UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE CIÊNCIAS CONTÁBEIS
CURSO DE CIÊNCIAS CONTÁBEIS

FLÁVIA DA SILVA CÂMARA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) – APLICADA ÀS EMPRESAS DE CONTABILIDADE

NATAL/RN
2020

FLÁVIA DA SILVA CÂMARA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) – APLICADA ÀS EMPRESAS DE CONTABILIDADE

Monografia apresentada à Banca Examinadora do Trabalho de Conclusão do Curso de Ciências Contábeis, em cumprimento às exigências legais como requisito parcial à obtenção do título de Bacharel em Ciências Contábeis.

Orientador: Prof. Dr. João Maria Montenegro Ribeiro

NATAL/RN
2020

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Setorial do Centro Ciências Sociais Aplicadas - CCSA

Câmara, Flávia da Silva.
Lei Geral de Proteção de Dados Pessoais (LGPD) - Aplicada às Empresas de Contabilidade / Flávia da Silva Câmara. - 2020.
50f.: il.

Monografia (Graduação em Ciências Contábeis) - Universidade Federal do Rio Grande do Norte, Centro de Ciências Sociais Aplicadas, Departamento de Ciências Contábeis. Natal, RN, 2020.
Orientador: Prof. Dr. João Maria Montenegro Ribeiro.

1. Lei Geral de Proteção de Dados Pessoais (LGPD) - Monografia. 2. Proteção de dados - Monografia. 3. Empresas de Contabilidade - Monografia. I. Ribeiro, João Maria Montenegro. II. Universidade Federal do Rio Grande do Norte. III. Título.

RN/UF/Biblioteca CCSA CDU 342.721:657

Elaborado por Eliane Leal Duarte - CRB-15/355

FLÁVIA DA SILVA CÂMARA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) – APLICADA ÀS EMPRESAS DE CONTABILIDADE

Monografia apresentada à Banca Examinadora do Trabalho de Conclusão do Curso de Ciências Contábeis, em cumprimento às exigências legais como requisito parcial à obtenção do título de Bacharel em Ciências Contábeis.

BANCA EXAMINADORA DA MONOGRAFIA:

Prof. Dr. João Maria Montenegro Ribeiro – Orientador

Prof. Dr. Edmilson Jovino de Oliveira – Membro da Banca

Prof. Dr. Luis Manuel Esteves da Rocha Vieira – Membro da Banca

Aprovada em: Natal/RN, 23 de julho de 2020

AGRADECIMENTOS

Agradeço primeiramente a Deus pelo dom da minha vida e por me ajudar a ultrapassar todos os obstáculos encontrados ao longo do curso.

A minha mãe Maria José pelo seu amor incondicional, dedicação e incentivo durante toda a minha vida pessoal e acadêmica. Ao meu noivo Eduardo por sempre me apoiar e encorajar desde o meu primeiro dia de curso, ele sempre acreditou no meu potencial e me ajudou da melhor forma.

À Universidade Federal do Rio Grande do Norte, todo o corpo docente e ao meu orientador Prof. Dr. João Maria Montenegro, que através dos seus ensinamentos contribuíram para o meu crescimento profissional e intelectual.

Aos meus familiares e amigos, e em especial as meninas da casa 24 da residência universitária biomédica, que estiveram presentes desde o segundo semestre do curso. Agradeço também a minha equipe de trabalho que me ajudou a pôr meus conhecimentos em prática, e a todos os que contribuíram direta ou indiretamente para minha formação.

DEDICATÓRIA

Dedico este trabalho a minha mãe, ao meu noivo e aos meus irmãos, que sempre se fizeram presentes em toda a minha jornada pessoal e acadêmica.

“Não há lugar para a sabedoria onde não há paciência.”

Santo Agostinho

RESUMO

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) dispõe sobre o tratamento de dados pessoais, inclusive por meios digitais, por pessoa natural ou jurídica. A implantação da lei propõe maior comprometimento com a segurança e transparência em relação ao tratamento dos dados, propiciando a pessoa natural maior proteção ao seu direito de liberdade e de privacidade e o livre desenvolvimento de sua personalidade. O objetivo deste estudo é analisar a aplicabilidade da Lei Geral de Proteção de Dados nas empresas de contabilidade. A coleta de dados foi realizada por meio de questionário, composto por 20 perguntas, sendo a primeira parte relativa ao perfil demográfico dos entrevistados, e a segunda parte relacionada a aplicação da LGPD nos escritórios de contabilidade. A pesquisa teve ao todo 82 respostas e foi destinada a profissionais contábeis. Através da análise dos dados, conclui-se que os escritórios contábeis estão preparados para aplicação da Lei Geral de Proteção de Dados, 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. Esta pesquisa contribui para enfatizar a importância da lei para sociedade, trazendo para as empresas mais clareza a respeito da regulação sobre coleta, tratamento, armazenamento e compartilhamento dos dados, e garantindo aos cidadãos mais privacidade e proteção dos seus dados.

Palavras-chave: LGPD. Proteção de dados. Empresas de Contabilidade.

ABSTRACT

The General Law On The Protection Of Personal Data (Law nº 13.709; August 14, 2018) disposes about the treatment of personal datas, including throught digital media, by natural or legal person. The implantation of the law purposes a bigger commitment with the security and transparency related to the treatment of the datas, providing to natural person a biggest protection to their liberty right of privacy and free development of their own personality. The objective of this study is to analyze the aplicability of the The General Law On The Protection Of Personal Data in the accounting firms. The datas collection was accomplished through a questionnaire, consisting in 20 questions, the first part concerning the demographic profile of the interviewees, and the second part related to the aplication of GLPPD in accounting offices. The research has 82 question in total and was destined to accounting professionals. Through the datas analyze, we conclude that the accounting offices are prepared to the aplication of The General Law On The Protection Of Personal Data , once that they consider indispensable the holder consent for the datas treatment, assist to the principles predicteds on the law and adopt the necessary security measures. This research contributes to emphasizes the importance of the law to the society, bringing a clearest view related do the regulation of the collect, treatment , storage and datas sharings, and guaranteeing to the citizien more privacy in their life protection of their datas.

Key words: GLPPD. General Law On The Protection Of Personal Data.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade nacional de proteção de dados

ART. – Artigo

CC – Código Civil

GDPR – General Data Protection Regulation

ISO – International Organization for Standardization (Organização Internacional de Normalização)

LGPD – Lei Geral de Proteção de Dados

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO DO PROBLEMA

O mundo tecnológico criou novas formas de comunicação e facilitou a interação, em virtude disso faz-se necessário tomar cuidados com os dados que estão sendo compartilhados, pois quase todo clique é passível de rastreamento, causando insegurança. Entende-se como dados pessoais toda e qualquer informação que permite identificar um indivíduo, seja pelo seu nome, apelido, endereço residencial, renda, localização, e-mail, hábitos de navegação ou consumo.

Os dados pessoais são utilizados em inúmeras situações, e com isso é comum que a segurança de tais dados seja negligenciada e a vida particular do titular esteja desprotegida, já que muitas vezes os dados pessoais são utilizados sem o consentimento do dono. Porém, o direito à privacidade trata-se da necessidade de permitir espaço para o desenvolvimento particular do indivíduo e de sua personalidade, sem a intervenção de terceiros, seja autoridade pública ou não.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 é a legislação brasileira que entrará em vigor em 3 de maio de 2021, foi inspirada na General Data Protection Regulation (GDPR), a norma geral da União Europeia, que trata da proteção específica sobre os dados pessoais, e as informações que identificam ou tornam identificável uma pessoa natural.

Conforme expõe Doneda (2017), ainda que exista na Constituição Federal o direito à privacidade, este não possui o mesmo alcance do direito à proteção de dados pessoais, que engloba privacidade, direito à igualdade, a liberdade de escolha o direito à não discriminação.

Na visão de Alves (2019) devido a evolução em aspectos tecnológicos e econômicos, deveria acontecer uma evolução jurídica, surgindo a necessidade de constitucionalizar a proteção de dados pessoais, a fim de dar aparato jurídico a privacidade dos dados.

Ao se falar em proteção de dados, pode-se pensar que apenas as empresas de tecnologia devem se adequar à nova lei, no entanto a LGPD afeta todas as empresas, públicas ou privadas, e de todos os ramos de atividade, que solicitam dados dos clientes, sejam eles internos ou externos a organização, tendo em vista que a proteção de dados pessoais é extremamente importante pela forma como são divulgados e tratados, considerando que na maioria dos casos os titulares ficam em condição de vulnerabilidade.

No presente estudo será tratado em especial das empresas de contabilidade, uma vez que todo contador processa dados pessoais diariamente, e todas as informações contábeis, fiscais e

financeiras das empresas e de seus colaboradores, e de pessoas físicas são tratadas nos escritórios.

Se a lei não for cumprida ou se houver qualquer incidente que coloque em risco os dados pessoais ou dados pessoais sensíveis, as empresas estarão passíveis de sofrer penalidades previstas na LGPD, além de perder credibilidade no mercado, pois qualquer vazamento de informação deve ser imediatamente exposto para o cliente e autoridade competente.

É possível notar que a lei traz muitos aspectos positivos para sociedade, pois permite aos cidadãos maior segurança para seus dados e dá a eles autoridade sobre as informações particulares. E o ponto negativo seria a falta de confiança em que a lei possa realmente dar certo no Brasil, e se as empresas, entre elas, as de contabilidade, estão preparadas para esse tipo de legislação.

Diante disso, o trabalho busca responder a seguinte questão: **As empresas de contabilidade estão adequadas para aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD)?**

1.2 OBJETIVOS

1.2.1 Objetivo geral

O objetivo geral do trabalho é analisar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais (LDPD) nas empresas de contabilidade.

1.2.2 Objetivos específicos

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

a) Demonstrar as principais características da LGPD;
b) Identificar e descrever os possíveis impactos da lei para as empresas de contabilidade;
c) Identificar se as empresas de contabilidade têm ciência da LGPD e se estão aptas a adotar os procedimentos necessários a aplicação da lei.

1.3 JUSTIFICATIVA

Em virtude da falta de segurança com relação aos dados, surgiu a necessidade de criação da lei de proteção de dados pessoais. Em países como na União europeia já existiam legislação específica para proteção de dados e privacidade dos seus cidadãos, e agora o Brasil passou a fazer parte dos que se preocupam com a segurança e privacidade das informações que estão sendo compartilhadas.

É necessário que todos os tipos de empresas que solicitam dados de seus clientes, pessoa natural identificada ou identificável estejam adequadas para aplicação da LGPD, e em especial os escritórios de contabilidade, que processa dados pessoais diariamente dos seus clientes, e principal tipo de empresa tratada no presente estudo.

Este trabalho possui aporte teórico, baseado em normas regulamentares, bem como artigos científicos e referências bibliográficas de autores especialistas no assunto de proteção de dados pessoas. A pesquisa traz, em especial, os impactos da lei para as empresas de contabilidade.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

No Brasil, a Constituição Federal de 1988 já apresentava em seu inciso X do art. 5º como direito fundamental inviolável, a intimidade, a vida privada e a imagem das pessoas, e não apenas isso, mas também a inviolabilidade do sigilo de correspondência, podendo haver indenização pelo dano material ou moral decorrente de sua violação.

Segundo o CC (lei n° 10.406, de 10 de janeiro de 2002), "Art. 1º. Toda pessoa é capaz de direitos e deveres na ordem civil.". Ou seja, todo ser humano é capaz de direito ou deveres mediante um conjunto de leis e princípios que regulamentam o comportamento e os interesses privados de uma sociedade.

De acordo com art. 1º da LGPD (Lei n° 13.709, de 14 de agosto de 2018) 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:

> Art. 1°. a lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e livre desenvolvimento da personalidade da pessoa natural.

A Lei Geral de Proteção de Dados Pessoais foi sancionada pela Lei nº 13.709, em 14 de agosto de 2018 e estava prevista para entrar em vigor 24 meses após a sua a data de publicação, em 14 de agosto de 2020, porém, devido a pandemia causada pelo novo corona vírus (COVID-19), o prazo para entrar em vigor foi prorrogado para 3 de maio de 2021, conforme disposto pela medida provisória 959, de 29 de abril de 2020, tendo sua validade em todo território nacional e se sobrepondo a qualquer lei estadual ou municipal.

Entende-se que o intervalo de 18 meses foi dado para que as organizações pudessem se adequar as novas obrigações referente ao uso, armazenamento e proteção de dados pessoais, e tempo suficiente para criar uma entidade fiscalizadora para lei (Autoridade nacional de proteção de dados - ANPD), e foi prorrogada devido a difícil situação em que se encontra todas as organizações nesse momento de crise não apenas no Brasil, mas no mundo inteiro.

A lei foi baseada na GPDR (regulamentação europeia de proteção de dados) e regulamenta como as empresas devem utilizar os dados pessoais enquanto se relaciona com a pessoa natural identificada ou identificável. A LGPD surgiu com a visão de preservar o direito

constitucional a liberdade e a privacidade de todos os cidadãos e assim protegê-los que quais quer danos.

> Essa Lei define que deverão estar em conformidade tanto a portaria de um prédio, que registra os dados dos visitantes em um livro, quanto um laboratório de análises clínicas que registra os dados pessoais de seus funcionários na área de RH e disponibiliza os resultados das análises clínicas dos clientes na Web. Esta é a primeira Lei que punirá por inércia: além de as instituições serem obrigadas a se adequar à Lei, deverão demonstrar (evidenciar) a sua conformidade, tanto para o titular quanto para a autoridade nacional, para evitarem as penalizações. Site Governanças (2019)

Antes da vigência desta lei as empresas deveriam seguir as diretrizes contidas em leis esparsas, como por exemplo, a Lei do Sigilo Bancário, Marco Civil da Internet, Código de Defesa do Consumidor. E assim a lei surgiu com a necessidade de observar a forma como os dados são processados, e não somente pelo fato de que se deve respeitar a privacidade. A proteção de dados se trata de uma evolução demandada pela humanidade e tem como grande diferencial uma visão moderna de como o dado deve ser processado, observando-se sempre a finalidade do tratamento e tendo o cidadão como aquele que tem a propriedade dos dados, pois ele é o titular.

Os fundamentos da proteção de dados disciplinados pela LGPD são: o respeito a privacidade, autodeterminação informativa, liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico, tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

2.1.1 Aplicação e princípios da LGPD

A Lei Geral de Proteção de Dados Pessoais serve para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A lei dispõe sobre o tratamento de dados feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

A lei se aplica para pessoa física ou jurídica que gerencie bases com fins econômicos; dados tratados dentro do território nacional, independentemente do meio aplicado; e dados usados para fornecimento de bens ou serviços. A lei não se aplica a dados de fora do Brasil e que não sejam objeto de transferência internacional, não se aplica para fins jornalísticos e

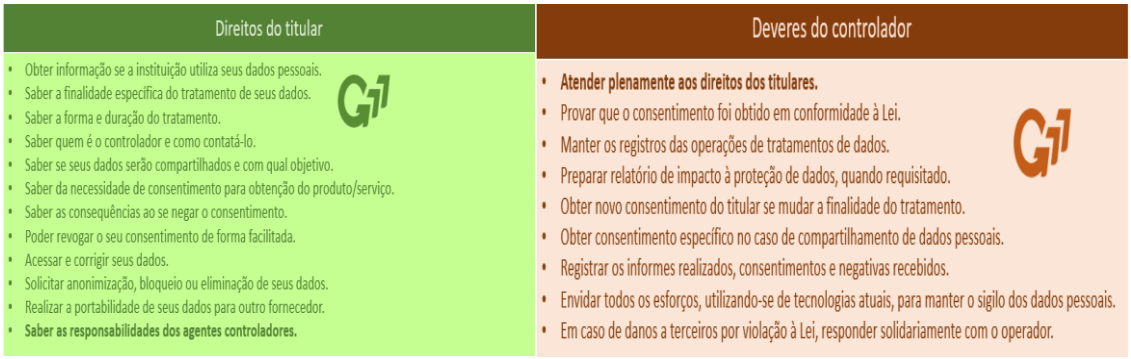
artísticos; de segurança pública; de defesa nacional; de segurança do Estado; de investigação e repressão de infrações penais; e a particulares.

A LGPD nos traz em seu art. 6° os princípios que devem ser seguidos ao realizar tratamentos de dados pessoais:

> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X – Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Tendo em vista que o tratamento de dados diz respeito a uma intromissão da vida pessoal do titular, é fundamental que sejam seguidos princípios determinados em lei, e que o titular tenha total liberdade para aceitar ou recusar tal tratamento, bem como ficar ciente de quais dados serão processados e com qual finalidade. Na figura 1 a seguir é possível verificar os direitos do titular e os deveres do controlador.

Figura 1 – Direitos do titular e deveres do controlador



Fonte: Dados do site governanças

2.1.2 Dados Pessoais

A comissão europeia define dados pessoais como:

> Dados pessoais são informação relativa a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa. Dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, mas que possam ser utilizados para reidentificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do RGPD. Dados pessoais que tenham sido tornados anónimos de modo a que a pessoa não seja ou deixe de ser identificável deixam de ser considerados dados pessoais. Para que os dados sejam verdadeiramente anonimizados, a anonimização tem de ser irreversível.

São exemplos de dados pessoais o nome ou apelido, o endereço de uma residência ou de correio eletrônico, o número de um cartão de identificação, dados de localização, um endereço IP, o número do seu telefone e até mesmo os dados detidos por um hospital ou médico, que permitam identificar uma pessoa de forma inequívoca.

Para Ribeiro (2016), os dados pessoais são cumulações de fatos e acontecimentos que formam a personalidade de cada indivíduo, os dados pessoais podem contar de forma precisa a história de vida de cada cidadão.

Pela LGPD existem três tipos de dados, os dados pessoais, os dados pessoais sensíveis e dados anônimos. Sendo considerado como dados pessoais toda e qualquer informação que possa ser vinculada a uma pessoa identificada ou identificável. Dados pessoais sensíveis são qualquer dado que pode levar a algum tipo de discriminação, por exemplo, religião, vida sexual, dado genético. E dado anônimo é aquele que deixa de ser diretamente relacionado a uma pessoa, ou seja, quando um conjunto de dados se torna estatística.

Entende-se por titular aquele indivíduo dono dos dados pessoais que serão tratados, e ele quem deve autorizar ou não o tratamento dos dados. Já agentes de tratamentos são os controladores e operadores. Controlador é o responsável pelas decisões relacionadas ao tratamento dos dados pessoais, bem como por qualquer incidente que venha a ocorrer. E operador é aquele quem trata os dados e deve seguir todas as ordens do controlador em relação ao tratamento dos dados. Já a pessoa responsável por intermediar a comunicação entre os titulares, o controlador e a Autoridade Nacional de Proteção de Dados é conhecido como encarregado.

Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável por implementar e gerenciar as regras da LGPD, garantindo que a Lei seja cumprida, e é também o responsável por realizar auditorias, assim como aplicar as devidas sanções em descumprimento da Lei.

2.1.3 Tratamento de dados

Tratamento de acordo a LGPD é:

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

A LGPD se aplica a todo e qualquer tratamento de dado, realizado por pessoa física ou jurídica, e é voltada para fins comerciais, desde que o tratamento seja realizado todo ou em parte no território nacional. A Lei não será aplicado em tratamentos de dados com fins não econômicos, ou que seja realizado para fins jornalístico e artísticos, em casos de segurança pública e do estado e defesa nacional, e de dados de fora do país e que não seja compartilhado com agentes brasileiros.

A Lei Geral de Proteção de Dados traz outros conceitos interessantes para que haja ou não o tratamento de dados:

> Consentimento: permissão dada pelo titular para que determinado(s) dado(s) pessoal(is) seja(m) tratado(s). Deve ser pedido de forma explícita, clara e transparente pelo operador ou controlador, e se referir a uso específico e limitado.
> Bloqueio: suspensão do tratamento de dados, que não isenta o operador e o controlador de precisarem proteger os dados pessoais e o banco de dados em que eles se encontram.
> Eliminação: exclusão de dados pessoais.

Segundo Ribeiro (2016), o consentimento para o tratamento de dados é parte importante para que haja o respeito ao direito à liberdade de escolha, e deve ser livre, informada, inequívoca, específica, determinada e expressa.

O consentimento é a principal ferramenta para que haja o tratamento de dados, e deve ser respeitada a forma prevista em lei, seja por escrito ou qualquer meio que demonstre a vontade do titular. Tal consentimento pode ser ainda revogado a qualquer momento pelo titular.

O consentimento não é sempre obrigatório, não é necessário em casos que o tratamento visar o cumprimento de leis e de políticas públicas, para órgãos de pesquisa, porém estes devem trabalhar com dados anonimizados sempre que possível, na execução de contratos ou para o exercício regular de direitos, que é o caso de uma ação judicial, e também em casos de tutela da saúde e proteção da vida.

Não se tratando das exceções que dispensam o consentimento do titular, o controlador mesmo que já esteja de posse dos dados, se precisar tratá-los com outra finalidade, deve pedir novamente o consentimento do titular.

2.2 SEGURANÇA DOS DADOS PESSOAIS

A segurança pode ser entendida como um conjunto de medidas que visam à proteção de riscos, perigos ou perdas a pessoas ou coisas. "A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos." [BLUEPHOENIX, 2008].

Conforme expõe Mário Antunes (2019), “as perdas não são apenas monetárias, já que há custos que poderão ser de difícil contabilização, como a perda de credibilidade ou a publicidade negativa”.

Os dados pessoais e dados sensíveis tem um valor exponencial, e casos esses dados sejam roubados ou perdidos, as empresas podem pagar um preço muito alto para recuperá-los ou para sanar os efeitos dos danos causados. Além da multa em dinheiro, pode perder a confiança dos seus clientes, investidores e parceiros.

2.2.1 A importância da segurança dos dados na internet

As pessoas não conhecem o quão valioso os seus dados pessoais são para o mercado, e nem como os mesmos são coletados, armazenados e compartilhados, de forma que uma simples falha de segurança os deixe expostos.

De acordo com Ricardo (2018):

> Diariamente, algoritmos são alimentados por informações pessoais que indicam como pensamos e quais os nossos desejos, criando perfis de consumo dos usuários, para fins de publicidade direcionada e venda desses dados pessoais para outras empresas. Nesse sentido, a proteção da privacidade passa pela proliferação dessas práticas comerciais de “big data”, “targeting” e “profiling” dos usuários, deixando as pessoas presas dentro de uma realidade on-line customizada (“tailored reality”).

A maioria das pessoas ao efetuar uma compra na internet já se deparou com a situação de ser obrigado a preencher cadastros com diversas informações pessoais, que teoricamente não servem para nada. Hoje em dia, com os programas de educação fiscal, informar o CPF no momento de uma compra é imprescindível, mas nem todos os dados solicitados são necessários. E o que as pessoas não sabem é que esses dados ficam registrados, seja para criar um perfil do usuário, a fim de oferecer conteúdo publicitário direcionado, ou para vendê-los a outras empresas.

De acordo com Ricardo (2018), a vida de uma sociedade hiper conectada é decidida por algoritmos automatizadas, e vários dos tratamentos desses algoritmos são feitos por

inteligências artificiais. No entanto, com a LGPD, é possível solicitar a exclusão desses dados após o término da relação comercial entre as partes.

O direito à eliminação de dados está disposto no art.18° da LGPD, onde estabelece que o titular pode solicitar ao controlador, a qualquer momento e mediante requisição:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> 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, exceto nas hipóteses previstas no art. 16 desta Lei;
> 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.

As organizações que tratam os dados pessoais também devem sempre observar o disposto na LGPD, pois para elas é obrigatório está de acordo com as normas e implantar os procedimentos necessários para garantir a segurança dos dados, afim de evitar as penalidades previstas.

2.2.2 Gestão de incidentes e vazamentos de Dados

De acordo com o dicionário: “incidente é um episódio inesperado ou situação que altera a ordem normal das coisas”. Ao se falar em incidentes relacionado aos dados os efeitos são diversos e atualmente as consequências e penalidades estão asseguradas na lei de proteção de dados.

As empresas mantêm um banco de dados, no qual contém uma série de informações pessoais dos seus clientes ou colaboradores, que devem ser mantidos em segurança. E para isso é necessário tomar algumas medidas, a fim de evitar vazamentos ou incidentes que possam colocar em risco a proteção desses dados e a imagem da empresa.

"O custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir" [DAVIS, 1997 APUD BLUEPHOENIX, 2008]. É mais viável para empresa tomar medidas preventivas e realizar análises de riscos, ao invés de assumir uma multa de até 2% do seu faturamento, que a depender da receita da empresa, chegaria até 50 milhões por infração.

De acordo com o artigo 48 da Lei nº 13.709/18 (Lei Geral de Proteção de Dados), o controlador tem a responsabilidade de comunicar a autoridade nacional e ao titular qualquer incidente de segurança que possa acarretar risco aos titulares, devendo ser feita em prazo razoável, mencionando no mínimo:

> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata;
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

De acordo com Baxauli (2018), os principais tópicos de uma abordagem correta sobre incidentes de segurança são a elaboração prévia de um plano de respostas a incidentes, a devida comunicação a autoridade nacional e titulares e a aplicação de medidas que mitiguem ou neutralizem os riscos ou danos causados.

Quanto ao plano de resposta a incidentes deve englobar a todos os funcionários da empresa, mesmo aqueles de baixo escalão, pois eles devem obrigatoriamente informar sobre qualquer irregularidade operacional relacionada a proteção de dados, podendo sofrer penalidades caso não haja a notificação e será necessário criar um fluxo de comunicações que facilitem a chegada da informação sobre o vazamento de dados, para que medidas sejam tomadas. Também devem estar integrados ao plano os prestadores de serviços que processam os dados.

Deve ser comunicado à autoridade nacional de proteção de dados e aos titulares quanto a qualquer incidente e vazamentos de dados. O controlador deve em conjunto com a autoridade nacional analisar qual será as medidas necessárias para neutralizar os riscos causados pelos incidentes. E quanto a comunicação aos titulares deve ser o mais transparente possível e de forma estratégica.

Relatório de impacto à proteção de dados pessoais de acordo com art. 5º da LGPD:

> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

O controlador deve manter o relatório de impacto à proteção de dados pessoais sempre que houver qualquer risco de que determinado tratamento de dados possa vir a causar danos ao titular, com isso é possível entender os perigos envolvidos em cada incidente. Esse relatório é uma documentação que contém a descrição dos processos de tratamento de dados pessoais que

podem gerar riscos, bem como medidas e mecanismos de mitigação de risco. Com ele é possível comprovar os devidos cuidados para evitar tais risco no tratamento de dados.

De acordo a art. 38 da Lei Geral de Proteção de Dados Pessoais:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Para Alves (2019), o encarregado de proteção de dados poderá ser alguém da área de TI, advocacia, não importa. O que importa é que as pessoas que auxiliarem esse encarregado formem uma assessoria técnica multidisciplinar, pois assim é que a organização poderá ter uma adequação mais efetiva da legislação.

2.3 GOVERNANÇA

Segundo o Banco Mundial, em seu documento Governance and Development (1992), a definição geral de governança é o exercício da autoridade, controle, administração, poder de governo. Ou seja, é toda a forma de governar seja através de leis, normas ou poder de uma sociedade.

Dentre os diversos tipos de governança, é importante citar a governança corporativa, que é o sistema em que as entidades são dirigidas, monitoradas e incentivadas, a qual permite um contato entre as diferentes partes existentes numa organização, garantindo a confiabilidade entre elas.

As governanças que são extremamente importante para o presente estudo são: a Governança dos Dados e a Governança da Privacidade, tendo em vista que a Lei Geral de Proteção de Dados (LGPD) exige a formulação de boas práticas, estabelecimento de políticas e padronização, ações educativas, organização, supervisão e mitigação de riscos.

2.3.1 Governança de Dados

A governança de dados é uma gestão eficiente de toda informação gerada, e tem como objetivo a organização, a estruturação e o uso estratégico dos dados que são coletadas,

armazenados e tratados dentro da organização, tendo em vista que esses dados são capazes de auxiliar no planejamento e tomada de decisão.

Segundo Kauer (2019, p. 80), “a governança de dados abrange em si a compreensão de como é realizado o processamento de dados dentro da companhia.” Sendo assim, entende-se processamento como tratamento, e de acordo com inciso X do artigo 5º da LGPD:

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Não se pode falar em governança de dados sem antes falar sobre a segurança da informação, a respeito desse assunto Telium Networks afirma:

> A segurança da informação é um dos temas mais importantes dentro das organizações em função do grande número de ataques virtuais orquestrados por cibercriminosos no mundo todo. Devido a isso, esse tópico se tornou um objetivo constante não só das equipes de TI, como das próprias organizações. Contudo, para que ele possa ser reforçado nas empresas, é preciso atenção aos três pilares que sustentam a segurança em TI: confidencialidade, integridade e disponibilidade. Networks (2019)

Confidencialidade, integridade e disponibilidade devem existir para que uma organização possa adotar suas políticas e procedimentos de gestão de dados. É importante antes de tudo, que seja realizado um mapeamento de como ocorre as entradas e saídas dos dados em cada setor da empresa, e após essa etapa deve ser elaborado um parecer de mapeamento de dados, com os fluxos dos dados, bem como suas formas de tratamentos.

> Sendo assim, o que podemos concluir acerca da governança de dados é que, tal como determinado pelas normas de segurança da informação, é necessário que as informações da empresa estejam em bases de dados estruturadas. Isso é essencial para que o programa possa ser implementado de forma plena, e será relevante para elaboração de políticas, procedimentos, e até mesmo em caso de incidente, para que se saiba o que fazer para mitigar, em quais áreas e fluxos será necessário agir, e até mesmo para que se identifique qual foi a porta de entrada que gerou o incidente. Kauer (2019, p. 82).

Ao se conservar a segurança da informação na empresa, é possível adotar um modelo de governança, e implementar recursos tecnológicos para tratar todo o processamento e armazenamento dos dados. Conforme exposto no site Xerpa (2018), para investir em uma boa governança de dados, é necessário identificar quais setores que mais geram dados, certificar-se de que a empresa possui estrutura para acomodar novas tecnologias e capacitar as equipes envolvidas.

2.3.2 Governança de Privacidade

Para Yun (2019, p. 89 e 90), apesar de complexo e desafiante definir uma abordagem de governança de privacidade, se assim o fizer, a organização fica assegurada quanto à conformidade com as obrigações legais, e alinhada com os objetivos do negócio que devem estar suportados por todos os níveis da organização.

Com o intuito de criar um programa de compliance sobre privacidade e segurança dos dados, Gutterman (2018) considera importante tratar sobre os seguintes pontos:

> Definir e identificar informações não públicas que estão sob poder da companhia e documentar como essa informação flui interna e externamente por toda a estrutura organizacional da corporação;
>
> Estabelecer uma responsabilidade gerencial e o controle sob o programa de Compliance, além de alocar recursos financeiros e demais necessidades para o programa;
>
> Estabelecer programas focados em lidar com riscos específicos relacionados à privacidade de dados, como coleta de informações online e o agrupamento de informações durante o andamento do relacionamento com o cliente;
>
> Introduzir programas educacionais para todos os funcionários da companhia, além de parceiros de negócio, sobre os requerimentos de privacidade de dados e segurança da informação, incluindo orientação contínua de novos avanços e também as ameaças a executivos e gerentes diretamente envolvidos no programa de compliance;
>
> Entender e monitorar todas as leis e regulamentação relacionadas a privacidade e segurança da informação, incluindo tendências emergentes que podem culminar em transformações no ambiente regulatório em um futuro próximo;
>
> Instituir procedimentos de retenção e destruição de informações;
>
> Estabelecer e aplicar procedimentos de notificação de incidentes e violação de dados privados;
>
> Entabular e reforçar políticas disciplinares a respeito de violações com funcionários e parceiros de negócios a fim de que cumpram com as políticas de segurança de dados e privacidade da companhia;
>
> Comunicar a política de segurança de informação e privacidade da companhia para importantes stakeholders, incluindo funcionários, clientes, parceiros comerciais, órgãos financeiros e reguladores;
>
> Prover relatórios frequentes sobre a eficácia desse programa para o conselho de administração e lideranças da organização;

A preocupação em criar um programa de compliance de privacidade e segurança dos dados surgiu antes de ser publicada a Lei Geral de Proteção de Dados, porém, após sua existência se torna ainda mais importante adotar um programa como este para assegurar que os dados possam tratados de forma segura. Inicialmente é relevante perceber o tipo de informação e com quais tipos de dados se trabalha e em seguida escolher um responsável para coordenar e monitorar todas as leis, além de estabelecer um programa que tenha o foco em possíveis riscos que envolvem a privacidade dos dados.

O responsável gerencial deve comunicar e reforçar para toda a organização as políticas de segurança, e também notificar aos executivos, gerentes, titulares e a entidade fiscalizadora

sobre qualquer incidente ou violação dos dados pessoais. Deve ainda ser implantado programas educacionais voltados para todos os colaboradores sobre privacidade e segurança dos dados.

Na visão de Yun (2019, p. 83), deve ser observado alguns componentes na governança de privacidade, tais como: missão e visão da privacidade da organização; escopo do programa de privacidade; adoção de uma estrutura de privacidade; estratégia de privacidade da organização; e estrutura de um time de privacidade.

O programa de privacidade deve está diretamente ligado ao propósito da organização, ou seja, com sua missão e visão. Ao alinhar o programa com o propósito da empresa, é interessante identificar as normas que devem ser seguidas para deixar todas as suas atribuições em conformidade com a lei, e antes de tudo deve-se identificar quais dados são coletados e tratados.

Uma estrutura apropriada deve ser adotada para garantir a proteção dos dados através de um programa eficiente de privacidade, e assim estabelecer estratégias para o suporte necessário do programa e uma comunicação mais efetiva, tendo em vista que todos da organização devem estar totalmente empenhados em manter a segurança de todo o ciclo de vida dos dados pessoais.

Para Freitas (2019), é interessante garantir que a política de privacidade da organização esteja facilmente disponível. Por conseguinte, essa transparência no tratamento dos dados pessoais é constatada através do seu compromisso profissional.

2.4 IMPLANTAÇÃO DA LGPD NAS EMPRESAS DE CONTABILIDADE

Todas as empresas que coletam, armazenam e processam dados pessoais de pessoas naturais devem se adequar as regras da Lei Geral de Proteção de Dados, inclusive os escritórios de contabilidade. Essas empresas deverão adotar a implementação de mecanismos internos e sistemas de controle para garantir a conformidade com a legislação, a fim de proteger os dados pessoais de quaisquer riscos de incidentes que possam ocorrer.

As empresas devem atender a todos os princípios da LGPD antes de processar qualquer dado pessoal, e para isso é necessário provar que possui o consentimento do titular e que tem a infraestrutura para manter em segurança todas as informações. Em virtude disso, é possível contar com a certificação da ISO 27001.

De acordo com o site Advisera (2020):

> A ISO 27001 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, privada ou pública, pequena ou grande. Ela é escrita pelos melhores especialistas mundiais no campo de segurança da informação e provê metodologia para a implementação da gestão da segurança da informação em uma organização. Ela

> também possibilita que organizações obtenham certificação, o que significa que um organismo certificador independente confirmou que uma organização implementou a segurança da informação em conformidade com a ISO 27001.

A implantação da LGPD nas empresas de contabilidade, assim como em qualquer outro tipo de organização não se trata de uma tarefa fácil, porém é uma lei que deve ser seguida à risca, a fim de garantir a proteção dos dados pessoais com que se trabalha e evitar penalidades. Para isso, será necessário realizar análises de riscos e adotar medidas preventivas, com o intuito de adequar a execução das atividades da organização as normas.

De acordo com Marcelo Tostes (2020), uma equipe de TI capacitada pode contribuir muito com a segurança de dados da empresa, podendo evitar grandes riscos através da elaboração de uma política interna de uso de recursos digitais.

Além de adotar todas as medidas possíveis, é importante elaborar relatórios de riscos, evidenciando as fragilidades, os riscos a que cada setor da empresa está exposto, bem como os incidentes ocorridos e como foram resolvidos, fazendo com que as políticas internas criadas sejam direcionadas e tenha maior eficácia.

2.4.1 Dados tratados em Empresas de Contabilidade

Segundo Elivieri (2019): "O advento da LGPD, a par das obrigações práticas e rotinas novas que impõe aos empregadores, agora controladores, e a par das consequências administrativas do seu eventual descumprimento, força a necessidade de um novo olhar sobre a natureza das informações pessoais e a forma como elas devem ser tratadas numa empresa."

A nova legislação cria regras claras sobre como as organizações devem coletar, armazenar e compartilhar dados pessoais de usuários, sejam em meios digitais ou físicos. E assim como toda e qualquer organização, os escritórios devem cumprir o que exige a lei.

Os profissionais já seguem o código de ética profissional do contador que se preocupa em guardar o sigilo em relação a dados e informações confidenciais, e a partir do momento de sua entrada em vigência deverá atender também aos princípios da Lei Geral de Proteção de Dados, onde estarão sujeitos as penalidades.

Um escritório contábil processa dados não apenas dos seus clientes, mas também de seus funcionários, dos funcionários dos seus clientes, dados esses como: nome, endereço residencial, e-mail, RG, CPF. E Todos esses dados são protegidos por lei, e devem ser solicitados, além de

informados ao titular de forma clara sobre como serão tratados, qual a finalidade ou se serão compartilhados.

O e-Social é um dos sistemas gerenciados pelos escritórios contábeis, que associa diversos dados de colaboradores, seus familiares e até mesmo de ex-funcionários da empresa, com isso é muito importante informar ao empregado que seus dados serão coletados e transferidos ao governo por meio do e-Social. Apesar de que, a coleta e o envio dessas informações se refiram a uma exigência legal, é extremamente necessário que haja transparência na relação entre a organização e o funcionário.

O setor de RH dos escritórios e também de outras empresas, normalmente solicita e processa grandes quantidades de dados pessoais, tais como telefone, endereço residencial e de e-mail, diversos documentos pessoais, e por vezes até registros médicos, orientação sexual, política e religiosa. Esse setor solicita dados desde o momento da pré-seleção para um cargo de trabalho, na celebração desse contrato de trabalho, durante a execução do contrato até a sua rescisão.

2.4.2 Impactos positivos e negativos da lei nas empresas de contabilidade

A LGPD trará impactos positivos e negativos para os escritórios de contabilidade, pois essas empresas trabalham com muitos dados pessoais importantes. Contudo, é possível estar de acordo com as normas se houver preocupação com as questões de privacidade, adoção de medidas e procedimentos corretos de segurança e proteção de dados.

Conforme expõe o site Jornal do comércio (2020), “o e-Social é um dos sistemas gerenciados pelos contadores que concatena uma série de dados de colaboradores das empresas e até mesmo de seus familiares e de ex-funcionários, que merecem sigilo e cuidado.”

Segundo o site Domínio Sistemas (2020), o mais importante para os escritórios é gerenciar os documentos dos clientes, pois são os responsáveis por demonstrar para as autoridades que eles atuam dentro da legalidade.

É certo que se houver qualquer tipo de vazamento de dados, e os cliente tomarem conhecimento, eles serão os primeiros a denunciar a empresa por tal descuido e a perder a credibilidade na empresa por não ter investido em segurança para proteger seus dados. E ainda se tal incidente acarretar em problemas mais graves, a depender ou não da culpabilidade da empresa, ela deverá pagar multas.

Um dos impactos positivo da lei para as empresas contábeis, é que elas poderão trabalhar com maior comprometimento com relação a segurança dos dados dos seus clientes, onde poderá

contar com a ajuda de excelentes profissionais em privacidade de dados. E também deverão investir muito mais em segurança a fim de evitar ataques de hackers e vazamentos de informações importantes.

Como impacto negativo para todo e qualquer agente de tratamento de dados, é possível citar as sanções previstas no artigo 52 da Lei Geral de Proteção de Dados:

> 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.

Conforme exposto, poderão ser aplicados sanções e multas bem pesadas que impactam significativamente os escritórios, como multa de até R$ 50.000.000,00 (cinquenta milhões de reais). E além das perdas em valor, o impacto maior pode ser a falta de credibilidade na empresa, que é mais difícil de recuperar que qualquer dinheiro.

Um dos principais investimentos a serem feitos nas organizações contábeis, segundo o Jornal do comércio (2020) seria a criação de um responsável pela segurança das informações armazenadas e geradas, seja um comitê de segurança ou agentes de tratamento de dados pessoais.

2.4.3 Como as empresas de contabilidade podem se adaptar a LGPD

As empresas de contabilidade deverão tomar diversas medidas com o propósito de se adaptar a Lei Geral de Proteção de Dados. É bastante importante e necessário que as empresas possam documentar os dados que serão tratados, como serão armazenados, qual software é utilizado, com são processados, com quem são compartilhados, por quanto tempo ficarão armazenados e qual a finalidade para utilização de cada dado.

Segundo Ferreira (2019), para se adaptar à LGPD, será necessário também "colocar ordem na casa", que consiste em mapear os dados, classificá-los, organizá-los de acordo com a

base legal que autoriza o seu tratamento e, depois, torná-los mais seguros. "Devem ser adotadas várias mudanças, que podem garantir a adequação à lei e à proteção das atividades."

Diversos escritórios contratam fornecedores de software para armazenagem de dados em nuvem, com isso, é indispensável está inteirado sobre a responsabilidade que esses fornecedores tem com os dados, quais são suas políticas e principalmente saber se o mesmo atende aos princípios da LGPD.

De acordo com o site Thomson Reuters (2020), as medidas que os escritórios de contabilidade devem adotar para se adaptar a LGPD, são:

> **1. Consentimento no recolhimento e uso de dados**
> A única pessoa que pode autorizar os escritórios de contabilidade a usá-los é o titular dos dados. Esse consentimento explícito deve ser reforçado especialmente em sistemas digitais.
> **2. Diferenciação entre controlador e operador**
> A Lei também exige que as empresas definam quem irá fazer uso dos dados. Isso é determinado em dois níveis de trabalho: de controlador e de operador. A responsabilidade de cada um é diferente: o controlador direcionará o que será feito com os dados. Já o operador é quem lida com eles, na prática.
> **3. Comitês de segurança da informação**
> Os escritórios de contabilidade devem criar um Comitê de Segurança da Informação para avaliação das medidas de proteção de dados próprios e dos clientes. Neste comitê haverá um profissional exclusivo, o Data Protection Officer, responsável pelo cumprimento da nova lei.
> **4. Medidas de redução de exposição**
> O escritório contábil deve utilizar técnicas de segurança administrativas e de operações diversas, implementadas de forma ampla, para que todos os colaboradores possam praticar. Isso também é parte do trabalho do comitê de segurança da informação.
> **5. Responsabilidade das terceirizadas**
> Os escritórios de contabilidade que tiverem subcontratadas devem exigir que elas também se adaptem às medidas de proteção de dados, porque estarão também sujeitas às sanções em casos de vazamentos. Assim, é fundamental ter clareza quanto aos procedimentos de segurança.

Toda e qualquer empresa que trabalha com a coleta, armazenamento e tratamento de dados deve estabelecer uma política interna para proteção desses dados, onde deverá ser escolhido responsáveis para preservá-los conforme as normas. É importante estabelecer as formas de obtenção do consentimento de seus clientes, e de como agir em casos de violação de segurança ou vazamento de dados, bem como as resoluções desses casos.

Para Ferreira (2019), a computação em nuvem é um dos recursos que trazem muito mais praticidade para os profissionais do escritório, facilitando a interação com os clientes e a conclusão das atividades. Além disso, garante a segurança dos dados e aumenta a produtividade do time.

3 METODOLOGIA

3.1 ENQUADRAMENTO METODOLÓGICO

Gerhardt e Silveira (2009, p.13) afirmam que “a metodologia vai além da descrição dos procedimentos (métodos e técnicas a serem utilizados na pesquisa), indicando a escolha teórica realizada pelo pesquisador para abordar o objeto de estudo.”

Para Filho e Santos (2000), a metodologia da pesquisa prepara os recursos utilizados na coleta dos dados para apresentá-los na pesquisa. De outra maneira estabelece que o levantamento das informações pode ser de diversas formas, seja por meio de questionário, formulário, teste, pesquisa de mercado, entrevista, dados estatísticos, livros, jornais, revistas, entre outros.

A abordagem do problema utilizada foi quantitativa, visto que os dados coletados através do questionário aplicado foram selecionados, codificados e tabulados com o intuito de avaliar a aplicação da LGPD nas empresas de contabilidade. A população da pesquisa foi composta por profissionais dos escritórios contábeis de Natal.

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.”

De acordo com Marconi e Lakatos (2003), a pesquisa “é um procedimento formal, com método de pensamento reflexivo, que requer tratamento científico e se constitui no caminho para conhecer a realidade ou para descobrir verdades parciais.”

3.2 PROCEDIMENTOS PARA COLETA E ANÁLISE DOS DADOS

Quanto aos procedimentos de coleta de dados, destaca-se neste trabalho a pesquisa descritiva, que se baseia na Lei nº 13.709/2018 (LGPD) e na realização de questionário a respeito da aplicação da lei nas empresas de contabilidade, tendo como público alvo os profissionais atuantes em escritórios contábeis da cidade de Natal, onde foi obtido 82 respostas na 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 através de questionário e observação sistemática.

O questionário utilizado na pesquisa é composto por 20 perguntas, dentre elas duas perguntas sobre idade e gênero, e as demais envolvendo o tema da LGPD voltado para área contábil. Foi aplicado apenas de forma online, confeccionado a partir da ferramenta Google formulários, e repassado por meio das redes sociais como WhatsApp, Instagram, e pelo fórum do curso de ciências contábeis. Os dados foram codificados e analisados por meio do Microsoft Office Excel.

A pesquisa se baseia também no conhecimento de diversos estudiosos do assunto que analisaram a lei desde quando foi publicada e que opinam sobre a sua importância para o titular de dados, bem como o impacto que irá causar em diversas organizações, em especial aos escritórios de contabilidade, devido à complexidade que envolve o tratamento dos dados e a sua segurança.

A lei é extremamente importante para sociedade, pois trará mais clareza para as empresas sobre a regulação a respeito da coleta, tratamento, armazenamento e compartilhado dos dados, e para os cidadãos garante a privacidade e proteção dos seus dados pessoais.

3.3 LIMITAÇÕES DA PESQUISA

É importante aludir que as informações contidas no presente estudo foram em sua maioria obtidas em sites. Tendo em vista que o tema é bem atual, não foi possível coletar muitas informações através de artigos, monografias ou teses, no entanto o conteúdo informativo apresentado em tais sites são de grande relevância.

A limitação encontrada na pesquisa foi com relação a ausência de estudos mais aprofundados sobre o tema. Embora tenha diversos artigos e sites com conteúdo bem relevante e explicativos sobre a Lei Geral de Proteção de Dados, não existe muitas pesquisas sobre a aplicação dessa lei nas empresas de contabilidade. Apesar da lei ter sido publicada em 2018, o que se conhece a respeito dos seus impactos nas empresas ainda é um assunto bem atual, uma vez que a lei estava prevista para entrar em vigor em agosto de 2020, porém está sendo adiada ainda mais, devido a pandemia causada pelo COVID-19.

Uma outra limitação encontrada perante o momento de isolamento social, foi a dificuldade para que as pessoas respondessem a pesquisa, pois foi divulgada apenas de forma online, e geralmente quando o questionário é aplicado presencialmente, a chance de obter respostas é bem maior.

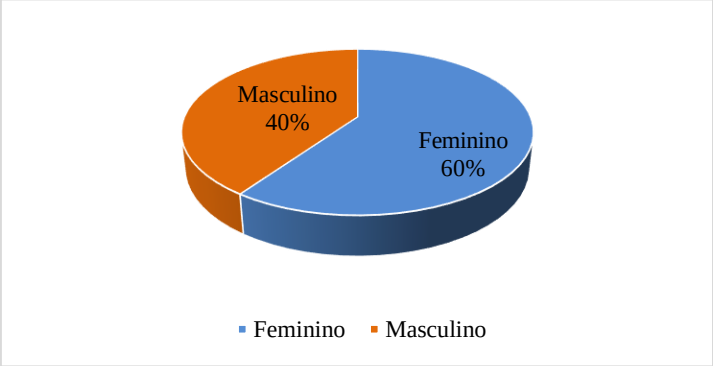
4 ANÁLISE DOS RESULTADOS

4.1 DESCRIÇÃO DAS VARIÁVEIS

A pesquisa foi realizada através de um questionário, composto por 20 perguntas, dentre elas questões de múltipla escolha, com escala linear de 1 a 5, sendo 1 menos importante e 5 mais importante, e questões que poderia selecionar mais de uma opção. As duas primeiras perguntas eram relativas ao perfil demográfico dos entrevistados, e as demais perguntas foram relacionadas a aplicação da Lei Geral de Proteção de Dados nos escritórios contábeis.

A população total do presente estudo é de 82 indivíduos, dos quais 49 são do gênero feminino (60%) e 33 são do gênero masculino (40%).

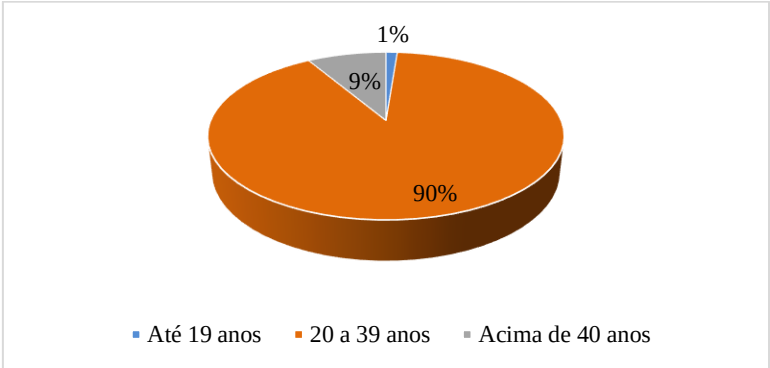
Gráfico 1 – Gênero



Fonte: elaborado pelo autor.

Em relação a idade dos entrevistados, cerca de 74 indivíduos estão na faixa etária dos 20 a 39 anos (90%), 7 indivíduos estão acima de 40 anos (9%), e apenas 1 indivíduo está na faixa até os 19 anos (1%).

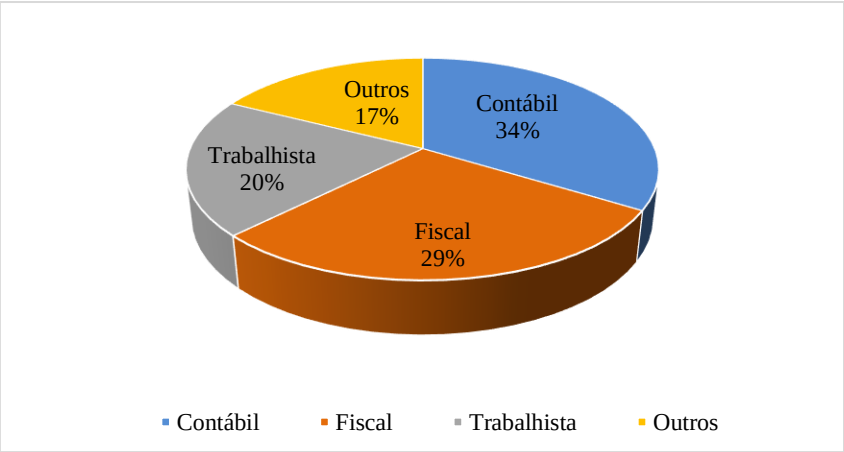
Gráfico 2 – Idade



Fonte: elaborado pelo autor.

Quanto ao setor em que os entrevistados trabalham, 27 indivíduos trabalham no setor contábil (34%), 23 trabalham no setor fiscal (29%), 16 no setor trabalhista (20%) e 14 nos demais setores (17%), dentre eles, no simples nacional, TI, auditoria, administrativo e na direção.

Gráfico 3 – Setor de trabalho no escritório

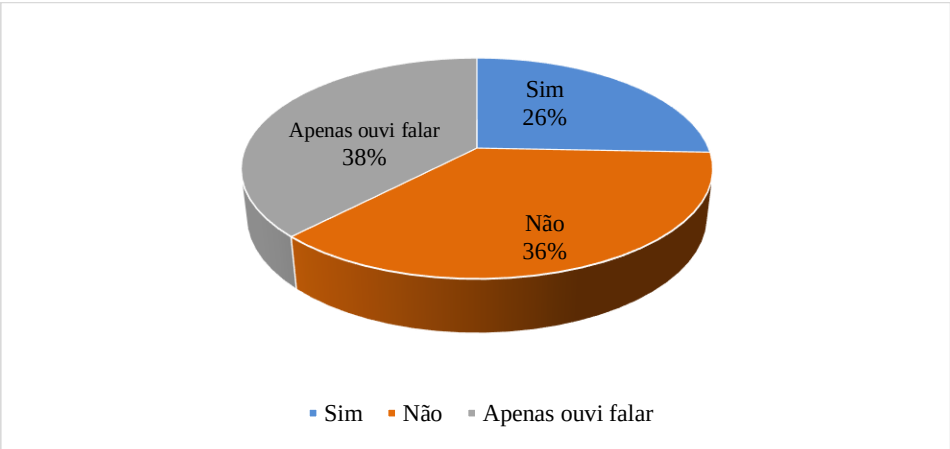


Fonte: elaborado pelo autor.

4.2 ANÁLISE DOS DADOS

Conforme evidenciado no gráfico abaixo, somente 21 dos entrevistados (26%) conhecem a Lei Geral de Proteção de Dados Pessoais, 31 indivíduos (38%) apenas ouviram falar sobre a lei por terceiros, e 30 indivíduos (36%) não conhecem a LGPD.

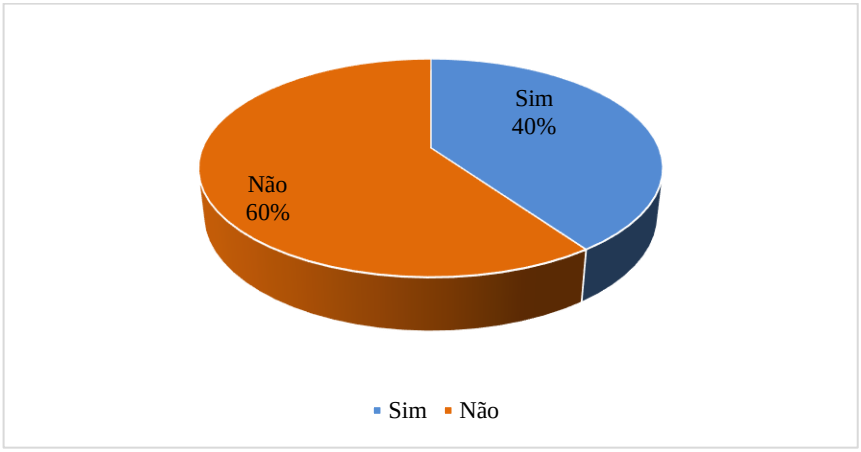
Gráfico 4 – Nível de conhecimento sobre a LGPD



Fonte: elaborado pelo autor.

Tendo em vista que o objetivo do estudo é analisar a aplicabilidade da LGPD nos escritórios contábeis, uma questão importante aplicada foi sobre a preocupação das empresas em disseminar a importância da Lei Geral de Proteção de Dados Pessoais aos seus colaboradores, pois é interessante que todos tenham o conhecimento e estejam empenhados para implantá-la. Todavia, apenas 33 dos indivíduos (40%) responderam que o escritório em que trabalham disseminam a importância da lei, e 49 indivíduos (60%) responderam que ainda não divulgam sua relevância.

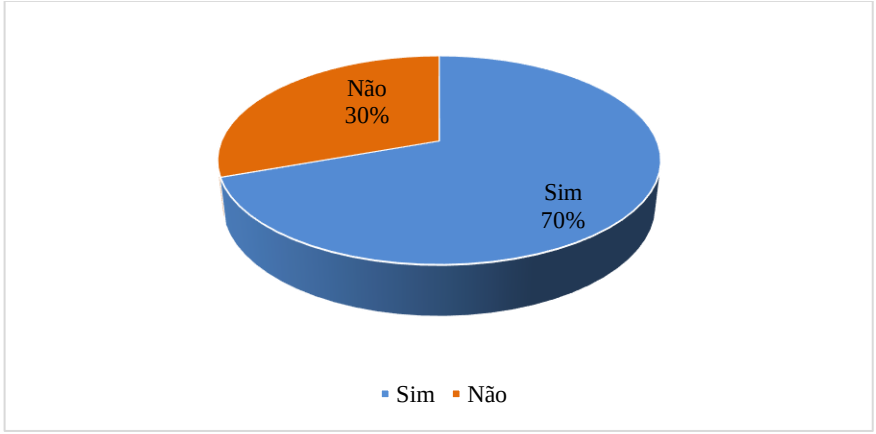
Gráfico 5 – Disseminação da LGPD nos escritórios contábeis



Fonte: elaborado pelo autor.

A maioria dos setores da área contábil trabalham com o tratamento de dados pessoais, 57 dos indivíduos (70%) responderam que o setor em que trabalham realizam o tratamento de dados pessoais, enquanto 25 deles (30%) responderam que não tratam dados pessoais.

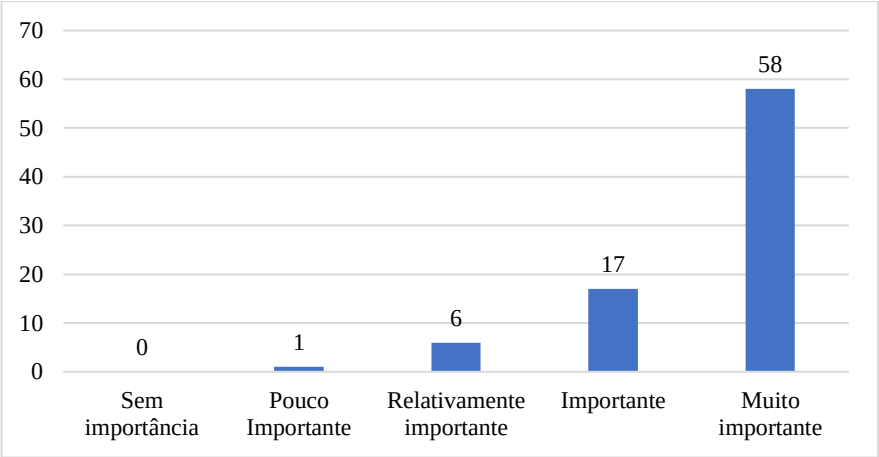
Gráfico 6 – Tratamento de dados pessoais no setor de trabalho



Fonte: elaborado pelo autor.

Com relação ao nível de importância atribuído a Lei Geral de Proteção de Dados Pessoais, nenhum dos indivíduos considera que a lei não seja importante, apenas 1 indivíduo (1,2%) considera pouco importante, 6 indivíduos (7,3%) consideram relativamente importante, 17 respondentes (20,7%) consideram importante e 58 dos indivíduos (70,7%) a consideram de vital importância.

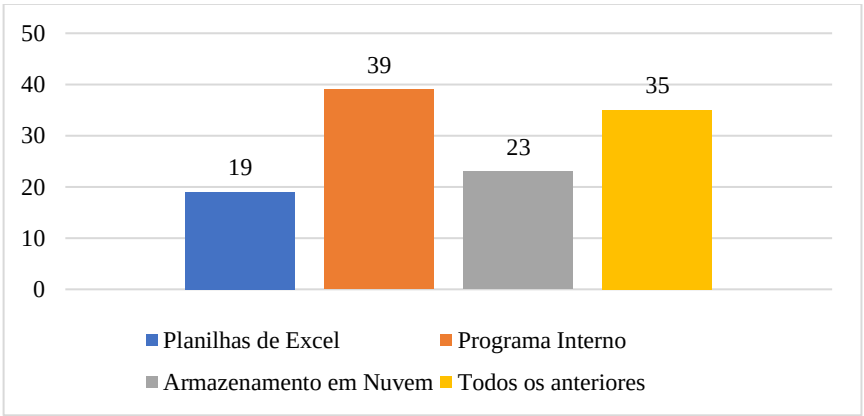
Gráfico 7 – Importância da LGPD



Fonte: elaborado pelo autor.

A respeito do armazenamento de dados nos escritórios, 19 indivíduos (23,2%) responderam que os dados são armazenados em planilhas de Excel, 23 indivíduos (28%) disseram que são armazenados na nuvem, 39 indivíduos (47,6%) responderam que os dados são armazenados em programa interno, enquanto que 35 deles (42,7%) responderam que os dados são armazenados tanto em planilhas, e na nuvem, quanto em programa interno.

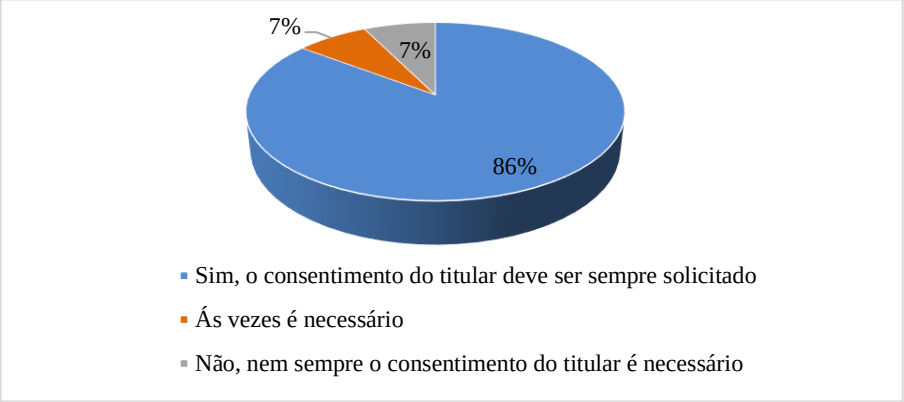
Gráfico 8 – Armazenamento dos dados



Fonte: elaborado pelo autor.

Um dos requisitos fundamentais para que haja o tratamento de dados pessoais é o consentimento do titular, salvo algumas exceções, sem essa expressão da vontade do titular, não deve existir o tratamento dos seus dados. Dessa forma, 70 dos entrevistados (86%) consideram que o consentimento do titular de dados deve ser sempre solicitado, 6 indivíduos (7%) acreditam que as vezes é necessário, e 6 deles (7%) não consideram necessário que o consentimento do titular seja sempre solicitado.

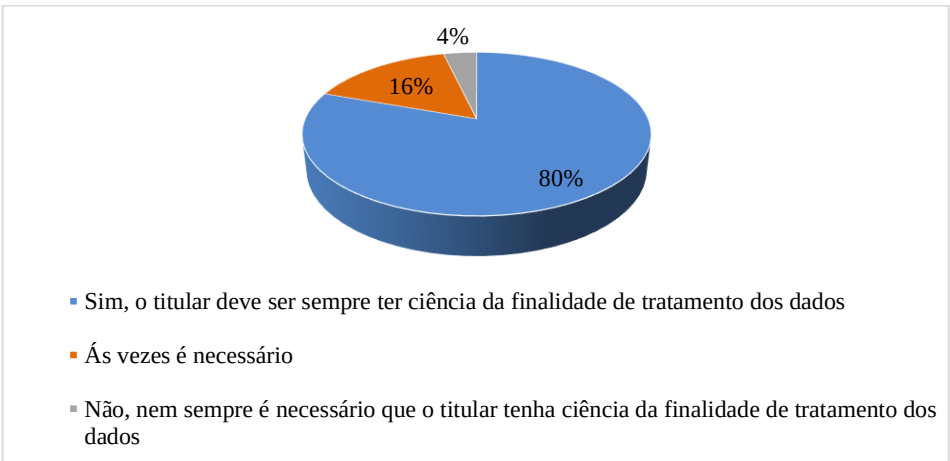
Gráfico 9 – Consentimento do titular dos dados



Fonte: elaborado pelo autor.

De acordo com a LGPD, o titular dos dados deve ser informado sobre a finalidade de tratamento dos dados que foi solicitado. Com isso, 66 dos entrevistados (80%) consideram que o titular de dados deve ser informado sobre a finalidade do dado, 13 indivíduos (16%) acreditam que as vezes é necessário, e 3 deles (4%) não consideram necessário que o titular seja informado sobre a finalidade de tratamento dos dados.

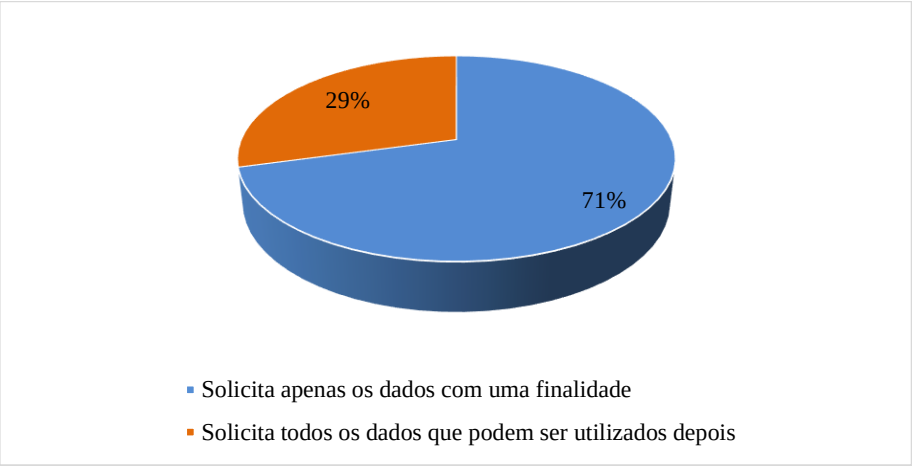
Gráfico 10 – Finalidade do tratamento dos dados



Fonte: elaborado pelo autor.

Conforme a Lei Geral de Proteção de Dados, todos os dados devem ser solicitados com uma finalidade específica, e as empresas não devem solicitar dados mais que o necessário. Com relação a isso, 58 dos indivíduos (71%) afirmam solicitar apenas dados com uma determinada finalidade, enquanto 24 indivíduos (29%) solicitam dados sem finalidade, por acharem que podem ser armazenados para utilizar quando necessitar deles.

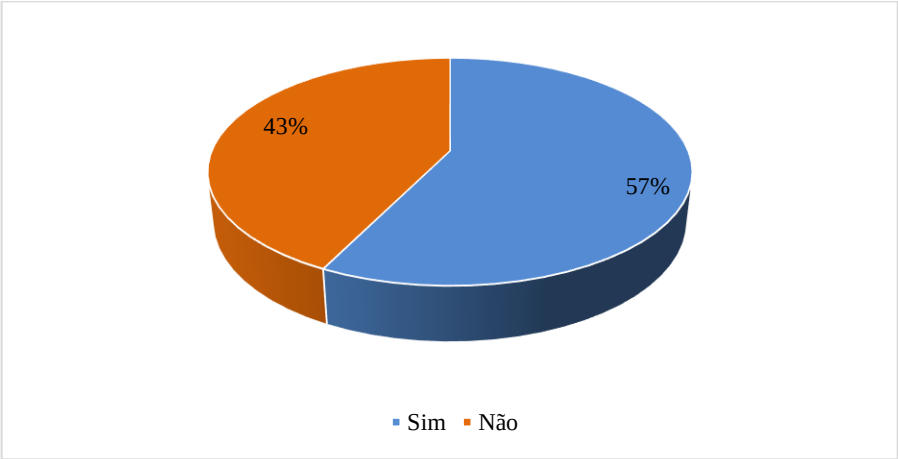
Gráfico 11 – Necessidade dos dados



Fonte: elaborado pelo autor.

De acordo com inciso II do art. 18 da LGPD, o titular dos dados pessoais tem direito de obter do controlador, a qualquer momento e mediante requisição o acesso aos seus dados. Dentre os profissionais contábeis que responderam ao questionário, 47 deles (57%) afirmaram que seus clientes tem livre acesso aos dados pessoais que eles possuem, porém, 35 indivíduos (43%) responderam que os clientes não tem acesso aos seus dados.

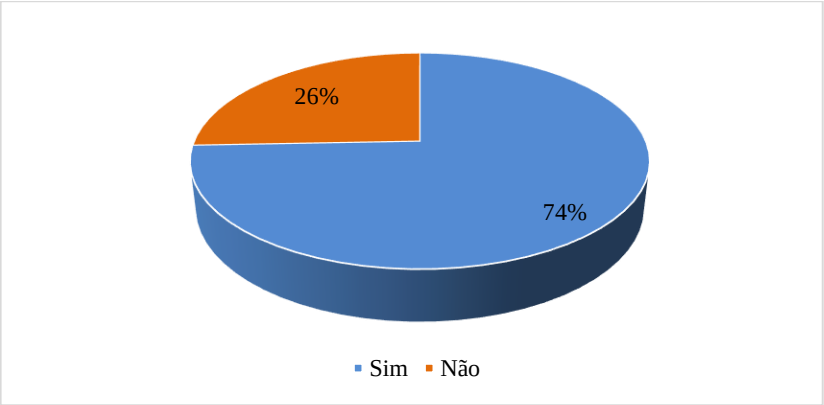
Gráfico 12 – Livre acesso aos dados



Fonte: elaborado pelo autor.

Ainda referente ao artigo 18 da lei, em seu inciso IV, o titular tem direito a eliminação aos dados que consideram desnecessários, excessivos ou tratados em desconformidade. Com isso, foi questionado se os dados pessoais são excluídos sempre que solicitados por eles, 61 dos profissionais (74%) responderam que os dados são excluídos mediante solicitação, enquanto que 21 indivíduos (26%) afirmaram que os dados não são excluídos quando solicitados.

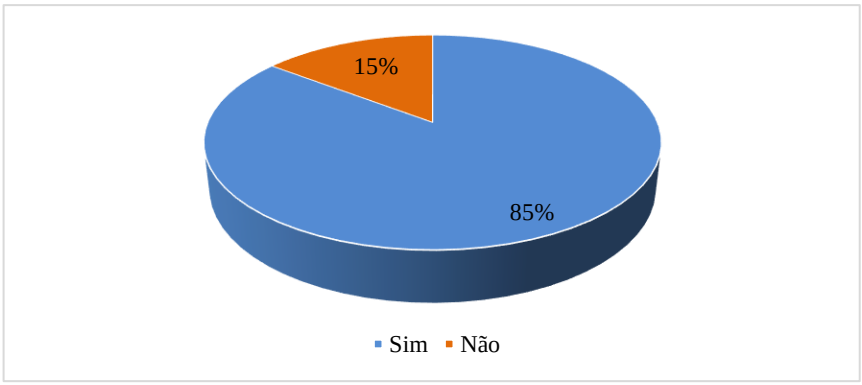
Gráfico 13 – Eliminação dos dados



Fonte: elaborado pelo autor.

Todas as empresas que trabalham com o tratamento ou armazenamento de dados pessoais deve contar com uma equipe capacitada e comprometida com a segurança dos dados. 70 dos profissionais contábeis (85%) contam com uma equipe de TI capacitada para garantir a segurança dos dados, no entanto 12 dos profissionais (15%) afirmaram não contar com uma equipe de TI, seja pelas condições financeiras para investir em segurança ou por não considerar tão importante.

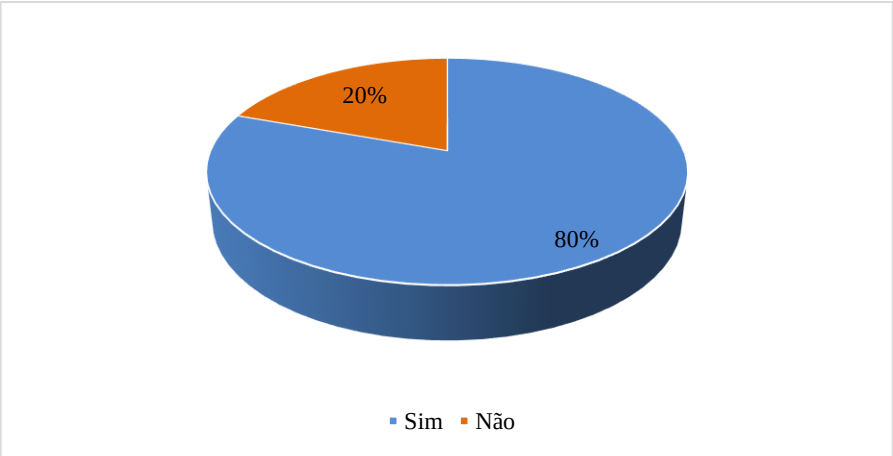
Gráfico 14 – Segurança dos dados



Fonte: elaborado pelo autor.

Com relação a segurança dos dados, 66 dos indivíduos (80%) afirmaram ter políticas de segurança e sistema eficiente que garantam a proteção dos dados pessoais nos escritórios em que trabalham, enquanto que 16 profissionais (20%) responderam não ter sistemas eficientes onde trabalham.

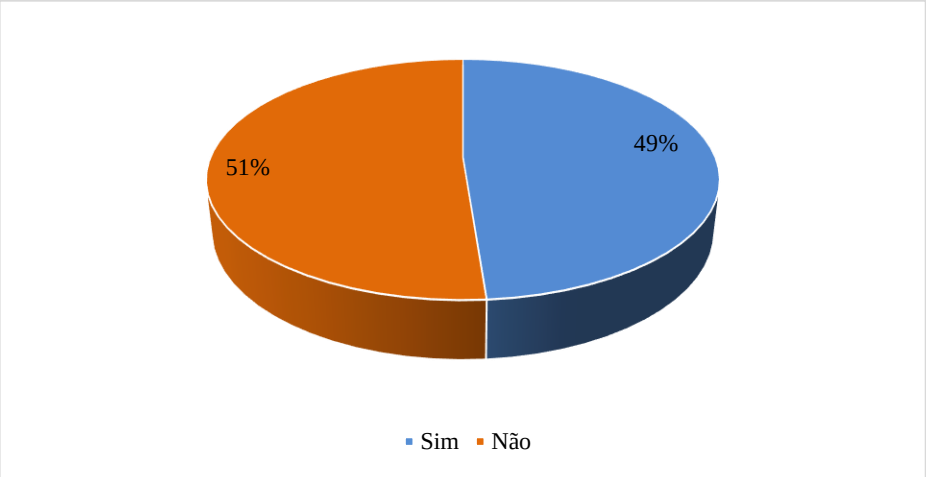
Gráfico 15 – Proteção dos dados



Fonte: elaborado pelo autor.

Negligenciar a segurança pode sair mais caro que investir em sistema de proteção. 40 profissionais (49%) responderam que o sistema utilizado no escritório já foi invadido por um hacker, e 42 (51%) disseram nunca ter havido invasão nos sistemas.

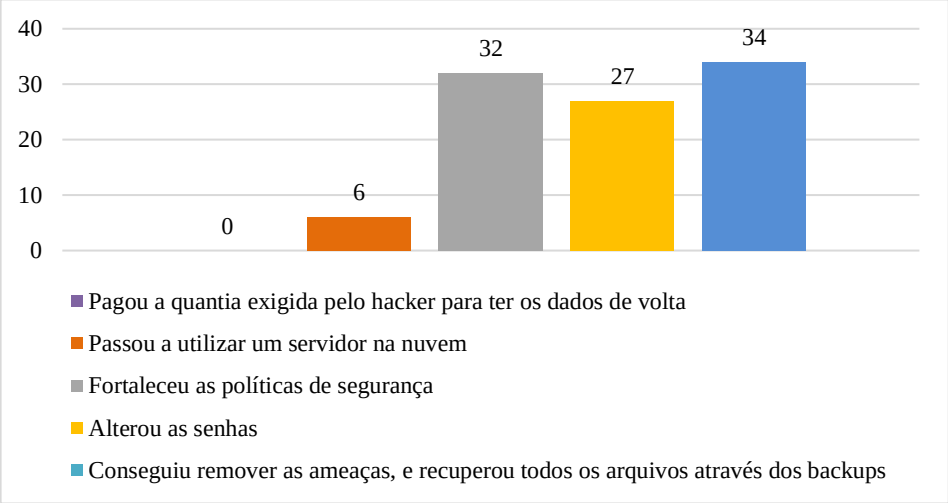
Gráfico 16 – Invasão aos sistemas



Fonte: elaborado pelo autor.

Dentre as empresas que tiveram seus sistemas invadidos por hacker, nenhuma pagou a quantia exigida pelo hacker para obter os dados de volta, e como medida de prevenção para futuros ataques, 6 dos indivíduos (14,3%) passaram a utilizar um servidor em nuvem, 32 (76,2%) fortaleceu as medidas de segurança, 27 (64,3%) passou a alterar as senhas frequentemente, e 34 dos profissionais (81%) conseguiu remover as ameaças e recuperar todos os arquivos através dos backups

Gráfico 17 – Procedimentos após sistemas terem sidos hackeados



Fonte: elaborado pelo autor.

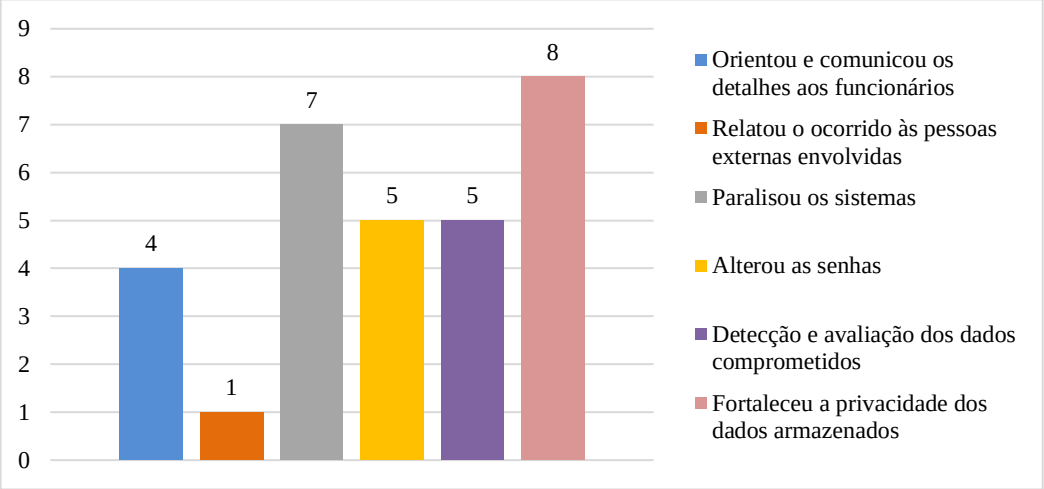
Seja por problemas nos sistemas, fraudes no armazenamento das informações ou ataques de hackers, o vazamento de dados é um problema cada vez mais frequente em empresas de diversos ramos. Apenas 5 dos profissionais (6%) afirmaram já ter existido vazamento de dados no escritório em que trabalham, enquanto que 77 indivíduos (94%) responderam não ter ocorrido vazamento de dados.

Gráfico 18 – Vazamento de dados

Fonte: elaborado pelo autor.

Com relação as empresas em que houveram o vazamento de dados, 4 profissionais (40%) afirmaram ter existido a orientação e comunicação sobre os detalhes aos funcionários, apenas 1 (10%) relatou o ocorrido às pessoas externas envolvidas, 7 (70%) paralisou os sistemas, 5(50%) alterou as senhas para aumentar a segurança, 5 (50%) conseguiu proceder com a detecção e avaliação dos dados comprometidos, 8 (80%) fortaleceu a privacidade dos dados armazenados.

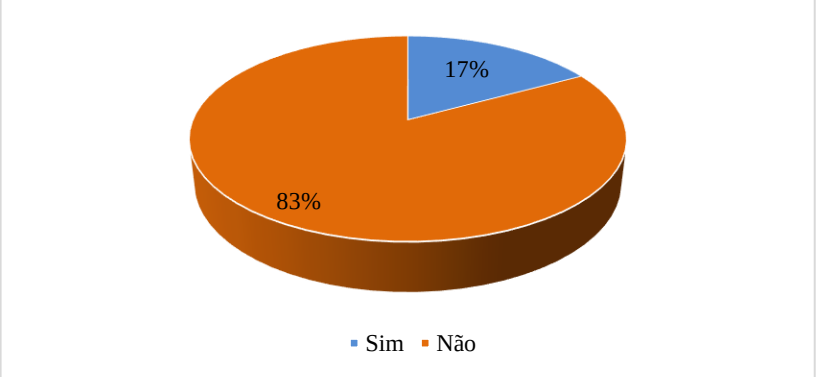
Gráfico 19 – Procedimentos após incidentes e vazamentos de dados



Fonte: elaborado pelo autor.

De acordo com art. 52 da Lei Geral de Proteção de Dados Pessoais, haverá sanções administrativas aplicáveis aos agentes de tratamento de dados que cometerem infrações às normas, dentre elas multa de 2% do faturamento, limitado a 50 milhões por infração cometida. Apenas 14 dos profissionais (17%) responderam ter conhecimento sobre a multa, enquanto 68 profissionais (83%) não tem ciência sobre a multa de 50 milhões.

Gráfico 20 – Multa por infrações a LGPD



Fonte: elaborado pelo autor.

5 CONSIDERAÇÕES FINAIS

Mediante os dados analisados da pesquisa, identificou-se que muitos dos profissionais contábeis não conhecem a Lei Geral de Proteção de Dados ou apenas ouviu falar, e menos de 50% dos escritórios difundem a importância da lei para os seus colaboradores, entretanto a maioria desses profissionais consideram a LGPD de vital importância.

Visto que o objetivo geral do trabalho é analisar a aplicabilidade da Lei Geral de Proteção de Dados nos escritórios contábeis, observou-se que as respostas diretamente relacionadas a lei foram favoráveis. Com relação ao armazenamento dos dados, os escritórios se preocupam em armazená-los de forma segura, como em programas internos e na nuvem, e não somente em planilhas de Excel. No tocante ao consentimento do titular, a maioria dos profissionais o consideram importante e solicitam sempre que necessário, bem como o informa a respeito da finalidade de tratamento dos dados e não solicitam dados mais que o necessário para tal finalidade.

Além de consentir a utilização dos seus dados, o titular deve ter total acesso aos dados em posse do controlador e sempre que desejar, pode solicitar a eliminação dos mesmos, conforme observado nos escritórios do presente estudo. A respeito da segurança dos dados, os escritórios contam com equipes de TI capacitadas, sistemas e políticas de segurança eficientes para cumprir as exigências da lei.

Embora as empresas de contabilidade invistam em segurança, quase 50% afirmaram ter o sistema invadido por hacker, sendo que a maioria conseguiu remover as ameaças e todos os arquivos foram recuperados, além de fortalecer as medidas de segurança e alterar as senhas frequentemente. Com relação ao vazamento de dados, apenas 6% afirmou ter ocorrido, e nesses escritórios em que ocorreu, foram tomadas as medidas necessárias para contornar a situação. No entanto, a maioria dos colaboradores não tem o conhecimento de que incidentes como esses poderão ser multados a partir do momento em que a lei entrar em vigor.

Na obtenção dos objetivos específicos, demonstrou-se as principais características da LGPD de acordo com a sua base legal, os impactos da Lei Geral de Proteção de Dados nos escritórios contábeis e a sua importância, na visão de estudiosos. A Lei Geral de Proteção de Dados sugere maior comprometimento com a segurança dos dados e transparência com relação ao tratamento dos dados, propiciando aos cidadãos maior proteção aos seus direitos fundamentais de liberdade e livre desenvolvimento de sua personalidade.

Como limitação da pesquisa identificou-se a ausência de estudos mais aprofundados sobre o tema e o fato do enfrentamento a pandemia e isolamento social, tornando inviável a

aplicação do questionário de forma presencial nos diversos escritórios, e sua divulgação foi realizada apenas de forma online, tendo como consequência o número da amostra reduzido.

No que concerne a estudos futuros, a pesquisa poderia ser realizada também com os membros da gestão e o pessoal de Tecnologia da Informação (TI), uma vez que estes detêm mais conhecimento sobre as questões de segurança de dados e possivelmente entendam melhor como está sendo a aplicação da Lei Geral de Proteção de Dados na empresa.

Com a análise dos resultados obtidos, conclui-se que as empresas de contabilidade estão adequadas para aplicação da Lei Gera de Proteção de Dados Pessoais, visto que consideram o consentimento do titular imprescindível para o tratamento dos dados, adotam as medidas de segurança necessárias para a proteção dos dados e atendem aos princípios da LGPD, tais como finalidade, adequação, necessidade, livre acesso, qualidade dos dados , transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

É importante ressaltar que outras medidas devem ser tomadas para melhor se adequar a lei, como criar um projeto de proteção de dados e definir uma pessoa para liderar e mapear todas as questões de segurança, e por fim implementar 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 do escritório.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 jan. 2020

BRASIL. [Constituição (2018)]. **Lei nº 13.709, de 14 de Agosto de 2018**. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 16 jan. 2020

BRASIL. [Constituição (2002)]. **Lei nº 10.406, de 10 de Janeiro de 2002**. Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm Acesso em: 29 jan. 2020

LEAL, Rhand. **O que é a ISO 27001**. Disponível em: https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/. Acesso em: 17 mar. 2020.

GERHARDT, Tatiana; SILVEIRA, Denise. **Métodos de pesquisa**. Rio Grande do Sul: UFRGS Editora, p. 13, 2009.

FERREIRA, Adriano. **O impacto da LGPD nos escritórios de contabilidade**. 2019. Disponível em: https://www.dominiosistemas.com.br/blog/o-impacto-da-lgpd-nos-escritorios-de-contabilidade/. Acesso em: 26 jan. 2020.

NETWORKS, Telium. **Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação**. 2018. Disponível em: https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao. Acesso em: 29 mar. 2020.

XERPA. **O que é governança de dados e qual é sua importância para a empresa**. 2018. Disponível em: https://www.xerpa.com.br/blog/governanca-de-dados/. Acesso em: 28 mar. 2020.

GOVERNANCAS (ed.). **Governança da Privacidade agora é Lei e multará por inércia**. 2018. Disponível em: https://www.governancas.com.br/2019/03/22/lgpd/. Acesso em: 25 mar. 2020.

FREITAS, Carla. **Como elaborar uma política de privacidade aderente à LGPD?** 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais. Acesso em: 05 abr. 2020.

GUTTERMAN, Alan. **Como criar um programa de Compliance sobre privacidade e segurança de dados**. 2018. Disponível em: https://www.thomsonreuters.com.br/pt/juridico/blog/como-criar-um-programa-compliance-sobre-privacidade-seguranca-dados.html. Acesso em: 01 abr. 2020.

YUN, Remilina et al. **Guia prático de programa de adequação a proteção de dados pessoais.** Brasil: [s. n.], p. 83 - 90, 2018.

EUROPEIA, Comissão. **O que são dados pessoais?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt. Acesso em: 05 mar. 2020.

TOSTES, Marcelo. **Segurança de dados na Internet: como proteger a sua empresa?** 2019. Equipe Marcelo Tostes. Disponível em: https://transformacaodigital.com/juridico/seguranca-de-dados-na-internet-como-proteger-a-sua-empresa/. Acesso em: 03 mar. 2020.

RIBEIRO, L. **Proteção de dados pessoais: Estudo comparado do regulamento 2016/679 do parlamento europeu e conselho e o projeto de lei brasileiro n. 5.276/2016.** Brasília, p. 5 – 24, 2016.

ALVES, Fabrício. **Proteção de dados pessoais é a evolução da privacidade**. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/protecao-dados-evolucao-privacidade. Acesso em: 04 fev. 2020.

KLUWER, Wolters. **Você sabe o impacto da LGPD nos escritórios de contabilidade?** Jornal do Comércio. Disponível em: https://www.wolterskluwer.com.br/blog/voce-sabe-o-impacto-da-lgpd-nos-escritorios-de-contabilidade/. Acesso em: 26 jan. 2020.

DONEDA, Danilo. **Privacidade e Proteção de Dados Pessoais.** Brasília, 2017.

RICARDO, Sérgio. **A regulação jurídica da proteção de dados pessoais no Brasil.** Monografia de pós graduação – Curso de Direito da propriedade intelectual da PUC- Rio, Pontifícia Universidade Católica do Rio de janeiro. Rio de Janeiro, 2018.

FERREIRA, Adriano. **Ética na contabilidade e LGPD juntas a favor da segurança**. 2019. Thomson Reuters. Disponível em: https://www.dominiosistemas.com.br/blog/etica-na-contabilidade-e-lgpd-juntas-a-favor-da-seguranca/. Acesso em: 16 mar. 2020.

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

GIL, A.C. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2007.

RICHARDSON, Roberto Jarry et al. **Pesquisa Social: métodos e técnicas**. 3. ed. São Paulo: Atlas, 1999.

LAKATOS, E. M. de A.; MARCONI, M. de A. **Fundamentos da metodologia científica**. São Paulo: Atlas, 2003.

APÊNDICE A – QUESTIONÁRIO

1. **Idade: _____**
2. **Gênero:**
   ( ) Masculino
   ( ) Feminino
   ( ) Outro_____

3. **Em qual setor do escritório de contabilidade você trabalha?** _____

4. **Você conhece a Lei Geral de Proteção de Dados (LGPD)?**
   ( ) Sim
   ( ) Não
   ( ) Apenas ouvi falar

5. **O escritório Contábil em que você trabalha dissemina a importância dessa Lei?**
   ( ) Sim
   ( ) Não

6. **O setor do qual você faz parte trabalha com o tratamento de dados pessoais?**
   ( ) Sim
   ( ) Não

7. **Pra você, qual o nível de importância dessa lei, atribua de 1 a 5 (sendo 1 menos importante e 5 mais importante):**
   ( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5

8. **Como os dados são armazenados?**
   ( ) Em planilhas de Excel
   ( ) Programa interno
   ( ) Armazenamento em Nuvem
   ( ) Todos os anteriores

9. **Você entende que o consentimento do titular do dado é necessário para que haja qualquer tratamento de dados?**

   ( ) Sim, o consentimento do titular deve ser sempre solicitado

   ( ) Às vezes é necessário

   ( ) Não, nem sempre o consentimento do titular é necessário

10. **Na sua opinião, o titular dos dados deve ser informado sobre a finalidade do tratamento do dado ou é desnecessário?**

    ( ) Sim, o consentimento do titular deve ser sempre solicitado

    ( ) Às vezes é necessário

    ( ) Não, nem sempre o consentimento do titular é necessário

11. **Você solicita ao cliente somente os dados que são necessários para uma finalidade específica? Ou solicitam todos os dados que acham que podem utilizar em algum momento?**

    ( ) Solicito apenas os dados com uma finalidade

    ( ) Solicito todos os dados que podem utilizados depois

12. **Os seus clientes tem livre acesso a todos os dados que vocês possuem deles?**

    ( ) Sim

    ( ) Não

13. **Os dados dos seus clientes são excluídos quando solicitados por eles?**

    ( ) Sim

    ( ) Não

14. **No escritório em que você trabalha existe uma equipe de TI capacitada para contribuir com a segurança dos dados?**

    ( ) Sim

    ( ) Não

15. **Existem sistemas eficientes que garantam a proteção dos dados e políticas de segurança conforme a legislação?**

    ( ) Sim

( ) Não

16. Algum hacker já invadiu o sistema do escritório?

( ) Sim

( ) Não

17. Se você marcou SIM para pergunta anterior, responda como o escritório em que você trabalha procedeu após ter seu sistema invadido por um hacker e seus dados expostos, pode marcar mais de uma alternativa:

( ) Pagou a quantia exigida pelo hacker para ter os dados de volta

( ) Passou a utilizar um servidor na nuvem

( ) Fortaleceu as políticas de segurança

( ) Alterou as senhas

( ) Conseguiu remover as ameaças, e recuperou todos os arquivos através dos backups

18. Já existiu algum vazamento de dados?

( ) Sim

( ) Não

19. Se você marcou SIM para pergunta anterior, responda como o escritório em que você trabalha procedeu após ter ocorrido vazamento de dados, pode marcar mais de uma alternativa:

( ) Orientou e comunicou os detalhes aos funcionários

( ) Relatou o ocorrido às pessoas externas envolvidas

( ) Paralisou os sistemas

( ) Alterou as senhas

( ) Detecção e avaliação dos dados comprometidos

( ) Fortaleceu a privacidade dos dados armazenados

( ) Não tomou nenhuma medida e não comunicou aos envolvidos

20. Você tem conhecimento sobre a multa de 2% do faturamento, limitado a 50 mil por infração que a empresa pode sofrer se estiver em desacordo com a LGPD?

( ) Sim

( ) Não