TRATAMENTO DE DADOS EM SISTEMAS DE INFORMAÇÕES CONTÁBEIS A PARTIR DA LEI 13.709/2018 (LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS): UM ESTUDO MULTICASO

João Luiz Scherer Filho
Prof. Ma. Sinara Jaroseski
1º semestre/2020

Resumo

O presente estudo tem por objetivo identificar quais medidas devem ser tomadas por escritórios de contabilidade de Farroupilha – RS para adequação à Lei Geral de Proteção de Dados (LGPD) no que se refere ao tratamento de dados. O dado pessoal é um ingrediente indissociável da privacidade do cidadão e também é o principal insumo de uma economia globalizada e tecnológica. Nesse contexto, o Brasil passou a integrar o grupo de países que dispõe de uma legislação própria, que entrará em vigor em maio de 2021, a depender da aprovação da Medida Provisória 959/2020, e poderá requerer diversas mudanças em sistemas de informação e implementação de medidas administrativas para atender aos fundamentos e princípios elencados na nova legislação. A ideia metodológica foi realizar um levantamento em livros, artigos, legislações, e outros atos normativos que tratam do assunto em estudo. Com base nas questões mais relevantes identificadas no levantamento inicial, foram elaboradas questões respondidas em entrevistas e, por meio destas, foram identificadas dificuldades e dúvidas para total adequação à LGPD, bem como os setores mais afetados nas organizações avaliadas.

Palavras-chave: privacidade, proteção, dados, tratamento.

1 Introdução

A nova legislação brasileira tem como modelo o regulamento europeu para proteção de dados pessoais, a *General Data Protection Regulation* (GDPR), que passou a vigorar na Europa em 2018, ano em que também ocorreu uma emenda à Convenção 108 do Conselho da Europa, incluindo-se a proteção de direitos fundamentais dos indivíduos no processamento automático de dados pessoais, considerando, entre outras questões, a necessidade de garantir a dignidade e a proteção do ser humano, dada a diversificação, intensificação e globalização do processamento e fluxo de dados pessoais. (BORELLI *et al*., 2019). Nesse mesmo contexto, no ano de 2017, o Fórum de Governança da *Internet* das Nações Unidas, por meio da Carta de Direitos Humanos e Princípios da *Internet*, lançou os Dez Princípios Poderosos da *Internet*, consignando, entre outros, a privacidade e a proteção de dados pessoais (*ibidem*).

Dentre as novidades trazidas pela nova legislação está o princípio da segurança, que determina a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais. Contudo, a implementação de sistemas seguros envolve desafios, que não são apenas questão de implementação do sistema, mas também o fator humano. (STALLINGS, 2015). Essa importância da proteção eletrônica e a sua dificuldade é reconhecida também pela ABNT (NBR 27002:2005, p. 9):

> A informação é um ativo que, como qualquer outro ativo é importante para os negócios de uma organização e consequentemente precisa ser adequadamente

> protegida […] Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados.

Foi realizada uma pesquisa exploratória onde, por meio de levantamentos dos assuntos relacionados ao tema a ser pesquisado, buscou-se evidenciar os diversos aspectos que devem ser considerados para adequação à LGPD.

A escolha do tema adequação à LGPD no que se refere ao tratamento de dados se dá por ser uma legislação nova no Brasil, que traz, dentre outras novidades, responsabilizações dos agentes pelo tratamento de dados, portanto afeta também os profissionais da área contábil. Outro motivo que importa para a escolha do tema é que segurança de dados não é uma matéria abordada com tanto rigor nos cursos de graduação em ciências contábeis. Como resultado, alguns artefatos que envolvem segurança de dados, tais como *tokens*, chaves digitais, autenticação de dados e criptografia, podem até não ser incomuns para os profissionais da área contábil, porém, esses profissionais podem não entender ao certo se esses artefatos deixam as informações mais seguras, e, portanto, se as salvaguardas e mecanismos de mitigação de risco estão adequados.

2 Referencial Teórico

2.1 Dados pessoais na era das sociedades informacionais

Informações são um dos principais insumos de uma economia globalizada e tecnológica. Segundo Silveira (2017, sem numeração):

> As sociedades informacionais são sociedades pós-industriais que têm a economia fortemente alicerçada em tecnologias que tratam informações como seu principal produto. Portanto, os grandes valores gerados nessa economia não se originam principalmente na indústria de bens materiais, mas na produção de bens imateriais, aqueles que podem ser transferidos por redes digitais.

O poder público também participa desse processo de produção de informações no formato digital. Segundo Pinheiro (2016) no âmbito de Direito Administrativo, os princípios de publicidade dos atos públicos e probidade administrativa fazem com que a *Internet* seja um meio adequado para publicar o que está sendo feito e como um canal direto de comunicação com cidadãos e contribuintes. Existe ainda a tendência de cada vez mais o fisco ser digital (*ibidem*). Um exemplo da prevalência dos meios digitais é o Sistema Público de Escrituração Digital (SPED), que é instrumento que unifica as atividades de recepção, validação, armazenamento e autenticação de livros e documentos que integram a escrituração contábil e fiscal dos empresários e das pessoas jurídicas, mediante fluxo único, computadorizado de informações. (BRASIL, 2007).

Todas essas mudanças proporcionadas pela tecnologia também transformam o cotidiano de muitos profissionais, inclusive do setor contábil, conforme Breda (2019, não paginado):

> Sem dúvida, são inúmeros os benefícios advindos do avanço da tecnologia. Aspectos como segurança, tempestividade e qualidade das informações estão em pauta a todo o momento. Com os dispositivos móveis e a tecnologia em nuvem, tem-se acesso imediato a um incontável número de informações, pessoas e serviços. […] sobre outros pontos que merecem destaque quanto aos riscos envolvidos no avanço tecnológico, destaca-se a ameaça da utilização de máquinas que possam substituir a mão de obra; o alto custo financeiro que demanda a produção de equipamentos/sistemas com IA (Inteligência Artificial); a vulnerabilidade dos sistemas; e situações que violam os códigos de ética.

De acordo com Borelli *et al.* (2019), com a revolução da informática, na década de 1970, houve um aumento no uso de processamento de dados e o surgimento de blocos

econômicos que compartilhavam dados, inclusive os pessoais, aumentando a necessidade de tutela dos direitos fundamentais, portanto, busca-se um equilíbrio da preservação do fluxo aberto de dados pessoais e a proteção das liberdades individuais. Segundo Pinheiro (2016) é um desafio do Direito Digital equilibrar interesse comercial, privacidade, responsabilidade e anonimato gerados pelos novos veículos de comunicação.

A revolução da informática também provocou ressignificações. Segundo Rodotà (2008) a visão tradicional para o termo 'privacidade' era tida muito mais como instrumento para ser deixado só. Contudo, esse termo hoje exalta muito mais a possibilidade de cada um controlar o uso de informações que lhe dizem respeito, sobretudo por conta da possibilidade do exercício de poder com base na disposição de informações (*ibidem*). Esse exercício de poder pode ser exemplificado no caso envolvendo uma empresa de consultoria estratégica em mídias sociais, que analisou dados de usuários de uma rede social para identificar suas personalidades e influenciar seus comportamentos, manipulando-os eleitoral e politicamente, conforme parecer do relator da LGPD. (SENADO FEDERAL, 2018).

O controle sobre o fluxo dos dados relativos ao titular, citado por Rodotà, é o que fundamenta a autodeterminação informativa, que subsiste durante todo o ciclo de vida dos dados e nos mais variados meios nos quais possam circular. (BORELLI *et al.*, 2019). Paesani (2013, p. 24 e 25) ressalta a importância do consentimento do titular dos dados na regulamentação europeia, a *General Data Protection Regulation* (GDPR):

> No âmbito da União Europeia, nasceu um modelo diverso de tratamento dos dados pessoais. Esse modelo parte da transposição dos ordenamentos nacionais e reconhece a autodeterminação informativa que atribui a cada pessoa o poder de impedir determinados usos das próprias informações e o arbítrio de controlar o uso que outros façam dessas informações. O elemento-chave desse modelo é o consentimento do interessado.

Segundo Pinheiro (2018) o regulamento europeu provocou um "efeito dominó", visto que exigiu dos demais países e empresas que mantém relações comercias com a União Europeia uma legislação do mesmo nível. Nesse contexto é que surgiu a legislação brasileira, inspirada no regulamento europeu. (BORELLI *et al.*, 2019).

2.2 A Lei Geral de Proteção de Dados

A LGPD tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018). Segundo Pinheiro (2018) a regulamentação de proteção de dados pessoais é uma legislação principiológica, e a melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, o princípio não está atendido. Essa metodologia encontrada pelo regulador para tratar uma regra que necessita de uma aplicação procedimental dentro dos modelos de negócios das estruturas empresariais (*ibidem*).

O primeiro princípio elencado é o da finalidade. Borelli *et al*. (2019) defende que esse princípio vincula o tratamento de dados pessoais ao motivo que fundamentou a sua coleta, assim, a motivação permanece até o fim da coleta e deve ser levada em consideração em qualquer tratamento posterior.

No que se refere aos conceitos, destaca-se o consentimento. Segundo Pinheiro (2018), o consentimento é a linha mestra que deve ser aplicada aos tratamentos de dados e estar vinculado às finalidades apresentadas. Na LGPD, nas hipóteses em que o consentimento é requerido, se houver mudança da finalidade não compatível para o consentimento originador, o controlador deverá informar previamente ao titular sobre a mudança da finalidade, podendo o titular revogar esse consentimento. (BRASIL, 2018)[1]. A relação do consentimento e

1 LGPD: § 6º do Art. 8º.

finalidade também exige o acompanhamento do ciclo de vida dos dados pelo controlador, pois, dentre outros motivos, após o alcance da finalidade e encerramento do tratamento dos dados, os dados deverão ser eliminados, ressalvadas as hipóteses previstas no Art. 16 da LGPD (*ibidem*).

Outro conceito importante é o de dado pessoal. Bioni (2018) destaca que esse conceito é central, pois um dado que não seja pessoal não tem a tutela jurídica da LGPD, então, o vocabulário para prescrever tal definição é composto por palavras que restringem ou alargam essa proteção, daí cabe a interpretação reducionista ou expansionista. Sobre este aspecto Borelli *et al*. (2019) destaca que o Brasil adotou o conceito expansionista de dado pessoal, pelo qual não só a informação relativa à pessoa diretamente identificada é protegida, como também àquela que tem o potencial de identificá-la, e exemplifica esse rol com gostos, interesses, hábitos de consumo, profissão, sexo, idade e geolocalização. Já os dados anonimizados, definidos no inciso III do Art. 5º da LGPD, não são dados pessoais, pois, considerando a utilização de meios tecnológicos razoáveis, não é possível identificar o titular dos dados, portanto, resulta na inaplicabilidade da legislação. (BRASIL, 2018)[2]. Pinheiro (2018) destaca que o dado deve ser anonimizado com um método que possa demonstrar impossibilidade de reversão.

A segunda definição trazida pela LGPD é a de dado pessoal sensível. Para o tratamento desses dados, de acordo com o Art. 11 da LGPD, é necessária a obtenção do consentimento do titular dos dados, ou, sem consentimento quando for indispensável nas hipóteses previstas em lei. Uma dessas hipóteses é para o cumprimento de obrigação legal ou regulatória pelo controlador, porém, cabe observar que essa dispensa depende da publicação, pelos órgãos e pelas entidades públicas, de informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades. (BRASIL, 2018)[3].

Além do princípio da finalidade, a LGPD enumera outros princípios, que estão elencados no Quadro 1. Estes princípios devem ser observados mesmo quando houver dispensa do consentimento, conforme § 6º do Art. 7º da LGPD. (BRASIL, 2018).

Quadro 1 – Alguns princípios definidos pela LGPD.

Princípio	**Descrição**
Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
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.
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
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.
Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Fonte: Adaptado de Brasil (2018).

2 LGPD: Art. 12.
3 LGPD: § 2º do Art. 11 e Art. 23.

O Quadro 2 elenca alguns conceitos definidos pela LGPD.

Quadro 2 – Alguns conceitos definidos pela LGPD.

Conceito	**Descrição**
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
Dado anonimizado	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
Banco de dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
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).
Agentes de tratamento	O controlador e o operador.
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.
Anonimização	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
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.

Fonte: Adaptado de Brasil (2018).

A LGPD, em diversos dispositivos, relaciona o cumprimento de obrigações e responsabilidades ao papel exercido nas atividades de tratamento de dados. O Quadro 3 apresenta algumas dessas responsabilidades, bem como o responsável.

Quadro 3 – Relação de papéis e algumas responsabilidades relacionadas na LGPD.

Responsável (eis)	**Responsabilidade**	**Dispositivo (LGPD)**
Controlador	Provar que houve o consentimento do titular dos dados e informar o mesmo a respeito de alterações do consentimento para tratamento de dados, com destaque de forma específica do teor das alterações, quando se tratar de mudança de finalidade, prazo, controlador e do compartilhamento dos dados.	§ 2º e § 6º do Art. 8º
	Adotar medidas para garantir a transparência do tratamento de dados e dar acesso ao relatório de impacto à proteção de dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD), quando requerido.	§ 2º e § 3º do Art. 10
	Fornecer ao titular dos dados pessoais, mediante requisição: a confirmação da existência de tratamento de dados, bem como, acesso, correção e ainda a anonimização, bloqueio ou eliminação desses dados, observadas as disposições da LGPD;	Art. 18
	Elaborar relatório de impacto à proteção de dados pessoais.	Art. 38
	Elaborar instruções para o tratamento de dados feitos por operador, observando as próprias regras e as normas sobre a matéria.	Art. 39
	Nomear o encarregado, salvo nas hipóteses de dispensa, a critério da ANPD.	Art. 41
	Comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.	Art. 48
Controlador e Operador	Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.	Art. 6º, inciso X
	Manter registro das operações de tratamento de dados pessoais que realizarem.	Art. 37
	Reparar o titular dos dados quando, em razão do tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, observadas as demais disposições legais.	Art. 42
	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
	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.	Art. 50
Operador	Realizar o tratamento segundo as instruções fornecidas pelo controlador.	Art. 39
Encarregado	Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.	Art. 41
	Receber comunicações da autoridade nacional e adotar providências.	
	Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.	

Fonte: Adaptado de Brasil (2018).

A LGPD obriga tanto o operador como ao controlador a adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados

pessoais, bem como, a eficácia dessas medidas. Nesse sentido, Pinheiro (2018, p. 43) fornece um *check-list* de providências a serem tomadas para adequação à LGPD:

> Para iniciar a implementação dos requisitos de conformidade à LGPD, o primeiro passo é a realização de um levantamento. Ou seja, deve-se fazer uma análise de diagnóstico para identificar como a instituição está no tocante aos indicadores de conformidade e o que falta para atender aos controles exigidos. Para tanto, a primeira atividade é fazer o inventário dos dados pessoais (quais são e onde estão). Depois, deve-se montar a matriz de tratamento dos dados pessoais (quais os tipos de tratamento e para que finalidades). Em seguida, como está sendo feito o controle de gestão de consentimentos. Com esse panorama, é desenvolvido o mapa de risco e elaborado o plano de ação, que permite fazer a cotação dos investimentos necessários às conformidades implementadas, em geral, em quatro níveis: no nível técnico (ferramentas), documental (atualizar normas, políticas, contratos), procedimental (adequar a governança e a gestão dos dados pessoais) e cultural (realizar treinamentos e campanhas de conscientização das equipes, dos parceiros, fornecedores e clientes).

E continua citando documentos que precisam ser atualizados (*ibidem*, p. 46 e 47):

> Mapa de fluxo de dados pessoais (*Personal Data Flow Map*). Tabela de temporalidade de guarda de *log*s de consentimento. Política de gestão de dados pessoais (que deve ser assinada inclusive *inter companies* – entre empresas do mesmo grupo econômico, entre matriz e filiais). Política para tratamento de dados pessoais para terceirizados (*providers* que realizam tratamento de dados pessoais – vários procedimentos trazidos no GDPR e na LGPD sobre fluxo, padrão de criptografia, guarda de *log*s, etc.). Termo de uso e Política de privacidade (atualizar batendo tratamento *versus* finalidade de uso *versus* justificativa jurídica *versus* matriz de consentimentos, novos direitos dos usuários como portabilidade, exclusão, minimização de uso, limitação e outros). […] Código de Conduta (atualizar com cláusulas que preveem respeito à proteção de dados pessoais). Política de Segurança da Informação (atualizar com cláusulas que preveem GDPR e LGPD). [...]

Nesse aspecto, Borelli *et al*. (2019) destaca que a disciplina de segurança da informação é norteada pela ABNT NBR ISO/IEC 27002, considerada um código que reúne as melhores práticas e segurança de informações. Esta norma é citada pelo governo federal no documento de referência da estrutura básica para a estratégia de governo eletrônico (e-PING), em seus tópicos relacionados à segurança de sistemas de informação. (MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, 2017).

2.3 Medidas de proteção

A ABNT (NBR 27002:2005, p. 9) define o termo ‘segurança da informação’, bem como, estabelece a forma de obtê-la:

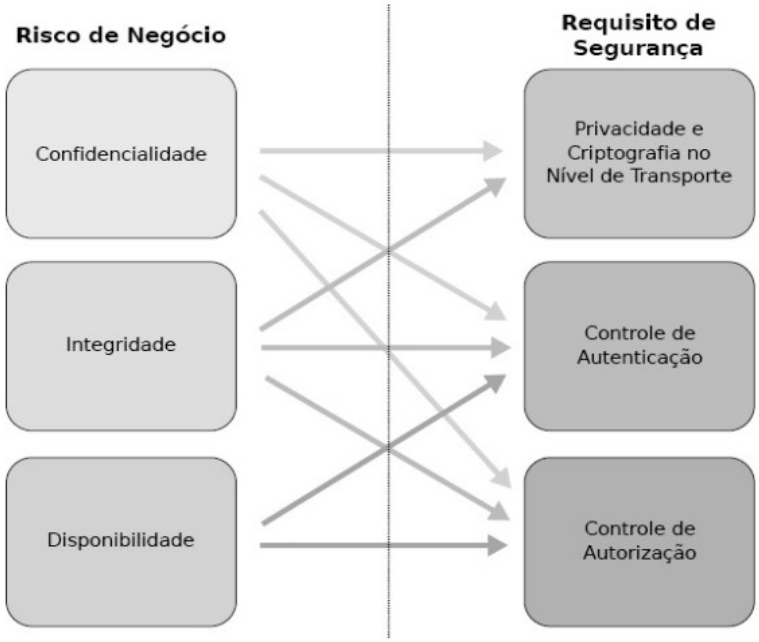
> Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

Contudo, a implementação de um conjunto de controles adequados para promover segurança de informação é critério da gerência de negócios e geralmente envolve custos. Para Sommervile (2011) é critério da gerência do negócio decidir se aceita ou não o custo de proteção ou exposição resultantes da falta de procedimentos de proteção, ou seja, é um

problema de negócio e não um problema técnico, e, nesse caso, não é função dos engenheiros de *software* decidir quais os controles devem ser inclusos no sistema. Cabe a estes fornecer orientação técnica e julgamento sobre questões de segurança (*ibidem*).

O gerenciamento de risco se preocupa com possíveis perdas em relação ao custo de procedimentos de proteção, de acordo com as atividades do negócio. Weidman (2014) ressalta que o gerenciamento de riscos é importante porque permite que uma empresa faça avaliações de sua postura atual e entenda melhor os riscos, definindo prioridades e implementando medidas para reduzir os riscos a um nível aceitável, de acordo com as atividades do negócio principal da empresa. O gerenciamento de proteção de sistemas inclui atividades como gerenciamento de usuários e permissões, monitoração, detecção e recuperação de ataques. (SOMMERVILE, 2011). A Figura 1 ilustra vulnerabilidades associadas aos requisitos de segurança.

Figura 1 – Vulnerabilidades associadas aos requisitos de segurança



Fonte: Hintzbergen *et al.* (2018)

Esse gerenciamento de risco talvez seja um dos maiores desafios para os escritórios de contabilidade visto que a LGPD deixa a cargo dos operadores e controladores a efetiva indenização ao titular dos dados no caso de dano patrimonial, moral, individual ou coletivo. No entanto, existem algumas hipóteses de exclusão dessa responsabilidade, uma das quais é a culpa do titular dos dados ou de terceiros[4]. Segundo Borelli *et al*. (2019) a LGPD não é clara quanto à aplicabilidade da responsabilidade subjetiva (aquela decorrente de conduta voluntária ou negligente, imperita ou imprudente) ou objetiva (independente de culpa, bastando a prova do dano e o nexo de causalidade), mas, independente da modalidade da responsabilidade, com o uso das melhores técnicas de proteção do seu ambiente admite-se a excludente de responsabilidade por fator terceiro.

Nesse sentido Magalhães (2018, p. 12) discorre sobre a possibilidade de exclusão de responsabilidade prevista também no Regulamento Geral sobre a Proteção de Dados (RGPD):

> Mais do que garantir que não existirá nenhuma violação de dados – missão impossível! – deve o Responsável pelo Tratamento ou Subcontratante centrar os seus esforços no cumprimento das obrigações e regras de tratamento do

4 LGPD: Arts. 42 e 43.

> Regulamento e nas evidências de tal *compliance* por forma a ser exonerado de qualquer responsabilidade que lhe possa ser imputável.

A ABNT (NBR 27002:2005) aponta algumas técnicas que podem ser implementadas para, dentre outros objetivos, proteger a confidencialidade, a autenticidade ou a integridade das informações, manter a segurança na troca das mesmas, prevenir e detectar a ocorrência de erros, perdas, modificação não autorizada ou mau uso, bem como, prevenir acesso não autorizado a sistemas de informação. Nesse sentido, a norma sugere o uso de políticas formais, compatíveis com as legislações pertinentes, que especifique o uso de controles criptográficos e o controle e distribuição de direitos de acesso a sistemas de informação e serviços, além disso, também recomenda que para o processamento correto controles sejam incorporados no projeto das aplicações, que validem os dados de entrada, processamento interno, dados de saída e controles adicionais para informações sensíveis.

Para adoção dessas práticas, a norma descreve diversos mecanismos, alguns dos quais são citados no Quadro 4.

Quadro 4 – Descrição e/ou funcionamento de ferramentas de segurança.

Ferramenta	**Definição e/ou Funcionamento**	**Norma**
Token	Dispositivo físico para autenticação. Exemplos: *tokens* criptográfico, *token* de senha dinâmica, *token* de memória, entre outros.	ABNT NBR ISO/IEC 27002:2005
Hash	Representação matemática única de um conjunto de dados.	
Controles criptográficos	Técnica que tem por objetivo proteger a confidencialidade, a integridade e a autenticidade das informações.	
Loggin	Processo de estocagem de informações sobre eventos que ocorreram num *firewall* ou numa rede.	
Técnicas de chaves secretas	Onde duas ou mais partes compartilham a mesma chave, a qual é utilizada tanto para cifrar quanto para decifrar a informação.	ABNT NBR ISO/IEC 11770-1:2010
Técnicas de chaves públicas	Onde cada usuário possui um par de chaves; uma chave pública (que pode ser revelada para qualquer um) e uma chave privada (que deve ser mantida secreta); técnicas de chaves públicas podem ser utilizadas para cifrar e para produzir assinaturas digitais.	

Fonte: Adaptado da ABNT 27002:2005.

Essas ferramentas podem servir como padrão técnico para mitigação de riscos, conforme requisito para implementação do programa de governança e para demonstrar a efetividade deste em privacidade, previsto no Art. 50 da LPGD. Dentre essas ferramentas, a chave pública é exigida por lei para manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital[5]. (BRASIL, 2012).

Além das soluções em *software* e *hardware*, a segurança da informação é obtida a partir da implementação dos controles adequados incluindo políticas, processos, procedimentos, estruturas organizacionais. (ABNT NBR 27002:2005).

2.4 Políticas de segurança

Para Stallings e Brown (2014), desenvolver uma política de segurança é a primeira etapa para planejar serviços e mecanismos de segurança.

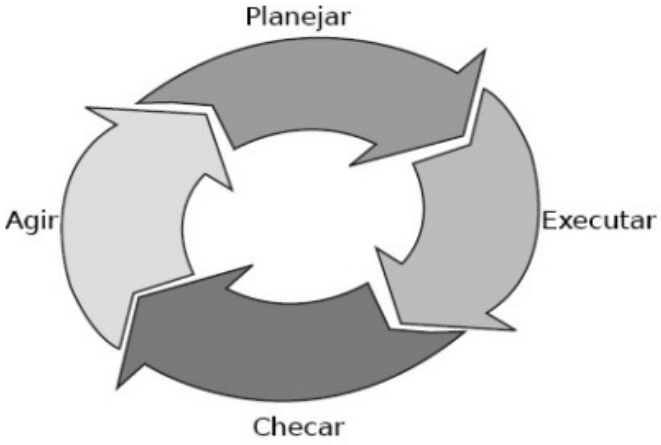
O modo mais útil de implementar políticas de segurança é por meio de uma declaração formal de regras e práticas que especificam ou regulamentam como um sistema ou organização provê a segurança de ativos de sistema sensíveis e críticos, considerando valores, vulnerabilidades, probabilidades e a potencialidade de ataques (*ibidem*). Nesse mesmo

5 Lei 12.682/2012: Art. 3º.

sentido, Hintzbergen *et al*. (2018) afirmam que ao estabelecer uma política para a segurança da informação, a administração provê as diretivas e o apoio para a organização, que devem ser escritas e estar em conformidade com os requisitos do negócio, leis e os regulamentos relevantes, então, esse material é então distribuído para o pessoal interno, clientes e fornecedores. Para Tanenbaum e Maarten (2008) qualquer sistema de computação deve fornecer serviços de segurança com os quais seja possível implementar uma vasta coleção de políticas de segurança, levando em conta a facilidade de uso, a segurança, o custo da segurança e da falha.

A política de segurança deve ser revista a fim de assegurar sua contínua conformidade, adequação e eficácia, como resposta a mudanças no ambiente organizacional, nas circunstâncias de negócio, nas condições legais ou no ambiente técnico e também para melhorias (ABNT 27002:2005). Nesse sentido, Hintzbergen *et al*. (2018) afirmam que muitas empresas utilizam o ciclo PDCA (*Plan*, *Do*, *Check*, *Act*, em inglês), ilustrado na Figura 2.

Figura 2 – Representação do ciclo PDCA



Fonte: Hintzbergen et al. (2018).

Stallings e Brown (2014) elenca tópicos mínimos que devem estar presentes nessa documentação, entre os quais: o escopo e a finalidade da política; a relação entre os objetivos de segurança e as obrigações legais e de regulamentação da organização e seus objetivos de negócio; requisitos de segurança de TI (Tecnologia da Informação) em termos de confidencialidade, integridade, disponibilidade, responsabilidade, autenticidade e confiabilidade; atribuição de responsabilidades relacionadas ao gerenciamento de segurança de TI e à infraestrutura organizacional; abordagem de gerenciamento de riscos adotada pela organização, como a conscientização e o treinamento de segurança devem ser tratados; quaisquer sanções legais que possam ser impostas ao pessoal e as condições sobre as quais se aplicam tais penalidades; definição do esquema de classificação das informações usadas em toda a organização; planejamento de contingências e continuidade do negócio; como e quando essa política deve ser revisada.

De acordo com os requisitos elencados pela literatura, a LGPD trata no seu Art. 50 de critérios mínimos para o estabelecimento de programas de governança em privacidade, dentre os quais, a necessidade de manter atualizada constantemente as regras de boas práticas e segurança e de publicação dessas regras. (BRASIL, 2018).

Além da política de segurança, há outras políticas a serem discutidas para uma eficaz governança de TI inclusive o controle de acesso.

2.5 Controles de acesso

Segundo Hintzbergen *et al*. (2018, p. 138), “os controles de acesso são uma combinação de controles de acesso lógico, relacionados a sistemas de informação, e controles de acesso físico”. Nesse mesmo sentido Stallings e Brown (2014), destacam que a utilização desse mecanismo em sistemas informatizados se dá com a mediação de um usuário e recursos do sistema, tais como: aplicações, arquivos e bancos de dados; de forma que um usuário não tenha acesso ao que não lhe é permitido, além disso, uma função de auditoria monitora e mantém um registro dos acessos do usuário a recursos do sistema.

Tanenbaum e Maarten (2008, p. 244) citam alguns exemplos sobre o uso de controle de acesso em bancos de dados, ressaltando a importância da definição de papéis de usuário:

> […] Por exemplo, um banco de dados de um banco pode ser protegido negando acesso a todos, exceto ao primeiro escalão de gerência e às pessoas especificamente autorizadas a acessá-lo. Com outro exemplo, em muitas universidades a utilização de certos dados e aplicações está restrita a professores e ao pessoal de determinada faculdade, e os estudantes não têm permissão para usá-los. Na verdade, o controle é focalizado na definição de papéis que os usuários desempenham e, uma vez verificado o papel de um usuário, o acesso a um recurso pode ser concedido ou negado. Por conseguinte, na elaboração do projeto de um sistema seguro é necessário definir papéis que as pessoas podem desempenhar e fornecer mecanismos para suportar o controle de acesso […]

Nesse sentido, segundo Stallings e Brown (2014), um sistema de controle de acesso de banco de dados inclui diferentes direitos, incluindo criar, inserir, remover, atualizar, ler e escrever, que fornecem considerável controle sobre a granularidade dos direitos de acesso, que podem ser ao banco de dados inteiro, a tabelas individuais ou a linhas ou colunas selecionadas dentro de uma tabela.

Como os bancos de dados organizacionais tendem a concentrar informações sensíveis em um único sistema lógico, incluindo, por exemplo, dados financeiros, informações do cadastro de clientes e fornecedores, eles podem ser alvo de ameaças internas e externas com utilização indevida ou modificações não autorizadas (*ibidem*).

Hintzbergen *et al*. (2018, p. 207), relacionam o risco do acesso indevido por parceiros externos, como fornecedores de serviço de armazenamento em nuvem, mencionando a importância dos acordos de confidencialidade nesse sentido:

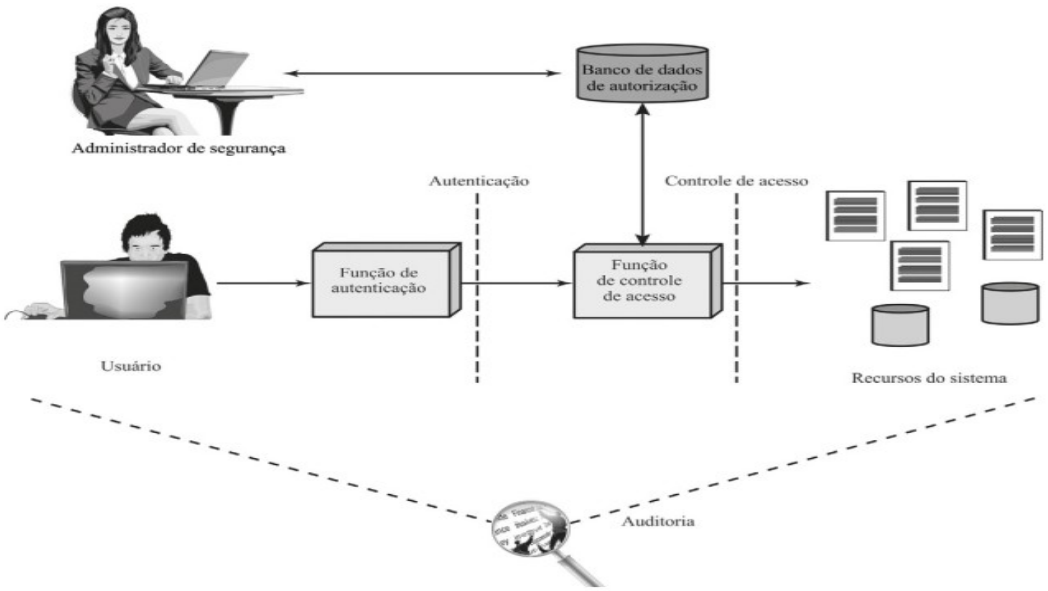
> Informações sensíveis devem ser devidamente identificadas e adequadamente protegidas, mas as pessoas de dentro da empresa e os parceiros externos precisam de acesso a informações sensíveis, ou podem obter acesso a tais informações. Tome como exemplo um administrador de banco de dados que pode ter acesso a informações sensíveis devido à natureza de seu trabalho. Ou que a empresa concordou que o novo sistema de TI deve ser localizado na nuvem, o que potencialmente significa que o fornecedor de serviços em nuvem pode ter acesso a dados sensíveis da empresa. Para ser capaz de proteger as informações e criar uma estrutura juridicamente exequível, devem existir acordos de confidencialidade ou de não divulgação elaborados e assentados.

Um dos controles previstos para organizar a segurança da informação, conforme ABNT (NBR 27002:2005), são os acordos de confidencialidade ou de não divulgação. Para esses acordos a norma elenca elementos que sejam considerados, dentre os quais, a definição de informação a ser protegida, o tempo de duração, ações requeridas quando do encerramento do acordo, direito de auditar, a responsabilidade pela divulgação não autorizada e as ações esperadas. Além dos acordos, a norma também prevê a análise crítica independente, por exemplo, por uma organização terceira especializada e com experiência em tais análises.

A Figura 3, ilustra um esquema de controle de acesso: um usuário se autentica e, a

partir de um banco de dados com as informações de acesso, são concedidas permissões para acesso aos ativos do sistema. Um administrador de segurança controla as permissões. Esse processo envolve questões de autenticação, autorização e auditoria.

Figura 3 – Relação entre a função de controle de acesso e outras funções de segurança.



Fonte: Stallings e Brown (2014).

Em relação a outros ativos, tais como aplicações e arquivos, sistemas operacionais, tais como, Windows ®, Mac ® e Linux ®, incorporam mecanismos de controle de acesso, que podem ser expandidos com a utilização de outros *softwares*, bem como pela utilização de dispositivos externos à aplicação, tais como *firewalls.* (STALLINGS; BROWN, 2014). A ABNT (NBR 27002:2005) também recomenda o uso desse mecanismo como uma das contramedidas contra *softwares* maliciosos.

Além da LGPD, existem outras legislações que exigem a proteção de documentos digitais contra acesso, uso, alteração, reprodução e destruição não autorizados, tal como a Lei 12.682/2012, que dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. (BRASIL, 2012).

2.6 Conscientização, treinamento e educação de segurança

Segundo Stallings e Brown (2014, p. 502, grifos do autor), programas de conscientização, treinamento e educação de segurança proporcionam benefícios importantes às organizações:

> Programas de conscientização, treinamento e educação de segurança podem reduzir o problema de erros e omissões. Tais programas podem impedir fraudes e ações executadas por empregados insatisfeitos porque eles passam a saber mais sobre suas **responsabilidades** e potenciais penalidades. [...] Além disso, impor tais políticas e procedimentos é mais difícil se os empregados puderem alegar ignorância quando pegos em uma situação de violação. Programas continuados de conscientização, treinamento e educação de segurança também são importantes para **limitar a responsabilidade civil e criminal** de uma organização. Com esses programas, uma organização poderá alegar que adotou um padrão de cuidado devido para proteger informações. Finalmente, programas de conscientização, treinamento e educação de segurança podem ser necessários para cumprir **regulamentações e obrigações**

> **contratuais**. Por exemplo, empresas que têm acesso a informações de clientes podem estar sujeitas a exigências específicas de conscientização e treinamento para todos os empregados que têm acesso a dados de clientes.

Esse tema também é mencionado em diversas normas dentre as quais, a ABNT (NBR 27002:2005), que reconhece que os objetivos de aprendizado de segurança para um empregado dependem do papel que ele desempenha.

Programas de conscientização, treinamento e educação, além de serem recomendados pela literatura, também podem estar no escopo de 'ações educativas', que é mencionado na LGPD, Art. 50, como regras de boas práticas e de governança. Cabe observar que a LGPD utiliza o termo 'poderão', quando menciona tais regras, de forma que a obrigatoriedade dessa prática pode ser discutível.

3 Aspectos Metodológicos

3.1 Delineamento da pesquisa

Quanto aos procedimentos técnicos, realizou-se um estudo multicaso com escritórios de contabilidades situados em Farroupilha – RS e com empresas de consultoria envolvidas com a implementação da LGPD em escritórios de contabilidade com vistas a verificar o grau de comprometimento em segurança de dados pessoais e quais dificuldades são enfrentadas nesse sentido. Um estudo de caso, de acordo com Almeida (2014), permite observar e compreender com profundidade a realidade de uma organização, grupo ou indivíduo. Quando é realizado com mais de um objeto de estudo, passa a ser denominado 'estudo multicaso' (*ibidem*).

Quanto ao objetivo da pesquisa, trata-se de pesquisa exploratória, onde, por meio de levantamentos dos assuntos relacionados ao tema a ser pesquisado, evidenciaram-se os diversos aspectos que devem ser considerados para identificar quais medidas devem ser tomadas para adequação à LGPD.

De acordo com Gil (2008, p. 3), a pesquisa exploratória "tem como propósito a formulação de um problema para investigação mais aprimorada ou para a construção de hipóteses". Ainda, segundo Creswell (2010), quando um conceito de um fenômeno precisa ser entendido, pois houve pouca pesquisa realizada a seu respeito, esse fenômeno merece uma abordagem qualitativa exploratória. Para Marconi e Lakatos (2010), o tipo exploratório serve para uma das três finalidades: desenvolver hipóteses, aumentar a familiaridade do pesquisador com o ambiente, fato ou fenômeno, e para realização de pesquisa futura, ou modificar e clarificar conceitos.

Em relação à abordagem do problema, o estudo é qualitativo, pois, segundo Yin (2016), essa modalidade permite a realização de estudos aprofundados sobre uma ampla variedade de tópicos, além de possibilitar a liberdade na seleção de temas de interesse, o que não é permitido por outros métodos. Para Appolinário (2016) é muito difícil que alguma pesquisa seja totalmente qualitativa ou quantitativa, nesse caso, naquelas que sejam preponderantemente qualitativas a coleta dos dados é feita a partir de interações sociais do pesquisador com o fenômeno pesquisado e são típicas das ciências sociais.

Diante das colocações dos autores, entende-se que as metodologias escolhidas são as mais adequadas para o tipo de estudo proposto.

3.2 Procedimentos de coleta e análise dos dados

A análise dos dados tem por objetivo investigar as medidas adotadas para adequação à LGPD nos escritórios de contabilidade e quais dificuldades são enfrentadas nesse sentido.

A forma de coleta de dados foi por meio de entrevistas semiestruturadas realizadas com membros da gerência dos escritórios de contabilidade W e X e também com uma

empresa que fornece consultoria jurídica Y e uma de sistemas de informação Z, que oferecem seus serviços para escritórios de contabilidade. O entrevistado A trabalha há 12 anos no escritório W tem graduação em ciências contábeis e pós-graduação em Direito Tributário, Gestão Empresarial e mais um curso extensivo de ICMS e tributação federal. O entrevistado B trabalha há 40 anos na área contábil e possui graduação em ciências contábeis e ciências econômicas. C é proprietária da consultoria Y há aproximadamente 15 anos e tem formação jurídica há mais de 20 anos. D tem formação em gestão de tecnologia da informação e ciência da computação, trabalha há mais de 30 anos na área em que atua e é gestor de TI na empresa Z.

As respostas das questões da entrevista estão descritas na sequência.

4 Resultados da pesquisa

Na questão 01 foi questionado se o tratamento de dados pessoais é motivo de preocupação e quais seriam os motivos desta, considerando que a LGPD elenca algumas responsabilidades aos controladores e operadores, por exemplo, elaborar um relatório de impacto a proteção de dados, manter um registro das operações de tratamento de dados e adoção de medidas de proteção. As respostas foram afirmativas no sentido de que há preocupação com o tratamento de dados pessoais. Os motivos citados foram pouco diferentes entre os entrevistados.

Para o entrevistado A, o Imposto de Renda das Pessoas Físicas e a contratação de pessoal por parte dos clientes são origem dos dados sensíveis. Já o entrevistado B destaca que o escritório havia implementado medidas de segurança e que, além do sigilo obrigatório aos profissionais da contabilidade, a nova legislação exige várias outras providências, dentre elas dos controles de acesso, com identificação dos responsáveis, mapeamento dos fluxos dos processos, obtenção do consentimento e aponta os setores de Recursos Humanos e de Tecnologia da Informação como os mais afetados pela nova legislação, citando algumas dificuldades como currículos, tempo de guarda da documentação, sigilo de dados com prestadores de serviço e exclusão de dados.

C ressalva a necessidade de adaptação e adequação e que a legislação se aplica a empresas de todos os portes e de todos os segmentos. Quanto ao Relatório de Impacto a Proteção de Dados, exemplificado na pergunta, informou que de primeiro momento essa exigência se dará apenas para empresas que tratam dados pessoais de forma automatizada e em grande volume. Para D a LGPD difere das demais legislações por que aponta para bases de dados não virtuais (físicas); a nova legislação deve facilitar o trabalho de implementação de algumas práticas de segurança que antes eram evitadas pelos gestores pois geralmente envolviam algum investimento, por exemplo, adotar um plano de contingenciamento e adquirir equipamentos e *softwares*, o que dificultava o trabalho técnico dos profissionais da TI, e informa que sempre foi objetivo evitar o sequestro ou perda das informações.

Na questão 02 foi questionado se já estavam sendo avaliadas medidas para melhoria da segurança da informação, considerando que a segurança e a prevenção são princípios a serem observados nas atividades de tratamento de dados. Ambas respostas foram afirmativas para esse item.

O entrevistado A foi enfático nas questões que envolvem treinamento de pessoal e alteração de documentos para obtenção do consentimento do tratamento de dados e que já está providenciando com seu gerente de TI que exercerá o papel de encarregado, *softwares* e equipamentos de segurança.

B afirmou que ainda não tem todas as medidas implementadas, que precisa reavaliar os contratos com fornecedores de serviço, citando como exemplo o acesso não autorizado ao banco de dados do escritório. Também afirmou que começará as mudanças a partir da elaboração da política de segurança, que será divulgada internamente e externamente, e que

precisará trabalhar o aspecto cultural.

C afirma que tem ferramentas de segurança de que necessita e que auxiliou na implementação em clientes. Recomenda que seja realizado o mapeamento dos dados que trafegam pelos sistemas e redes, identificando-os e classificando-os (dados sensíveis, dados pessoais, obrigações legais, etc.), após esse procedimento, deve ser realizado o que se denomina *gap analysis*, onde verifica-se brechas de segurança e, com isso, inicia-se o processo de implementação com todas as áreas.

D informa que já tem medidas implementadas como climatização, *backup*, controle de acesso por senha, mapa de riscos, entre outros, e que realiza análise de riscos de segurança. Porém, ainda restam medidas documentais que devem serem realizadas e que a adaptação à LGPD demanda o trabalho de todos envolvidos no processo, desde a recepção de documentos, o fluxo interno, armazenamento e devolução de dados a clientes, quando estes deixam de ser clientes dos escritórios.

Na questão 03 houve questionamento se a LGPD causará mudanças significativas nas rotinas do escritório e em quais aspectos. O entrevistado A afirmou que haverá mudanças se houver fiscalização e multa. O entrevistado B afirmou que haverá uma burocracia nas rotinas do escritório por causa da maior necessidade de controle e que, de início, também haverá alguns transtornos e custos. C considera mais importante o desenvolvimento de uma cultura de proteção de dados, privacidade, confidencialidade, sigilo de informações, práticas e códigos de conduta. Para D, a LGPD demandará o envolvimento de todos os envolvidos com o tratamento de dados.

A questão 04 abordou os impactos que haviam sido identificados a partir da necessidade de eliminação de dados pessoais após o término do tratamento. O entrevistado A afirmou que não tem controle sobre a eliminação dos dados, que tem muitas dúvidas nesse aspecto e não sabe como tratar essa questão, citando como exemplo questões previdenciárias e trabalhistas. O entrevistado B afirma que tem tratado com empresas junto aos setores jurídicos, que essa questão deve constar na política de tratamento de dados, que a eliminação de dados varia conforme a empresa e também que isso também trará mais burocracia.

O consultor C não tem prática quanto a esse aspecto, e explicou que a eliminação dos dados pode se dar pelo processo de anonimização ou pseudoanonimização e que, por determinação legal, empresas de certos segmentos precisarão armazenar determinados dados por um período especificado, ou seja, depende das obrigações do operador e do controlador. Sugere o uso da anonimização em empresas que não tem obrigação especificada de manter dados na forma bruta por longos períodos.

Para D não existe grande impacto no que se refere a processos, uma vez que nos contratos existirão cláusulas que especificam a forma de utilização das informações pessoais disponibilizadas e que algumas práticas deverão ser abolidas dos escritórios, por exemplo, a reutilização de papéis (aproveitamento do verso para outro conteúdo).

A quinta pergunta foi a respeito da realização dos treinamentos, que é recomendado pela ABNT NBR 27002:2005 como medida para minimizar possíveis riscos de segurança da informação. Se ocorreram treinamentos e se havia previsão de novas capacitações nesse sentido. O entrevistado A afirma que já está mobilizando os colaboradores para treinamentos, que estes recebem um manual com orientações quando da sua contratação e que planeja fazer palestras com os clientes, justamente para informar sobre mudanças nos procedimentos. Enfatiza também que deve haver fiscalização para que a nova legislação tenha eficácia. O entrevistado B respondeu que não deu capacitações, apenas para os responsáveis pela TI, mas que já ocorreram reuniões e que após a criação da política de segurança realizará capacitações específicas. C não realizou treinamentos e informa que estes dependem das fases anteriores, ou seja, devem ser feitos na etapa que segue após o mapeamento dos dados, *gap analysis* e formalização da política de segurança, e que a frequência destes treinamentos sejam

realizados dependendo do porte da empresa. D esclarece que o *compliance* deve estar organizado para a realização de treinamentos.

Na questão 06 foi questionado se existe uma política de segurança formal ou informalmente estabelecida e quais os tópicos abordados. Ambas as respostas foram afirmativas para essa questão. O entrevistado A respondeu que existe o manual que é entregue aos funcionários contratados que aborda sobre uso de equipamentos pessoais, direitos e deveres, entre outros tópicos que não envolvem necessariamente segurança de informação, mas que com a nova legislação precisa dar base legal a esse regulamento. Enfatiza ainda a questão dos currículos recebidos, e que precisará avaliar os contratos com clientes para tratar desse assunto. O entrevistado B afirmou que existem regulamentos formais, por conta do sistema de qualidade, e que existe alguns informais, mas tudo precisará ser reavaliado com a nova legislação. Afirma que existe regulamento sobre o controle de acesso aos documentos. C informou que está implementando medidas de segurança. O entrevistado D informa que parte da política de segurança está implementada, e que esta abrange análise e prevenção de riscos, melhores práticas, *backup*, *firewall* de controle e controladoria, porém somente para os dados em meio digital.

A sétima pergunta questionou sobre a frequência da revisão das políticas de segurança, conforme recomendação da ABNT. O entrevistado A afirmou que ocorre uma revisão do manual mencionado na questão 06 quando ocorre algum problema e cita como exemplo o fato de o sistema ficar inacessível. O entrevistado B diz que não estabeleceu uma frequência de revisão da política de segurança e que antes ocorria a cada 6 meses ou na ocorrência de algum caso que levasse a essa revisão. Enfatiza que pelas normas de qualidade sempre que houver um processo novo existe a necessidade de revisão da política de segurança. O entrevistado C afirma que revê políticas de segurança anualmente. O entrevistado D esclarece que os ajustes são realizados de acordo com a necessidade e que o *compliance* da base de dados em meio físico será analisado quando da implementação da política necessária, e que esta ainda não foi realizada.

Na oitava questão foram citados os quatro níveis de investimentos citados por Pinheiro (2018) para adequação à LGPD, os quais são: o nível técnico (ferramentas), o documental (atualizar normas, políticas, contratos), o procedimental (adequar a governança e a gestão dos dados pessoais) e o cultural (realizar treinamentos e campanhas de conscientização das equipes, dos parceiros, fornecedores e clientes) e foi questionado se houve recentemente em quais desses níveis.

O entrevistado A afirmou que houve investimento em todos os quatro níveis, estão sendo chamados profissionais especializados para tratar de assuntos jurídicos (normas e contratos) e de TI (ferramentas), estão oferecendo treinamento aos colaboradores e o nível cultural vai depender do tempo, mas que estão ocorrendo treinamentos e campanhas.

B afirmou que estão trabalhando nesse sentido, estudando a melhor forma de fazê-los, existem ferramentas que precisam ser adequadas e o nível cultural será o mais demorado pois as pessoas precisarão adequar a forma de trabalhar, tanto dentro do escritório como nos clientes.

O consultor C afirma possuir o nível ferramental, documental, ressalva a governança dos dados pessoais que ainda não foi implementada, informou ainda que no tratamento de dados nos *sites* deve ser observado o princípio da transparência, na política de privacidade deste *site* informando se há *cookies*, por exemplo, e que a questão cultural é trabalhada no dia a dia da empresa.

D informou que ainda não houve investimento em nenhum desses níveis recentemente e que a estrutura de informática requer adequação para fornecer maior segurança.

Na nona questão foi apresentado o conceito de dado pessoal sensível, de acordo com o artigo 5º da LGPD, e foi questionado se esses dados são tratados nas rotinas do escritório,

para quais finalidade e se existe algum controle de acesso para esses dados. A maioria dos entrevistados confirmou a existência de tratamento de dados pessoais sensíveis, porém, apresentam respostas distintas para a finalidade e em relação ao controle de acesso.

O entrevistado A afirmou que, por obrigações do e-Social, dados da admissão de funcionários relacionados a cor da pele são tratadas, por exemplo, e inclusive alterou formulários de admissão, e que está tratando com um profissional da área jurídica os contratos. Apresentou dúvidas quanto ao tempo de guarda dos documentos e a maneira de tratar esses dados. Contudo, afirmou que existe algum controle de acesso a dados relativos a folha de pagamento por meio de *loggin* de acesso, contudo, as informações em meio físico carecem de controle.

O entrevistado B afirmou que é discutido com clientes e com os colaboradores do escritório sobre o tratamento desses dados, citou o caso dos funcionários com ponto eletrônico, que contém dados biométricos destes e não existe obrigação legal de tê-lo, enfatizou novamente a burocracia ocasionada pela nova legislação e da necessidade de revisão dos contratos já existentes, inclusive os trabalhistas. Também apresentou dúvidas quanto ao consentimento obtido na forma eletrônica. Mencionou que está realizando o mapeamento dos trabalhos, identificando as pessoas responsáveis, o que é utilizado, e o que não é possível tratar.

O consultor C afirma que esse tipo de dado é tratado pelos escritórios e que são oriundos ou dos próprios colaboradores, citando como exemplo a contratação de um plano de saúde, caso em que são tratados dados dos familiares do colaborador, como também dos clientes dos escritórios dependendo do segmento ao qual atuam. Ressalva que para os dados sensíveis sempre deve haver uma finalidade específica e esta deve ser informada ao titular destes quando da obtenção do consentimento, que o princípio da necessidade deve ser observado e que o acesso deve ser limitado de acordo com os departamentos afetos, por exemplo, o setor de Recursos Humanos deve ter acesso apenas a informações que interessam a este setor, sempre mantendo os controles de *loggin* e proteção da rede.

O consultor D informa que não realiza tratamento de dados sensíveis.

A questão 10 foi sobre os tópicos relacionados à segurança existentes nos contratos junto a fornecedores e clientes, quais seriam estes tópicos. O entrevistado A afirmou não ter nada específico relacionado à LGPD, questões da forma de tratamento e o procedimento após o uso dos dados serão definidos conforme adendo em contrato de prestação de serviço, procedimento que ainda deve ser feito. O entrevistado B não enumerou as cláusulas pois cada contrato tem suas especificidades, afirma que existe um padrão de contrato ditado pelo Conselho Federal de Contabilidade, que existe um sigilo profissional e que devem ser revistos, visto que a LGPD requer cuidados mais rigorosos em relação aos dados de pessoas naturais. Apresenta ainda algumas dúvidas de como trabalhar com dados pessoais em relação a fornecedores de serviço e cita como exemplo os testes psicológicos em entrevista de emprego e, nesse caso, questiona o que fazer com os dados dos indivíduos não habilitados nos testes.

Para C o primeiro passo é identificar se os fornecedores têm uma política de segurança de informação, inclusive solicitando um relatório que mencione as ferramentas utilizadas, e no contrato mencionar cláusulas que estabeleçam responsabilidades relacionadas a falhas de segurança, sigilo de informações, finalidades do tratamento e armazenamento de dados. Salientou que a prática da segurança das informações é realidade para muitas empresas e que é importante que as empresas de porte pequeno e médio se adaptem pois as de grande porte podem necessitar dos serviços destas e por isso a rede inteira mantenha as informações protegidas, citando o exemplo dos escritórios que prestam serviço para grandes empresas, e que outras legislações, tal como Marco Civil da *Internet*, o Código de Defesa do Consumidor e a Lei de Cadastro Positivo já tem exigências relacionadas a proteção de dados.

D informa que atualmente não há adequação neste quesito.

A pergunta 11 é relacionada aos tópicos que mencionam o limite e o tempo para uso de dados nos contratos com clientes e fornecedores. O respondente A menciona que essa questão ainda terá que ser tratada, principalmente em relação aos documentos de funcionários, e que um profissional especializado está auxiliando nesse aspecto. Hoje os documentos entregues aos clientes têm um protocolo de entrega, porém, precisa definir o tempo para os documentos que ficam armazenados no escritório. O respondente B afirmou que hoje não tem limitação do tempo de tratamento e afirma que os contratos com clientes não têm tempo definido, que após 12 meses sem manifestação de qualquer das partes o contrato se torna por tempo ilimitado e que a LGPD não afetará esses contratos, porém, os contratos com fornecedores de *software* serão afetados pois estes tratam de dados pessoais e que são sigilosos, por isso serão aditivados. Para o respondente C, o tempo de armazenamento das informações depende da natureza jurídica destas e de acordo com a legislação pertinente. O respondente D informa que atualmente não há adequação neste quesito.

Comparando as respostas obtidas junto ao referencial teórico observa-se que algumas medidas de segurança já estão sendo implementadas pelos escritórios de contabilidade entrevistados, estes também reconhecem que ainda há mudanças a serem feitas para total adequação à LGPD, que estão revendo contratos, que existe preocupação por parte dos escritórios de contabilidade em relação à proteção dos dados pessoais e que há expectativa de mudanças nas rotinas dos escritórios a partir da nova legislação. Os entrevistados A e B afirmam buscar auxílio junto a profissionais especializados para trabalhar a parte jurídica e tecnológica, serviços que são fornecidos por C e D, respectivamente.

Os entrevistados A e B reconhecem que não tem total implementação das medidas de segurança previstas na legislação e recomendadas pela literatura, o que pode motivar responsabilização pois, de acordo com Pinheiro (2018), uma vez que trata-se de uma legislação principiológica e se os itens de controle não estão aplicados e implementados, os princípios não estão atendidos. Existe também a expectativa que a nova legislação venha a facilitar o trabalho dos profissionais da TI para implementação de algumas práticas de segurança que antes eram evitadas pelos gestores.

A maior parte dos entrevistados confirma a existência de tratamento de dados sensíveis nas organizações avaliadas, mencionam o cumprimento de obrigações tributárias, sociais e trabalhistas como origem desses dados, apresentam dúvidas quanto a maneira e tempo de tratamento destes, obtenção de consentimento na forma eletrônica e apontam necessidade de ajuste em contratos nesse quesito. Para esse tipo de dado, a legislação exige a publicação da dispensa de consentimento pelos órgãos e pelas entidades públicas[6] ou da obtenção de consentimento dos titulares dos dados. Uma vez que os entrevistados apresentam dúvidas quanto ao consentimento, é possível que as organizações estejam tratando dados sensíveis sem o consentimento exigido, o que pode ser motivo para responsabilizações.

Em relação aos controles de acesso, de acordo com os entrevistados, as organizações têm algum controle utilizando meio tecnológico ou apresentam algum regulamento sobre o controle de acesso aos documentos. Verificou-se em uma das respostas dos entrevistados a preocupação com o risco citado por Hintzbergen *et al*. (2018) de acesso indevido ao banco de dados por parceiros externos, no caso, o fornecedor do *software*. Como forma de limitá-lo, o entrevistado apontou a necessidade de implementar política de segurança e ajuste de contrato. Para esses casos a ABNT recomenda a utilização de acordos de confidencialidade ou de não divulgação.

Foi citado nas entrevistas o fato de que a LGPD também exige medidas de segurança para as bases de dados em meio físico, onde as soluções tecnológicas ficam mais limitadas, e que estas ainda não haviam sido implementadas pelas organizações. Existem recomendações

6 LGPD: Art. 11º, § 2º.

na ABNT NBR 27002:2005 para o controle de ativos em meio físico, incluindo a gestão (classificação e responsabilização), recursos humanos (direito de acesso) e controle de acesso (política), que podem servir como base para implementação da segurança dessas informações.

Quanto à eliminação dos dados pessoais, verificou-se junto aos entrevistados que existe falta de controle ocasionada pelos prazos estabelecidos nas legislações previdenciárias e trabalhistas ou critérios diferentes de acordo com as empresas que são clientes das organizações interessadas. Também foi citado o fato de que a eliminação dos dados pode se dar pelo processo de anonimização (quando, por meio técnico razoável, um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo) ou pseudoanonimização (quando um dado depende de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro para associá-lo a um indivíduo). A LGPD determina a eliminação dos dados pessoais após o término do tratamento, tendo uma ressalva para hipótese de cumprimento de obrigação legal ou regulatória pelo controlador[7]. Para esse quesito, Pinheiro (2018) recomenda o mapeamento do fluxo de dados para definição da nova governança dos controles de consentimento. O ciclo de vida do dado compreende a coleta, uso, compartilhamento, enriquecimento, armazenamento, eliminação e portabilidade (*ibidem*).

Quanto à pseudoanonimização, o uso das técnicas de *hash* e criptografia é uma forma de mitigar riscos de segurança em geral durante o tempo de guarda das informações, porém, de acordo com Borelli *et al*. (2019), ainda são consideradas informações pessoais, dada a interpretação expansionista adotada pelo Brasil, não se aplicando, portanto, a hipótese prevista no Art. 12 da LGPD, ou seja, quando os dados passam por um processo e deixam de ser considerados pessoais.

No que se refere aos critérios mínimos para o estabelecimento de programas de governança em privacidade, conforme Art. 50 da LGPD, dentre os quais, a necessidade de manter atualizada constantemente as regras de boas práticas e segurança e de publicação dessas regras, verifica-se que os entrevistados reconhecem a necessidade de implementação e publicação do programa de governança em privacidade, porém, não tem regras definidas para atualização das mesmas.

Quanto aos itens de investimentos apontados por Pinheiro (2018), verifica-se que a maioria dos entrevistados fizeram-no na maior parte, isto é, ainda há investimentos a serem feitos, apontam que o nível cultural como o mais difícil de ser trabalhado, pois demanda mudanças nas rotinas do trabalho e por depender de fator humano, e também que os setores responsáveis pela Tecnologia de Informação e Recursos Humanos como os mais afetados pela LGPD. Dentre outras medidas apontadas pela autora para implementação dos requisitos de conformidade à LGPD, há menção indireta à matriz de tratamento dos dados pessoais, ao mapeamento dos fluxos, ao controle de gestão de consentimentos, e à política para tratamento de dados com terceiros.

Quanto às medidas de segurança recomendadas pela ABNT verifica-se que nenhum dos entrevistados implementou-as seguindo o rigor da norma, porém, existem medidas sendo avaliadas para melhoria da segurança da informação como controle de acesso, treinamentos e política de segurança.

Quanto aos fornecedores de serviços, os entrevistados não apresentam respostas contundentes em relação aos tópicos relacionados à segurança nem ao limite e tempo de uso de dados pessoais nos contratos junto a fornecedores e clientes, porém, mencionam que estes itens têm sido objeto de revisão para adequação à nova legislação. Um dos entrevistados citou a necessidade de contratação apenas de parceiros que mantêm uma política de segurança de informação e que sejam estipuladas cláusulas que estabeleçam responsabilidades relacionadas a falhas de segurança, sigilo de informações, finalidades do tratamento e armazenamento de dados, uma vez que a proteção dos dados pessoais é exigida não apenas pela LGPD como por

7 LGPD: Art. 16, incio I.

outras legislações. Essa cautela é pertinente pois somente por meio de prova da culpa exclusiva de terceiro ou do titular dos dados é que os agentes de tratamento podem não ser responsabilizados no caso de falhas ou danos decorrentes da violação à legislação de proteção de dados pessoais, conforme Arts. 42 e 43 da LGPD. Pinheiro (2018) recomenda a atualização da política para tratamento de dados pessoais para terceirizados, estabelecendo procedimentos relacionados a GDPR e a LGPD sobre fluxo, padrão de criptografia, guarda de *log*s, entre outros tópicos relacionados à segurança.

O entrevistado D, que é um profissional especializado por trabalhar aspectos tecnológicos, cita o problema relatado por Sommervile (2011) de gerência de negócios, ou seja, ocorre um comprometimento da segurança em virtude da não aceitação do custo de proteção, contudo, de acordo com o entrevistado, a nova legislação levou a gerência a uma maior aceitação dos custos da segurança.

Além dos tópicos relacionados à segurança, houve menção nas entrevistas a outros princípios elencados pela LGPD, tais como o da transparência e da necessidade. A LGPD obriga o atendimento a todos os princípios elencados no Art. 6º, mesmo nas hipóteses de dispensa do consentimento do titular, motivo pelo qual devem ser observados nas atividades de tratamento de dados.

5. Conclusão

Esta pesquisa teve por objetivo avaliar quais medidas devem ser tomadas por escritórios de contabilidade de Farroupilha – RS para adequação à Lei Geral de Proteção de Dados (LGPD) no que se refere ao tratamento de dados e, por meio de um estudo multicaso, verificar o grau de comprometimento com segurança de dados pessoais e quais dificuldades são enfrentadas nesse sentido.

Por meio de entrevistas qualitativas com escritórios de contabilidades situados em Farroupilha – RS e com empresas de consultoria envolvidas com a implementação da LGPD em escritórios de contabilidade, foi possível obter informações necessárias para a análise de dados e sobre as dificuldades identificadas, inclusive com alguns exemplos vivenciados pelos entrevistados.

As respostas obtidas mostram que os escritórios reconhecem que não tem o *compliance* exigido pela LGPD e que são necessárias adequações para melhoria da segurança dos dados pessoais, em especial, a revisão dos contratos, implementação de uma política de segurança e controle de acesso. Os escritórios estão se adequando à nova legislação de forma parcial em relação ao *check-list* identificado na literatura e também com as recomendações do profissional especializado.

Dentre as dificuldades identificadas para adequação à nova legislação estão dúvidas quanto a maneira e tempo de tratamento de dados pessoais sensíveis, sigilo de dados com prestadores de serviço, segurança de dados em formato físico, obtenção de consentimento e tempo de guarda e exclusão de informações. Nesse último aspecto, os entrevistados apontam para dificuldade de adequação da nova legislação em relação ao que está previsto nos regramentos previdenciários, trabalhistas e tributários. Os entrevistados também apontam que os setores mais afetados pela LGPD são os setores de Recursos Humanos e de Tecnologia da Informação e que o aspecto cultural será o mais difícil de ser trabalhado pois dependem do fator humano e demandam mudanças de rotinas nos escritórios de contabilidade.

O estudo abordou meios de proteção para informação em formato digital, porém, de acordo com as entrevistas foi possível observar a presença de muitos dados em formato físico. Não foram explorados todos os aspectos relacionados na ABNT 27002:2005, em especial a segurança em recursos humanos, gestão de ativos, segurança física e do ambiente e no decorrer das entrevistas foi possível identificar dificuldades relacionadas a esses tópicos. Também não foram abordados todos os princípios elencados e demais obrigações e direitos

que estão previstos na legislação, nem foram realizados questionamentos relacionados ao livre acesso, qualidade dos dados e transparência. Por fim, houve resistência por parte dos escritórios de contabilidade em conceder entrevistas.

Esta pesquisa pode servir de base para o trabalho de profissionais das áreas de Direito e de Tecnologia da Informação, pois demonstra que os gestores dos escritórios de contabilidade apresentam dúvidas e dificuldades para adequação à LGPD, para os profissionais da contabilidade, pois traz recomendações da literatura e de profissionais especializados, e também servir de orientação para estudos futuros na área. Nesse último aspecto, sugere-se um estudo mais detalhado sobre o controle de consentimentos, transferência internacional e portabilidade de dados pessoais e também em relação aos princípios da adequação, necessidade e finalidade no tratamento de dados pessoais em escritórios de contabilidade.

Para os profissionais de contabilidade a nova legislação deve ser tratada como uma oportunidade de rever procedimentos internos e de formular regras de boas práticas e de governança em privacidade, visto que as informações são ativos importante para os negócios das organizações e precisam ser adequadamente protegidas.

Referências

ALMEIDA, Mário de Souza. **TCC, dissertação e tese**: uma abordagem simples, prática e objetiva. 2. ed. São Paulo: Altas S.A. 2014.

APPOLINÁRIO, Fábio. **Metodologia Científica**. São Paulo: Cengage Learning Edições Ltda., 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 11770-1: Tecnologia da informação - Técnicas de segurança - Gerenciamento de chaves.** Rio de Janeiro, 2010.

_____. **NBR 27002: Tecnologia da informação - Técnicas de segurança - Código de práticas para gestão da segurança da informação.** Rio de Janeiro, 2005.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A fundação e os limites do consentimento**. Rio de Janeiro: Forense, 2018.

BORELLI *et al.* **LGPD: Lei Geral de Proteção de Dados Comentada**. São Paulo: Thomson Reuters, 2019.

BRASIL. **Decreto nº 6.022, de 22 de janeiro de 2007.** Institui o Sistema Público de Escrituração Digital – SPED. Brasília, DF: Presidência da República, [2007]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/d6022.htm>. Acesso em: 29 out. 2019.

_____. **Lei nº 12.682, de 9 de julho de 2012.** Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Brasília, DF: Presidência da República, [2012]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12682.htm>. Acesso em: 29 out. 2019.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 ago. 2019.

_____. **Medida Provisória nº 959, de 29 de abril de 2020.** Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. Brasília, DF: Presidência da República, [2020]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv959.htm>. Acesso em: 11 mai. 2020.

BREDA, Zulmir Ivânio, **Uma reflexão sobre os impactos da tecnologia na Contabilidade**. Fev. 2019. Disponível em: <https://cfc.org.br/destaque/uma-reflexao-sobre-os-impactos-da-tecnologia-na-contabilidade/>. Acesso em: 18 set. 2019.

CRESWELL, John W. **Projeto de Pesquisa**: método qualitativo, quantitativo e misto. 3. ed. São Paulo: Artmed S. A., 2010.

GENERAL DATA PROTECTION REGULATION (GDPR), 2016. Disponível em: <https://gdpr-info.eu/> Acesso em: 17 out. 2019.

GIL, Antônio Carlos. **Estudo de Caso**. São Paulo: Atlas S.A., 2009.

HINTZBERGEN, Jule *et al*. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2018.

MAGALHÃES, Filipa. **Regulamento Geral de Proteção de Dados**. Portugal, 2018. Disponível em: <https://www.occ.pt/fotos/editor2/rgpd-fmagalhaesmanual.pdf>. Acesso em: 31 ago. 2019.

MARCONI, Marina de Andrade. LAKATOS, Eva Maria. **Fundamentos de metodologia científica.** 7. ed. São Paulo: Atlas S. A., 2010.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. **Padrões de Interoperabilidade de Governo Eletrônico**: documento de referência. 2017. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/e-ping/e-PING_v2017_20161221.pdf>. PDF. Acesso em: 03 nov. 2019.

PAESANI, Liliana Minardi *et al*.. **O Direito na Sociedade da Informação III**: A evolução do Direito Digital. São Paulo: Atlas, 2013.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2016.

_____. Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2018.

RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de janeiro: 2008. *In:* BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A fundação e os limites do consentimento**. Rio de Janeiro: Forense, 2018.

SENADO FEDERAL. **Parecer da Comissão de Assuntos Econômicos sobre o projeto de lei da Câmara nº 53/2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <http://legis.senado.leg.br/sdleg-getter/documento?dm=7751566&ts=1534796215492&disposition=inline&ts=1534796215492>. PDF. Acesso em: 16 ago. 2019.

SILVEIRA, Sérgio Amadeu. **Tudo sobre todos**: Redes digitais, privacidade e venda de dados pessoais. São Paulo: Edições SESC, 2017.

SOMMERVILE, Ian. **Engenharia de Software**. 9. ed. São Paulo: Pearson, 2011.

STALLINGS, Willian. **Criptografia e Segurança de Redes**: princípios e práticas. 6. ed. São Paulo: *Pearson Education* do Brasil, 2015.

STALLING, Willian. BROWN, Lawrie. **Segurança de Computadores**. 2. ed. São Paulo: Pearson Education do Brasil, 2014.

TANENBAUM, Andrew S. MAARTEN Van Steen. **Sistemas Distribuídos**: **princípios e paradigmas**. 2. ed. São Paulo, 2008.

WEIDMAN, Georgia. **Testes de Invasão: uma introdução prática ao *hacking***. São Paulo: Novatecm. 2014.

YIN, K. Robert. **Pesquisa qualitativa**: do início ao fim. Porto Alegre: Penso Editora Ltda., 2016.

Anexo A - Instrumento de Pesquisa – Roteiro de Entrevista

1. Responda em qual escritório você trabalha, qual o seu cargo, quantos anos você trabalha nesse local, sua formação e idade.

2. Considerando que a LGPD elenca algumas responsabilidades aos controladores e operadores, por exemplo, elaborar um relatório de impacto a proteção de dados, manter um registro das operações de tratamento de dados e adoção de medidas de proteção. Na sua opinião, o tratamento de dados pessoais é motivo de preocupação? Por quê?

3. Considerando que a segurança e a prevenção são princípios a serem observados nas atividades de tratamento de dados, já estão sendo avaliadas medidas para melhoria da segurança da informação? Quais são essas medidas?

4. Na sua opinião, a LGPD causará mudanças significativas das rotinas do escritório? Em quais aspectos?

5. Quais os impactos identificados a partir da necessidade de eliminação de dados pessoais após o término do tratamento?

6. Considerando que a ABNT NBR 27002:2005 menciona a realização de treinamentos como uma medida para minimizar possíveis riscos de segurança da informação, quais os treinamentos relacionados à segurança de informações que foram realizados? Existe previsão de novos treinamentos nesse sentido?

7. Existe uma política de segurança na entidade formal ou informalmente estabelecida? Quais tópicos foram abordados?

8. Considerando que a ABNT NBR 27002:2005 recomenda a revisão das políticas de segurança a fim de assegurar sua contínua conformidade, adequação e eficácia. Com qual frequência são revistas as medidas de segurança adotadas pela entidade?

9. Peck (2018), cita 4 níveis de investimentos para adequação à LGPD: o nível técnico (ferramentas), o documental (atualizar normas, políticas, contratos), o procedimental (adequar a governança e a gestão dos dados pessoais) e o cultural (realizar treinamentos e campanhas de conscientização das equipes, dos parceiros, fornecedores e clientes). Houve investimento em quais desses níveis recentemente?

10. A LGPD define no artigo 5º dado pessoal sensível como “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”, e no artigo 11 estabelece hipóteses para o tratamento de dados pessoais sensíveis. Ocorre tratamento de

dados pessoais sensíveis nas rotinas do escritório? Essas informações são utilizadas para quais finalidades? Existe algum controle de acesso para esse tipo de informação?

11. Quais os tópicos relacionados à segurança junto aos contratos com clientes e fornecedores?

12. Quais os tópicos que mencionam o limite e o tempo para uso de dados nos contratos com clientes e fornecedores?