AS IMPLICAÇÕES DO *COMPLIANCE* À LGPD NA ÁREA DE TECNOLOGIA DA INFORMAÇÃO EM UMA ASSOCIAÇÃO COMERCIAL

THE IMPLICATIONS OF LGPD COMPLIANCE IN THE AREA OF INFORMATION TECHNOLOGY IN A COMERCIAL ASSOCIATION

Karlla Soares Couto, Faculdade de Tecnologia de Santana de Parnaíba,
karlla.couto@fatec.sp.gov.br

Karoline Macedo de Lima, Faculdade de Tecnologia de Santana de Parnaíba,
karoline.macedo@fatec.sp.gov.br

Yara Rodrigues Amorim, Faculdade de Tecnologia de Santana de Parnaíba,
yara.amorim@fatec.sp.gov.br

Irapuan Glória Júnior, Faculdade de Tecnologia de Santana de Parnaíba,
irapuan.gloriajr@fatec.sp.gov.br

Resumo

A Lei Geral de Proteção de Dados (LGPD) é uma das diversas leis criadas no Brasil para regulamentar proteção de dados pessoais. O presente artigo pretendeu entender os impactos da aplicação da lei para a tecnologia da informação, e utiliza como base de análise uma associação comercial. Baseado na avaliação de documentos e a realização de entrevistas com os funcionários, foram criadas 22 melhorias para a *compliance* dos métodos de manipulação de dados conforme a legislação. O estudo agrega a academia por meio de estudos relacionados à adequação à LGPD, e como a exposição das dificuldades principais em sua realização, os quais estão incluídos na contribuição para a prática.

Palavras-chave: LGPD, Associação Comercial, Segurança da Informação, Tecnologia da Informação.

Abstract

The Brazilian General Data Protection Law (LGPD) is one of the various laws created in Brazil to regulate personal data protection. The present study has the aim to understand the impacts of the law application to information technology, using as object of study a trade association. From the analysis of documentation and conducting interviews with the staff, twenty-two recommendations for the compliance of the data processing with the law were created. The study adds to the academy with studies related to the compliance to LGPD, and how the exposition of the principal challenges in its accomplishment are included in the contribution to the practice.

Keywords*: LGPD, Trade Association, Information Security, Information Technology.*

1. Introdução

A Lei Geral de Proteção de Dados (LGPD), vigente desde 2020, determina as práticas corretas de manipulação de dados nos meios digitais. Seu o objetivo é proteger os direitos fundamentais de liberdade e de privatividade e criar um ambiente virtual sólido para organizações e consumidores. O descumprimento desta nova normativa pode manchar a reputação da empresa e gerar dispêndios financeiros (RAPÔSO et al., 2019).

Os aspectos da utilização da LGPD vão além de evitar gastos com as multas, mas como forma de educar o departamento de tecnologia da informação sobre anonimização, exclusão, consentimento, os agentes de tratamento e finalmente a manipulação de dados dos consumidores.

Nesta conjuntura, a questão de pesquisa deste estudo é: "Quais os impactos no setor de TI nos métodos de adequação dos processos com Lei Geral de Proteção de Dados em uma Associação Comercial?" e pretende sugerir mudanças para a adequação à LGPD. Ademais, visa ampliar a privacidade dos funcionários e associados, de maneira a estabelecer conformidade legal, e contribuir com a academia com estudos sobre Associações Comerciais e LGPD.

2. Referencial Teórico

2.1 Segurança da Informação

A informação pode ser definida como o resultado de um conjunto de dados sobre alguém ou algo que em sua junção possuem valor, pois trazem um significado, utilizado na passagem de conhecimento ou de negócio. No contexto de proteção de dados, a segurança da informação aspira também a segurança de softwares, sistemas, hardwares, recursos e sistemas contra possíveis ataques, falhas e tratamentos não autorizados, atenuando incidentes (FREUND; SEMBAY; DE MACEDO, 2019).

Uma instituição que não possua procedimentos e políticas de proteção consistentes pode sofrer comprometimentos de ativos e informações via vulnerabilidades, que podem ser descobertos por meio de auditorias, sistemas de gestão e monitoramento (FREUND; SEMBAY; DE MACEDO, 2019). A tríade CIA conceitua os fundamentos da segurança dos dados, composta pelo NIST (National Institute of Standards and Technology): (1) Confidencialidade/Confidentiality; (2) Integridade/Integrity; e (3) Disponibilidade/Availability.

2.2 Lei Geral de Proteção de Dados Pessoais

A Lei n° 13.709, que recebe o nome de Lei Geral de Proteção de Dados Pessoais, foi aprovada em 2018 pelo presidente em exercício Michel Temer, possui em seu texto dez capítulos e sessenta e cinco artigos ao total, e regula a manipulação de dados para promover a proteção das informações pessoais em âmbito comercial (BRASIL, 2018). É baseado na *General Data Protection Regulation*, lei europeia de propósito similar, que regula a segurança dos dados (MOTTA et al., 2021).

A lei conceitua que (BRASIL, 2018): (1) dado pessoal, é uma informação relacionada à pessoa natural viva e identificada ou identificável; (2) titular, pessoa natural à qual pertence o dado; (3) controlador, pessoa natural ou jurídica responsável pelas decisões da manipulação dos dados; (4) operador, pessoa natural ou jurídica que participa do tratamento; (5) encarregado, pessoa natural determinado pelo controlador e operador que atua como ponto de comunicação entre o titular, o controlador e a autoridade; e (6) tratamento de dados, todas as operações que envolvem dados pessoais, como a coleta, análise, acesso, classificação, compartilhamento e exclusão.

A instituição responsável por deliberar punições administrativas, implementar normativas e fiscalizar o cumprimento da LGPD no Brasil é a Autoridade Nacional de Proteção de Dados (ANPD). É previsto na legislação a obrigatoriedade da ANPD em promover a disseminação de conhecimento relacionado a proteção de dados (MELLO; MIRAMONTES, 2022).

A lei prevê o direito do titular de solicitar seus dados armazenados pela empresa e o acesso facilitado aos métodos de tratamento e compartilhamento, mesmo antes da concessão dos dados (BRASIL, 2018). É requerido que o controlador detenha a autorização explícita dos titulares para a coleta e o tratamento dos dados, que haja registro destes, e se houverem alterações no processo de manipulação das informações, o controlador deve notificar o titular que, em casos em que seu consentimento é exigido, poderá revogar a autorização e interromper o tratamento de seus dados (RAMPAZZO, 2021).

A LGPD trata da manipulação dos dados pessoais sensíveis, que são aqueles em que caso haja exposição não autorizada das informações, o usuário pode ter sua privacidade comprometida. São relacionados a características da personalidade do indivíduo e suas escolhas

pessoais, como raça ou etnia, religião, orientação sexual, dados referentes à saúde, genética, biometria etc. (PINHEIRO, 2020).

Ao terminar a finalidade do tratamento da informação, sua utilização não ser essencial para o andamento, o prazo para utilização ter finalizado, ocorrência de violação dos direitos ou solicitação do titular, o tratamento das informações deve ser encerrado (BRASIL, 2018).

2.3 Associação Comercial e Empresarial

Associações Comerciais e Empresariais (ACEs) são organizações populares sem fins lucrativos que representam outros órgãos com interesses comuns, podendo representar um nicho em específico ou negócios em geral. Tem como objetivo promover o comércio na região ao qual está vinculado, divulgar o trabalho dos membros e utilizá-los como fornecedores principais, além de discutir a política da região relacionada aos empreendimentos (SHAFARAT; SHAH, 2017).

Fundada no ano de 1980 por moradores de um município na Grande São Paulo, a ACE usada como objeto de pesquisa deste artigo, que será mantida sob sigilo conforme acordo firmado entre as partes para a proteção da organização, possui cerca de 30 associados e trabalha com serviços de consulta de CPF, consulta de crédito, solicitação de certificados digitais (em parceria com uma autoridade certificada), alocação de espaço para confraternizações das empresas etc.

3. Metodologia

O estudo possui natureza qualitativa (THEOPHILO; MARTINS, 2016) e metodologia de estudo de caso único (YIN, 2017), para conduzir a criação do *compliance* dos processos internos de uma associação com a lei. Os dados utilizados para análise são provenientes de entrevistas e verificação documental (GIL, 2022). As características empregadas no artigo estão descritas na Tabela 1.

Tabela 1 - Características do estudo

Item	Descrição	Autor(es)
Questão de Pesquisa	- Quais os impactos no setor de TI no Processo de Adequação da Lei Geral de Proteção de Dados em uma Associação Comercial?	
Natureza	- Qualitativa	GIL (2022)
Metodologia	- Estudo de Caso Único	YIN (2017)
Coleta de Dados	- Entrevista - Análise documental	THEOPHILO e MARTINS (2016)
Unidade de análise	- Associação Comercial	

Fonte: elaborado pelos autores

3.1 Procedimentos Metodológicos

As etapas de realização do estudo, apresentadas na Figura 1, são:

Etapa 1: Criação do questionário. A partir do texto da legislação, foram elaboradas algumas questões para a correta coleta de informações em entrevista com os funcionários (Apêndice A);

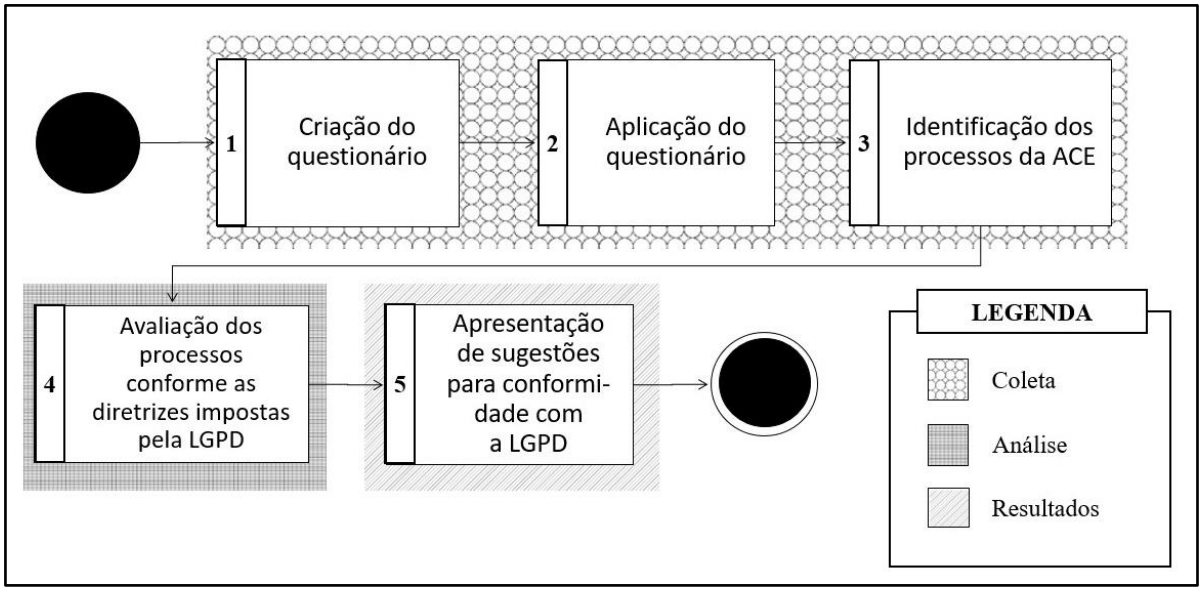
Etapa 2: Aplicação do questionário. Conforme os passos do protocolo de entrevista (Apêndice B), as questões foram respondidas em entrevista com os colaboradores da Associação;

Etapa 3: Identificação dos processos da ACE. Coleta realizada por meio de entrevistas e análise de documentos;

Etapa 4: Avaliação dos processos conforme as diretrizes impostas pela LGPD, foram avaliados os processos de acordo com as diretrizes da lei; e

Etapa 5: Apresentação de sugestões para conformidade com a LGPD, diante da necessidade de criar o *compliance* à LGPD foram elencadas as sugestões de adequação**.**

Figura 1 - Processo Metodológico



Fonte: elaborado pelos autores

4. Resultados e Discussões

Os resultados deste estudo derivam de uma entrevista com os gestores da associação e da análise dos documentos fornecidos pela empresa.

4.1 Funcionamento da Associação Comercial

A ACE troca dados pessoais de associados e funcionários com empresas terceiras para o auxílio na realização de suas atividades, sendo elas:

Associados: são os principais clientes da associação, compartilham seus dados pelos meios de comunicação da organização, como telefone, e-mail etc. Enviam dados sobre suas empresas, dados de funcionários e dados pessoais, que são armazenados pela ACE em um *software* de gestão de contratos;

Banco (instituição de crédito): a ACE possui filiação com uma instituição para consulta de crédito, onde são realizadas consultas de CPF. Os dados para consulta de associados são enviados para instituição;

Empresa de desenvolvimento e hospedagem de site: parceiro encarregado de desenvolver e hospedar o site da associação e armazenar as informações em seu banco de dados, tais como *banners* de publicidade ou dados de cadastro de candidatos à estagiários. A associação informou

que houve um cancelamento no contrato com a empresa em atuação e um novo site será desenvolvido pela companhia que provém o sistema de gestão;

Comunicação: instituição que realiza gestão de imagem da associação e sua publicidade;

Suporte de TI: desempenham manutenções nos equipamentos, e possuem acesso aos documentos físicos e lógicos, à rede interna e as máquinas;

4.2 Sugestões para a adequação a LGPD

Com base nos dados coletados da associação, foram elaboradas 22 sugestões para e a adequação à LGPD. Visando a segurança dos processos da associação, não serão apresentadas neste artigo todas as sugestões elencadas, em concordância a um acordo de confidencialidade consolidado entre as partes. Para a análise dos resultados, as sugestões foram segmentadas em seis categorias: Compartilhamento de dados, segurança de acessos, transparência, descarte, revisão de contratos e armazenamento.

A Figura 2 apresenta o percentual de possíveis melhorias por categoria. Referente ao **Compartilhamento de Dados**, foi constatado a troca de informações com terceiros para apoio aos serviços prestados, o que corresponde a 27% do total de melhorias. Entre as sugestões desta categoria, está a revisão dos contratos firmados, e se houver necessidade, a inclusão de cláusulas sobre confidencialidade e exclusão ou anonimização de informações dos associados.

Contemplando também 27% das sugestões totais, na categoria de **Segurança de Acessos**, pontua-se a necessidade de garantir a confidencialidade dos dados, propõe-se a elaboração de políticas para acesso físico e lógico, visando aumentar a segurança e evitar acessos não autorizados.

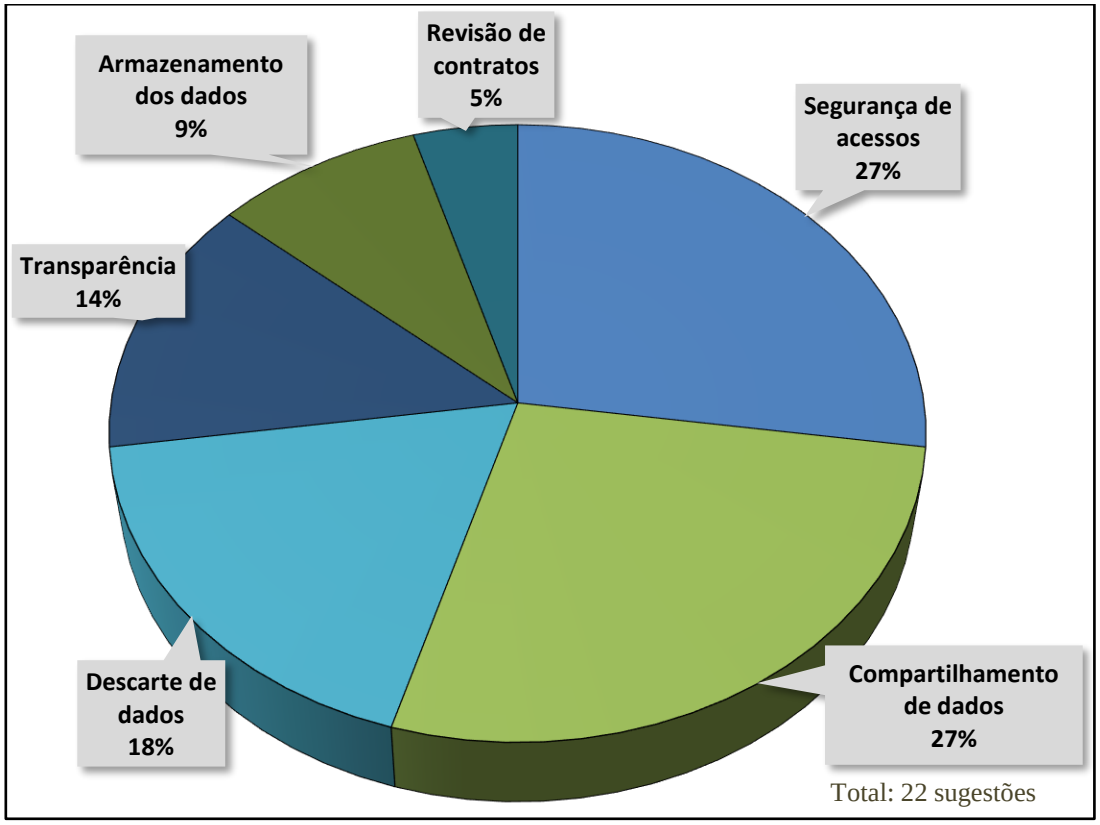
Com base na análise dos documentos, a ACE não possui um procedimento padrão para **Descarte** dados, devido a isso, foi recomendado questionar os processos dos fornecedores sobre a anonimização e descartes realizados, podendo ser ampliando para adendo nos contratos de prestação de serviço. 18% das sugestões referem-se ao descarte de dados.

Conforme informado pela lei, é necessário que haja **Transparência** na utilização dos dados, os titulares devem ter ciência de porque seus dados foram coletados, como são utilizados e estes devem ser fornecidos em caso de solicitação. As sugestões de melhorias desta área contemplam 14% do total.

O **Armazenamento de Dados** contempla 9% das sugestões. Baseado no estudo dos processos, foi identificada a carência de uma política de *backup*, e foi sugerida a elaboração de um procedimento padrão, com detalhamento das atividades relacionadas, armazenamento, cópias e responsáveis.

Por fim, considerando a troca de dados entre associados e empresas parceiras foi recomendada a **Revisão de contratos**, e inclusão de uma cláusula de confidencialidade e responsabilidade em todos. Esta categoria representa 5% do total das sugestões.

Figura 2 - Sugestões de Adequação por categoria



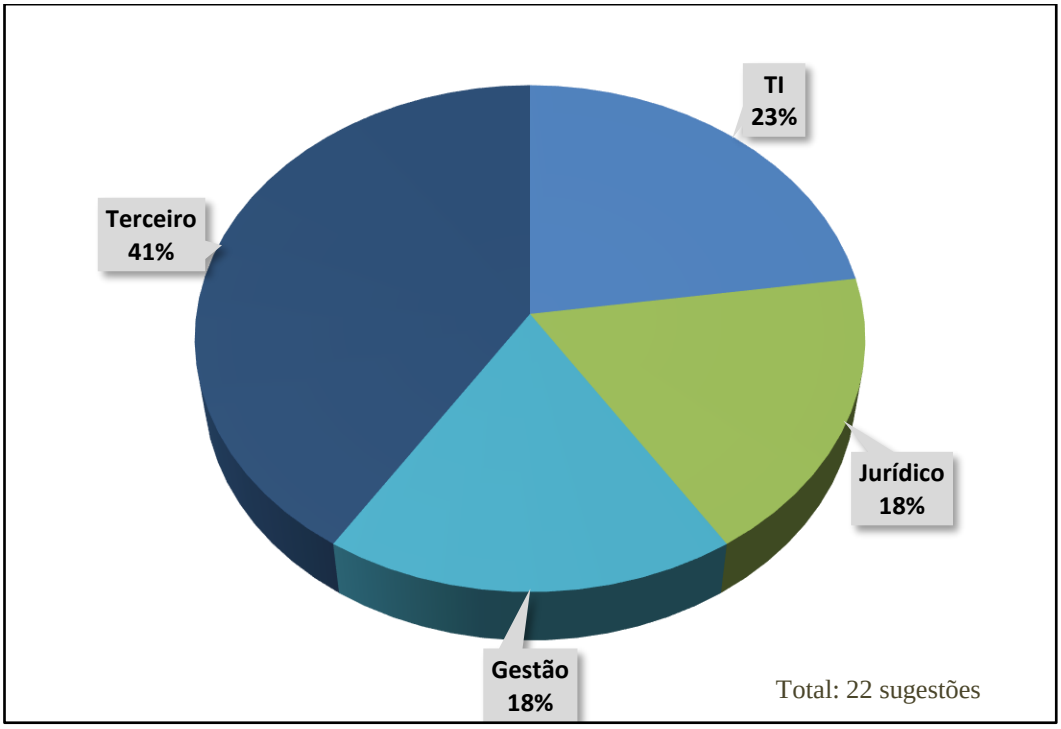
Fonte: elaborado pelos autores

Após analisar os impactos das sugestões na rotina da associação, apresentados no gráfico da figura 3, foram elencados os responsáveis por implementar novas políticas. 41% das ações são relacionadas a terceiros, o que incluí tópicos tais como contratos de confidencialidade e políticas para descarte e tornar os dados compartilhados em anonimizados.

Seguido pelo segmento da tecnologia da informação, cujo atuará em 23% das melhorias em criação de diretrizes para backup e acessos. Em sequência, as alterações performadas pela gestão abrangem 18% das sugestões, estas, com enfoque no ciclo de tratamento das informações.

Por fim, o setor jurídico atuará em 18% das sugestões com a modificação em contratos e termos de concessão de dados.

Figura 3 - Responsáveis pela implementação das sugestões



Fonte: elaborado pelos autores

4.3 Discussão

Um dos principais problemas encontrados nos processos internos da ACE foram faltas de cláusulas contratuais que especificassem as responsabilidades no tratamento das informações enviadas para terceiros, deixando brechas para a utilização irregular das informações. Por este motivo, os Terceiros são descritos como os principais responsáveis pela execução de sugestões, reavaliando os contratos ou criando aditivos.

A associação esclareceu que um processo interno de adequação já havia sido iniciado, demonstrando sua preocupação e interesse em estar em concórdia com a legislação. Apontava-se uma resistência pelos terceiros em adequar seus processos à legislação e a troca de informações com a ACE e titulares da forma cujos dados são tratados. A mudança dos processos internos impacta os parceiros que devem também realizar mudanças no tratamento das informações.

O desenvolvimento da adequação iniciado pela associação, por não ser acompanhado por um profissional qualificado, ainda deixava vulnerabilidades que poderiam ser penalizadas pela legislação. Este problema mostra que há uma necessidade de especialistas no assunto, com conhecimento em Tecnologia da Informação, para criar um suporte às empresas na mudança dos processos.

5. Considerações Finais

Apesar da importância da LGPD ter sido firmada com sua aprovação em 2018, e sua vigência apenas mais tarde em 2020, muitas organizações não alteraram seus processos para a conformação com as imposições previstas em lei, que possui como propósito transparecer os direitos dos proprietários no tratamento de informações e as imposições e direitos de operadores e controladores.

Atesta o fato de que apesar da aplicação de sanções, existem empresas que estão alheias aos requisitos previstos no texto da lei, estando propensas a multas e notas na mídia. Os titulares também podem sofrer prejuízos e discriminação com o vazamento das informações, decorrentes do tratamento e descarte incorreto dos dados.

Este estudo contribui para a teoria agregando pesquisas relacionadas à Lei Geral de Proteção de Dados, e com métodos de adequações de processos. Contribui para a praxis elucidando os principais problemas e possíveis lapsos de segurança cujo podem ser encontrados durante as mudanças. Trabalhos futuros podem analisar os dados apresentados e compará-los com outras organizações.

Referências

BRASIL. Lei Geral de Proteção de Dados (LGPD). **Governo Federal**, 2018.

FREUND, G. P.; SEMBAY, M. J.; DE MACEDO, D. D. J. Proveniência de Dados e Segurança da Informação: relações interdisciplinares no domínio da Ciência da Informação. **Revista Ibero-Americana de Ciência da Informação**, v. 12, n. 3, p. 807–825, set. 2019.

GIL, A. C. **Como elaborar projetos de pesquisa**. 7. ed. São Paulo: Atlas, 2022.

MELLO, A. P.; MIRAMONTES, G. C. LGPD: agentes De Tratamento, Resposável E ANPD. **Cadernos Jurídicos da Faculdade de Direito de Sorocaba**, v. 3, n. 1, p. 73–80, mar. 2022.

MOTTA, I. D. D. et al. GENERAL DATA PROTECTION LAW AND ITS IMPLEMENTATION IN THE MUNICIPALITY OF PARANAVAÍ IN COVID-19 TIMES. **Revista Jurídica**, v. 02, n. 64, p. 184–202, 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Security and Privacy Controlsfor Information Systems and Organizations. **NIST Special Publication 800-53**, n. 5, p. 492, 2020.

PINHEIRO, P. P. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD**. São Paulo: Saraiva Educação SA, 2020.

RAMPAZZO, S. Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD: diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade. **Revista IBERC**, v. 4, n. 2, p. 18–46, jul. 2021.

RAPÔSO, C. F. L. et al. LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EMTECNOLOGIA DA INFORMAÇÃO: Revisão Sistemática. **Revista de Administração - RACE**, v. 4, p. 58–67, 2019.

SHAFARAT, S.; SHAH, N. A. An Analytical Study on Role of Trade Association for Women Entrepreneurship and Their Capacity Building. **Journal of Gender Studies**, v. 15, n. 1, p. 175–198, 2017.

THEOPHILO, C. R.; MARTINS, G. DE A. **Metodologia Da Investigação Cientifica**. 3ª ed. São Paulo: Atlas, 2016.

YIN, R. K. **Case Study Research and Applications: Design and Methods**. 6. ed. Nova York: Sage Publications, Inc, 2017.

APÊNDICE A – Protocolo de Entrevistas

O protocolo de entrevistas adotado neste estudo contém as seguintes etapas:

- **Etapa 1.** Apresentar as informações referentes aos pesquisadores e o estudo a ser realizado;
- **Etapa 2.** Detalhar como será conduzida a entrevista;
- **Etapa 3.** Firmar compromisso com a confidencialidade e privacidade dos entrevistados. Esclarecer como será realizada a anonimização dos dados coletados;
- **Etapa 4.** Realizar questionário (Apêndice B);
- **Etapa 5.** Perguntar se existem observações úteis para a pesquisa;
- **Etapa 6.** Encerrar a entrevista.

APÊNDICE B – Questionário

Tema Principal: Privacidade

#	Pergunta
Q01	Existem políticas de acesso e de privacidade? Quais?
Q02	Há algum contrato de confidencialidade?

Tema Principal: Tratamento de dados

#	Pergunta
Q03	Os dados são atualizados em qual periodicidade?
Q04	Possui registro das operações de tratamento de dados pessoais?
Q05	Onde e como os dados são armazenados?
Q06	Nos processos de coleta de dados, o titular tem conhecimento do tratamento das informações?
Q07	Como o titular dos dados pode solicitar a revogação do direito consentimento sob o tratamento?
Q08	Quais são os métodos de coleta de dados?
Q09	Há um protocolo para o término do tratamento dos dados? Os dados são excluídos ou anonimizados?
Q10	Como é solicitado a permissão da utilização destes dados?

Tema Principal: Comunicação

#	Pergunta
Q11	O cliente é comunicado em caso de alterações no processo?

Tema Principal: Preparos para a lei

#	Pergunta
Q12	A empresa revisou seus procedimentos de TI após a LGPD entrar em vigor?
Q13	A empresa possui um DPO? Quais as atividades que ele realiza?