LGPD. Deixar claro para clientes internos e externos a política de segurança da empresa.	ABNT NBR ISO/IEC 27002:2013
Separação do uso do dispositivo para negócio e para fins pessoais	Política de Segurança e Politica de Privacidade	Art. 50 da LGPD. Deixar claro para clientes internos e externos a política de segurança da empresa.	ABNT NBR ISO/IEC 27002:2013
Requisitos de firewall e proteção antivírus	TI Atribuições	Na LGPD Capítulo VII, Segurança e das boas práticas. Como atribuição da TI, ser sempre firewall e antivírus atualizados e verificados, evitando possíveis invasões e vazamento de dados.	ABNT NBR ISO/IEC 27002:2013 e Instituto Brasileiro de Governança Corporativa

(continua)

Tema	Artefato	Descrição	Fonte
Política de Segurança	Política de Segurança	No Art. 50, o controlador tem que demonstrar políticas internas que assegurem o cumprimento. Deixar claro para clientes internos e externos a política de segurança da empresa.	ABNT NBR ISO/IEC 27002:2013 e e Instituto Brasileiro de Governança Corporativa
Política de privacidade	Política de Privacidade	No art. 50, estabelece regras de boas práticas, demonstrando o comprometimento em adotar processos e políticas de transparência.No que tange ao site da empresa e se coleta dados pessoais, deixar clado para o cliente externo quais dados são coletados e para qual finalidade, autorizando ou não essa coleta.	ABNT NBR ISO/IEC 27701:2019 e e Instituto Brasileiro de Governança Corporativa
Governança da organização	Sobre a LGPD	Art. 49 e 50 da LGPD. Envolve a implementação de uma estrutura organizacional, com políticas internas, medidas de segurança, treinamentos para mitigação de riscos de vazamento de dados pessoais.	ABNT NBR ISO/IEC 27701:2019 e e Instituto Brasileiro de Governança Corporativa

(conclusão)

Tema	**Artefato**	**Descrição**	**Fonte**
Compliance	Sobre a LGPD	Também se remete aos artigos 49 e 50 da LGPD. É fazer com que as pessoas que trabalham com dados pessoais na empresa criem uma cultura organizacional ética e transparente no cuidado desses dados.	ABNT NBR ISO/IEC 27701:2019 e Instituto Brasileiro de Governança Corporativa
Plano de Ação	Plano de Ação	Na LGPD, Capítulo VII, da Segurança e das Boas Práticas. Identificada vulnerabilidade, se classifica no Plano de Ação, cabe a diretoria da empresa a implementação ou não para a resolução para mitigação do risco identificado	5w2h (NAKAGAWA, 2014)
Comunicação à ANPD	Cadastro no Sei, Formulários e Modelos	Art. 48 da LGPD. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.	Conforme disposição do Art. 48 da LGPD.

APÊNDICE D – ROTEIRO DE ADEQUAÇÃO À LGPD - ARTEFATO

(continua)

	Etapa		Descrição	Fonte
1	Levantamento inicial 1 (empresa)		Identificação da empresa, relações, negócios, área de TI, controle. Identificar o quanto a empresa conhece sobre a LGPD e o quanto o negócio atua com a proteção de dados.	ABNT NBR ISO/IEC 27002:2013
2	Levantamento inicial 2 (negócio)			
3	Conscientização dos funcionários - LGPD		Os funcionários devem estar cientes sobre a LGPD, apresentação do que é um vazamento de dados, os agentes da LGPD e o que pode inferir nas rotinas do trabalho.	IBGC
	3.1	Palestra Conscientização da LGPD	Modelo como sugestão de apresentação sobre a Conscientização da LGPD.	LGPD, exemplos de vazamento de dados,
	3.2	Lista de presença da Conscientização LGPD	Lista de presença de quem participou da "Conscientização", essa lista deve ser assinada e arquivada em uma pasta intitulada como "Adequação à LGPD".	
4	Definição do Encarregado de Dados (DPO)		O Encarregado de Dados é um dos agentes da LGPD. Não é obrigatório para micro e pequenas empresas conforme RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022, seção IV, porém se identificar um Encarregado pode ser visto com bons olhos em relação à Proteção de Dados.	LGPD, artigo 5º inc. VIII. Seção II
	4.1	Nomeação do DPO	É um documento que foi criado para nomear o Encarregado de Dados, nele tem atribuições e boas práticas	LGPD, artigo 5º inc. VIII. Seção II
	4.2	Atribuições do DPO		
	4.3	Boas práticas do DPO		

(continua)

5	Definição do Comitê (não é obrigatório)	O Comitê não é obrigatório, mas se a empresa optar por criar, é uma boa opção para ajudar a manter a conformidade à LGPD. A sugestão é fazer reuniões mensais, uma pessoa por área, para trocar ideias e sugerir melhorias sobre a proteção de dados pessoais que circulam nesse setor.	A LGPD não menciona sobre um comitê.
5.1	Ata Nomeação do Comitê	Disponibilizado modelo de Ata.	A LGPD não menciona sobre um comitê.
5.2	Nomeação do Comitê	Disponibilizado modelo de nomeação do comitê.	
6	Ativos de informações	Fazer uma relação dos ativos da empresa, sejam de produção, máquina, software, se há licença e se estão atualizados. Art. 6º, inciso VI e VII da LGPD, observados os segredos comercial e industrial.	ABNT NBR ISO/IEC 27002:2013
7	Tecnologia da informação	Art. 5, inciso X da LGPD reporta sobre armazenamento e arquivamento das informações. Validar se há backup das informações da empresa, com que frequência, se se precisar voltar um backup, quanto tempo é necessário.	ABNT NBR ISO/IEC 27002:2013
7.1	Inventário das máquinas	Art. 5, inciso X da LGPD reporta sobre armazenamento e arquivamento das informações. Validar se há backup das informações da empresa, com que frequência, se se precisar voltar um backup, quanto tempo é necessário.	ABNT NBR ISO/IEC 27002:2013
7.2	Atribuições TI	Na LGPD Capítulo VII, Segurança e das boas práticas. Como atribuição da TI, ser sempre firewall e antivírus atualizados e verificados, evitando possíveis invasões e vazamento de dados.	ABNT NBR ISO/IEC 27002:2013 e Instituto Brasileiro de Governança Corporativa

(continua)

8	Identificação dos fornecedores	Art. 7 da LGPD. Identificar fornecedores, se há contratos, políticas. Identificar os contratos, se estão adequados a LGPD. Termos e Conscentimentos. Conhecer o ambiente da empresa e identificar permissões e controles de acesso.	ABNT NBR ISO/IEC 27002:2013
9	Identificação dos processos (geral ao específico)	Art. 5, inciso XVII da LGPD. Identificar o processo, principalmente onde passam dados pessoais.	ABNT NBR ISO/IEC 27002:2013
10	Mapeamento dos processos e RIPD	Art. 5, inciso XVII da LGPD. Identificar o processo, principalmente onde passam dados pessoais. Identificar de onde o dado vem, o que é feito com o dado e onde é armazeado. Art. 7 da LGPD. Identificar fornecedores, se há contratos, políticas. Identificar os contratos, se estão adequados a LGPD. Termos e Conscentimentos. Conhecer o ambiente da empresa e identificar permissões e controles de acesso. Durante o mapeamento, identificado o risco, esse deve ser passado ao Plano de Ação.	ABNT NBR ISO/IEC 27002:2013
10.1	Recursos Humanos	Exemplos de áreas a serem mapeadas, essas podem ser excluídas ou podem ser inclusas outras áreas.	Exemplos de áreas a serem mapeadas, essas podem ser excluídas ou podem ser inclusas outras áreas.
	10.1.1 Check List Admissão		
	10.1.2 Check List Demissão		
10.2	Comercial		
10.3	Marketing		
10.4	Financeiro		
10.5	Atendimento Consumidor (SAC)		

(continua)

11	Plano de Ação - 5w2h	Na LGPD, Capítulo VII, da Segurança e das Boas Práticas. Identificada vulnerabilidade, se classifica no Plano de Ação, cabe a diretoria da empresa a implementação ou não para a resolução para mitigação do risco identificado.	5w2h (NAKAGAWA, 2014)
12	Procedimentos por área	É um "manual" de processo onde passam dados pessoais. Aqui tem um link que direciona para um modelo "Procedimentos do RH". É um documento que detalha os procedimentos, por área, para ser seguido com padrão.	É um modelo de manual de procedimento.
13	Política de Segurança da Informação	Art. 50 da LGPD. Deixar claro para clientes internos e externos a política de segurança da empresa. Definidos os procedimentos por área, é necessário realizar a Política de Segurança da Informação. É um documento interno que deve ser aprovado pela diretoria. No artefato, há um modelo que pode ser seguido.	ABNT NBR ISO/IEC 27002:2013
14	Política de Privacidade	Art. 50 da LGPD. Deixar claro para clientes internos e externos a política de segurança da empresa. É referente aos dados pessoais coletados durante o acesso ao site da empresa (Cookies), esses devem ser informados ao visitante, quais dados são coletados, qual a finalidade, por quanto tempo serão armazenados e para quem serão transferidos.	ABNT NBR ISO/IEC 27002:2013
15	Governança Corporativa e de Segurança da Informação	Na LGPD Capítulo VII, Segurança e das boas práticas. Como atribuição da TI, ser sempre firewall e antivírus atualizados e verificados, evitando possíveis invasões e vazamento de dados. Praticar o que está demonstrado na Política de Privacidade e na Política de Segurança da Informação	ABNT NBR ISO/IEC 27002:2013 e Instituto Brasileiro de Governança Corporativa

(conclusão)

16	Incidentes de vazamento de dados	Art. 48 da LGPD. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.	Conforme disposição do Art. 48 da LGPD.
16.1	Formulário para reportar à ANPD	Modelo de formulário disponível no link.	Conforme disposição do Art. 48 da LGPD.
16.2	Formulário para reportar ao Titular (cliente)	Modelo de formulário disponível no link.	
16.3	Cadastro no Sei	Link de acesso à ANPD para realização do cadastro da empresa.	

APÊNDICE E – COMPARAÇÃO DOS TIPOS DE INOVAÇÃO DAS 3ª E 4ª EDIÇÕES DO MANUAL DE OSLO

Tipo de Inovação	Subcomponente da 3ª ed. Manual de Oslo	4ª ed. Manual de Oslo	Diferenças
Produto	Bens e Serviços	Bens e Serviços (Inclui produtos que capturam conhecimento e combinações dos mesmos e inclui as características de design de bens e serviços)	Inclusão de características de design de produto, incluídas na inovação de marketing no OM3.
Processo	Produção Entrega e logística Serviços auxiliares, incluindo compras, contabilidade e serviços de TIC	Produção Distribuição e logística Sistemas de informação e comunicação	Os serviços auxiliares no OM3 foram transferidos para administração e gestão.
Organizacional	Práticas de negócios Organização do local de trabalho (distribuição de responsabilidades) Relações externas	Administração e gestão	As inovações organizacionais no OM3 estão nas subcategorias de administração e gerenciamento do OM4 Serviços auxiliares em administração e gerenciamento foram incluídos na inovação de processo no OM3.
De Marketing	Design de produtos Colocação e embalagem do produto Promoção de produtos Preços	Suporte de marketing, vendas e pós-venda	As inovações de marketing no OM3 estão incluídas nas subcategorias do OM4. Inovações em vendas, serviços pós-venda e outras funções de suporte ao cliente não foram incluídas no OM3. As inovações relacionadas ao design de produtos estão incluídas na inovação produto do OM4.

Fonte: OCDE/Eurostat (2018, p. 75)