UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE FINANÇAS E CONTABILIDADE
CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS

NAYELLE LUCAS DE MENDONÇA

LGPD E CONFORMIDADE NAS ORGANIZAÇÕES CONTÁBEIS DA PARAÍBA

JOÃO PESSOA
2022

NAYELLE LUCAS DE MENDONÇA

LGPD E CONFORMIDADE NAS ORGANIZAÇÕES CONTÁBEIS DA PARAÍBA

Monografia apresentada ao Curso de Ciências Contábeis, do Centro de Ciências Sociais Aplicadas, da Universidade Federal da Paraíba, como requisito parcial para a obtenção do grau de Bacharel em Ciências Contábeis.

Orientador(a): Prof.ª Dr.ª Rossana Guerra de Sousa

JOÃO PESSOA
2022

Catalogação na publicação
Seção de Catalogação e Classificação

M5391 Mendonca, Nayelle Lucas de.
LGPD e conformidade nas organizações contábeis da Paraíba / Nayelle Lucas de Mendonca. - João Pessoa, 2022.
91 f. : il.

Orientação: Rossana Guerra de Sousa.
TCC (Graduação) - UFPB/CCSA.

1. Ciências Contábeis. 2. Lei Geral de Proteção de Dados Pessoais (LGPD). 3. Compliance. 4. Contabilidade. 5. Proteção de Dados. 6. Conselho Regional de Contabilidade da Paraíba. I. Sousa, Rossana Guerra de. II. Título.

UFPB/CCSA CDU 657

Elaborado por ANA CLAUDIA LOPES DE ALMEIDA - CRB-15/108

NAYELLE LUCAS DE MENDONÇA

LGPD E CONFORMIDADE NAS ORGANIZAÇÕES CONTÁBEIS DA PARAÍBA

Esta monografia foi julgada adequada para a obtenção do grau de Bacharel em Ciências Contábeis, e aprovada em sua forma final pela Banca Examinadora designada pela Coordenação do TCC em Ciências Contábeis da Universidade Federal da Paraíba.

BANCA EXAMINADORA

ROSSANA GUERRA DE SOUSA:67588379472

Assinado de forma digital por ROSSANA GUERRA DE SOUSA:67588379472
Dados: 2022.12.07 16:25:08 -03'00'

Presidente: Prof.(a) Dra. Rossana Guerra de Sousa
Instituição: UFPB

Adriana F. de Vasconcelos

Membro: Prof.(a) Dra. Adriana Fernandes de Vasconcelos
Instituição: UFPB

Membro: Prof.(a) Ma. Ludinaura Regina Souza dos Santos
Instituição: UFPB

João Pessoa, 06 de dezembro de 2022

DECLARAÇÃO DE AUTORIA PRÓPRIA

Eu, Nayelle Lucas de Mendonça, matrícula n.º 20170007057, autor(a) do Trabalho de Conclusão de Curso intitulado LGPD e conformidade nas organizações contábeis da Paraíba, orientado(a) pelo(a) professor(a) Dra Rossana Guerra de Sousa, como parte das avaliações do Curso de Ciências Contábeis no período letivo 2022.1 e requisito parcial à obtenção do grau de Bacharel(a), declaro que o trabalho em referência é de minha total autoria, não tendo sido copiado ou extraído, seja parcial ou integralmente, de forma ilícita de nenhuma fonte, além daquelas públicas consultadas e corretamente referenciadas ao longo do trabalho, obedecendo aos padrões nacionais para referências diretas e indiretas, ou daquelas cujos dados resultaram de investigações empíricas por mim realizadas para fins de produção deste trabalho. Afirmo que em hipótese alguma representa plágio de material disponível em qualquer meio, e declaro, estar ciente das penalidades previstas nos artigos 184 e 298 do Decreto-Lei n.º 2.848/1940 – Código Penal Brasileiro, como também declaro não infringir nenhum dispositivo da Lei n.º 9.610/98 – Lei dos Direitos Autorais.

Assim, se houver qualquer trecho do texto em questão que configure o crime de plágio ou violação aos direitos autorais, assumo total responsabilidade, ficando a Instituição, o orientador e os demais membros da banca examinadora isentos de qualquer ação negligente da minha parte, ou pela veracidade e originalidade desta obra, cabendo ao corpo docente responsável pela sua avaliação não aceitá-lo como Trabalho de Conclusão de Curso da Universidade Federal da Paraíba - UFPB, no Curso de Ciências Contábeis, e, por conseguinte, considerar-me reprovado no Trabalho de Conclusão de Curso.

Por ser verdade, firmo a presente.

João Pessoa, 01 de dezembro de 2022.

gov.br Documento assinado digitalmente
NAYELLE LUCAS DE MENDONCA
Data: 21/12/2022 22:27:10-0300
Verifique em https://verificador.iti.br

_____

Assinatura do(a) discente

Dedico este trabalho primeiramente a Deus e aos meus pais, Cláudio e Norma por serem a minha maior inspiração em conquistar todos os meus objetivos e por me ensinarem a enfrentar todos os obstáculos da vida com força, fé e gratidão.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por seu infinito amor e bondade, por sempre estar presente na minha vida, ser minha fortaleza nos momentos de dificuldades e por me oferecer a oportunidade de todos os dias me tornar uma pessoa melhor.

Agradeço aos meus pais, Cláudio e Norma, por sempre acreditarem nos meus sonhos, por estarem presentes em cada momento que passei ao longo da graduação, compartilhando muitas conquistas, alegrias e aflições. Meu coração se alegra, por saber que sou o orgulho da minha família.

A Profª Drª Rossana Guerra, minha orientadora, por todos os direcionamentos e ensinamentos, por sempre estar disposta a auxiliar os alunos, ter empatia com o outro, por me entender, quando nem eu mesma conseguia. E por fazer o seu trabalho com muito amor e profissionalismo.

Aos meus amigos, que foram essenciais na minha jornada na universidade, com muito compromisso, lealdade e trabalho em equipe, fizeram todos os meus dias, os melhores.

Por fim, a todos que me ajudaram direta ou indiretamente nesta caminhada e que sempre acreditaram em meus sonhos.

“Eu o instruirei e o ensinarei no caminho que você deve seguir; eu o aconselharei e cuidarei de você”.

Salmos 32:8

RESUMO

As tecnologias direcionadas ao processamento de dados estão em constante evolução, aliadas ao uso intensivo de dados, inclusive pessoais, como impulsionadores de negócios e fonte de lucros. Casos de escândalos corporativos, envolvendo espionagem, divulgação, uso e comercialização de dados pessoais de posse das organizações, contribuem para a preocupação de governos com regulações que visam estimular o compromisso das empresas com a transparência e governança para a proteção dos dados pessoais sob sua guarda. Nesse contexto, o Brasil publicou em 2021 a Lei Geral de Proteção de Dados Pessoais (LGPD). Tal norma se aplica às organizações contábeis que, de modo especial, realiza o tratamento de dados de sua organização e, adicionalmente como parte de seu trabalho regular, trata dados pessoais de responsabilidade de seus clientes, culminando na necessidade de adequação da governança interna para prestação do serviço contábil também com foco na LGPD. O objetivo deste estudo é identificar o nível de estruturação dos requisitos para cumprimento da Lei Geral de Proteção de Dados nas organizações de contabilidade registrados no Conselho Regional de Contabilidade da Paraíba. A coleta de dados foi realizada por meio de questionário, que avaliou o nível de conformidade dos requisitos da LGPD em 75 organizações contábeis paraibanas, avaliando-os posteriormente com uso de uma escala de maturidade. A análise dos resultados identificou no pilar de governança que 59% das organizações contábeis não estabelecem os preceitos mínimos a serem seguidos pelos agentes de tratamento de dados na instituição de um programa de *compliance*. O pilar de segurança da informação e proteção de ativos demonstra que as 47% organizações contábeis reconhecem que não possuem o *compliance* exigido pela LGPD, e que são necessárias adequações para melhoria da segurança dos dados pessoais. Na avaliação do pilar de *compliance* 62% das organizações não possuem as adequações exigidas pela LGPD nos requisitos estabelecidos. Na avaliação geral dos pilares, foi identificado que 86% das organizações se enquadram em um nível de maturidade inicial, ou seja, essas organizações ainda não adotaram medidas que atendam aos requisitos de estruturação determinados pela LGPD, enquanto 14% atingem um nível de maturidade de forma estruturada, no qual foi identificado que os processos que envolvem tratamento de dados pessoais acontecem de maneira alinhada com os requisitos da LGPD. A não conformidade com a legislação acarreta multas e sanções e insegurança para seus clientes, tendo ainda a empresa o risco de dano reputacional, caso esteja envolvida em eventos de falta de segurança a vazamento de dados.

Palavras-chave: LGPD. *Compliance*. Contabilidade. Proteção de Dados.

ABSTRACT

Technologies aimed at data processing are constantly evolving, combined with the intensive use of data, including personal data, as business drivers and a source of profits. Cases of corporate scandals, involving espionage, disclosure, use and commercialization of personal data held by organizations, contribute to the concern of governments with regulations that aim to encourage companies' commitment to transparency and governance for the protection of personal data under their custody . In this context, Brazil published in 2021 the General Law for the Protection of Personal Data (LGPD). This rule applies to accounting organizations that, in a special way, process their organization's data and, additionally, as part of their regular work, process personal data under the responsibility of their clients, culminating in the need to adapt internal governance to provide of the accounting service also focusing on the LGPD. The objective of this study is to identify the level of structuring of the requirements for compliance with the General Data Protection Law in accounting organizations registered with the Regional Accounting Council of Paraíba. Data collection was carried out through a questionnaire, which assessed the level of compliance with the LGPD requirements in 75 accounting organizations in Paraíba, subsequently evaluating them using a maturity scale.The analysis of the results identified in the governance pillar that 59% of accounting organizations do not establish the minimum precepts to be followed by data processing agents in the institution of a compliance program. The information security and asset protection pillar shows that 47% of accounting organizations recognize that they do not have the compliance required by the LGPD, and that adjustments are needed to improve the security of personal data. In assessing the compliance pillar, 62% of organizations do not have the adjustments required by the LGPD in the established requirements. In the general assessment of the pillars, it was identified that 86% of the organizations fit into an initial maturity level, that is, these organizations have not yet adopted measures that meet the structuring requirements determined by the LGPD, while 14% reach a maturity level of structured way, in which it was identified that the processes involving the processing of personal data happen in line with the requirements of the LGPD. Non-compliance with legislation entails fines and sanctions and insecurity for its customers, with the company still at risk of reputational damage if it is involved in events of lack of security or data leakage.

Keywords: LGPD. *Compliance*. Accounting. Data Protection

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
AP	Avaliação de Privacidade
CFC	Conselho Federal de Contabilidade
CPF	Cadastro de Pessoas Físicas
CRC	Conselho Regional de Contabilidade
DUDH	Declaração Universal dos Direitos Humanos
DPO	*Data Protection Officer*
EC	Emenda Constitucional
GDPR	*General Data Protection Regulation*
ISTR	*Internet Security Threat Report*
KPIs	*Key Performance Indicators*
LGPD	Lei Geral de Proteção de Dados
NBC	Norma Brasileira de Contabilidade
PEC	Proposta de Emenda Constitucional
PSI	Política de Segurança da Informação
RIPD	Relatório de Impacto à Proteção de Dados
TI	Tecnologia da Informação

SUMÁRIO

1. INTRODUÇÃO

O crescimento do volume de dados gerados pelas organizações e as tecnologias direcionadas ao seu processamento, é uma realidade desde o século XX, sendo, os dados, em suas múltiplas categorizações, utilizados para as mais diversas finalidades no ambiente econômico, contribuindo para o surgimento de novos negócios. Casos como os escândalos das empresas *Cambridge Analytica* e Facebook, envolvendo espionagem e divulgação de dados de clientes, contribuem para o questionamento sobre o compromisso das empresas com a transparência e a proteção dos dados de seus usuários (CARVALHO et al., 2019).

Diante deste cenário, aumentou a necessidade de se instituir uma regulação que abarcasse padrões mínimos para o uso e tratamento de dados pessoais, não somente para proteger o titular contra possíveis ingerências, como também dar maior segurança e estabilidade a este mercado que surge a partir da utilização massiva de dados pessoais. Desta forma, se fortalece a segurança das relações jurídicas e a confiança do titular no tratamento de seus dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo (NUNES, 2019).

Diversos países têm intensificado seus esforços para produzir regulamentos sobre proteção de dados pessoais. Em 27 de abril de 2016 a União Europeia promulgou o Regulamento Geral de Proteção de Dados Pessoais Europeus (*General Data Protection Regulation* - GDPR) que segundo Pinheiro (2020), tem o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecidos pela expressão "*free data flow*" (fluxo livre de dados, em tradução livre).

O regulamento europeu de proteção de dados serviu como referência para que diversos países implementassem legislações sobre o tratamento de dados. A Lei Geral de Proteção de Dados (LGPD), tendo como base o GDPR, é precursora em se adequar aos novos parâmetros estabelecidos internacionalmente sobre proteção de dados, tornando o Brasil um dos maiores países do mundo, em termos populacionais, que conta com uma lei geral de proteção de dados pessoais (ABRUZIO, 2018).

Legislações anteriores à LGPD, como o Código de Defesa do Consumidor e o Marco Civil da Internet, já tratavam sobre a necessidade de regulação do uso e coleta de dados. Por meio da LGPD foram consolidadas em uma única legislação as

principais normas referentes ao tratamento de dados pessoais – como definições, bases legais, princípios, direitos do titular e obrigações dos agentes de tratamento – conferindo assim maior segurança e transparência para todo o sistema de processamento de dados (NUNES, 2019).

A Lei Geral de Proteção de Dados - LGPD (Lei n° 13.709/2018) tem como objetivo regular o tratamento, armazenamento e compartilhamento de dados pessoais de pessoas físicas e jurídicas, garantindo o pleno direito de liberdade e privacidade de seus usuários. A LGPD motiva a mudança de paradigma na gestão dos dados, evidenciando a necessidade de adequações internas e a construção de uma cultura de proteção de dados no Brasil, promovendo mais investimentos para o país, ampliando o uso da economia digital e favorecendo uma maior segurança das informações aos titulares de dados (CABRAL; CRISCUOLO, 2020).

Nesse contexto, após a edição da LGPD, foi elaborada uma Proposta de Emenda Constitucional (PEC 17/2019). A PEC 17/2019 propôs a inserção da proteção de dados pessoais como direito fundamental na Constituição Federal, prevendo a alteração do inciso XII do art. 5º para garantir o direito à proteção dos dados pessoais, inclusive nos meios digitais.

A Proposta de Emenda Constitucional 17/19 deu origem à Emenda Constitucional 115/22, que foi promulgada pelo Congresso Nacional em 10 de fevereiro de 2022, acrescentando o inciso LXXIX ao art. 5º da Constituição Federal. Além disso, a emenda insere o inciso XXX ao art. 22 da CF, estabelecendo que a competência para legislar sobre proteção e tratamento de dados pessoais passa a ser privativa da União.

Segundo Furtado (2022), o direito à proteção de dados pessoais na Constituição Federal visa fortalecer a importância do cumprimento da LGPD, elevando o grau de segurança da informação, conferindo maior visibilidade junto à comunidade internacional, que fortalece o relacionamento do Brasil com os países que têm alto nível de adequação.

No âmbito da operação dos serviços contábeis, a LGPD também exige diversas mudanças operacionais e sistêmicas que garantam a conformidade das empresas com suas diretrizes e princípios, visto que as empresas de contabilidade movimentam dados pessoais de forma ordinária e regular para a prestação dos serviços que ofertam, assim como informações financeiras e fiscais de pessoas físicas (CRUZ; PASSAROTO; THOMAZ JUNIOR, 2021).

Desta forma, caso as empresas que operam serviços contábeis (tratadas a partir de então de Organizações Contábeis) não estejam em conformidade com a LGPD, estarão sujeitas às sanções previstas na LGPD, além de potencialmente poderem arcar com risco da reputação junto aos clientes, fornecedores e concorrência. Adicionalmente, pode-se ainda citar o chamado “efeito dominó” da LGPD quando clientes que se adequam a LGPD solicitam adequação de seus operadores de dados, como no caso das organizações de contabilidade.

A LGPD objetiva alcançar melhorias na governança e gestão de dados pessoais, através de mudanças na cultura interna das empresas, atuando na organização e estruturação dos ciclos de vida dos dados pessoais nas organizações, especialmente naquelas que utilizam para sua finalidade o processamento de grande volume de dados pessoais, como as organizações contábeis. No entanto, esse processo ainda é embrionário no Brasil e cercado de muitos desafios, desde a expertise dos profissionais contábeis sobre a LGPD, até a preparação e difusão da cultura de proteção de dados nas organizações.

A implementação de normas de governança, como a LGPD, não se faz de modo uniforme e imediato sendo, em geral, realizada em fases que classificadas em níveis específicos indicam a maturidade da implementação da norma. Dessa forma, a conformidade com a LGPD além de demonstrar transparência perante os clientes, confere segurança jurídica em relação ao tratamento de dados pessoais, resultando em uma vantagem competitiva às organizações contábeis.

Certamente é importante compreender o cenário atual de adequação das empresas de contabilidade quanto à estruturação interna para a conformidade com os requisitos da LGPD, e consequente implementação de uma cultura de proteção de dados em seus negócios.

Considerando o que foi exposto, o problema de pesquisa deste trabalho consiste em responder o seguinte questionamento**: Qual o nível de estruturação dos requisitos da Lei Geral de Proteção de Dados (LGPD) nas organizações contábeis da Paraíba?**

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Esta pesquisa tem como objetivo identificar o nível de estruturação dos requisitos para cumprimento da Lei Geral de Proteção de Dados nas organizações de contabilidade registradas no Conselho Regional de Contabilidade da Paraíba.

1.1.2 Objetivos Específicos

A fim de alcançar o objetivo geral proposto, são elencados os seguintes objetivos específicos:

1. Detalhar os requisitos para conformidade de organizações com a LGPD;

2. Definir uma escala de níveis de conformidade a partir do atendimento da série de requisitos exigidos pela LGPD para organizações.

3. Analisar os requisitos declarados como atendidos pelas organizações de contabilidade da Paraíba e posicioná-los na escala definida.

1.2 JUSTIFICATIVA

No mundo tecnológico as empresas costumam absorver cada vez mais dados pessoais dos usuários. As organizações coletam informações disponíveis dos usuários, como: nome, *e-mail*, endereço, informações de contato e suas preferências. Os fatos comprovam que esses dados são de suma importância no campo econômico, pois definem hábitos de consumo pessoal e facilitam às organizações um melhor direcionamento de produtos para atender as demandas dos seus possíveis consumidores (ZANDONAI; ARGILES, 2019).

As organizações detêm a responsabilidade de tratar as informações pessoais de maneira legal, justa e transparente. Para isso, precisam adotar medidas técnicas e organizacionais para garantir que dados pessoais sejam efetivamente protegidos em alinhamento com a LGPD.

Tendo em vista que as empresas de contabilidade, para processar informações contábeis, fiscais e financeiras de seus clientes e de sua própria unidade como empresa contábil, necessitam tratar dados pessoais, quer como operador ou como controlador, no âmbito da LGPD, podem auxiliar no direcionamento de esforços da academia e do regulador profissional (CFC), na formação, conscientização e apoio institucional aos profissionais contábeis, visando a construção, em conjunto, de uma cultura de privacidade na profissão contábil.

Assim, entender a importância da conformidade com os requisitos estabelecidos na LGPD, considerando as possíveis sanções estabelecidas pelo descumprimento das normas e as vantagens que podem ser alcançadas pela utilização de um sistema de *compliance* em toda a organização contábil é necessário.

Entre os benefícios possíveis pode-se citar: a prevenção de riscos, normas de conduta voltadas à conscientização dos funcionários, identificação e mitigação prévia de eventuais incidentes. Além disso, credibilidade e notoriedade no mercado, tanto por parte de fornecedores quanto de clientes pode ser notada, em decorrência de uma boa política de conformidade que permita a correta aplicação da LGPD.

Com a contenção de riscos, um bom código de conduta e um canal de denúncias que seja eficaz e disseminado dentro da empresa, as sanções podem ser evitadas e possíveis multas por irregularidades deixadas de ser aplicadas.

A pesquisa em questão justifica-se, portanto, por considerar a legislação recente que afeta vários ramos de atividade, incluindo a contabilidade. Além disso, este estudo contribui ao indicar os níveis de cumprimento dos requisitos da LGPD nas organizações contábeis registrados no Conselho Regional de Contabilidade da Paraíba, fornecendo uma visão geral do cenário local que pode ser utilizada pelo CRC ou pelas próprias organizações contábeis para caminhar de forma estruturada no processo de adequação.

Este trabalho suscita possibilidades de reflexão acerca da estruturação da LGPD nas organizações contábeis, assim como pode ser utilizada como base para ampliação do tema em futuros estudos.

2 REVISÃO DE LITERATURA

2.1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados (LGPD - Lei 13.709/2018) representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil. A legislação brasileira necessitava de um regulamento específico sobre proteção de dados pessoais, pois antes os conceitos eram dispersos em muitas outras normas, como a Lei de Defesa do Consumidor, o Marco Civil da Internet e a Lei do Registro Positivo (CELIDONIO; NEVES; DONÁ, 2020).

Inicialmente a LGPD entraria em vigor a partir de 14 de agosto de 2020, porém houve um pedido de adiamento da vigência da lei, entrando a legislação em vigor a partir de 18 de setembro de 2020 através da MP 959/2020, mas as sanções só entraram em vigor a partir de 1º de agosto de 2021, por força da Lei nº 14.010/20, devido à pandemia do Coronavírus (Covid-19) (CRUZ; PASSAROTO; THOMAZ JUNIOR, 2021).

A LGPD foi influenciada pelo GDPR (*General Data Protection Regulation* – Regulamento Geral de Proteção de Dados), instituído na União Europeia. A idealização do projeto GDPR teve início em 2012 e a aprovação foi concluída em 2016. Embora LGPD e GDPR sejam leis diferentes, em diferentes regiões, a principal semelhança é o controle sobre a aquisição, processamento, compartilhamento e proteção de dados (CRUZ; PASSAROTO; THOMAZ JUNIOR, 2021).

O Congresso Nacional Brasileiro, no dia 10 de fevereiro de 2022, promulgou a Emenda Constitucional (EC 115), que incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais, e fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. De acordo com o texto da EC 115, foi acrescido o inciso LXXIX ao artigo 5º, da Constituição Federal, dispondo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

A proteção de dados pessoais é um direito fundamental, uma cláusula pétrea da matriz constitucional, inerente aos indivíduos, ou seja, é irrenunciável, inalienável, inviolável e essencial a uma vida digna, fazendo com que essa proteção se torne um dever do Estado. A EC 115/22 também incluiu os incisos XXVI e XXX, respectivamente, aos artigos 21 e 22 da Carta Magna, atribuindo à União competência

para organizar e fiscalizar a proteção e o tratamento de dados pessoais, bem como competência privativa para legislar sobre a matéria (GUARIENTO; MARTINS, 2021).

O reconhecimento da proteção de dados pessoais como direito fundamental também traz benefícios econômicos, aumento dos níveis de segurança da informação e aumento da visibilidade junto à comunidade internacional, fortalecendo assim as relações do Brasil com países de alta adequação das leis de proteção de dados.

2.1.1 Os fundamentos e princípios da LGPD

Um conjunto de princípios fundamentais regulamentados pela LGPD promove não apenas a privacidade e a segurança dos dados pessoais, mas também a livre iniciativa e a liberdade de expressão dos titulares dos dados, ou seja, o titular dos dados ganha uma nova camada de proteção e autonomia, sem ter que abrir mão de sua liberdade de informação, tecnologia e comunicações gerais (CRUZ; PASSAROTO; THOMAZ JUNIOR, 2021).

De acordo com o artigo 2º da LGPD são fundamentos para proteção de dados pessoais:

> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL,2018)

Segundo Saldanha (2019), o fundamento do respeito à privacidade proposto pelo inciso I do art. 2º da LGPD, visa estabelecer que todas as operações de tratamento de dados pessoais no Brasil devem ser pautadas pela proteção e a segurança da privacidade e da intimidade dos titulares dos dados pessoais.

A garantia do direito à privacidade também está garantida na Lei 12.965/14, que regula os direitos e deveres do uso da internet no Brasil. Do ponto de vista prático, é importante que as empresas possam estabelecer processos claramente definidos e mapeados, além de uma ostensiva política de transparência e informação, que assegurem o direito de privacidade do titular de dados pessoais.

O segundo fundamento, previsto no artigo 2º, inciso II, é a autodeterminação informativa, cujo significado está em assegurar ao indivíduo o direito de determinar sobre a coleta, armazenamento, utilização e transmissão de seus dados pessoais (COUTO, 2021).

São fundamentos da LGPD a liberdade de expressão, informação, comunicação e opinião, que advém do artigo 19° da Declaração Universal dos Direitos Humanos (DUDH). Nessa declaração, "todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão".

A LGPD aborda os fundamentos de inviolabilidade da intimidade, honra e imagem, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade da pessoa humana e o exercício da cidadania, que também estão previstos na Constituição Federal de 1988.

Como forma de direcionar o tratamento de dados e estabelecer orientações quanto aos cuidados e regras que devem ser seguidos na utilização e tratamento de dados, o art. 6º da LGPD estabelece um conjunto de princípios que devem ser adotados, além da observância à boa-fé, ilustrado na figura 1.

Figura 1 - 10 Princípios definidos pela LGPD

Fonte: Elaborado pela autora, adaptado da Lei n° 13.709/2018, art. 6°.

De acordo com o art.6° da LGPD, os princípios da finalidade, adequação e necessidade indicam que os dados coletados devem ter finalidades determinadas e específicas, devendo estar adstrita ao mínimo necessário para a realização de suas finalidades e compatíveis ao contexto transmitido ao titular na coleta de seus dados.

O princípio de livre acesso, qualidade de dados e transparência, nada mais é que a consagração da necessidade de utilização de uma linguagem e procedimentos transparentes. O responsável pelo tratamento deve adotar medidas adequadas para fornecer ao titular todas as informações necessárias para o devido cumprimento dos direitos do titular. Além de a comunicação ser de forma clara, simples, coesa e de fácil acesso, possibilitando que o cidadão comum consiga entender as informações que lhe estão sendo prestadas, respeitando os segredos comercial e industrial (NUNES, 2019).

Os princípios da segurança, de não discriminação, da responsabilização e da prestação de contas tratam sobre questões relacionadas à segurança no tratamento dos dados e na sua utilização, vedando práticas discriminatórias, que possam interferir de forma negativa na esfera pessoal do titular, além de prever mecanismo de *accountability* para os agentes de tratamento de dados.

O princípio de segurança e de prevenção da LGPD, respectivamente nos incisos VII e VIII do art. 6°, são pilares da segurança da informação e referem-se à utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas como destruição, perda, alteração, comunicação ou difusão. Além disso, inclui a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

De acordo com o inciso IX do art. 6° da LGPD, o princípio da não discriminação garante a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. O princípio da responsabilização e prestação de contas é o último princípio da LGPD e dispõe no inciso X sobre a demonstração, pelo agente de tratamento, 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.

É importante destacar que não há hierarquia entre os referidos fundamentos e princípios, sendo certo que o objetivo é que toda operação de tratamento de dados pessoais se dê com a sua convergência positiva, evitando a violação de qualquer um.

2.1.2 Tratamento de Dados

A LGPD visa proteger os direitos fundamentais de liberdade e privacidade e a livre formação da personalidade de cada pessoa. De acordo com o art. 1º da LGPD, a lei se aplica a todo e qualquer tratamento de dados, por qualquer meio, seja realizado por pessoa natural ou pessoa jurídica de direito público ou privado.

A lei aplica-se a pessoas físicas ou jurídicas que gerem uma base para fins econômicos, aos dados tratados em território nacional, independentemente do método utilizado, e aos dados utilizados para o fornecimento de bens ou serviços.

Esta lei não se aplica ao tratamento de dados para fins não econômicos, ou para fins jornalísticos e artísticos, no âmbito da segurança pública, defesa nacional, e dados originados no exterior e não compartilhados com agentes nacionais. Segundo o art. 5º da LGPD, tratamento é definido como:

> Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL,2018).

Segundo o art. 5º inciso I da LGPD, considera-se dado pessoal a informação relacionada à pessoa natural identificada ou identificável, como nome, endereço residencial, número de celular e CPF, entre outros. A legislação, no inciso II do referido artigo, também trata sobre o dado pessoal sensível, que são os dados pessoais que se referem à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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.

O dado pessoal é coletado para atender uma finalidade específica e pode ser eliminado a pedido do titular, ao cumprimento de uma sanção aplicada pela Autoridade Nacional de Proteção de Dados (ANPD) ou ao término do seu tratamento. Neste cenário, o ciclo de vida do tratamento de dados tem início com a coleta e se encerra com a eliminação ou o descarte do dado. Cada fase do ciclo de vida tem correspondência com operações de tratamento definidas pela LGPD, conforme a figura 2.

Figura 2 - Ciclo de vida dos dados pessoais

Fonte: Xpositum (2022)

A primeira etapa concerne aos dados pessoais coletados, que marca o início do ciclo de vida do dado pessoal internamente às empresas. Esse ciclo diz respeito às formas de produção ou recepção do dado, seja em formato físico ou eletrônico. Na sequência, o ciclo inclui o armazenamento dos dados, em diversos meios (arquivo, banco de dados, documento físico ou digital). Um processo robusto de backup e recuperação deve ser implementado para garantir a retenção de dados durante o ciclo de vida.

O processamento de dados refere-se ao que pode ser feito com o dado, ou seja, classificação, reprodução, processamento, avaliação ou controle das informações, bem como possíveis modificações nos dados pessoais. Os dados também podem ser compartilhados com outras pessoas fora da organização. Nessa etapa estão incluídos os processos de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhado. Ao compartilharem os dados pessoais com empresas terceiras parceiras de negócio, assumem a condição de responsáveis solidárias e devem possuir cuidados específicos para evitar a violação de segurança dos dados.

A última etapa é a eliminação do dado, ou seja, sua exclusão do local onde foi armazenado, física ou eletronicamente. Caso esses dados sejam documentos

arquivísticos, é preciso considerar o devido tratamento dele. O tratamento de dados pessoais poderá ser realizado desde que seja enquadrado em uma das hipóteses elencadas no Art. 7º da LGPD.

A figura 2 elenca as principais hipóteses de tratamento autorizadas pela LGPD, informando, em cada caso, a base legal referente ao tratamento de dados pessoais em geral (Art. 7º), bem como a correspondente base legal para o tratamento de dados pessoais sensíveis (Art. 11):

Figura 3 - Hipóteses para o tratamento de dados pessoais

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art. 11, I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, "a"
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, inciso III	LGPD, art. 11, II, "b"
Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, inciso IV	LGPD, art. 11, II, "c"
Hipótese 5: Para a execução ou preparação de contrato	LGPD, art. 7º, inciso V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, inciso VI	LGPD, art. 11, II, "d"
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, art. 7º, inciso VII	LGPD, art. 11, II, "e"
Hipótese 8: Para a tutela da saúde do titular	LGPD, art. 7º, inciso VIII	LGPD, art. 11, II, "f"
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, inciso IX	Não se aplica
Hipótese 10: Para proteção do crédito	LGPD, art. 7º, inciso X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, art. 11, II, "g"

Fonte: CRPetean (2020)

Na primeira hipótese é necessária a autorização de tratamento em função do consentimento do titular, que conforme o inciso XII do artigo 5º da LGPD é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Os titulares devem ter direito a escolha acerca de que dados desejam autorizar o tratamento, serem informados dos riscos a que podem estar sujeitos, bem como das medidas que serão tomadas pelos agentes de tratamento para mitigar esses riscos

(CANTO et al., 2019). O consentimento deve ser fornecido, seja por escrito ou qualquer meio que demonstre a vontade do titular, e tal consentimento pode ser ainda revogado a qualquer momento pelo titular (CÂMARA, 2020).

O tratamento de dados também pode ser necessário para cumprir com alguma obrigação regulatória ou prevista em lei, que consiste na segunda hipótese legal prevista na LGPD (art. 7º, II). Para tanto, é necessário que se consiga identificar a norma legal específica ou fonte apropriada que claramente demonstre a sua obrigação. Por outro lado, órgãos da administração pública, autoridades ou empresas públicas que necessitem realizar o tratamento de dados pessoais para realização de uma política pública (de saúde, educação, habitação, entre outras), podem fundamentar a realização do tratamento de dados com base em outro requisito legal, indicado no art. 7º, III, da LGPD (CAMARGO, 2019).

Órgãos de pesquisa, cuja definição consta no art. 5º, XVIII, da LGPD, com o intuito exclusivo de realizar pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico, preferencialmente a partir da anonimização dos dados, também podem realizar o tratamento de dados pessoais, desde que com base no art. 7º, IV, da LGPD (CAMARGO, 2019).

Quando o tratamento for necessário para cumprir com as obrigações estabelecidas contratualmente com o indivíduo, ou caso deva ser satisfeita alguma condição para que o contrato se concretize, assim sendo, dentro daquilo que se espera para a execução do contrato, o fundamento legal indicado é o previsto no art. 7º, V, da LGPD (CAMARGO, 2019).

A sexta hipótese legal consiste no tratamento de dados necessário para o exercício regular de direito em processo judicial, administrativo ou arbitral (art. 7º, VI, da LGPD). Este requisito também vale como base legal para justificar a retenção dos dados por prazo adicional ao do término do relacionamento entre o controlador e o titular dos dados, usando como parâmetro os prazos prescricionais para cada situação (CAMARGO, 2019).

As hipóteses que abrangem situações de vida ou morte servem à proteção da vida do indivíduo e de seus interesses vitais. Mediante a constatação dessas situações, o tratamento pode ser justificado com base no art. 7º, VII, da LGPD, sem que seja necessário o consentimento prévio do indivíduo. Outro requisito indicado no âmbito do bem-estar e da saúde e que justifique o tratamento de dados pessoais é o da tutela da saúde (art. 7º, VIII, da LGPD), o qual serve de amparo em ocasião da

utilização de dados pessoais por profissionais da saúde, serviços de saúde ou autoridades sanitárias, mas desde que para fins não econômicos (CAMARGO, 2019).

A nona base legal informa que os dados pessoais estritamente necessários para a finalidade específica poderão ser tratados para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecer os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. O interesse legítimo do controlador significa que há uma necessidade para o uso de dados no intuito de alcançar finalidade específica, a qual não envolve violação de direito do usuário, não sendo necessário obter o seu consentimento (CANTO et al., 2019).

Por fim, na décima base legal, está autorizado o tratamento de dados pessoais para proteção de crédito (art. 7º, X, da LGPD), quando da realização de análise de crédito a partir de informações sobre adimplência ou inadimplência dos titulares. Para tanto, deve ser observado o disposto na Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Código de Proteção e Defesa do Consumidor (Lei nº 8.078/90).

Ressalte-se que apesar das bases legais dispostas nos incisos II a X da LGPD dispensarem o consentimento do titular, não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente a observância dos princípios gerais e da garantia dos direitos do titular, conforme disposto no parágrafo 6º do art. 7 da LGPD.

Destaca-se que não há hierarquia entre as bases legais para o tratamento de dados. Os direitos dos titulares estabelecidos pela LGPD efetivamente asseguram a autonomia da pessoa humana na era digital, e possuem a dimensão no sentido de viabilizar o exercício do controle pelo titular, assim como oferecendo conhecimento sobre a cadeia dos agentes de tratamento.

2.1.3 Direitos dos titulares de dados

Segundo o artigo 5º, inciso V da LGPD, titular é pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Conforme o art. 18, os principais direitos garantidos aos titulares dos dados são:

> I - confirmação da existência de tratamento;
> II - acesso aos dados;

> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (BRASIL,2018)

O inciso I do art. 18 da LGPD garante ao titular o direito à confirmação da existência do tratamento de seus dados pessoais por parte do controlador. A confirmação da existência de tratamento deve ser disposta imediatamente e em formato simplificado, quando for possível. Contudo, quando tal demandar uma declaração clara e completa com as informações apontadas na norma, será admitido um prazo de quinze dias, a ser computado a partir do requerimento (KORKMAZ e SACRAMENTO, 2021).

O titular possui o direito de acesso aos dados, conforme o inciso II do art. 18, sendo possível obter uma cópia dos dados pessoais que a empresa possui em seus arquivos. O titular também possui o direito de correção de dados incompletos, inexatos ou desatualizados, de acordo com o inciso III. Nesse sentido, a complementação, a correção e a atualização dos dados pessoais se apresentam como importantes mecanismos para garantir que a pessoa seja representada de forma fidedigna (RIGOLON KORKMAZ; SACRAMENTO, 2021).

De acordo com o inciso IV, a LGPD garante ao titular o direito de exigir que os dados vistos por ele como desnecessários, excessivos ou não tratados de acordo com as normas da lei, sejam anonimizados, bloqueados ou excluídos do banco de informações do controlador. A portabilidade, apresentada no inciso V, também poderá ser exercida, segundo a redação do parágrafo 3º, do art. 18, da LGPD, por um representante legal, além do titular, diante do agente de tratamento, sem quaisquer custos (parágrafo 5º).

O inciso VI aborda o direito de eliminação dos dados pessoais tratados com o consentimento do titular. Diferentemente do que ocorre com a correção, o direito à eliminação é irreversível, pois não há mais o consentimento para que seja mantida uma linha histórica de informações pessoais prévias. É apresentado no inciso VII o direito de o titular saber exatamente com quem o controlador está compartilhando

seus dados. Com efeito, deve ser garantido ao titular que, mediante requerimento, tenha acesso às suas informações que foram repassadas, para que, se for o caso, possa exercer as demais prerrogativas, como a eliminação ou correção dessas informações, quando impertinentes (RIGOLON KORKMAZ; SACRAMENTO, 2021).

De acordo com o inciso VIII, o titular dos dados não é obrigado a compartilhar suas informações pessoais diante da ausência de obrigatoriedade legal e é também seu direito ter conhecimento sobre a possibilidade de não fornecer o consentimento para o tratamento de seus dados. Além da possibilidade de não fornecer o consentimento, o inciso IX da LGPD também garante ao titular dos dados a possibilidade de revogar o consentimento, que pode ocorrer a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado nos termos do art. 8º, parágrafo 5º, da LGPD.

2.1.4 Agentes de tratamento de dados pessoais

A LGPD define, no art. 5º, os agentes de tratamentos e quais são seus efeitos:

> VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL,2018)

São agentes de tratamento o controlador e o operador de dados pessoais, os quais podem ser pessoas naturais ou jurídicas, de direito público ou privado. Os agentes de tratamento são os responsáveis pelo tratamento dos dados pessoais, sujeitos às regras da LGPD e à fiscalização da ANPD. No contexto de uma pessoa jurídica, a organização é o agente de tratamento para os fins da LGPD, já que é esta que estabelece as regras para o tratamento de dados pessoais, a serem executadas por seus representantes ou prepostos.

O controlador é o agente responsável por tomar as decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Embora o tratamento não precise ser realizado diretamente pelo controlador, o elemento distintivo é o poder de decisão, admitindo-se que o controlador forneça instruções para que um terceiro (operador) realize o tratamento em seu nome (art. 5º, VII; art. 39).

Segundo a ANPD, quando há a contratação de um operador, é usual e legítimo que parte das decisões à respeito do tratamento, limitadas aos seus elementos não essenciais, fique sob a alçada do operador. Dessa forma, o controlador mantém sob sua influência e controla as principais decisões, relativas aos elementos essenciais para o cumprimento da finalidade do tratamento. O controlador também é o responsável por estabelecer outros elementos essenciais relativos ao tratamento, como a definição da natureza dos dados pessoais tratados e da duração do tratamento, incluindo o estabelecimento de prazo para a eliminação dos dados.

O operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada. O operador é uma pessoa jurídica, que na maioria das vezes, é contratada pelo controlador para realizar o tratamento de dados. Contudo, não há nenhum impedimento para que uma pessoa natural contratada como prestadora de serviços para uma finalidade específica possa ser considerada operadora de dados.

Embora o controlador tenha a principal responsabilidade e o operador deva atuar em nome dele, o art. 37 da LGPD determina que ambos partilham obrigações, e, consequentemente, a responsabilidade de manter o registro das operações de tratamento. Além disso, nos termos do art. 42 da LGPD, ambos possuem a obrigação de reparação se causarem dano patrimonial, moral, individual ou coletivo a outrem, no âmbito de suas respectivas esferas de atuação

Conforme o artigo 41 da LGPD, o encarregado pelo tratamento de dados pessoais deve ser indicado pelo controlador de dados. No exercício de suas atribuições, o encarregado pode desempenhar um importante papel de fomentar e disseminar a cultura da proteção de dados pessoais na organização, como, por exemplo, ao receber solicitações de titulares e da autoridade nacional, e adotar providências ou, ainda, ao orientar funcionários e contratados à respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

Considerando as boas práticas internacionais, o encarregado poderá ser tanto um funcionário da instituição quanto um agente externo, de natureza física ou jurídica. Recomenda-se que o encarregado seja indicado por um ato formal, como um contrato de prestação de serviços ou um ato administrativo.

2.1.5 Autoridade Nacional de Proteção de Dados (ANPD)

Conforme o Art. 55-J da LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) foi criada com o objetivo de monitorar, introduzir e fiscalizar o cumprimento efetivo da LGPD no território nacional e impor sanções cabíveis a pessoas e organizações que não cumpram a lei. Além dessas funções, a ANPD também é responsável por manter regulamentos e procedimentos aplicáveis à segurança de dados pessoais para promover o entendimento por parte dos titulares dos dados e dos agentes de tratamento.

A ANPD atua com diligência contra eventuais descumprimentos da Lei nº 13.709/2018 e trabalha junto às demais autoridades competentes para promover a responsabilização e punição dos envolvidos. A responsabilidade do contador no exercício das suas funções é ilimitada, dessa forma, o contabilista responde por quaisquer danos causados aos seus clientes.

Destaca-se que a Autoridade Nacional de Proteção de Dados é responsável pela promoção de medidas destinadas a instruir, reconhecer e educar os agentes de tratamento, titulares de dados pessoais e outros membros ou membros interessados no tratamento de dados pessoais. A ANPD também deve restabelecer a plena conformidade dos agentes de processamento por meio de divulgações, ou para evitar ou remediar situações que possam gerar risco ou danos aos titulares de dados pessoais.

Para controlar e garantir que todos os agentes de tratamento de dados observem e cumpram todas as regras estabelecidas por lei, a LGPD adota uma série de ações para processar e punir os infratores. Segundo o Art. 52 da LGPD, as empresas ficam sujeitas às seguintes sanções administrativas aplicáveis pela ANPD:

> 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)

Além do possível impacto financeiro de sanções e multas, as empresas que não cumprem a LGPD correm o risco de serem avaliadas negativamente pela sociedade e terem sérios problemas de reputação e confiabilidade, nesse caso, a empresa terá dificuldade para recuperar sua imagem perante o mercado (CRUZ; PASSAROTO; THOMAZ JUNIOR, 2021).

A LGPD traz a oportunidade e a necessidade de aprimorar o programa de *compliance* nas organizações contábeis, para garantir que a segurança jurídica seja alcançada. A partir disso, o *compliance* torna-se um pilar da LGPD, uma vez que adequa as empresas às regras da legislação, garantindo que seja seguido o que está disposto na lei com a aplicação dos melhores mecanismos e práticas.

2.2 COMPLIANCE NAS ORGANIZAÇÕES CONTÁBEIS

A expressão *compliance* tem origem no verbo inglês *to comply*, que significa, na melhor das traduções, conformidade. Refere-se a estar em conformidade com a ordem legal ou ordem interna de uma empresa. Em outras palavras, é agir segundo a lei, uma instrução interna ou preceitos éticos (BERTOCELLI; CARVALHO, 2019).

Além do mais, é um conjunto de estratégias e esforços voltados a uma organização, e seus membros, a fim de que façam cumprir as normas legais e regulamentares, bem como políticas e diretrizes de caráter procedimental e ético determinadas pela mesma (ARTESE; CARVALHO, 2019). O *compliance* consiste em uma estrutura de procedimentos e políticas corporativas que representam ações com o objetivo de cumprir os preceitos normativos por meio da prevenção do ato ilícito ou a minorar seus efeitos e sancionar os possíveis responsáveis.

A LGPD na área contábil aumentou consideravelmente o gerenciamento de processos que orientam a coleta, tratamento, armazenamento de dados de empregados, prestadores de serviços, clientes e fornecedores. Segundo Veiga (2021), em uma perspectiva geral, a conformidade pode ser alcançada quando o

agente de tratamento for capaz de atender às demandas dos titulares de dados e promover a redução do risco de incidentes.

Organizações contábeis com faturamento médio anual menor podem dispor de recursos mais limitados, considerando a falta de conhecimento em relação ao tema, falta de tempo para uma adequada divulgação e conscientização, bem como a falta de condições econômicas, visto que existe um custo necessário para uma correta adequação, pode não ser suportado pelo empresário.

Todavia, o processo adaptativo para as grandes empresas, como multinacionais, empresas de capital aberto e empresas de grande porte em geral, foi consideravelmente acessível, visto que a maioria dispõe de recursos, setor jurídico para assessoria e demandas em geral, bem como sistemas organizacionais bem estruturados (SILVA; JALES, 2022).

Considerando a Resolução CFC n° 1555/2018, as pessoas jurídicas, matriz ou filial, constituídas para exploração das atividades contábeis, deverão ser registradas em Conselho Regional de Contabilidade de cada jurisdição. Para efeitos de cumprimento da LGPD, as sociedades empresárias enquadradas como micro ou pequena empresa poderão beneficiar-se das simplificações a que possuem direito de acordo com a legislação em vigor, e poderão gozar das indicações, flexibilizações e regulamentações apresentadas pela ANPD.

2.2.1 LGPD para Agentes de Tratamento de Pequeno Porte

Considerando a maior dificuldade dos agentes de pequeno porte, e com o objetivo de trazer paridade e isonomia à adequação dos agentes, cumprindo suas competências definidas no art. 55-J da LGPD e suprindo expectativas de toda sociedade, a Autoridade Nacional de Proteção de Dados (ANPD), no dia 27 de janeiro de 2022, publicou a Resolução CD/ANPD N° 2.

O texto especifica quem são os agentes de pequeno porte e resguarda um tratamento diferenciado quanto à aplicação da lei 13.709/2018, em pontos como os prazos, registro das operações de tratamento, as comunicações dos incidentes de segurança, o encarregado pelo tratamento de dados pessoais e a segurança e boas práticas (SILVA; JALES, 2022). A Resolução CD/ANPD N° 2, o qual, no art. 2°, traz as seguintes definições:

> I - Agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, *startups*, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador;
> II - Microempresas e empresas de pequeno porte: sociedade empresária, sociedade simples, sociedade limitada unipessoal, nos termos do art. 41 da Lei nº 14.195, de 26 de agosto de 2021, e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º e 18-A, §1º da Lei Complementar nº 123, de 14 de dezembro de 2006;

No Anexo I da Resolução CD/ANPD N° 2 é descrito o regulamento que deve ser considerado pelos agentes de pequeno porte, sendo eles, de acordo com art. 2°, as microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos. Vale ressaltar o disposto no art. 3°, que veda o benefício de tratamento jurídico para os agentes de pequeno porte que:

> I - realizem tratamento de alto risco para os titulares, ressalvada a hipótese prevista no art. 8º;
> II - aufiram receita bruta superior ao limite estabelecido no art. 3º, II, da Lei Complementar nº 123, de 2006 ou, no caso de startups, no art. 4º, § 1º, I, da Lei Complementar nº 182, de 2021; ou
> III - pertençam a grupo econômico de fato ou de direito, cuja receita global ultrapasse os limites referidos no inciso II, conforme o caso.

A regulamentação cria um ambiente mais favorável ao cumprimento da legislação de proteção de dados brasileira, equilibrando a viabilidade operacional e de recursos das pequenas empresas com a efetivação dos direitos e das liberdades dos titulares. A Resolução CD/ANPD N° 2 busca flexibilizar as normas previstas na LGPD para estes agentes, facilitando e reduzindo os custos da implementação das normas de LGPD.

Conforme o art. 7° da Resolução CD/ANPD n° 2, os agentes de tratamento de pequeno porte devem disponibilizar informações sobre o tratamento de dados pessoais e atender às requisições dos titulares, em conformidade com o disposto nos arts. 9º e 18 da LGPD, por meio eletrônico, impresso ou qualquer outro que assegure os direitos previstos na LGPD e o acesso facilitado às informações pelos titulares.

A ANPD fornecerá modelo para o registro das operações de tratamento de dados pessoais para agentes de tratamento de pequeno porte, prevista no art. 37 da LGPD, de forma simplificada. Assim como disporá sobre flexibilização ou

procedimento simplificado de comunicação de incidente de segurança, nos termos da regulamentação específica.

De acordo com o art. 11 da Resolução CD/ANPD n° 2, os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD. Ao não indicar um encarregado, o agente de tratamento de pequeno porte deve disponibilizar um canal de comunicação com o titular de dados para atender o disposto no art. 41, § 2º, I da LGPD. A indicação de encarregado por parte dos agentes de tratamento de pequeno porte será considerada política de boas práticas e governança para fins do disposto no art. 52, §1º, IX da LGPD.

De acordo com o art. 12 da Resolução CD/ANPD n° 2, os agentes de tratamento de pequeno porte devem adotar medidas administrativas e técnicas, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais, considerando, ainda, o nível de risco à privacidade dos titulares de dados e a realidade do agente de tratamento.

Podem também estabelecer política simplificada de segurança da informação conforme art. 13 da Resolução CD/ANPD n° 2, que contemple requisitos essenciais e necessários para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Os agentes de tratamento de pequeno porte podem fornecer a declaração simplificada no prazo de até quinze dias, contados da data do requerimento do titular.

O artigo 16 da Resolução n° 2 da ANPD dispõe que “a dispensa ou flexibilização das obrigações dispostas neste regulamento não isenta os agentes de tratamento de pequeno porte do cumprimento dos demais dispositivos da LGPD, inclusive das bases legais e dos princípios, de outras disposições legais, regulamentares e contratuais relativas à proteção de dados pessoais, bem como direitos dos titulares”. Ou seja, apesar de dispensar ou flexibilizar obrigações, todas as demais disposições da LGPD devem ser devidamente cumpridas.

2.2.2 Política de governança e boas práticas

Os princípios das boas práticas e governança estão previstos no art. 50º da LGPD, o qual estabelece os preceitos mínimos a serem seguidos pelos agentes de tratamento de dados na instituição de um programa de *compliance*, de modo que deverão estabelecer:

> 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).

Dentre essas novas práticas, pode-se inserir o bom relacionamento que as empresas deverão ter com os titulares dos dados coletados. Esse relacionamento é de fundamental importância até mesmo no estabelecimento de um bom programa de *compliance* (BIONI, 2019). A LGPD incentiva a participação ativa dos titulares de dados no processamento de seus dados, isto se torna claro ao analisarmos o art. 50, §2º, inciso I e o art. 51º:

> I - implementar programa de governança em privacidade que, no mínimo:
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; (BRASIL, 2018).

O programa de governança em privacidade é o conjunto de regras de boas práticas e governança a serem utilizadas pelos agentes de tratamento de dados

pessoais. Assemelha-se com a política de segurança da informação, mas com o objetivo de cumprir as ordens legais (BLUM; MORAES; CARVALHO, 2020). Tal programa encontra-se alinhado com as políticas de governança e *compliance*, que objetivam, no geral, realizar uma gestão de riscos, mediante boas práticas, observância da legislação e regulamentos internos, e criação de controles internos (COTS; OLIVEIRA, 2019).

As boas práticas e as regras de governança devem ser publicadas e atualizadas regularmente, e podem ser endossadas e divulgadas pela Autoridade Nacional de Proteção de Dados, permitindo que as empresas demonstrem, por meio de evidências objetivas, seu compromisso genuíno com o cumprimento das leis pertinentes, normas organizacionais, princípios de governança corporativa e melhores práticas de mercado (BLUM; MORAES; CARVALHO, 2020).

A LGPD estabelece também uma obrigação central dos agentes de tratamentos de dados, que é a divulgação dos procedimentos adotados para a coleta e tratamento de dados, além de informar quais medidas de segurança são empregadas para garantir a inviolabilidade dos dados (COTS; OLIVEIRA, 2019).

Este é um passo fundamental para demonstrar a preocupação da empresa em estar em *compliance*, como também de dar maior transparência para os processos e procedimentos adotados, dando assim uma maior confiabilidade à organização e maior segurança para os titulares sobre o tratamento de seus dados.

Dessa forma, a LGPD determina que os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito (art.46).

2.2.3 Medidas de Segurança da Informação

De acordo com o guia de segurança da informação para agentes de tratamento de pequeno porte da ANPD, a segurança da informação pode ser definida como o conjunto de ações que visam à preservação da confidencialidade, integridade e disponibilidade da informação. Esse conjunto de ações impacta todo o ambiente institucional das empresas, com objetivo de prevenir, detectar e combater as ameaças digitais.

Ao tratar de medidas de segurança para proteção dos dados, o artigo 46 da LGPD informa que os responsáveis pelo tratamento das informações pessoais devem adotar medidas de segurança, técnicas e administrativas, a fim de proteger os dados pessoais de acessos não autorizados e de situações geradas por incidentes de segurança de forma acidentais ou ilícitas que acarretem destruição, perda, alteração, comunicação ou de qualquer forma que venha oferecer tratamento inadequado ou ilícito.

Diante dos impactos da LGPD nas empresas, a ISO/IEC 27701 (2019) possui um foco adicional em privacidade de dados em relação às outras normas, como a NBR ISO/IEC 27001 (2013) que era voltada aos requisitos de gestão da segurança da informação e a NBR ISO/IEC 27002 (2005) aos controles de segurança da informação. A ISO/IEC 27701 (2019) atinge a privacidade através de técnicas para proteção de dados e aplica-se aos controladores e operadores.

A NBR/ISO 27701 (2019) tem o objetivo de estabelecer, instituir, manter e melhorar continuamente o Sistema de Gestão da Privacidade da Informação (SGPI). O SGPI é integrado ao Sistema de Gestão da Segurança da Informação (SGSI), definido na NBR/ISO 27001 e, portanto, as normas 27701 (2019) e 27001 (2013) são correlacionadas (CARVALHO, 2021).

A NBR ISO/IEC 27001 (2013) especifica os requisitos necessários para que seja criado, implantado, operado, monitorado, analisado, mantido e melhorado um Sistema de Gestão de Segurança da Informação (SGSI).

Um SGSI fornece apoio para que incidentes de segurança sejam reduzidos, transferidos, evitados e haja aceitação do risco de forma consciente. Ao realizar a implantação de um SGSI, toda empresa tem como foco garantir que o pilar de segurança, definido pela NBR ISO/IEC 27001 (2013), seja atingido. Isso significa garantir que os dados sejam confidenciais, íntegros e disponíveis somente a quem possua direito de acesso a eles (TRISTÃO et al., 2021).

A partir da aplicação das normatizações estabelecidas pela ISO, portanto, a empresa estará apta a obter certificações, as quais atestam o alinhamento com as melhores práticas de manejo de informações, demonstrando, ainda, o comprometimento na proteção dos direitos individuais dos cidadãos, o que traz reflexos positivos para imagem e para credibilidade da empresa.

A APND trouxe à luz também o entendimento de segurança da informação para as pequenas empresas. A Autoridade Nacional entende que há uma complexidade e

especificidade na gestão da segurança de informação, que pode gerar investimentos elevados. Nesse sentido, foram apresentadas algumas medidas para auxiliar essas instituições nas boas práticas, e devem ser complementadas com outras que possam ser identificadas como necessárias para promover a segurança no fluxo informacional da organização. Na figura 4, estão evidenciadas as medidas de segurança, técnicas e administrativas estabelecidas pela ANPD.

Figura 4 - Medidas de segurança da informação para agentes de tratamento de pequeno porte

Fonte: ANPD (2021)

Como medidas administrativas, a ANPD sugere que seja estabelecida pela organização uma política de segurança da informação, que contemple controles relacionados ao tratamento de dados pessoais. É necessário também conscientizar todos os funcionários da organização, especialmente aqueles diretamente envolvidos na atividade de tratamento de dados, sobre as obrigações legais existentes na LGPD e em normas e orientações editadas pela ANPD. É indicado que seja realizado o gerenciamento de contratos e aquisições, para atenção à distribuição de funções e responsabilidades entre as partes.

Em relação às medidas técnicas, como o controle de acesso, a ANPD sugere que, caso o agente de tratamento de pequeno porte detenha uma rede interna de computadores, seja implementado um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com

o sistema e de acessar dados pessoais. Deve-se atentar também para a segurança dos dados pessoais armazenados, das comunicações, manutenção programa de gerenciamento de vulnerabilidades em equipamentos da instituição, políticas de segurança em relação ao uso de dispositivos móveis e ao serviço em nuvem.

De acordo com a ANPD, as medidas sugeridas devem ser entendidas como boas práticas e devem ser complementadas com outras que possam ser identificadas como necessárias para promover a segurança no fluxo informacional da organização. Essas medidas contribuem para estabelecer um ecossistema de proteção de dados pessoais mais seguro e, consequentemente, para um aumento na confiança dos titulares de dados nos agentes de tratamento de dados pessoais de pequeno porte.

2.2.4 Requisitos para efetividade dos programas de *compliance*

Inicialmente é relevante ressaltar que cada empresa possui especificidades que deverão ser levadas em consideração na elaboração de um programa de *compliance*, sendo assim, não é possível montar um modelo universal ao qual se adequem às necessidades particulares de todas as organizações.

Os programas de *compliance*, também conhecidos como programas de conformidade, cumprimento ou integridade, são ferramentas de governança corporativa tendentes a garantir que as políticas públicas sejam implantadas com maior eficiência (CUEVA, 2018). Os programas de *compliance* permitem a adequada gestão de risco da atividade, viabilizam a identificação de eventual descumprimento e os danos resultantes, auxiliam na diminuição dos prejuízos, potencializam a criação de uma cultura corporativa de observância às normas jurídicas, bem como servem como atenuante no caso de sanções administrativas (FRAZÃO; ABILIO, 2019).

Diante disso, para cumprimento do objetivo específico de definição de modelo para avaliação dos níveis de conformidade com a LGDP, após pesquisas, foi firmado termo de parceria com a empresa SANATTI CONSULTORIA, a qual disponibilizou para uso nesta pesquisa o seu *framework* (Estrutura) de apoio à estruturação e apoio à implementação da LGPD dos seus clientes, que estrutura uma escala de níveis de conformidade a partir do atendimento de uma série de requisitos exigidos pela LGPD para organizações.

A Estrutura, denominada PRIVACIDADE, estabelece os níveis de estruturação de cada organização a partir de uma medida de maturidade (neste trabalho tratada

como níveis), que foi utilizado como base para a coleta e posterior avaliação neste trabalho conforme detalhado na Figura 5.

Figura 5 - Modelo de níveis de maturidade

Fonte: SANATTI CONSULTORIA

O framework contempla o exame dos 11 pilares que foram customizados pela empresa para atender aos requisitos da LGPD, conforme Figura 6.

Figura 6 - 11 Pilares do programa de *compliance*

Fonte: SANATTI CONSULTORIA

É necessário definir os pressupostos mínimos para garantir a eficácia do programa de *compliance*, tais como governança, avaliação de risco, capacitação e comunicação, monitoramento, segurança, ciclo de vida do dado, transparência, consentimento, compartilhamento, exercícios de direitos do titular e respostas a incidentes.

O pilar de governança estabelece a existência de uma estrutura que garanta a accountability do Programa de Privacidade, bem como o posicionamento do encarregado e engajamento da liderança. O programa de privacidade e proteção de dados é definido através da estrutura de Governança (DPO, Comitê de Privacidade, alçadas de decisão etc.) e desenho das políticas e procedimentos internos. Nesta etapa, o encarregado é fundamental para que o programa de privacidade seja, de fato, incorporado ao dia a dia da organização (BLUM; 2020).

Como forma de garantir que esses novos padrões tenham atenção às regras de Privacidade, a LGPD adota a figura do *Privacy by Design* (Privacidade desde a concepção), que engloba obrigatoriedade de que aos novos produtos ou serviços (incluídos o desenvolvimento de sistemas, hardware ou software e processos internos) seja feita análise sobre aderência a medidas de segurança, técnicas e administrativas que garantam a proteção dos dados e evitem formas de tratamento inadequados ou ilícitos (BLUM; 2020).

A avaliação de riscos permite um programa de *compliance* de forma personalizada, que confronte os aspectos mais sensíveis da entidade. Em consequência, compõe um dos principais elementos desse programa, pois caso não seja executada adequadamente, poderá refletir na deficiência dos mecanismos implantados. (FRAZÃO; ABILIO, 2019).

Após identificar os riscos, faz-se essencial a elaboração de Códigos de Ética e de Conduta. Este possui a necessidade de consolidar os princípios e valores da entidade, bem como apontar quais condutas são aceitas e vedadas, além de estruturar os canais de orientação e dúvidas. Desse modo, deve ser um documento expresso, concreto e de simples leitura, bem como de linguagem clara e direta (FRAZÃO; ABILIO, 2019).

Quanto à existência de canais de comunicação, estes devem assegurar que seus funcionários possam esclarecer e sanar suas dúvidas quanto ao comportamento que se deseja, bem como promover denúncias. Nesse sentido, garante ao funcionário

que não será prejudicado por recorrer a este meio, além de sua manifestação ser mantida em sigilo de modo permanente. Além disso, os treinamentos periódicos fornecidos aos funcionários permitem a melhor compreensão das áreas em que inexistam normas aplicáveis ou daquelas que não sejam tão claras, bem como o comportamento esperado por eles (FRAZÃO; ABILIO, 2019).

O programa de *compliance* de dados pessoais, com o propósito da garantia da segurança, deve ser constantemente monitorado e atualizado, com a instauração de salvaguardas diante da avaliação de impactos e riscos à privacidade (FRAZÃO; ABILIO, 2019). É necessário monitorar se todas as regras, políticas, processos e procedimentos estão sendo observados na prática. Além de identificar inconsistências, o monitoramento pode gerar indicadores que auxiliam na gestão do Programa de Privacidade (BLUM; 2020).

Os dados devem ser tratados de forma segura, portanto, a organização deve possuir um programa de segurança da informação que garanta a aplicação das medidas de segurança necessárias, alinhadas aos riscos identificados e implementadas desde a concepção de novos produtos, serviços e processos (BLUM; 2020).

É preciso ter conhecimento de todos os processos de dados inerentes à organização e mapear todo o ciclo, desde a coleta até o armazenamento. Na verdade, deve-se observar que tipos de dados estão sendo processados e se obedecem aos pressupostos legais do processamento autorizado. Portanto, a avaliação deve ser a mais completa possível, no sentido de definir os comportamentos a serem seguidos no tratamento dos dados e garantir a redução do risco e o sucesso do plano (FRAZÃO; ABILIO, 2019).

Caso a organização utilize consentimento para tratar dados pessoais, deve-se garantir que todos os requisitos da LGPD sejam cumpridos (ser livre, informado e inequívoco). Além disso, a organização deve garantir controles para gerenciar a opção dos titulares – concessão ou revogação do consentimento (BLUM; 2020). Os titulares de dados precisam saber o que é feito com seus dados pessoais. Neste pilar, avalia-se a existência de mecanismos internos para identificar se a organização é suficientemente transparente com o titular do dado, assim como entender se os avisos de privacidade preenchem todos os requisitos legais (BLUM; 2020).

O programa de *compliance* consiste em assegurar que o tratamento permitirá o pleno exercício de direitos dos titulares, como, por exemplo, o acesso aos seus

dados, visto que a legislação de proteção de dados valoriza a transparência (FRAZÃO; ABILIO, 2019). A LGPD prevê a necessidade de que o programa de governança contenha um plano de resposta a incidente e remediação (art. 50, §2º, I, g), sendo esta mais uma garantia prevista na legislação para caso ocorra algum vazamento ou prática ilícita, a empresa esteja preparada para lidar em tais situações (FRAZÃO; ABILIO, 2019). Neste pilar, é entendido o nível de prontidão da organização para a resposta a um incidente (BLUM; 2020).

Para iniciar a adoção dos programas de *compliance* de dados pessoais, é necessário também a revisão e atualização do termo de uso e da política de privacidade, a atualização das cláusulas de contratos com os parceiros que exercem alguma operação com dados, o mapeamento do fluxo de dados pessoais, bem como da política de segurança da informação (PINHEIRO, 2018).

Por se tratar de um tema relevante para o desenvolvimento sustentável econômico e social das organizações contábeis e dos negócios com base nas melhores práticas internacionais, é pertinente reunir pesquisas já realizadas, a fim de trazer maior clareza ao trabalho a partir das informações citadas anteriormente.

2.3 ESTUDOS ANTERIORES

A Lei Geral de Proteção aos Dados, como tema presente nas discussões científicas e legais a partir de sua publicação em 2020, não dispõe ainda de um amplo acervo de estudos, no entanto, destaca-se a seguir estudos realizados sobre o tema de modo multidisciplinar devido a seu impacto e interesse em múltiplos campos do saber.

A pesquisa de Câmara (2020) teve como objetivo analisar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais (LDPD) nas empresas de contabilidade do estado de Rio Grande do Norte, havendo como público-alvo os profissionais que atuam em escritórios contábeis na cidade de Natal, tendo sido obtidas 82 respostas na pesquisa. A pesquisa concluiu que os escritórios contábeis estão preparados para aplicação da LGPD, uma vez que consideram indispensável o consentimento do titular para o tratamento dos dados, atendem aos princípios previstos na lei e adotam as medidas de segurança necessárias.

Cabe salientar que a necessidade de consentimento é apenas uma das hipóteses de tratamento, sendo possível a utilização de outras hipóteses sem

hierarquia entre elas, e que as organizações são, predominantemente, em razão da natureza da prestação dos serviços, operadores de dados, e como operadores não possuem o papel de definir bases legais para o tratamento de dados das atividades referentes ao uso de dados dos seus clientes.

A pesquisa de Ribeiro e Moreira (2021) buscou verificar as percepções dos empresários e dos profissionais da área contábil sobre a adoção da Lei Geral de Proteção aos Dados no estado de Minas Gerais. A pesquisa teve 104 respostas válidas, e concluiu sobre a existência de preocupações por parte dos profissionais contábeis no que se refere às proteções dos dados, apesar de alguns mecanismos disponíveis na referida lei ainda serem desconhecidos por parte dos entrevistados.

A pesquisa de Ribeiro e Moreira (2021) identificou que em relação à segurança dos dados, 76% dos respondentes afirmaram possuir uma política de segurança e um sistema eficiente que pode garantir a proteção dos dados pessoais nos escritórios de contabilidade, enquanto 24% responderam que onde trabalham não existe um sistema eficiente em vigor. Destaca-se que mediante os impactos da LGPD, garantir que a organização possua uma política de segurança da informação como ferramenta capaz de minimizar os riscos de perdas ou violação de ativos que promovem o controle estruturado da segurança da informação é vital para organizações contábeis que atuam com tratamento de dados.

Os avanços tecnológicos possibilitaram o acesso e compartilhamento rápido de dados e informações pessoais, o que demandou maior segurança e exigência de atitudes conscientes dos diversos profissionais que lidam com essas questões, dessa forma, Kruger et al. (2021) analisaram os determinantes para conformidade da LGPD junto aos profissionais de contabilidade. A pesquisa teve um total de 194 respondentes e concluiu que 26,3% dos profissionais estão em conformidade com a LGPD. De acordo com a pesquisa, os mecanismos de governança em prol da segurança de dados e informações pessoais foram determinantes para a conformidade da LGPD.

É incontestável a necessidade de implementação de mecanismos de governança de dados pessoais. As organizações contábeis devem assegurar a avaliação sistemática de impactos e riscos à privacidade integrados a sua estruturação geral de governança, com mecanismos de supervisão internos e externos, além de contar com planos de resposta a incidentes, para promover o cumprimento de boas práticas.

3 PROCEDIMENTOS METODOLÓGICOS

Neste capítulo está descrita a metodologia utilizada na pesquisa: o tipo de pesquisa, métodos e técnicas utilizadas, e método de análise dos dados.

3.1 CLASSIFICAÇÃO DA PESQUISA

De acordo com Prodanov (2013), a pesquisa descritiva observa, registra, analisa e ordena dados, sem manipulá-los, isto é, sem interferência do pesquisador, e envolve o uso de técnicas padronizadas de coleta de dados, como o uso de questionário e observação sistemática.

Dado a problemática da pesquisa, uma vez que visa identificar o nível de estruturação dos requisitos para cumprimento da Lei Geral de Proteção de Dados nas organizações de contabilidade registradas no Conselho Regional de Contabilidade da Paraíba, a pesquisa se caracteriza como descritiva, que tem como objetivo analisar o conhecimento e apresentar as características mediante a coleta de dados. (GIL, 1999).

A abordagem do problema utilizada será quantitativa, e conforme expõe Fonseca (2002, p. 20), “a pesquisa quantitativa se centra na objetividade. Influenciada pelo positivismo, considera que a realidade só pode ser compreendida com base na análise de dados brutos, recolhidos com o auxílio de instrumentos padronizados e neutros”. A pesquisa quantitativa requer que as informações sejam traduzidas através dos números e técnicas estatísticas.

O método utilizado foi pesquisa de campo que é uma investigação empírica realizada no local onde ocorre ou ocorreu um fenômeno ou que dispôs de elementos para explicá-los (VERGARA, 2010). Dentro da pesquisa de campo, foi aplicado um questionário às organizações contábeis ativas e registradas no Conselho Regional de Contabilidade da Paraíba, visando identificar o nível de maturidade dos requisitos da Lei Geral de Proteção de Dados nas organizações.

3.2 POPULAÇÃO E AMOSTRA

Para Pinheiro (2009), a amostragem é um processo de seleção de uma parcela de indivíduos que preserva as mesmas características ou atributos relevantes para a pesquisa, e ainda afirma que a definição da amostra deve ser definida logo no começo

do planejamento, e o nível de precisão é diretamente relacionado com o tamanho da amostra, a margem de erro aceitável e o nível de confiança. A Equação 1 mostra as fórmulas para o cálculo de tamanho de amostras.

Para o cálculo do tamanho de uma amostra, Cochran (1977, p. 90) destaca três variáveis que têm impacto direto sobre seu tamanho: o tamanho da população, margem de erro e o nível de confiança.

Equação 1 - Fórmula para o cálculo de tamanho de amostras

$$n = \frac{n0}{1+\frac{(n0-1)}{N}} = \frac{n0}{1+\left(\frac{n0}{N}\right)} \qquad (1)$$

Onde:

- n é o número de indivíduos que compõem a amostra.
- N é o número de indivíduos que compõem a população.
- O valor de n0 é obtido pela razão entre o grau de confiança e a margem de erro adotada no estudo.

A população objeto de estudo são as organizações contábeis registradas e ativas no CRC-PB. Para conhecer seu tamanho foram coletados dados junto ao Conselho Federal de Contabilidade, referentes ao estado da Paraíba, no mês de novembro de 2022. Obteve-se um total de 974 organizações contábeis ativas registradas no Conselho Regional de Contabilidade da Paraíba, que representa 1,16% das organizações contábeis do Brasil, sendo 302 sociedades, 330 empresários, 168 Microempreendedores Individuais e 174 sociedades limitadas unipessoais.

Para fins de cálculo da amostra do estudo foram consideradas as organizações contábeis sociedades e empresárias, totalizando 632 organizações, sendo desconsiderados os demais devido à indisponibilidade de contato para o envio do questionário.

Considerando essa questão, e aplicando a fórmula da Equação 1, foi definida a necessidade de uma amostra de ao menos 62 respostas, para um total de 632 organizações contábeis ativas registrados no Conselho Regional de Contabilidade da Paraíba, com um nível de confiança de 90% e 10% de margem de erro.

3.3 PROCEDIMENTO DE COLETA E ANÁLISE DOS DADOS

Inicialmente realizou-se a pesquisa bibliográfica, que foi base para construção e desenvolvimento da ideia de pesquisa, sendo que para sua realização foram realizadas pesquisas em artigos científicos, livros, entre outros. Conforme Marconi e Lakatos (2017), pesquisa bibliográfica é feita com recursos científicos disponíveis, o que torna possível ao pesquisador se munir de informações confiáveis para embasar sua pesquisa. Na segunda etapa foi realizada a análise documental, sendo o exame de documentos legais básicos para construir o arcabouço informativo do trabalho, com foco na Constituição Federal, LGPD e normas corretas.

Os dados para análise foram coletados através de um questionário estruturado, com perguntas fechadas, utilizando a ferramenta Google *Forms*, tendo como base a estrutura da SANATTI CONSULTORIA, que é uma empresa especializada em soluções de gestão organizacional para suporte, desenvolvimento e adequação de estruturas de proteção e apoio à gestão, em processos de controladoria, gestão de riscos, controles internos, *compliance*, prevenção a fraudes, auditoria interna e proteção de dados.

A terceira etapa consistiu no detalhamento e tabulação de requisitos de coleta de dados sobre o objeto, na definição e estabelecimento de critérios de classificações em níveis, conforme estrutura utilizada: inicial, estruturado, implementado e gerenciado, que avaliam o grau de evidências de maturidade das organizações contábeis aos requisitos da LGPD em todos os setores, para formatação do instrumento de coletas de dados definitivo.

A definição dos requisitos para a mensuração do nível de maturidade das organizações contábeis foi realizada com apoio da empresa de consultoria SANATTI da área de proteção de dados que disponibilizou sem custo, e sob declaração de uso para pesquisa científica, a metodologia já validada para esse fim. A mensuração do nível de maturidade visa fornecer as informações necessárias para um diagnóstico das empresas para a adequação da LGPD, trazendo subsídios para a formalização e cálculo dos parâmetros, conforme ilustrado na Tabela 1.

Tabela 1 - Índice do nível de maturidade em conformidade com a LGPD

Nível de adoção	Índice	Nível de Maturidade	Definição
Não	0,00 a 1	Inicial	Não há evidências para nenhum dos setores
Nível de adoção	**Índice**	**Nível de Maturidade**	**Definição**
Em curso	0,00 a 0,50	Estruturado	Há evidência para parte dos setores
Em curso	0,51 a 1	Implementado	
Nível de adoção	**Índice**	**Nível de Maturidade**	**Definição**
Sim	0,00 a 0,29	Estruturado	Há evidência completa para todos os setores
Sim	0,30 a 0,59	Implementado	
Sim	0,60 a 1	Gerenciado	

Fonte: SANATTI CONSULTORIA

Foram utilizados os seguintes pilares para analisar o nível de estruturação dos requisitos da LGPD nas organizações contábeis:

- GA (Governança e *Accountability*)
- SIPA (Segurança da Informação e Proteção de Ativos)
- CP (*Compliance*), bases da Estrutura utilizada como padrão avaliativo.

No pilar de governança foram avaliados os seguintes requisitos de estruturação da LGPD: governança, gestão e *accountability*, capacitação, avaliação de risco e monitoramento. Os requisitos de estruturação da LGPD avaliados no pilar de segurança da informação e proteção de ativos foram: Segurança, compartilhamento de dados pessoais, eliminação de dados pessoais, respostas a incidentes, desenvolvimento seguro e *backup.* No pilar de *compliance* foram avaliados os requisitos de ciclo de vida dos dados, retenção de dados, gestão de consentimento, direitos dos titulares e transparência.

Inicialmente, para a coleta de dados, foi solicitado a cada participante da pesquisa, a fim de esclarecer os preceitos éticos, em relação à preservação de identidade, guarda dos dados, informações e divulgação dos resultados da pesquisa, uma autorização através do Termo de Consentimento Livre e Esclarecido (TCLE), proteger a confidencialidade das respostas.

A fim de conseguir os dados necessários para o desenvolvimento do estudo, o questionário foi enviado via redes sociais do pesquisador e por e-mail a redes de

contadores registrados no Cadastro Nacional de Organizações Contábeis do site do CRC-PB. O questionário de coleta, além das questões para identificação do nível de maturidade, constava também de questões de perfil para subsidiar as análises finais.

Os dados foram tabulados e analisados a partir dos requisitos e critérios de classificação definidos para possibilitar o conhecimento quanto ao objeto da pesquisa e discussão dos resultados. A tabulação dos resultados foi obtida através do instrumento de construção de dados do software do *Microsoft Office* denominado *Excel*, em que os dados foram organizados por meio de gráficos e tabelas.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Nesta seção é apresentada a análise dos resultados obtidos, iniciando-se pelo perfil geral dos respondentes. Na sequência será realizado o detalhamento e a avaliação dos requisitos de cada pilar para analisar o nível de estruturação dos requisitos da LGPD nas organizações contábeis, para possibilitar uma ampla compreensão do cenário estudado.

Após a disponibilização do questionário para 632 organizações contábeis ativos no Conselho Regional de Contabilidade da Paraíba, foram obtidas respostas de 75 organizações, que superaram os critérios da amostra mínima estabelecida na metodologia no item 4.3, sendo apresentados os detalhes das análises.

É pertinente ressaltar que as respostas analisadas nesta seção são declaratórias, podendo não corresponder à realidade factual das organizações. Essa é uma limitação própria desta tipologia de pesquisa, e que precisa ser considerada pelos leitores na análise dos resultados apresentados.

4.1 PERFIL DOS PARTICIPANTES

Para delineamento do perfil das organizações contábeis participantes foram relacionadas informações sobre o faturamento, possibilitando assim ter uma dimensão do tamanho de suas operações.

Em relação ao faturamento, conforme o Gráfico 1, 81,3% dos respondentes declaram possuir um faturamento médio anual menor ou igual a R$ 360 mil/ano e 18,7% informaram que seu faturamento médio anual é maior que R$360 mil/ano e menor ou igual a R$4,8 milhões/ano.

Gráfico 1 - Faturamento médio anual das empresas

Fonte: Elaborado pela autora

De acordo com o site Sebrae (2006), conforme o faturamento bruto anual, a maior parte das empresas (81,3%) respondeu que possuem um faturamento bruto anual menor ou igual a R$ 360.000,00 que por sua classificação, se enquadram como Microempresa (ME). Em comparação com o estudo de Moreira (2021) 98,4% dos respondentes também se enquadram nesta classificação.

4.2 AVALIAÇÃO DO PILAR DE GOVERNANÇA

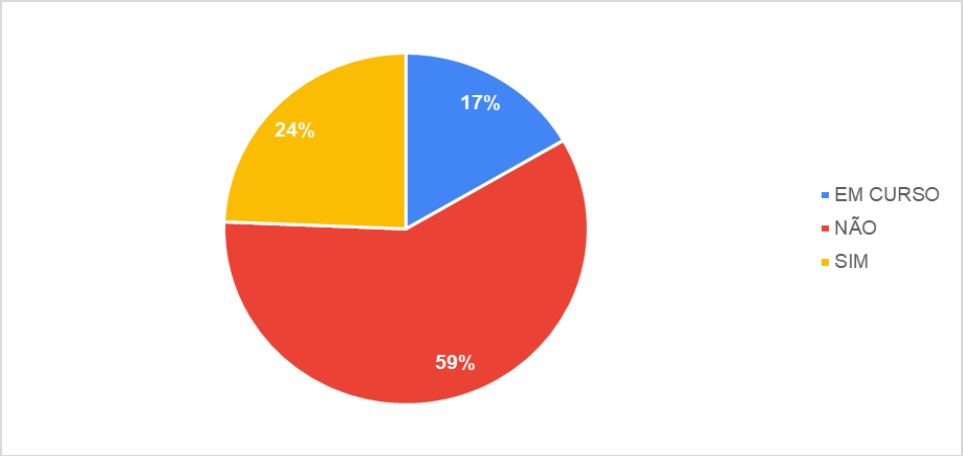
A LGPD, em sua Seção II, Das Boas Práticas e da Governança, no art. 50, § 2°, I, determina que o controlador, a quem competem as decisões referentes ao tratamento de dados pessoais, poderá implementar programa de governança em privacidade. Para análise do pilar de governança foi considerado o índice médio de maturidade do total de questões deste item. Diante disso, seguindo a metodologia adotada, no pilar de governança foram avaliados os seguintes requisitos:

- Governança, gestão e *accountability*
- Capacitação
- Avaliação de risco
- Monitoramento

A análise dos resultados do pilar de governança aponta um percentual médio de respostas negativas (59%), conforme o Gráfico 2, o que conduz ao enquadramento no nível de maturidade da estruturação da LGPD inicial, ou seja, os processos que

envolvem tratamento de dados pessoais acontecem de maneira ainda não estruturada, sem registros de adoção de políticas e procedimentos específicos para sua execução.

Gráfico 2 - Nível Médio de Maturidade de Governança, Gestão e *Accountability*



Fonte: Dados da pesquisa (2022)

É possível verificar que, o percentual de respostas afirmativas (24%) pode ser enquadrado no nível estruturado e 17% enquadrados como em fase de desenvolvimento. Esse resultado positivo (24%) pode ser devido a maior disponibilidade de recursos financeiros e técnicos para o desenvolvimento e adequação da organização aos requisitos regulatórios, tendo em vista que tal processo de *compliance* requer contratação de consultorias especializadas e outros recursos que demandam aportes financeiros.

4.2.1 Avaliação do requisito: Governança, gestão e *accountability*

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam as boas práticas de governança, gestão e *accountability* e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 2 evidencia o resultado das respostas.

Tabela 2 - Avaliação do requisito de governança, gestão e *accountability*

REQUISITOS	NÃO		SIM		EM CURSO	
	QTDE	%	QTDE	%	QTDE	%
Há, na organização, uma estrutura formal de Governança em Privacidade (comitês, conselhos, grupos de trabalho) com funcionamento documentado?	51	**68,0%**	11	**14,7%**	13	**17,3%**
Há, na organização, designação formal de usuários específicos como responsáveis setoriais pelo Programa de Privacidade para apoiar o Programa de Privacidade?	50	**66,7%**	15	**20,0%**	10	**13,3%**
Há definição, de forma documentada, de responsável pelo Programa de Privacidade da organização (Encarregado de Dados)?	52	**69,3%**	14	**18,7%**	9	**12,0%**
Há 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?	45	**60,0%**	17	**22,7%**	13	**17,3%**
Há cláusulas ou diretrizes específicas sobre privacidade e proteção de dados pessoais no Código de Conduta interno, que demonstrem a importância do tema?	43	**57,3%**	22	**29,3%**	10	**13,3%**
Há mapeamento de todos os terceiros, públicos e privados, dos quais a organização recebe ou com os quais a organização compartilha dados pessoais?	43	**57,3%**	22	**29,3%**	10	**13,3%**
Há análise sobre a existência de contratos e cláusulas de proteção de dados pessoais (forma de compartilhamento, responsabilidades, cooperação) com terceiros com os quais a organização compartilha ou dos quais a organização recebe dados pessoais?	33	**44,0%**	25	**33,3%**	17	**22,7%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Estrutura formal de funcionamento –** 68% das organizações apontaram a inexistência de uma estrutura formal documentada, 14,7% indicaram que está em desenvolvimento e 17,3% afirmaram possuir a estrutura formal implementada.
- **Designação formal de responsáveis pelo programa de privacidade –** 66,7% das organizações não possuem a designação dos

responsáveis, 13,3% informaram que está em curso e 20% afirmaram já ter designação.

- **Definição do responsável pelo Programa de Privacidade da organização (Encarregado de Dados) –** 69,3% das organizações contábeis informaram que não possuem a definição documentada do responsável, 12% informaram que está em curso e 18,7% já possuem a definição.
- **Adoção de medidas eficazes capazes para o cumprimento das normas de proteção de dados pessoais –** 60% das organizações informaram que não adotam essas medidas, 17,3% estão em fase de desenvolvimento e 22,7% demonstram na sua empresa a adoção de medidas que são eficazes e que cumprem a LGPD.
- **Cláusulas ou diretrizes específicas sobre privacidade e proteção de dados pessoais no Código de Conduta interno –** 57,3% dos responsáveis das organizações informaram que não possuem as indicações, 13,3% estão em curso e 29,3% informaram que possuem as disposições no código de conduta interno.
- **Mapeamento de terceiros, públicos e privados, dos quais a organização recebe ou compartilha dados pessoais –** 57,3% das organizações informaram que não possuem o controle de mapeamento,13,3% ainda estão em fase de desenvolvimento e 29,3% informaram que já realizam o mapeamento de terceiros.
- **Contratos e cláusulas de proteção de dados pessoais com terceiros com os quais a organização compartilha ou recebe dados pessoais –** 44% das organizações informaram que não há análise de contratos e cláusulas relacionados a LGPD ou proteção de dados, 22,7% estão em fase de desenvolvimento e 33,3% informaram que já realizam estas análises.

Conforme o artigo 50, inciso II da LGPD, os agentes de tratamento devem demonstrar a efetividade de seu programa de governança em privacidade quando apropriado, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, promovam o cumprimento da Lei, cabe destacar que 68% das organizações contábeis

informaram não demonstrar as medidas de efetividade do programa de governança em privacidade.

Em relação a indicação de um encarregado de dados, justifica-se a elevada quantidade de respostas negativas (59,3%), pelo motivo de que os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado de dados, tratando-se de uma flexibilização da exigência prevista no art. 41 da LGPD. Ainda que seja facultativo a indicação de um encarregado de dados, é necessário que o agente de tratamento de pequeno porte disponibilize um canal de comunicação para atender as demandas dos titulares de dados.

De acordo com o princípio de responsabilização e prestação de contas (art. 6° inciso X) é de responsabilidade do agente de tratamento, a demonstração de 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, dessa forma, 60% das organizações contábeis não cumprem essas medidas.

Tendo em vista que um dos principais objetivos do mapeamento de dados é diagnosticar a forma como a empresa lida com a privacidade e a segurança da informação de seus clientes, colaboradores e parceiros terceirizados, 57,3% das organizações contábeis, estão em desconformidade, pois de acordo com o art. 37 da LGPD, o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

Devido a elevada quantidade de respostas negativas (44%), é importante ressaltar que conforme o art. 42 da LGPD em qualquer contrato que haja o compartilhamento de dados pessoais, ambas as partes (controlador e operador) podem responder solidariamente por qualquer violação da LGPD.

4.2.2 Avaliação do requisito: Capacitação

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam a capacitação de seus colaboradores/servidores sobre a LGPD e proteção de dados e qual o seu grau de adoção dentro da organização. Para melhor apresentar o retorno dos gestores, a Tabela 3 evidencia o resultado das respostas.

Tabela 3 - Avaliação do requisito de comunicação

REQUISITOS	NÃO		SIM		EM CURSO	
	QTDE	%	QTDE	%	QTDE	%
Os colaboradores/servidores da organização já receberam algum tipo de capacitação sobre LGPD e proteção de dados?	34	**45,3%**	28	**37,3%**	13	**17,3%**
Há um plano de capacitação e comunicação sobre LGPD e proteção de dados pessoais para todos os colaboradores/servidores da organização?	37	**49,3%**	19	**25,3%**	19	**25,3%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Capacitação sobre LGPD e proteção de dados –** 45,3% informaram que os colaboradores não receberam o treinamento de capacitação,17,3% estão se capacitando e 37,3% informaram que seus colaboradores já possuem a capacitação sobre LGPD e proteção de dados.
- **Plano para capacitação e comunicação sobre LGPD e proteção de dados pessoais –** 49,3% informaram que não possuem um plano de capacitação para seus colaboradores/servidores da organização, 25,3% estão em fase de desenvolvimento e 25,4% informaram possuir um plano estabelecido.

As organizações contábeis que fazem tratamento de dados pessoais devem tomar uma série de medidas para garantir a sua conformidade com a LGPD e uma destas medidas é a capacitação de seus funcionários. Diante das respostas negativas das organizações contábeis (45,3%) é eficaz capacitar todos os colaboradores/servidores da empresa sobre a LGPD para ter uma postura preventiva em todos os processos diários, tanto na capacitação efetiva quanto no plano para capacitação dos colaboradores/servidores da organização, em que 49,3% informaram que não possuem um plano de capacitação.

4.2.3 Avaliação do requisito: Avaliação de Risco

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam a avaliação de risco no tratamento de dados pessoais e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 4 evidencia o resultado das respostas.

Tabela 4 - Avaliação do requisito de avaliação de risco

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
Foi realizada análise de riscos das atividades de tratamento de dados pessoais com base em riscos de privacidade?	49	**65,3%**	16	**21,3%**	10	**13,3 %**

Fonte: Elaborado pela autora

Para fins de análise detalhadas foram os seguintes os resultados:

- **Análise de riscos das atividades de tratamento de dados pessoais –** 65,3% das organizações informaram que não houve a análise de riscos, 13,3% ainda estão em desenvolvimento e 21,3% informaram que já realizam essa análise de riscos.

A Lei Geral de Proteção de Dados, na redação do dispositivo 5°, inciso XVII, menciona como uma das formas de risk assessment (avaliação de risco), a confecção do Relatório de Impacto à Proteção de Dados (RIPD), que é uma 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.

Diante dos resultados negativos (65,3%), as organizações contábeis devem investir em uma *privacy assessment* (avaliação de privacidade) que, portanto, tem a finalidade de mensurar o grau de conformidade da empresa com as normas previstas no ordenamento jurídico brasileiro vigente, assim como também tem a finalidade de verificar se as políticas internas estão sendo efetivas na empresa.

4.2.4 Avaliação do Requisito: Monitoramento

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam os indicadores de monitoramento para implantação da LGPD e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 5 evidencia o resultado das respostas.

Tabela 5 - Avaliação do requisito de monitoramento

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
Há indicadores de monitoramento e controles definidos para avaliação da aderência das ações para implantação da LGPD na organização?	50	**66,7%**	12	**16,0%**	13	**17,3%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Análise de riscos das atividades de tratamento de dados pessoais –** 66,7% das organizações informaram que não possuem os indicadores de monitoramento, 17,3% estão em fase de desenvolvimento das métricas e 16% informaram que possuem a medição de métricas de desempenho através dos KPIs.

Diante dos resultados negativos (66,7%), para um projeto de adequação à LGPD, é importante incorporar a definição e a medição de métricas de desempenho como os KPIs *(Key Performance Indicators)* nas rotinas das atividades de governança em proteção de dados.

4.3 AVALIAÇÃO DO PILAR DE SEGURANÇA E PROTEÇÃO DE ATIVOS

De acordo com o Código de Boas Práticas da Gestão de Segurança da Informação (NBR ISO/IEC 27002, 2007) e considerando o Art. 50 § 1º e 2º da LGPD, as informações estão seguras desde que sejam preservadas a sua confidencialidade, integridade e disponibilidade. Para análise do pilar de segurança da informação e proteção de dados foi considerado o índice médio de maturidade do total de perguntas

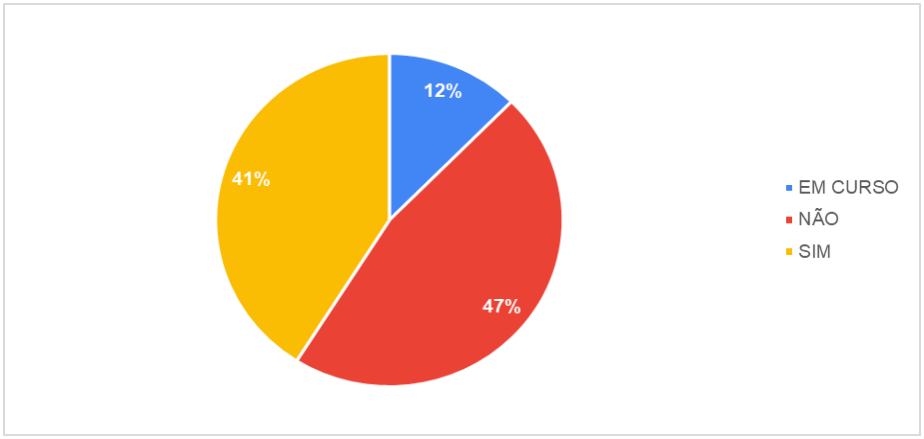
deste item. Diante disso, seguindo a metodologia adotada, no pilar de segurança e proteção de ativos foram avaliados os seguintes requisitos:

- Segurança
- Compartilhamento de dados pessoais
- Eliminação de dados pessoais
- Respostas a incidentes
- Desenvolvimento seguro
- *Backup*

Cada requisito neste pilar possui seu índice de maturidade individual, porém a

A análise dos resultados do pilar de segurança da informação e proteção de ativos, conforme o percentual médio de respostas negativas de 47%, conforme o Gráfico 3, conduz ao enquadramento no nível de maturidade da estruturação da LGPD inicial, ou seja, os processos que envolvem tratamento de dados pessoais acontecem de maneira ainda não estruturada, sem registros de adoção de políticas e procedimentos específicos para sua execução.

Gráfico 3 - Nível Médio de Maturidade de Segurança da Informação e Proteção de Ativos



Fonte: Dados da pesquisa (2022)

É possível verificar que o percentual médio de afirmações (41%), demonstram que as organizações contábeis com um faturamento médio anual maior possuem uma gestão de segurança e proteção de ativos que garantem o controle e finalidade de manter a confidencialidade, a integridade e a disponibilidade de informações e podem

ser enquadrados no nível implementado, e 12% podem ser enquadrados em fase de desenvolvimento.

4.3.1 Avaliação do requisito: Segurança

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam a segurança da informação e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 6 evidencia o resultado das respostas.

Tabela 6 - Avaliação do requisito de segurança

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
A organização possui uma Política de Segurança da Informação estabelecida e publicada?	50	**66,7%**	13	**17,3%**	12	**16,0%**
Há controle estruturado da utilização de arquivos eletrônicos (planilhas, documentos, arquivos) de forma desestruturada, locais ou em nuvem, que contenham dados pessoais (envolvendo armazenamento, transferência, download e eliminação)?	20	**26,7%**	48	**64,0%**	7	**9,3%**
Há registros na organização de lista de ativos, serviços e ferramentas básicas de tecnologia e segurança da informação (sistemas operacionais atualizados, antivírus ativos e atualizado, firewall, filtros anti-spam etc), incluindo definição de usuário responsável por atualização da lista, existentes em seu parque tecnológico?	22	**29,3%**	44	**58,7%**	9	**12,0%**
Há previsão de realização periódica de scan de vulnerabilidades dos principais serviços de TI da organização?	37	**49,3%**	27	**36,0%**	11	**14,7%**
Há norma/diretriz/procedimento interno estabelecendo a necessidade de mesa limpa na organização?	37	**49,3%**	25	**33,3%**	13	**17,3%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Política de Segurança da Informação –** 67,6% das organizações não possuem uma política de segurança da informação estabelecida, 16%

ainda estão em desenvolvimento e 17,3% informaram que possuem uma política já estabelecida e publicada.

- **Controle estruturado da utilização de arquivos eletrônicos –** 64% das organizações informaram que há o controle estruturado de forma desestruturada em planilhas, documentos e arquivos, 9,3% ainda estão em desenvolvimento e 26,7% informaram que não possuem esse controle.
- **Registros de lista de ativos, serviços e ferramentas básicas de tecnologia e segurança da informação –** 58,7% das organizações informaram que existem esses registros incluindo os usuários responsáveis por atualizar essa lista, 12% ainda estão em fase de desenvolvimento e 29,3% informaram que não possuem.
- **Realização periódica de scan de vulnerabilidades –** 49,3% das organizações informaram que não existe a realização periódica, 14,7% ainda estão em fase de desenvolvimento e 36% já realizam a previsão periódica de scan de vulnerabilidades.
- **Política de mesa limpa –** 49,3% das organizações informaram que não haveria necessidade de mesa limpa na organização, 17,3% ainda estão em fase de desenvolvimento e 33,3% já estabeleceram a política de mesa limpa.

De acordo com a pesquisa 67,6% das organizações contábeis não possuem a política de segurança da informação (PSI), que é um documento produzido para as organizações estarem em conformidade com o código de ética da empresa, com o conjunto de leis vigentes no país, com as melhores práticas e padrões de segurança reconhecidos internacionalmente e com a cultura da empresa.

De acordo com o art. 49 da LGPD, os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares, desta forma, 64% das organizações contábeis cumprem o requisito da LGPD.

A análise de riscos é inerente ao modelo de negócio das organizações contábeis, para identificação das ameaças e vulnerabilidades, 49,3% das organizações contábeis informaram que não existe a previsão de realização periódica

de scan de vulnerabilidade, ou seja, considerando esse resultado as empresas de contabilidade não conseguem identificar, corrigir e mitigar riscos, consequentemente não protegem seus ativos e não aprimoram sua infraestrutura a cada nova vulnerabilidade descoberta.

Considerando o art. 49 da LGPD, a política de mesa limpa em uma organização asseguram que sejam realizadas as práticas relacionadas a informações sensíveis, tanto em formato digital quanto físico não sejam deixados desprotegidos, cabe destacar que 49,3% das organizações contábeis não consideram que, informações e ativos em uma área de trabalho estão em um de seus lugares mais vulneráveis, diante disso, a adoção de uma política de mesa limpa é uma das principais estratégias a se utilizar na tentativa de reduzir os riscos de brechas de segurança.

4.3.2 Avaliação do requisito: Compartilhamento de dados pessoais

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam o compartilhamento de dados pessoais e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 7 evidencia o resultado das respostas.

Tabela 7 - Avaliação do requisito de compartilhamento de dados pessoais

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
Há norma/diretriz/procedimento interno com estabelecimento de controles e limites para transferências de dados pessoais por aplicativos de mensageria ou e-mail não institucionais?	35	**46,7%**	28	**37,3%**	12	**16,0%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Transferência de dados pessoais por aplicativos de mensageria ou e-mail não institucional –** 46,7% das organizações informaram que não existem controles e limites quando há transferência de dados, 16% ainda estão em fase de adaptação e 37,3% informaram que estabelecem o controle de forma estruturada.

De acordo com o art. 7 da LGPD, a comunicação ou compartilhamento de dados deve acontecer somente com o consentimento do titular, diante das respostas negativas (46,7%), é importante salientar que o uso compartilhado de dados é um ponto que requer atenção das organizações contábeis, porque a LGPD estabelece punições tanto para o controlador quanto para o operador no caso de inconformidades.

4.3.3 Avaliação do requisito: Eliminação de dados pessoais

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam a eliminação dos dados de acordo com a LGPD e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 8 evidencia o resultado das respostas.

Tabela 8 - Avaliação do requisito de eliminação de dados pessoais

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
Há norma/diretriz/procedimento interno para realização de eliminação de dados pessoais das bases da organização quando necessário?	33	**44,0%**	28	**37,3%**	14	**18,7%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Eliminação de dados pessoais das bases da organização –** 44% das organizações informaram que não existem normas/procedimentos internos, 18,7% ainda estão em fase de execução e 37,3% informaram que já possuem as normas.

É direito do titular à eliminação dos dados de acordo com o art. 18 da LGPD, portanto 44% das organizações contábeis ignoram a cláusula de direito à eliminação de dados que representa não apenas uma multa aplicada pela Autoridade Nacional, mas também um prejuízo significativo à imagem e à reputação da empresa diante da sociedade e do mercado.

4.3.4 Avaliação do requisito: Respostas a incidentes

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam a resposta a incidentes e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 9 evidencia o resultado das respostas.

Tabela 9 - Avaliação do requisito de respostas a incidentes

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
Há norma/diretriz/procedimento interno estabelecendo instruções no caso de ocorrência de um incidente de segurança envolvendo dados pessoais?	45	**60,0%**	16	**21,3%**	14	**18,7%**
A organização realizou o cadastro junto à ANPD para comunicar eventuais incidentes de segurança?	61	**81,3%**	6	**8,0%**	8	**10,7%**
Há, no documento interno sobre gestão de incidentes de segurança, instruções para análise da necessidade de comunicação do incidente à ANPD e aos titulares de dados, bem como como será realizada a comunicação?	59	**78,7%**	8	**10,7%**	8	**10,6%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Incidente de segurança envolvendo dados pessoais –** 60% das organizações informaram que não adotam nenhum procedimento padrão interno, 18,7% ainda estão em fase de desenvolvimento e 21,3% informaram que possuem alguma norma/procedimento que instrua no caso de incidentes de segurança.
- **Cadastro junto à ANPD para comunicação de incidentes de segurança –** 81,3% das organizações informaram que não realizaram o cadastro junto à ANPD para comunicar eventuais incidentes de segurança, 10,7% ainda estão em fase de cadastramento e 8% informaram que já realizaram o cadastro.
- **Gestão de incidentes de segurança e instruções para análise da necessidade de comunicação do incidente à ANPD –** 78,7% informaram que não realizam a gestão de incidentes, 10,6% ainda estão

em fase de desenvolvimento e 10,7% informaram que possuem o controle.

Considerando o art. 46 da LGPD, diante dos resultados negativos (60%), um incidente de segurança com dados pessoais que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, pode ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Diante dos resultados obtidos, 81,3% das organizações contábeis desconsideram o art. 48 da LGPD que determina a obrigação do controlador de comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Vale salientar que o art. 50 da LGPD estabelece que controladores e operadores, no âmbito de suas competências, poderão formular regras de boas práticas de governança para o tratamento de dados pessoais. Desta forma, 78,7% das organizações contábeis não cumprem o § 2º, inciso I do mesmo artigo que dispõe que deve ser implementado um programa de governança em privacidade que conte com planos de resposta a incidentes e remediação.

4.3.5 Avaliação do requisito: Desenvolvimento seguro

As questões deste requisito foram direcionadas a compreender as organizações contábeis que interpretam o desenvolvimento seguro de sistemas internos e qual o seu grau de adoção dentro da organização. Para melhor apresentar o retorno dos gestores, a Tabela 10 evidencia o resultado das respostas.

Tabela 10 - Avaliação do requisito de desenvolvimento seguro

REQUISITOS	NÃO		SIM		EM CURSO	
	QTDE	%	QTDE	%	QTDE	%
No âmbito do desenvolvimento interno de sistemas, ou mesmo na implantação de sistemas de terceiros, são analisados, documentados e testados requisitos que envolvam a proteção de dados pessoais?	39	**52,0%**	29	**38,7%**	7	**9,3%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Desenvolvimento interno de sistemas –** 52% informaram que não existem na implantação de sistemas a análise, a documentação e o teste dos requisitos, 9,3% ainda estão em fase de desenvolvimento e 38,7% informaram que os documentos são analisados e testados.

Portanto, é viável que 52% das organizações contábeis devem agir de forma preventiva, antecipar situações que põem em risco a privacidade dos dados do titular e corrigir ou minimizar os danos antes que aconteçam, espera-se que a equipe de desenvolvimento tome providências de mitigação de riscos antes que um incidente de dados aconteça, para que não afete a privacidade dos usuários durante a utilização do software.

4.3.6 Avaliação do requisito: Backup

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam o *backup* de dados pessoais e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 11 evidencia o resultado das respostas

Tabela 11 - Avaliação do requisito de *backup*

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
A organização realiza backups (cópias de segurança) com possibilidade de recuperação de dados?	5	**6,7%**	66	**88,0%**	4	**5,3%**
O local de armazenamento do backup é seguro e diferente daquele onde são tratadas as informações, bem como os backups são realizados de forma offline?	11	**14,7%**	62	**82,7%**	2	**2,7%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Cópias de segurança com possibilidade de recuperação de dados –** 88% das organizações informaram que existem os procedimentos de

realização de *backups*, 6,7% informaram que não possuem e 5,3% ainda estão em fase de desenvolvimento.

- **Local de armazenagem do backup –** 82,7% informaram que realizam o procedimento de *backups* de forma off-line*,* 14,7% informaram que não realizam o procedimento e 2,7% ainda estão em fase de desenvolvimento.

As organizações contábeis (88%) consideram o *backup* um dos itens mais importantes no quesito segurança da informação, sendo que somente através dele é possível restaurar um ambiente em caso de falha, seja uma falha física ou lógica de um sistema. Para 82,7% das organizações o *backup* pode ser armazenado nos mais diversos formatos e locais como em fita magnética, disco ou até mesmo em nuvem e consideram possuir mais de uma cópia do backup e em locais e tipo de mídias distintas. Para garantir a integridade dos backups, testes de restauração devem ser agendados, para que assim seja possível validar a eficácia deles, bem como planejar o tempo de recuperação.

4.4 AVALIAÇÃO DO PILAR DE COMPLIANCE

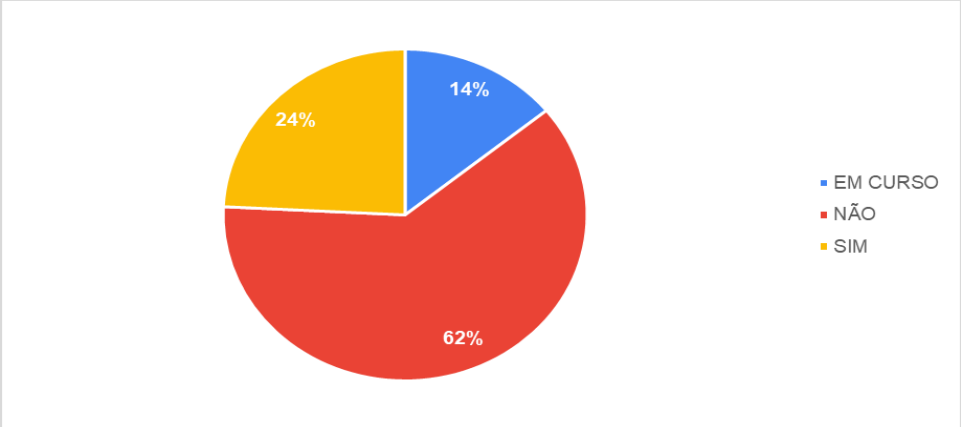
Através de um programa de *compliance* as organizações assumem um menor risco de se envolverem em atos ilícitos, o que consequentemente otimiza as suas relações internas e externas. É através de ações voltadas para a prevenção que a organização, por meio do programa de integridade, que a empresa consegue proteger a sua imagem e reputação não apenas para os seus integrantes, mas também para os seus clientes e fornecedores.

Para a análise do pilar de *compliance* foi considerado o índice médio de maturidade do total de perguntas deste item. Diante disso, seguindo a metodologia adotada, no pilar de *compliance* foram avaliados os seguintes requisitos:

- Ciclo de vida dos dados
- Retenção de dados
- Gestão de consentimento
- Direitos dos titulares
- Transparência

Portanto, o resultado das respostas do pilar de *compliance*, conforme o percentual médio de respostas negativas (62%), de acordo com o Gráfico 4, conduz ao enquadramento no nível de maturidade da estruturação da LGPD inicial, ou seja, os processos que envolvem tratamento de dados pessoais acontecem de maneira ainda não estruturada, sem registros de adoção de políticas e procedimentos específicos para sua execução.

Gráfico 4 - Nível Médio de Maturidade de *Compliance*



Fonte: Dados da pesquisa (2022)

Quando segmentados por faturamento, é possível verificar que, neste recorte, o percentual de respostas afirmativas às questões do pilar aumenta, e neste recorte observa-se que 24% possuem um programa efetivo de *compliance* em conformidade com a LGPD, e podem ser enquadrados no nível médio de maturidade estruturado dentro da organização, assim como 14% estão em fase de desenvolvimento.

4.4.1 Avaliação do requisito: Ciclo de vida dos dados

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam o ciclo de vida dos dados pessoais e qual o seu grau de adoção dentro da organização. Para melhor apresentar o retorno dos gestores, a Tabela 12 evidencia o resultado das respostas.

Tabela 12 - Avaliação do requisito de ciclo de vida dos dados

REQUISITOS	NÃO		SIM		EM CURSO	
	QTDE	%	QTDE	%	QTDE	%
A organização possui registros documentados do fluxo de dados pessoais em todos os setores (registro de atividades de processamento de dados pessoais - ROPAs)?	48	**64,0%**	18	**24,0%**	9	**12,0%**
O registro documentado do fluxo de dados incluiu reflexão sobre se os dados pessoais usados possuem finalidade legítima, explícita e informada, bem como são usados apenas para aquela finalidade, usando apenas os dados absolutamente necessários para o alcance do objetivo e de forma não discriminatória?	47	**62,7%**	18	**24,0%**	10	**13,3%**
O registro documentado do fluxo de dados permite demonstrar se há, na atividade, transferência internacional de dados?	57	**76,0%**	9	**12,0%**	9	**12,0%**
Há previsão em norma/diretriz/procedimento interno de revisão, ao menos anual, e atualização dos registros documentados das atividades de tratamento, bem como de registro de novas atividades?	45	**60,0%**	18	**24,0%**	12	**16,0%**
As atividades de tratamento de dados documentadas possuem hipóteses de tratamento de dados correspondentes (arts. 7º e 11)?	51	**68,0%**	14	**18,7%**	10	**13,3%**
Há definição dos papéis da organização como agente de tratamento de dados pessoais nas atividades de tratamento (controlador ou operador de dados)?	47	**62,7%**	20	**26,7%**	8	**10,6%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Registro de atividades de processamento de dados pessoais (ROPAs) –** 64% das organizações informaram que não é realizado o registro documentado do fluxo de dados pessoais em todos os setores, 12% ainda estão em fase de desenvolvimento e 24% informaram que realizam o registro do fluxo de dados.
- **Dados pessoais usados para finalidade legítima, explícita e informada –** 62,7% das organizações informaram que não possuem o registro documentado, 13,3% ainda estão em fase de desenvolvimento

e 24% informaram que os dados são usados apenas para determinada finalidade utilizando somente o que é necessário.

- **Transferência internacional de dados –** 76% das organizações não possuem o registro documentado do fluxo de dados permite demonstrar se há, na atividade, transferência internacional de dados, 12% ainda estão em fase de desenvolvimento e 12% informaram que são registrados no documento do fluxo de dados.
- **Revisão e atualização dos registros documentados das atividades de tratamento –** 60% das organizações informaram que não existem os procedimentos internos de revisões, 16% ainda estão em fase de desenvolvimento e 24% informaram que há previsão, ao menos, anual da revisão e atualização dos registros das atividades de tratamento de dados.
- **Hipóteses de tratamento de dados –** 68% dos responsáveis pelas organizações contábeis informaram que as atividades de tratamento de dados documentadas não possuem hipóteses de tratamento de dados correspondentes conforme os arts. 7 e 11 da LGPD, 13,3% ainda estão em fase de desenvolvimento e 18,7% informaram que as atividades de tratamento de dados correspondem às hipóteses estabelecidas.
- **Agente de tratamento de dados pessoais nas atividades de tratamento (controlador ou operador de dados) –** 62,7% informaram que não existem as definições, 10,7% ainda estão em fase de desenvolvimento e 26,7% informaram que já possuem a definição estabelecida dos papéis como agentes de tratamento.

Um dos requisitos para um programa efetivo de *compliance* é o registro documentado do fluxo de dados pessoais em todos os setores. Neste sentido, podemos avaliar que 64% das organizações contábeis necessitam de um sistema de controle padrão que deve ser voltado para dirimir e prevenir danos/conflitos, além de proporcionar maior transparência para as empresas, mantendo padrões éticos.

Toda empresa que realiza tratamento de dados pessoais, seja por meio físico ou virtual, precisa se adequar à LGPD, garantindo a observância aos seus princípios. Diante dos resultados negativos (67%), as organizações contábeis precisam garantir que os tratamentos de dados pessoais possuam finalidades legítimas e específicas,

usando apenas os dados absolutamente necessários para o alcance do objetivo e de forma não discriminatória.

Levando em consideração a globalização e a dinâmica dos fluxos de compartilhamento de informações em larga escala, sobretudo pela internet, 76% das organizações contábeis devem considerar que a LGPD exige que a regulação da transferência internacional, que é uma das condições de possibilidade não apenas da proteção da privacidade e dos direitos dos titulares, mas do desenvolvimento tecnológico e econômico em nível internacional e nacional.

A LGPD define no artigo 37 que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Cabe frisar, que 60% das organizações devem designar um responsável por revisar, e acompanhar a elaboração, atualização e manutenção do registro das operações de tratamento de dados pessoais, também tem a responsabilidade sobre os riscos identificados no respectivo registro de sua área de negócio.

A realização do tratamento de dados faz parte de um dos princípios da transparência e finalidade contidos na LGPD, obrigando as empresas a pedir o consentimento e fornecerem às titulares informações claras para essa finalidade. A lei prevê hipóteses que permitem que o tratamento de dados aconteça sem a necessidade do consentimento, desta forma, 68% das organizações contábeis, devem analisar a que se propõe o tratamento de dados, ou seja, qual a finalidade, e qual o melhor requisito legal para amparar esse propósito, de acordo com as circunstâncias. Qualquer operação de tratamento de dados pessoais que não se enquadre nas hipóteses previstas no artigo 7º da LGPD é ilícita, podendo acarretar em sanções àqueles que não realizarem o tratamento da forma legalmente prevista.

O controlador e o operador de dados compõem os agentes de tratamento, conforme prescreve o art. 5º, inciso IX, da LGPD. Considerando as respostas negativas (62,7%) às organizações contábeis devem estabelecer a definição de um controlador e um operador, pois além de estar fora do que é previsto pela LGPD, a empresa fica suscetível às sanções e a equipe se torna incapaz de efetuar algum tipo de procedimento com os dados.

4.4.2 Avaliação do requisito: Retenção de dados

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam a retenção dos dados pessoais e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 13 evidencia o resultado das respostas.

Tabela 13 - Avaliação do requisito de retenção de dados

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
Há definição de tempo de armazenamento para os dados pessoais na organização buscando eliminá-los quando atingida a finalidade do tratamento dos dados?	42	**56,0%**	22	**29,3%**	11	**14,7%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Tempo de armazenamento para os dados pessoais –** 56% informaram que não existem as definições de tempo de armazenagem, 14,7% ainda estão em fase de desenvolvimento e 29,3% informaram que estabeleceram o tempo de armazenamento e eliminando-os quando atingida a finalidade do tratamento dos dados.

O tempo de armazenamento para dados pessoais não pode ser por um período indeterminado, de acordo com a LGPD. Assim, 56% das organizações contábeis devem considerar que a definição do prazo deve ser de acordo com o objetivo do tratamento desses dados. É importante destacar que uma vez que o objetivo é alcançado, os dados devem ser arquivados, eliminados ou anonimizados.

4.4.3 Avaliação do requisito: Gestão do consentimento

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam a gestão do consentimento dos dados pessoais e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 14 evidencia o resultado das respostas.

Tabela 14 - Avaliação do requisito de gestão do consentimento

REQUISITOS	NÃO		SIM		EM CURSO	
	QTDE	%	QTDE	%	QTDE	%
Há norma/diretriz/procedimento interno para gestão do consentimento dos titulares de dados quando esta for a fundamentação da atividade de tratamento?	41	**54,7%**	23	**30,7%**	11	**14,6%**
Há registros padronizados para obtenção e gestão de consentimento de responsáveis legais quando da sua necessidade para o tratamento de dados de crianças?	51	**68,0%**	11	**14,7%**	13	**17,3%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Gestão de consentimento dos dados pessoais –** 54,7% informaram que não existem norma/diretriz/procedimento interno para gestão do consentimento dos titulares de dados quando esta for a fundamentação da atividade de tratamento, 14,6% ainda estão em fase de desenvolvimento e 30,7% informaram que em seus processos utilizam esta base legal da LGPD.
- **Gestão de consentimento de responsáveis legais no tratamento de dados de crianças –** 68% informaram que não realizam a gestão de consentimento dos responsáveis legais, 17,3% ainda estão em fase de desenvolvimento e 14,7% informaram que possuem a padronização na obtenção e gestão de consentimento.

Um dos pontos mais sensíveis na LGPD é a questão do consentimento de usuários quanto ao uso de seus dados. Diante das respostas negativas (54,7%), é importante ressaltar que, a gestão do consentimento é uma preocupação que se faz necessária nas atividades das empresas e nos seus processos que utilizam esta base legal da LGPD.

O consentimento de um dos pais ou do responsável legal é obrigatório para o tratamento de dados de crianças. O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado no seu melhor interesse, de acordo com o Art. 14 da LGPD. Destaca-se que 68% das organizações contábeis não realizam o tratamento

que deve ser feito sempre de forma a assegurar a proteção da criança e do adolescente, bem como a garantia dos seus direitos e a sua dignidade.

4.4.4 Avaliação do requisito: Direitos dos titulares

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam os direitos dos titulares de dados pessoais e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 15 evidencia o resultado das respostas:

Tabela 15 - Avaliação do requisito de direitos dos titulares

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
Há atenção diferenciada quando o tratamento de dados envolve titulares vulneráveis como crianças, adolescentes e idosos?	42	**56,0%**	21	**28,0%**	12	**16,0%**
A organização possui um canal para que os titulares de dados pessoais entrem em contato para obter mais informações ou exercer seus direitos previstos na LGPD?	49	**65,3%**	16	**21,4%**	10	**13,3%**
A organização possui norma/diretriz/procedimento interno para gerenciar o atendimento aos direitos dos titulares de dados pessoais, bem como responsável definido para realizar esse gerenciamento e monitoramento?	45	**60,0%**	15	**20,0%**	15	**20,0%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Titulares vulneráveis como crianças, adolescentes e idosos –** 56% informaram que não há atenção diferenciada, 16% ainda estão em fase de desenvolvimento e 28% informaram que realizam a diferenciação no tratamento de dados.
- **Canal de comunicação para os titulares de dados pessoais –** 65,3% das organizações informaram que não possuem um canal de comunicação, 13,3% ainda estão em fase de desenvolvimento e 21,3% informaram que possuem um canal para que os titulares de dados

pessoais entrem em contato para obter mais informações ou exercer seus direitos previstos na LGPD.

- **Gerenciamento e monitoramento do atendimento aos direitos dos titulares de dados pessoais –** 60% das organizações informaram que não realizam o gerenciamento do atendimento aos direitos dos titulares, 20% ainda estão em fase de desenvolvimento e 20% informaram que atendem e definem o responsável para realizar esse gerenciamento e monitoramento.

De acordo com o resultado da pesquisa, 65,3% das organizações contábeis, necessitam disponibilizar um canal de comunicação com o titular de dados para atender o disposto no artigo 41, § 2º, I da lei. Ainda na hipótese de dispensa, a resolução considera uma boa prática um canal de comunicação na organização, para que dessa forma reduza as sanções e responsabilidades que possam ocorrer no tratamento inadequado de dados pessoais. Diante disso, 60% das organizações contábeis assim que receberem a solicitação dos titulares de dados, devem informar que a solicitação será atendida e que os dados serão processados.

4.4.5 Avaliação do requisito: Transparência

As questões deste requisito foram direcionadas a compreender como as organizações contábeis interpretam a transparência dos dados pessoais e qual o seu grau de adoção dentro da organização.

Para melhor apresentar o retorno dos gestores, a Tabela 16 evidencia o resultado das respostas:

Tabela 16 - Avaliação do requisito de transparência

	NÃO		SIM		EM CURSO	
REQUISITOS	**QTDE**	**%**	**QTDE**	**%**	**QTDE**	**%**
Há, em casos de coleta diretamente do titular de dados, avisos de privacidade sobre finalidade do tratamento de seus dados?	36	**48,0%**	31	**41,3%**	8	**10,7%**

Fonte: Dados da pesquisa (2022)

Para fins de análise detalhadas foram os seguintes os resultados:

- **Coleta e avisos de privacidade de dados –** 48% das organizações informaram que não realizam avisos de privacidade sobre a finalidade do tratamento dos dados, 10,7% ainda estão em fase de desenvolvimento e 41,3% informaram que realizam em casos de coleta diretamente do titular de dados os avisos de privacidade sobre finalidade do tratamento de seus dados.

O aviso de privacidade é a forma na qual os agentes de tratamento devem comunicar-se com os titulares. Diante dos resultados negativos (48%), é dever das organizações tomarem todos os cuidados necessários com a privacidade dos dados e garantir, primeiramente, a segurança ao titular, ou seja, a empresa deverá ser capaz de identificar se a pessoa que está solicitando os dados, realmente é seu titular. A exposição de dados ou vazamentos pode gerar prejuízos tanto à empresa quanto ao titular, como por exemplo, a utilização indevida dos serviços, fraudes e multa à empresa.

5 CONSIDERAÇÕES FINAIS

Visto que o objetivo geral do trabalho é analisar o nível de estruturação dos requisitos da Lei Geral de Proteção de Dados nas organizações contábeis, com a aplicação do questionário foi possível identificar o grau de maturidade das empresas no que se refere à aplicabilidade dos requisitos da LGPD, e observou-se que as respostas diretamente relacionadas à lei foram desfavoráveis.

Mediante a análise dos dados da pesquisa, atendendo ao objetivo geral da pesquisa, identificou-se que das 75 organizações contábeis registradas no Conselho Regional de Contabilidade da Paraíba, 86% atingem um nível de maturidade da estruturação da LGPD de forma inicial. Isso significa que essas organizações ainda não adotaram medidas que atendam aos requisitos de estruturação determinados pela Lei Geral de Proteção de Dados, enquanto 14% atingem um nível de maturidade da estruturação da LGPD de forma estruturada, onde foi identificado que os processos que envolvem tratamento de dados pessoais acontecem de maneira alinhada com os requisitos da LGPD, com os registros de adoções de políticas e procedimentos específicos para sua execução.

Após a análise dos princípios das boas práticas e governança que estão previstos no art. 50º da LGPD, o qual estabelece os preceitos mínimos a serem seguidos pelos agentes de tratamento de dados na instituição de um programa de *compliance,* foi identificado que 59% das organizações contábeis não estão em conformidade com a legislação. Percebe-se a importância que a lei confere aos agentes de tratamento, principalmente ao controlador, sendo este o responsável para implementar o programa de governança em privacidade (§2º), e demonstrar o devido comprometimento da empresa com a adequação às normas de proteção de dados.

Após a análise dos resultados de segurança da informação e proteção de ativos, 47% das respostas obtidas demonstram que as organizações contábeis reconhecem que não possuem o *compliance* exigido pela LGPD, e que são necessárias adequações para melhoria da segurança dos dados pessoais, em especial, a avaliação de risco, gestão de consentimento, direito dos titulares e respostas a incidentes.

Após a análise dos resultados de *compliance*, 62% das respostas obtidas demonstram que as organizações contábeis não possuem adequações exigidas pela

LGPD nos requisitos de ciclo de dados, gestão de consentimento, direitos dos titulares e transparência, e que são necessárias adequações para melhoria dos requisitos.

Com base nos resultados obtidos da amostra examinada pela pesquisa, conclui-se que as organizações contábeis registradas no CRC-PB estão não estão em conformidade com a Lei Geral de Proteção de Dados Pessoais, visto que o nível médio de maturidade foi considerado inicial para todos os requisitos analisados, considerando que todos os processos questionados que envolvem tratamento de dados pessoais ainda não foram realizados pelas empresas.

É importante ressaltar que as organizações contábeis devem tomar medidas para melhor se adequarem à LGPD, além de implementarem um programa de *compliance* em proteção de dados pessoais que envolva a todos da organização, com o propósito de tornar a segurança parte da cultura da empresa.

Em relação à estruturação da LGPD nas organizações de contabilidade da Paraíba, propõe-se aos responsáveis a adequação imediata das medidas e procedimentos que atendam todos os requisitos listados pela LGPD, para evitarem sanções administrativas pela desconformidade com a legislação.

REFERÊNCIAS

ALMEIDA, Kátia de et al. Análise da Evolução da Metodologia utilizada nos artigos publicados na revista: contabilidade & finanças– USP. **Anais do Seminários em Administração–SEMEAD**, São Paulo, SP, Brasil, v. 12, 2009.

GEWANDSZNAJDER, Fernando; ALVES-MAZZOTTI, Alda Judith. **O método nas Ciências Naturais e Sociais**. São Paulo: Pioneira Thomson Learning, 2004.

BALSAN, J.; JACOBY, M. J.; MOHR, L.; BRUSTOLIN MOLINET. A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E SUAS APLICAÇÕES NO ÂMBITO CONTÁBIL: DESAFIOS PARA COM OS CONTABILISTAS DOS MUNICÍPIOS DE PINHALZINHO, SAUDADES, MODELO E NOVA ERECHIM DO ESTADO DE SANTA CATARINA. **Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste**, *[S. l.]*, v. 7, p. e30414, 2022. Disponível em: https://periodicos.unoesc.edu.br/apeusmo/article/view/30414. Acesso em: 08 jun. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** A função e os limites do consentimento. Gen, Editora Forense, 2019.

BLUM, Rita Peixoto Ferreira; MORAES, Helio Ferreira. **Lei Geral de Proteção de Dados Pessoais - LGPD.** In: CARVALHO, André Castro et. al. Manual de Compliance. 2. ed. Rio de Janeiro: Forense, 2020. p. 509;

BRASIL. Constituição da República Federativa do Brasil de 1988. **Planalto**, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: Acesso em: 25 fev. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre Lei Geral de Proteção de Dados Pessoais (LGPD). **Planalto**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 fev. 2022.

CABRAL, Felipe; CRISCUOLO, Filipe. **LGPD: Lei Geral de Proteção de Dados**. [S. l.], jan. 2020.

CÂMARA, Flávia da Silva. **Lei Geral de Proteção de Dados Pessoais (LGPD) – aplicada às empresas de Contabilidade**. 2020. 50f. Trabalho de Conclusão de Curso (Graduação em Ciências Contábeis) – Departamento de Ciências Contábeis, Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2020.

CAMARGO, Tiago Silveira. **Hipóteses para o tratamento de dados previstas na Lei Geral de Proteção de Dados**. Disponível em: <https://iwrcf.com.br/hipoteses-

para-o-tratamento-de-dados-previstas-na-lei-geral-de-protecao-de-dados/>. Acesso em: 25 out. 2022.

CARVALHO, Luiz; OLIVEIRA, Jonice; CAPPELLI, Claudia; MAJER, Violeta . **Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais. In: WORKSHOP DE TRANSPARÊNCIA EM SISTEMAS (WTRANS)**, Belém. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019. p. 21-30. ISSN 2595-6140.

CARVALHO, Artur Potiguara. **Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de Big Data**. 2021.215 f., il. Dissertação (Mestrado Profissional em Engenharia Elétrica) — Universidade de Brasília, Brasília, 2021.

CARVALHO, Rodrigo de Oliveira. **Segurança da informação nas organizações** / Rodrigo de Oliveira Carvalho. - - Brasília: UniCEUB, 2009.

CELIDONIO, Tiago; NEVES, Paulo Sergio; DONÁ, Claudio Melim. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira-Um estudo de caso/Methodology for mapping and adequacy of the requirements listed in LGPD (Brazil Data Protection General Law number 13 709/18) in a financial institution-A case study. **Brazilian Journal of Business**, v. 2, n. 4, p. 3626-3648, 2020.

COUTO, Ana. **A autodeterminação informativa: um dos pilares da LGPD.** Disponível em: <https://www.semprocesso.com.br/post/autodeterminacao-informativa-lgpd>. Acesso em: 12 jul. 2022.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 198

COCHRAN, W. G. Sampling techniques. 3. ed. Westlake Village: John Wiley & Sons, 1977. 428 p. **(Wiley series in probability and mathematical statistics: Applied probability and statistics)**. ISBN 0-471-16240-X.

DA CRUZ, Uniran Lemos; PASSAROTO, Matheus; JUNIOR, Nauro Thomaz. O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) NOS ESCRITÓRIOS DE CONTABILIDADE. **ConTexto - Contabilidade em Texto,** Porto Alegre, v. 21, n. 49, p. 30–39, 2021. Disponível em: https://www.seer.ufrgs.br/index.php/ConTexto/article/view/112561. Acesso em: 06 set. 2022.

DENZIN, Norman K.; LINCOLN, Yvonna S. (Ed.). **The Sage handbook of qualitative research**. sage, 2011.

DE PAULA RIBEIRO, Frank Richard; MOREIRA, Cristiano. A PERCEPÇÃO DOS PROFISSIONAIS DA ÁREA CONTÁBIL E DOS GESTORES SOBRE OS IMPACTOS DA IMPLEMENTAÇÃO DA LGPD. **RAGC**, v. 9, n. 39, 2021.

FERREIRA, Adriano. **O impacto da LGPD nos escritórios de contabilidade.** 2019. Disponível em: https://www.dominiosistemas.com.br/blog/o-impacto-da-lgpd-nosescritoriosde-contabilidade/. Acesso em: 29 out. 2022.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 686.

FURTADO, Samuel Nunes. **Críticas à ec 115/2022: a proteção de dados pessoais como direito fundamental intrínseco à privacidade**. 2022. 25 f. Trabalho de Conclusão de Curso (Graduação em Direito) -- Universidade Federal de Uberlândia, Uberlândia, 2022.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 6. ed. Editora Atlas SA, 2008.

GONÇALVES, Elisa Pereira. **Conversas sobre iniciação à pesquisa científica**. Editora Alínea, 2001.

Guariento, Daniel Bittencourt. Martins Ricardo Maffeis. **EC torna a proteção de dados pessoais um direito fundamental.** Disponível em: <https://www.migalhas.com.br/coluna/impressoes-digitais/359941/ec-torna-a-protecao-de-dados-pessoais-um-direito-fundamental>. Acesso em: 1 set. 2022.

GRAMINHO, Bruna Borges; VIER, Ailson José. O COMPLIANCE E SUA UTILIZAÇÃO COMO INSTRUMENTO DE CONTROLE E TRANSPARÊNCIA NAS COMPANHIAS GAÚCHAS LISTADAS NA BOLSA DE VALORES. **Revista Eletrônica de Ciências Contábeis**, v. 10, n. 1, p. 139-170, 2021. Disponível em:<https://seer.faccat.br/index.php/contabeis/article/view/1960/1239>. Acesso em: 5 maio. 2022.

HAYATI, Dariush; KARAMI, Ezatollah; SLEE, Bill. Combining qualitative and quantitative methods in the measurement of rural poverty: the case of Iran. **Social indicators research**, v. 75, n. 3, p. 361-394, 2006.

INFOMONEY. **Pesquisa indica que 64% das empresas não estão em conformidade com a LGPD.** Disponível em: https://www.infomoney.com.br/economia/pesquisa-indica-que-64-das-empresas-nao-estao-em-conformidade-com-a-lgpd. Acesso em: 13 set. 2022.

KIYOHARA, Jefferson. **A importância do PMO na adequação a LGPD**. Disponível em:< https://lexprime.com.br/2019/09/a-importancia-do-pmo-na-adequacao-a-lgpd>. Acesso em: 10 abril 2022.

KRÜGER, Cristiane et al. Lei Geral de Proteção de Dados Pessoais: uma análise dos determinantes junto aos profissionais de Contabilidade. **Revista Catarinense da**

Ciência Contábil, v. 20, p. e3220-e3220, 2021. DOI: 10.16930/2237-766220213220. Disponível em: https://revista.crcsc.org.br/index.php/CRCSC/article/view/3220. Acesso em: 10 out. 2022.

MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucri dos; PARANHOS, Mario Cosac Oliveira; **LGPD E GDPR: UMA ANÁLISE COMPARATIVA ENTRE AS LEGISLAÇÕES**. São Paulo, 13 set. 2018. Disponível em: https://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes. Acesso em: 1 mar. 2022.

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

MASCARENHAS, Pedro Tenório Neto. **Segurança da informação:** uma visão sistêmica para implantação em organizações / Pedro Tenório Mascarenhas Neto, Wagner Junqueira Araújo. João Pessoa: Editora da UFPB, 2019.

MOREIRA, Natanael de Jesus. **Lei geral de proteção de dados pessoais:** a adaptação das empresas prestadoras de serviços contábeis da região sul catarinense. Monografia - Ciências Contábeis, Universidade do Extremo Sul Catarinense, UNESC. Criciúma. 2021.

NEVES, José Luis. Pesquisa qualitativa: características, usos e possibilidades. **Caderno de pesquisas em administração, São Paulo**, v. 1, n. 3, p. 1-5, 1996.

NUNES, Gabriela Victória Miranda. **Governança e boas práticas na Lei Geral de Proteção de Dados Pessoais: dos programas de compliance**. 2019. 67 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) —Universidade de Brasília, Brasília, 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à lei 13.709/2018 (LGPD)**. 2. ed. São Paulo: Saraiva Educação, 2020. 152 p. ISBN 9788553613403.

PINHEIRO, R. M. **Inteligência competitiva e pesquisa de mercado**. Curitiba: Iesde Brasil, 2009.

PRODANOV, Cleber Cristiano; DE FREITAS, Ernani Cesar. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição**. Editora Feevale, 2013.

KORKMAZ, Maria Regina Rigolon; SACRAMENTO, Mariana. Direitos do titular de dados: potencialidades e limites na Lei Geral de Proteção de Dados Pessoais. **REVISTA ELETRÔNICA DA PGE-RJ**, v. 4, n. 2, 2021. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/234. Acesso em: 24 jul. 2022.

SANTOS, Viviane Bezerra de Menezes. **Lei Geral de Proteção de Dados: Fundamentos e Compliance**. 2019. 54 f. Monografia (Graduação em Direito) - Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2019.

TEIXEIRA, Andreia Nunes et al. **Modelo de avaliação da maturidade de um programa de compliance**: uma aplicação no SENAC/Bahia. 2021.

VERGARA, Sylvia Constant. **Projetos e Relatórios de Pesquisa em Administração**. 12. ed. São Paulo: Atlas, 2010.

APÊNDICE A – Questionário

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS

QUESTIONÁRIO

I- Identificação da empresa

1. Qual o porte da sua empresa (faturamento) de acordo com o IBGE?

( ) Microempresa (menor ou igual a R$360 mil).
( ) Pequena empresa (maior que R$360 mil e menor ou igual a R$4,8 milhões).
( ) Média empresa (maior que R$4,8 milhões e menor ou igual a R$300 milhões).
( ) Grande empresa (maior que R$300 milhões).

II- Governança, Gestão e Accountability

2. Há, na organização, uma estrutura formal de Governança em Privacidade (comitês, conselhos, grupos de trabalho) com funcionamento documentado?

( ) Sim
( ) Não
( ) Em curso

3. Há, na organização, designação formal de usuários específicos como responsáveis setoriais pelo Programa de Privacidade para apoiar o Programa de Privacidade?

( ) Sim
( ) Não
( ) Em curso

4. Há definição, de forma documentada, de responsável pelo Programa de Privacidade da organização (Encarregado de Dados)?

( ) Sim
( ) Não
( ) Em curso

5. Há 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?

( ) Sim
( ) Não
( ) Em curso

6. Há cláusulas ou diretrizes específicas sobre privacidade e proteção de dados pessoais no Código de Conduta interno, que demonstrem a importância do tema?

( ) Sim
( ) Não
( ) Em curso

7. Há mapeamento de todos os terceiros, públicos e privados, dos quais a organização recebe ou com os quais a organização compartilha dados pessoais?

( ) Sim
( ) Não
( ) Em curso

8. Há análise sobre a existência de contratos e cláusulas de proteção de dados pessoais (forma de compartilhamento, responsabilidades, cooperação) com terceiros com os quais a organização compartilha ou dos quais a organização recebe dados pessoais?

( ) Sim
( ) Não
( ) Em curso

II- Capacitação

9. Os colaboradores/servidores da organização já receberam algum tipo de capacitação sobre LGPD e proteção de dados?

( ) Sim
( ) Não
( ) Em curso

10. Há um plano de capacitação e comunicação sobre LGPD e proteção de dados pessoais para todos os colaboradores/servidores da organização?

( ) Sim
( ) Não
( ) Em curso

III- Avaliação de Risco

11. Foi realizada análise de riscos das atividades de tratamento de dados pessoais com base em riscos de privacidade?

( ) Sim
( ) Não
( ) Em curso

IV- Monitoramento

12. Há indicadores de monitoramento e controles definidos para avaliação da aderência das ações para implantação da LGPD na organização?

( ) Sim
( ) Não
( ) Em curso

V- Segurança

13. A organização possui uma Política de Segurança da Informação estabelecida e publicada?

( ) Sim
( ) Não

( ) Em curso

14. Há controle estruturado da utilização de arquivos eletrônicos (planilhas, documentos, arquivos) de forma desestruturada, locais ou em nuvem, que contenham dados pessoais (envolvendo armazenamento, transferência, download e eliminação)?

    ( ) Sim
    ( ) Não
    ( ) Em curso

15. Há registros na organização de lista de ativos, serviços e ferramentas básicas de tecnologia e segurança da informação (sistemas operacionais atualizados, antivírus ativos e atualizado, firewall, filtros anti-spam etc), incluindo definição de usuário responsável por atualização da lista, existentes em seu parque tecnológico?

    ( ) Sim
    ( ) Não
    ( ) Em curso

16. Há previsão de realização periódica de scan de vulnerabilidades dos principais serviços de TI da organização?

    ( ) Sim
    ( ) Não
    ( ) Em curso

17. Há norma/diretriz/procedimento interno estabelecendo a necessidade de mesa limpa na organização?

    ( ) Sim
    ( ) Não
    ( ) Em curso

VI- Compartilhamento de dados pessoais

18. Há norma/diretriz/procedimento interno com estabelecimento de controles e limites para transferências de dados pessoais por aplicativos de mensageria ou e-mail não institucionais?

    ( ) Sim
    ( ) Não
    ( ) Em curso

VII- Eliminação de dados pessoais

19. Há norma/diretriz/procedimento interno para realização de eliminação de dados pessoais das bases da organização quando necessário?

    ( ) Sim
    ( ) Não
    ( ) Em curso

VIII- Respostas a Incidentes

20. Há norma/diretriz/procedimento interno estabelecendo instruções no caso de ocorrência de um incidente de segurança envolvendo dados pessoais?

    ( ) Sim
    ( ) Não
    ( ) Em curso

21. A organização realizou o cadastro junto à ANPD para comunicar eventuais incidentes de segurança?

    ( ) Sim
    ( ) Não
    ( ) Em curso

22. Há, no documento interno sobre gestão de incidentes de segurança, instruções para análise da necessidade de comunicação do incidente à ANPD e aos titulares de dados, bem como como será realizada a comunicação?

    ( ) Sim
    ( ) Não
    ( ) Em curso

IX - Desenvolvimento seguro

23. No âmbito do desenvolvimento interno de sistemas, ou mesmo na implantação de sistemas de terceiros, são analisados, documentados e testados requisitos que envolvam a proteção de dados pessoais?

    ( ) Sim
    ( ) Não
    ( ) Em curso

X - Backup

24. A organização realiza backups (cópias de segurança) com possibilidade de recuperação de dados?

    ( ) Sim
    ( ) Não
    ( ) Em curso

25. A organização realiza backups (cópias de segurança) com possibilidade de recuperação de dados?

    ( ) Sim
    ( ) Não
    ( ) Em curso

XI – Ciclo de vida de dados

26. A organização possui registros documentados do fluxo de dados pessoais em todos os setores (registro de atividades de processamento de dados pessoais - ROPAs)?

    ( ) Sim
    ( ) Não
    ( ) Em curso

27. O registro documentado do fluxo de dados incluiu reflexão sobre se os dados pessoais usados possuem finalidade legítima, explícita e informada, bem como são usados apenas para aquela finalidade, usando apenas os dados absolutamente necessários para o alcance do objetivo e de forma não discriminatória?

    ( ) Sim
    ( ) Não
    ( ) Em curso

28. O registro documentado do fluxo de dados permite demonstrar se há, na atividade, transferência internacional de dados?

    ( ) Sim
    ( ) Não
    ( ) Em curso

29. Há previsão em norma/diretriz/procedimento interno de revisão, ao menos anual, e atualização dos registros documentados das atividades de tratamento, bem como de registro de novas atividades?

    ( ) Sim
    ( ) Não
    ( ) Em curso

30. As atividades de tratamento de dados documentadas possuem hipóteses de tratamento de dados correspondentes (arts. 7o e 11)?

    ( ) Sim
    ( ) Não
    ( ) Em curso

31. Há definição dos papéis da organização como agente de tratamento de dados pessoais nas atividades de tratamento (controlador ou operador de dados)?

    ( ) Sim
    ( ) Não
    ( ) Em curso

XII – Retenção de dados

32. Há definição de tempo de armazenamento para os dados pessoais na organização buscando eliminá-los quando atingida a finalidade do tratamento dos dados?

    ( ) Sim
    ( ) Não
    ( ) Em curso

XIII – Gestão de consentimento

33. Há norma/diretriz/procedimento interno para gestão do consentimento dos titulares de dados quando esta for a fundamentação da atividade de tratamento?

    ( ) Sim
    ( ) Não
    ( ) Em curso

34. Há registros padronizados para obtenção e gestão de consentimento de responsáveis legais quando da sua necessidade para o tratamento de dados de crianças?

    ( ) Sim
    ( ) Não
    ( ) Em curso

XIV – Direitos dos titulares

35. Há atenção diferenciada quando o tratamento de dados envolve titulares vulneráveis como crianças, adolescentes e idosos?

    ( ) Sim
    ( ) Não
    ( ) Em curso

36. A organização possui um canal para que os titulares de dados pessoais entrem em contato para obter mais informações ou exercer seus direitos previstos na LGPD?

    ( ) Sim
    ( ) Não
    ( ) Em curso

37. A organização possui norma/diretriz/procedimento interno para gerenciar o atendimento aos direitos dos titulares de dados pessoais, bem como responsável definido para realizar esse gerenciamento e monitoramento?

    ( ) Sim
    ( ) Não
    ( ) Em curso

XV – Transparência

38. Há, em casos de coleta diretamente do titular de dados, avisos de privacidade sobre finalidade do tratamento de seus dados?

    ( ) Sim
    ( ) Não
    ( ) Em curso