Journal of Technology & Information

A Adequação de uma Associação Comercial À LGPD: Um Estudo de Caso

The Adequacy of a Commercial Association to LGPD: A Case Study

Recebido: 12/09/2022 | Revisado: 22/09/2022 | Aceito: 28/09/2022 | Publicado: 29/09/2022

https://www.doi.org/10.5281/zenodo.7126030

Karlla Soares Couto
FATEC Santana de Parnaíba
https://orcid.org/0000-0001-9973-2663
karllasoares713@gmail.com

Karoline Macedo de Lima
FATEC Santana de Parnaíba
https://orcid.org/0000-0002-4962-2148
karolinemacedo.lima@gmail.com

Yara Rodrigues Amorim
FATEC Santana de Parnaíba
https://orcid.org/0000-0003-4950-9580
yaramorim06@gmail.com

Irapuan Glória Júnior
FATEC Santana de Parnaíba
https://orcid.org/0000-0003-2973-3470
ijunior@ndsgn.com.br

Resumo

O presente estudo analisa os processos de tratamento de dados de uma associação comercial com o objetivo de gerar recomendações para estarem em conformidade com a Lei Geral de Proteção de Dados. A pesquisa utilizou a metodologia de estudo de caso único, em que foram realizadas análises baseadas em uma entrevista com a diretoria e o uso de documentações da associação para localizar suas vulnerabilidades. Após a análise, foram identificados diversos pontos a serem melhorados no compartilhamento de informações de seus associados e nas tratativas realizadas dentro da organização, resultando em vinte e duas recomendações para adequação à legislação, principalmente a respeito de processos relativos ao compartilhamento de dados, segurança de acessos, armazenamento, descarte, revisão de contratos e transparência com o titular. A contribuição para a academia inclui a agregação a pesquisas futuras que envolvem a LGPD e suas adequações, já a contribuição para a prática é a elucidação dos principais desafios na conformidade legal de organizações.

Palavras-Chave: LGPD, Proteção de dados, Legislação, Associação Comercial, Segurança da Informação.

Journal of Technology & Information

Abstract

The present study analyzes the data processing processes of a trade association in order to generate recommendations to comply with the General Data Protection Law. The research used the single case study methodology, in which analyzes were carried out based on an interview with the board and the use of association documentation to locate its vulnerabilities. After the analysis, several points were identified to be improved in the sharing of information of its associates and in the negotiations carried out within the organization, resulting in twenty-two recommendations for adaptation to the legislation, mainly regarding processes related to data sharing, security of accesses, storage, disposal, review of contracts and transparency with the holder. The contribution to the academy includes the aggregation of future research involving the LGPD and its adaptations, while the contribution to practice is the elucidation of the main challenges in the legal compliance of organizations.

Keywords: LGPD, Data Protection, Legislation, Commercial Association, Information Security.

1. Introdução

A Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020, regulamenta o uso e manipulação de dados no país, criando um ambiente seguro para empresas e usuários e, caso seja infringida, poderá causar enorme prejuízo financeiro e macular a imagem das empresas (Botelho & Camargo, 2021).

Houve empresas autuadas por descumprimento da legislação, principalmente no que se refere ao artigo 6º da lei, que estabelece o limite de tratamento de informações. Em um destes casos a coleta de material biométrico foi considerada excessiva durante o tratamento, resultando em sanções pela falta de transparência sobre as empresas que recebem os dados de consumidores (Raes, 2022)

A conformidade legal com a LGPD vai além evitar dispêndio financeiro e desgaste da imagem da organização, implica na reorganização da área de TI sobre como manipular, anonimizar, excluir os dados e como os profissionais envolvidos devem pautar suas atividades perante os consumidores (Bax & Barbosa, 2020).

Em relação aos ataques cibernéticos como os ao banco Inter, o qual não notificou às autoridades quando os ataques foram detectados, gerando a violação de dados de milhares de clientes. Diante do ocorrido, foi acordada uma multa de cerca de 1,5 milhões de reais após o acordo com o ministério público, visto que o incidente foi classificado

apenas como baixo risco e não sendo um vazamento, mas uma quebra de sigilo (Zandona & Argiles, 2019).

A LGPD, criada após este incidente, pode ser aplicada em diversas empresas, dos mais variados setores econômicos, por exemplo, como Centauro, Leroy Merlyn, Privália e associações comerciais. Na Privália foram detectadas informações ambíguas em sua política de privacidade, ferindo assim o artigo 11° da LGPD. Pode-se exemplificar também o caso da Centauro, que a falta de clareza e exatidão na exposição de quais serão as empresas que recebem as informações de seus consumidores (Raes, 2022).

Diante deste cenário, este estudo possui como questão de pesquisa: "Quais as ações necessárias para uma Associação Comercial estar em conformidade à LGPD?" e possui como objetivos: (1) Identificar o funcionamento da Associação Comercial; e (2) Sugerir mudanças para a adequação à LGPD. Além disso, este estudo busca aumentar a privacidade dos colaboradores e associados, de forma a tornar o tratamento de dados legal, e contribuir com a academia com pesquisas que tratem de Associações Comerciais e LGPD.

2. Referencial Teórico

2.1. Segurança da Informação

A informação pode ser conceituada como o resultado do agrupamento e tratamento de informações acerca de algo ou alguém que juntos possuem valor, seja de negócio ou para transmissão de conhecimento. Transpondo o contexto de preservação dos dados, a segurança da informação visa também proteger softwares, hardwares, sistemas, recursos e serviços contra falhas, ataques e tratamento não autorizados, mitigando incidentes (Santos & Pontes, 2021).

Uma empresa que não possuí políticas e procedimentos de segurança bem definidos está sujeita a vulnerabilidades que podem comprometer seus ativos e dados.

Estes riscos podem ser identificados de maneira proativa via sistemas de gerenciamento, monitoramento e auditorias (Hintzbergen et al., 2018). Os princípios de segurança da informação estão conceituados na tríade CIA, composta pelo National Institute of Standards and Technology: (1) Confidencialidade/*Confidentiality*; (2) Integridade/*Integrity*; e (3) Disponibilidade/*Availability*.

O pilar da confidencialidade norteia as noções de acessibilidade dos dados definindo que estes devem ser obtidos, editados e manipulados apenas por pessoas e entidades autorizadas (ISO/IEC, 2013).

A integridade é a garantia de exatidão das informações, é necessário que os dados estejam precisos e atualizados. A preservação deste pilar inclui políticas contra uso não gerenciável de recursos e a possibilidade de fornecer registros da manipulação destes. Está diretamente ligado ao princípio de não repúdio e da irretratabilidade (Musonda et al., 2019).

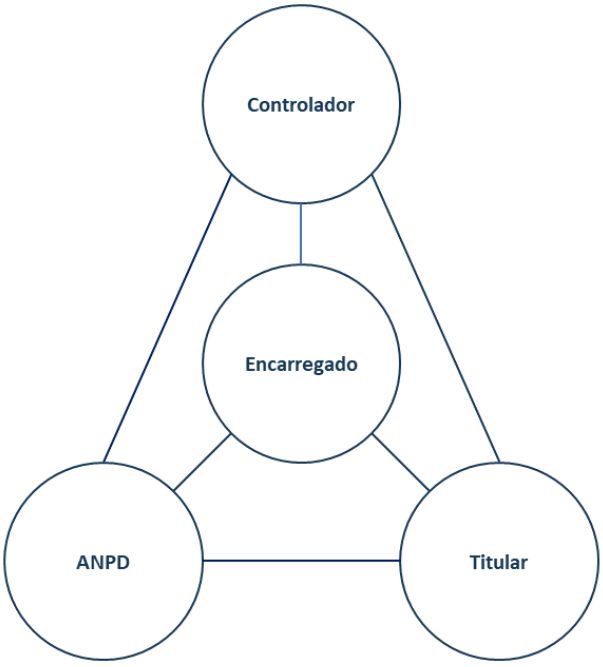
A disponibilidade dita que os dados não devem estar inacessíveis a pessoas e autoridades autorizadas que necessitam do mesmo, independentemente da localização e momento (ISO/IEC, 2013).

2.2. LGPD

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709) foi aprovada em 14 de agosto de 2018 pelo ex-presidente Michel Temer, composta por 10 capítulos e 65 artigos, tem como objetivo promover a proteção dos dados pessoais dos cidadãos e, possui como pilares o respeito à privacidade e intimidade dos usuários, a liberdade de expressão, de imprensa e da informação, a inovação, o desenvolvimento econômico e tecnológico, a livre iniciativa e concorrência, e os direitos humanos (Brasil, 2018). Tem como principal base a *General Data Protection Regulation*, legislação europeia para a proteção de dados (Celidonio et al., 2020).

A estrutura da LGPD é representada pela Figura 1, onde a lei estabelece os conceitos de (Brasil, 2018): (1) Dado pessoal, é a informação relativa à pessoa natural; (2) Titular, pessoa natural a quem confere a informação; (3) Controlador, pessoa natural ou jurídica que decide as ações relativas ao tratamento dos dados; (4) Operador, pessoa natural ou jurídica que realiza o tratamento a pedido do controlador; (5) Encarregado, pessoa natural indicada pelo controlador e operador que deve servir de canal de comunicação entre o titular, o controlador e a ANPD; e (6) Tratamento de dados, qualquer operação com dados pessoais, como a coleta, produção, análise, acesso, classificação, transferência e exclusão.

Figura 1 - Papel do DPO na empresa



Fonte: Elaborado pelos autores

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão público que tem a função de aplicar as sanções administrativas e criar metodologias para sua aplicação, estabelecer as atribuições do encarregado, criar padrões para medidas contra o acesso não autorizado, regulamentar o compartilhamento de informações sensíveis entre colaboradores etc. (Martins, 2021).

Além da criação da ANPD, a lei estabelece que as empresas devem nomear um encarregado para cuidar das operações de tratamentos de dados, citado normalmente como *Data Protection Officer* (DPO), termo criado na legislação europeia (European Union, 2016). Como informado em seu artigo 41, este deve ter seu nome e contato informado aos titulares, e tem como funções receber sugestões e reclamações dos clientes, orientar e treinar os associados, e executar atribuições requisitadas pela autoridade nacional (Brasil, 2018).

O DPO deve auditar as operações e mantê-las sempre de acordo com as necessidades da lei e com os requisitos da ANPD (Botelho & Camargo, 2021b). Apesar de criar o conceito de encarregado e delegar suas funções, a LGPD não informa uma obrigatoriedade ou quais empresas devem possuir um encarregado de tratamento de dados.

A LGPD exige que o controlador possua autorização clara dos titulares para o tratamento dos dados, e registrem a forma que estes serão tratados, pois eles têm o direito de a qualquer momento solicitar estas de informações de tratamento, e devem estar cientes de tudo que será realizado com as suas informações antes mesmo do consentimento. Com o uso de tecnologias da informação nos negócios, pode ser necessário adotar uma metodologia de registro de consentimento dos titulares e armazenados informações com relação a status do tratamento, e se houver qualquer mudança na forma de tratamento, o controlador deve informá-los imediatamente, em caso de discordância das mudanças, os titulares têm direito a revogar o consentimento (Teffé & Tepedino, 2020).

A lei apresenta a categoria de dados pessoais sensíveis, que se sofrerem vazamento, podem causar danos à privacidade do usuário maior do que os outros tipos, como informações sobre a saúde do titular, orientação sexual, raça, ideologia etc (Guanaes et al., 2018).

O término do tratamento pode ser realizado se a finalidade foi alcançada, o uso não é mais necessário, o prazo de utilização expirou, por solicitação do titular ou por decisão da ANPD em caso de violação de direitos (Brasil, 2018). Os dados devem ser excluídos pelo controlador, podendo ser mantidos em casos de cumprimento de jurisdição, uso em pesquisa, transferência a um terceiro (garantindo os requisitos de tratamento), e para uso exclusivo do controlador, sem interferência externa, sendo que em todas as situações deve-se anonimizar as informações sempre que possível (Brasil, 2018).

A anonimização dos dados se refere a uma série de técnicas de manipulação e exclusão de informações, a fim de tornar o rastreamento do titular impossível, sendo algumas formas a exclusão de identificadores como CPF, RG, nome completo, e-mail; informações específicas do dono como endereço; e telefone (Morellato & Santos, 2021).

2.3. Associação Comercial

Uma Associação Comercial (ACE) é um órgão sem fins lucrativos que representa outras empresas com interesses em comum, e podem cobrir um setor específico da indústria, processos e funções (Boléat, 2003). Promovem as atividades comerciais do município, divulgam os membros como fornecedores preferenciais e discutem a política relacionada aos negócios e a economia geral (Shafarat & Shah, 2017). Os membros representam suas empresas e sua identidade profissional, buscam interações comerciais e a legitimação de sua empresa, em que o grupo promove um poder representativo que influencia o consenso do mercado da região em que está alocado (Kahl, 2017).

A associação comercial usada como objeto de estudo para este artigo, a qual será mantida em sigilo protegido por um contrato de confidencialidade firmado entre as partes, foi fundado em 1980 por moradores do município. Conta com cerca de trinta associados atualmente, e trabalha com a consulta de CPFs, geração de certificados digitais, confraternização para empresas, banco de currículos etc.

3. Metodologia

A natureza da pesquisa é a qualitativa (Theophilo & Martins, 2016), com a utilização da metodologia estudo de caso único (Yin, 2017), pois o estudo deseja acompanhar e documentar a criação e aplicação de novas políticas referentes a LGPD em uma empresa regional. A coleta de dados (Gil, 2022) foi por meio de entrevistas e analises documentais. Foi observado o cenário do sistema de informação do ambiente e o tratamento de dados antes da atuação e o levantamento do panorama geral após a aplicação. A unidade de análise foi a associação comercial. Na Tabela 1 são apresentadas as características utilizadas para a realização do trabalho.

Tabela 1 - Características do estudo

Item	Descrição	Autor(es)
Questão de Pesquisa	- Quais as ações necessárias para uma Associação Comercial estar adequada à LGPD?	
Natureza	- Qualitativa	Theophilo & Martins (2016)
Metodologia	- Estudo de Caso Único	Yin (2017)
Coleta de Dados	- Entrevista - Análise documental	Gil (2022)
Unidade de análise	- Associação Comercial	

3.1. Processo Metodológico

Conforme a Figura 2, as etapas desta pesquisa são:

Passo 1: Criar o questionário. Foi criado um questionário para o levantamento de dados a ser encaminhado aos funcionários-chaves;

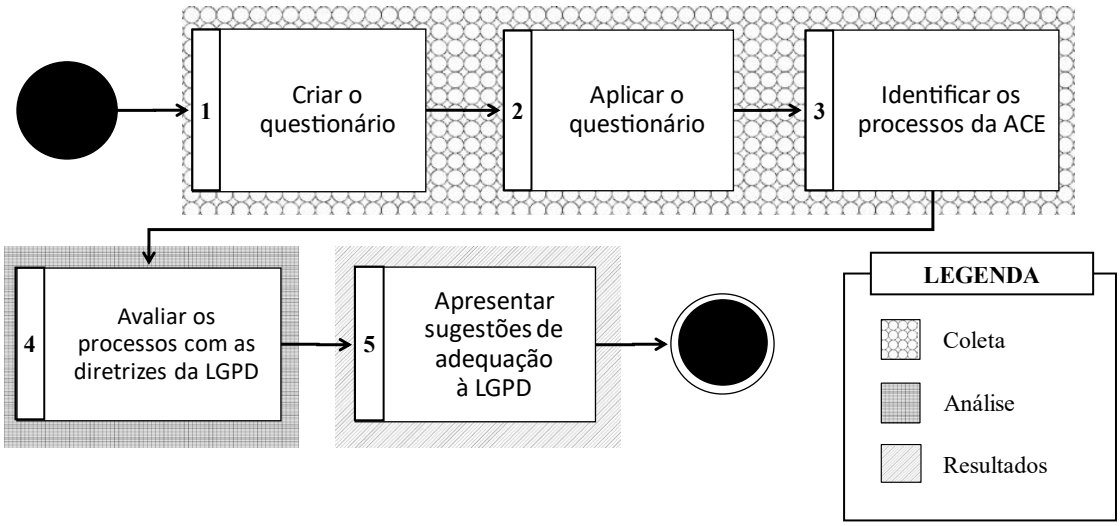
Passo 2: Aplicar o questionário. Foram entrevistadas as responsáveis pela Associação seguindo o protocolo de entrevistas (Apêndice B);

Passo 3: Identificar os processos da Associação Comercial. Foram levantados por meio de documentos digitais e entrevistas;

Passo 4: Avaliar os processos identificados com as diretrizes da LGPD;

Passo 5: Apresentar sugestões de adequação à LGPD.

Figura 2 - Processo Metodológico



Fonte: Elaborado pelos autores

3.2. Proposições

Diante do referencial teórico foram criadas sete proposições que deram subsídios para a criação das questões para as entrevistas (Tabela 2).

Proposição 1: Os dados devem ser precisos e atualizados para serem considerados íntegros. A preservação da integridade engloba a atualização e garantia de legitimidade (Musonda et al., 2019).

Proposição 2: As informações são manuseadas diversas vezes durante o processo de tratamento. Pode ser alterado a finalidade do uso e o ciclo de vida – incluso tempo para descarte (Hintzbergen et al., 2018).

Proposição 3: A segurança da informação e a revisão de processos são necessários para proteção da empresa. Existem vulnerabilidades que podem causar prejuízos a empresa e podem ser evitados com uma boa gestão da segurança da informação (Santos & Pontes, 2021).

Proposição 4: O titular deve consentir o uso dos dados e estar ciente para que os dados são utilizados. A lei exige que o controlador possua autorização clara dos titulares para o tratamento, e registrem a forma que estes serão tratados (Bax & Barbosa, 2020).

Proposição 5: **É preciso criar métodos de registro de consentimento para o armazenamento de dados, com foco em dados sensíveis.** Com o uso de tecnologias da informação nos negócios, pode ser necessário adotar uma metodologia de registro de consentimento dos titulares e armazenados informações com relação a status do tratamento (Guanaes et al., 2018).

Proposição 6: Deve haver um encarregado de tratamento de dados na empresa, e são necessárias realização de auditorias internas e registro em relatórios. A ANPD poderá realizar auditorias ou determinar sua execução, e a empresa estará sujeita a auditorias que podem resultar em multas; a lei estabelece que as empresas devem nomear um encarregado para cuidar das operações de tratamento, citado normalmente como DPO (Brasil, 2018; European Union, 2016).

Proposição 7: O término do tratamento pode ser realizado se a finalidade foi alcançada e as informações devem ser apagadas ou anonimizadas. Os dados devem ser excluídos pelo controlador, podendo ser mantidos em casos de cumprimento de jurisdição, uso em pesquisa, transferência a um terceiro com a garantia dos requisitos de tratamento, e para uso exclusivo do controlador, sem interferência externa, sendo que em todas as situações deve-se anonimizar as informações sempre que possível (Brasil, 2018).

Tabela 2 - Relação de questões e preposições

Item	Proposições	Questões Relacionadas
1	Os dados devem ser precisos e atualizados para serem considerados íntegros.	3
2	As informações são manuseadas diversas vezes durante o processo de tratamento.	2, 4, 5, 11
3	A segurança da informação e a revisão de processos são necessários para proteção da empresa.	1, 12
4	O titular deve consentir o uso dos dados e estar ciente para que os dados são utilizados.	6, 10
5	É preciso criar métodos de registro de consentimento para o armazenamento de dados, com foco em dados sensíveis.	7, 8
6	Deve haver um encarregado de tratamento de dados na empresa, e são necessárias realização de auditorias internas e registro em relatórios.	13
7	O término do tratamento pode ser realizado se a finalidade foi alcançada e as informações devem ser apagadas ou anonimizadas.	9

4. Análise e Interpretação dos Resultados

Os resultados do estudo foram obtidos a partir de uma entrevista com a associação e da análise de alguns documentos da empresa.

4.1 Funcionamento da Associação Comercial

A Figura 3 apresenta um diagrama das empresas terceiras que a Associação Comercial realiza o compartilhamento dos dados pessoais de funcionários e associados.

Figura 3 - Diagrama de compartilhamento de dados da ACE

Fonte: Elaborado pelos autores

Banco de talentos: a ACE envia as informações de jovens à uma organização de banco de talentos para auxílio na procura de oportunidades. Alguns dados enviados são CPF, RG, endereço, escolaridade ou instituição de ensino;

Suporte de TI: realizam manutenção dos equipamentos, e tem acesso aos arquivos da nuvem e locais, às máquinas e a rede interna;

Banco (instituição de crédito): a associação é afiliada à uma instituição de consulta de crédito, onde as consultas de CPF são realizadas. Os de credores dos associados são compartilhados com elas;

Software de gestão de contratos: utilizam um software para guardar todos os documentos e os contratos assinados. É gerenciado por uma empresa terceira e todos as informações e documentos dos associados ficam exclusivamente neste sistema;

Empresa de desenvolvimento e hospedagem de site: responsável pelo site da associação e informações inseridos neles, como os cadastros dos estagiários ou banners de divulgação. O contrato com ela foi cancelado e o novo site será criado pela mesma empresa que gerencia o software de gestão;

Contabilidade: realizam os balanços financeiros da ACE. Recebem as informações financeiras dos associados e colaboradores ao final do mês e devolvem de forma física;

Comunicação: empresa responsável pela imagem da associação e divulgação de conteúdo;

Associados: são os clientes principais da associação, e enviam suas informações através dos meios de contato da ACE, como e-mail, telefone etc. Enviam informações sobre a empresa e informações pessoais de funcionários, que são armazenadas no sistema de gestão.

4.2 Análise das Proposições

A coleta de dados junto ao respondente apresentou subsídios para responder as proposições criadas.

Proposição 1: Os dados devem ser precisos e atualizados para serem considerados íntegros. Apenas os dados de estagiários são atualizados a cada 6 meses e enviados para as empresas que estes estão alocados; os demais só são atualizados em caso de solicitação pelo titular.

Proposição 2: As informações são manuseadas diversas vezes durante o processo de tratamento. A ACE entrega um contrato de confidencialidade ao associado durante o início de sua associação, mas não há renovação deste contrato em caso de mudanças no processo de tratamento.

Proposição 3: A segurança da informação e a revisão de processos são necessários para proteção da empresa. A associação não possui política de privacidade e acesso. Houve alguns treinamentos sobre LGPD.

Proposição 4: O titular deve consentir o uso dos dados e estar ciente para que os dados são utilizados. O titular é informado sobre o uso no contrato de confidencialidade ao iniciar parceira com a associação, mas caso a forma de tratamento mude ao longo do processo não há aviso ao titular nem nova solicitação de consentimento.

Proposição 5: **É preciso criar métodos de registro de consentimento para o armazenamento, com foco em dados sensíveis.** Foi identificado há o registro de consentimento que podem ser coletados via e-mail, WhatsApp, formulário físico e online.

Proposição 6: Deve haver um encarregado de tratamento de dados na empresa, e são necessárias realização de auditorias internas e registro em relatórios. Atualmente a controladoria de tratamento é realizada por um oficial administrativo, responsável pela área financeiras.

Proposição 7: O término do tratamento pode ser realizado se a finalidade foi alcançada e as informações devem ser apagadas ou anonimizadas. Há um processo de exclusão lógica quando o titular se desassocia da ACE no sistema de gestão, porém só ocorre a inativação do usuário, as informações continuam no banco de dados e podem ser visualizados pelos funcionários.

4.3 Sugestões para a Adequação à LGPD

Após a análise das informações coletadas, foi elaborada vinte e duas sugestões de melhorias no processo visando a conformidade com a LGPD. Para a proteção das informações da organização, foi pactuado um contrato de confidencialidade em que as sugestões não serão explicitamente elencadas neste artigo, apenas segmentadas por categorias, sendo elas: (1) Compartilhamento de dados; (2) Segurança de Acessos; (3) Descarte; (4) Transparência; (5) Armazenamento; e (6) Revisão de contratos.

Conforme o gráfico da Figura 4, em relação ao **Compartilhamento de dados** foi identificado que a Associação Comercial realiza o compartilhamento com empresas terceiras para auxílio na realização dos trabalhos, que representa 27% do total de sugestões.

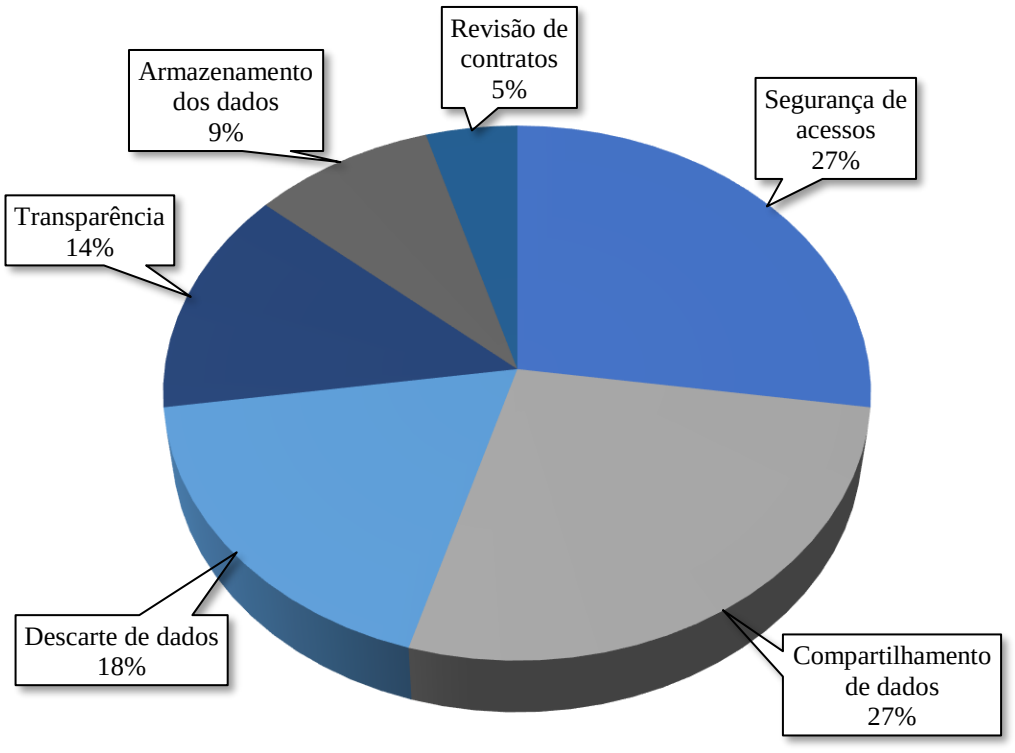
A sugestão é de que a Associação Comercial revise o contrato com a empresa fornecedora do software de contratos e, caso necessário, peça alterações, como a exclusão ou anonimização das informações de associados inativados. Também realize revisão de contratos com terceiros e insira uma cláusula de confidencialidade.

Já em relação a **Segurança de acessos**, que representa também 27% das sugestões, a sugestão é a criação de políticas de acessos e de senhas de rede, de modo a dificultar o acesso por um indivíduo não autorizado. Além disso, fortalecer a restrição de acesso dos ambientes físicos, liberando apenas para pessoas autorizadas.

Sobre o **Descarte** há a sugestão de validação e questionamento de seus fornecedores terceiros sobre a anonimização e descarte correto destes, tendo em vista que não foi identificado um processo padrão. O descarte corresponde três das sugestões, totalizando 18% das mesmas.

Referente a **Transparência**, como é previsto pela lei, se faz necessário que todas as informações detidas pela corporação sejam fornecidas a seus titulares caso sejam solicitados para análise. Contemplando 14% das sugestões, a transparência engloba três das melhorias.

Figura 4 - Sugestões de Adequação por categoria



Total: 22 sugestões

Fonte: Elaborado pelos autores

Relacionado a **Armazenamento de Dados** foram sugeridas duas possíveis melhorias. Durante a análise do caso, foi identificada a falta de uma política de backup, sendo recomendada a criação de uma política com detalhamento dos procedimentos de backup, armazenamento, cópia na nuvem e os responsáveis pela execução.

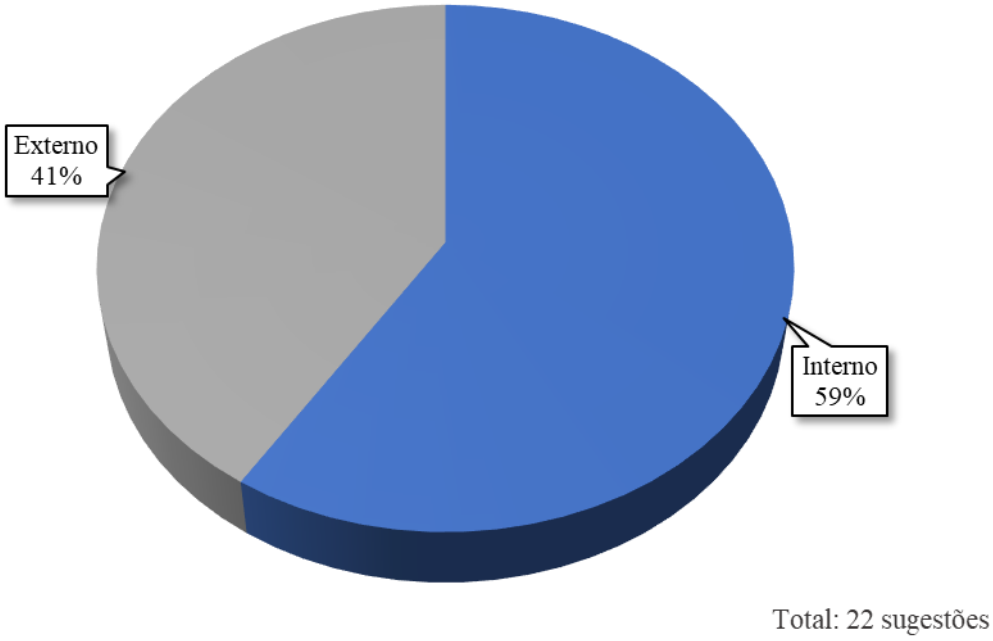
Por fim, levando em consideração os dados trocados entre associados, empresas parceiras recomendou-se a **Revisão de contratos**, incluindo em todos uma cláusula de confidencialidade e responsabilidade.

Em sua maioria, como mostra o gráfico da Figura 5, as mudanças de processos serão realizadas internamente, pela associação. Compondo 59% das recomendações, as treze melhorias internas incluem alterações no tratamento e armazenamento dos dados e políticas de acesso.

As treze mudanças externas, que representam 41% das sugestões incluem descarte, compartilhamento e transparência, estas alterações podem tornar a adequação mais difícil, visto que as empresas associadas podem não possuir processo de tratamento alinhados à LGPD.

Similarmente, como apresenta o gráfico da Figura 6, a associação será a mais impactada pela aplicação das melhorias. As treze sugestões que correspondem às 59% das mudanças comtemplam política de senhas, acessos, backups e alteração de contratos. As alterações realizadas pelas empresas parceiras são principalmente, referentes ao compartilhamento e descarte de dados.

Figura 5 - Mudança de Processos

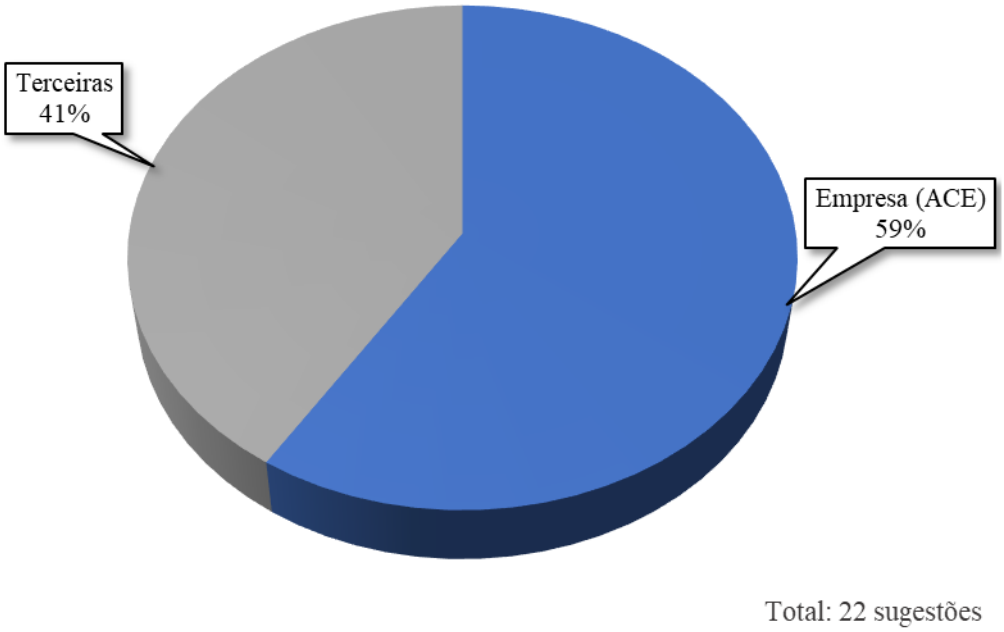


Fonte: Elaborado pelos autores

Ao elencar os responsáveis em aplicar cada uma das melhorias, apresentadas no gráfico da Figura 7, observamos que 41% correspondem a ação de terceiros, contendo itens como acordos de confidencialidade e política de descarte de dados compartilhados. Em sequência, com 23% está o setor de tecnologia da informação, que terá como encargo realizar as políticas de backup e de acessos.

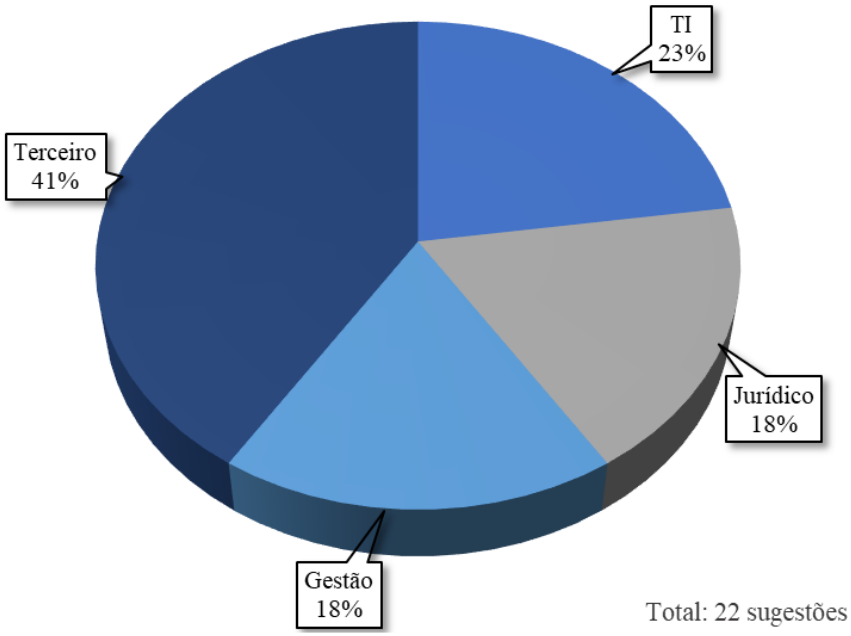
Seguido por mudanças realizadas pela gestão, que representam 18% das sugestões, focadas no tratamento de informações e em todo o ciclo de vida destes. Por fim, as mudanças a ser efetuadas pelo jurídico, também correspondem a 18%, sendo voltadas as áreas de alteração de contratos e termos de cessão de dados.

Figura 6 - Impactos das melhorias



Fonte: Elaborado pelos autores

Figura 7 - Responsáveis pela implementação das sugestões



Fonte: Elaborado pelos autores

4.4 Discussão

O compartilhamento de dados com terceiros se mostrou uma das maiores brechas de segurança e inconformidade com a lei, e foi possível observar que a associação e as empresas terceirizadas não tinham processos adequados aos requisitos da LGPD. Um dos problemas identificados é que o contrato entre as empresas não informa objetivamente as responsabilidades em relação ao tratamento.

Observou-se que há interesse e colaboração da ACE para gerar a conformidade prevista e necessária. Corrobora o fato de que a associação comercial informou que já haviam iniciado um processo de adequação à LGPD, apontando uma resistência por parte dos terceiros a adequarem processos e esclarecerem como era realizado a exclusão e anonimização dos dados detidos. Neste cenário, os novos processos aderidos pela associação impactam também os terceiros que terão de implementar mudanças relacionadas a legislação.

Diante deste contexto é possível observar que a associação, utilizada como objeto de estudo, mesmo realizando poucas operações de tratamento, ainda estava vulnerável a penalidades por não ter políticas de segurança aderentes ao que está previsto em lei. Percebe-se uma necessidade no apoio de profissionais especializados, principalmente de Tecnologia da Informação, para dar suporte à associação que não possui conhecimentos aprofundados no campo tecnológico e do direito digital.

5. Conclusões

A LGPD pretende esclarecer os direitos dos titulares e as obrigações de controladores e operadores quanto ao tratamento de dados. Apesar de sua importância ter sido fixada com a aprovação da lei em 2018, as empresas ainda não adequaram as obrigações previstas na legislação.

Apesar de já haver iniciado um processo de adequação à legislação, durante a pesquisa observou-se a presença de várias inconsistências ao que está previsto na lei, mostrando que mesmo pesquisando informações sobre o assunto ainda há uma desinformação em relação as mudanças que devem ser aplicadas para a conformidade.

Nota-se que mesmo com a aplicação de penalidades, existem empresas totalmente alheias aos padrões de tratamento criados pela LGPD. Neste cenário, as empresas estão vulneráveis a vazamentos e multas, e os titulares aos prejuízos legais que podem decorrer do mal uso e descarte.

As contribuições para a teoria incluem a agregação de pesquisas relacionadas a LGPD e métodos de adequação de organizações à lei. A contribuição para a prática é elucidar os principais desafios e falhas de segurança a serem enfrentados por gestores que queiram realizar sua adequação à lei. Em futuros trabalhos serão consideradas a aplicação da metodologia utilizada em empresas e organizações de ramos distintos e o estudo da adequação da LGPD em compartilhamentos com empresas terceiras.

Referencial Bibliográfico

Bax, M. P., & Barbosa, J. L. S. (2020). Proposta de Mecanismo de Consentimento na Lei Geral de Proteção a Dados—LGPD. *ONTOBRAS 2020*, 316–321. http://ceur-ws.org/Vol-2728/doctorate4.pdf

Boléat, M. (2003). *Managing Trade Associations*. Trade Association Forum. https://www.boleat.com/materials/managing_trade_associations_2003_1.pdf

Botelho, M. C., & Camargo, E. P. do A. (2021a). O Tratamento de Dados Pessoais Pelo Poder Público na LGPD. *Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)*, *9*(3), 549–580. https://doi.org/10.25245

Botelho, M. C., & Camargo, E. P. do A. (2021b). O tratamento de dados pessoais pelo poder público na LGPD. *Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)*, *9*(3), 549–580.

Brasil. (2018). Lei Geral de Proteção de Dados (LGPD). *Governo Federal*. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Celidonio, T., Neves, P. S., & Doná, C. M. (2020). Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira—Um estudo de caso. *Brazilian Journals of Business*, *2*(4), 3626–3648. https://doi.org/10.34140/bjbv2n4-012

European Union. (2016). General Data Protection Regulation (GDPR). *EU*. https://gdpr-info.eu

Gil, A. C. (2022). Como elaborar projetos de pesquisa. Em *GEN - Atlas*. (7º ed). Atlas.

Guanaes, P., Souza, A. R. de, Doneda, D., & Nascimento, F. J. T. do. (2018). *Marcos legais nacionais em face da abertura de dados para pesquisa em saúde: Dados pessoais, sensíveis ou sigilosos e propriedade intelectual*. Fiocruz.

Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2018). *Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002*. Brasport.

International Standarts Organization—ISO/IEC 27001, 27001:2013 23 (2013). https://www.iso.org/standard/54534.html

Kahl, S. J. (2017). The Role of Trade Associations in Market Discourse and Cognition. *Journal of Management Inquiry*, *27*, 13–15. https://doi.org/10.1177%2F1056492616688855

Martins, R. M. (2021). Proteção de dados pessoais e Administração Pública. *International Journal of Digital Law*, *2*(1), 133–149. https://doi.org/10.47975/IJDL/1martins

Morellato, A. C. B., & Santos, A. F. P. R. dos. (2021). O Capitalismo de vigilância e a lei geral de proteção de dados. *Revista Brasileira de Sociologia do Direito*, *8*(2), 184–211. https://doi.org/10.21910/rbsd.v8i2.455

Musonda, C., Monica, M., Nyirenda, M., & Phiri, J. (2019). Security, Privacy and Integrity in Internet of Things–A Review. *Proceedings of the ICTSZ International Conference in ICTs*, 148–152. https://doi.org/10.1109

National Institute of Standards and Technology. (2020). Security and Privacy Controlsfor Information Systems and Organizations. *NIST Special Publication 800-53*, *5*, 492. https://doi.org/10.6028/NIST.SP.800-53r5

Raes, A. (2022). *Procon/MS autua Leroy Merlin, Privália, James e Centauro por infração a LGPD*. Procon MS. https://www.procon.ms.gov.br/procon-ms-autua-leroy-merlin-privalia-james-e-centauro-por-infracao-a-lgpd/

Santos, R. B. dos, & Pontes, T. B. (2021). Gestão da segurança da informação e comunicações: Análise ergonômica para avaliação de comportamentos inseguros. *RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação*, *19*, 1–31. https://doi.org/10.20396/rdbci.v19i00.8665529

Shafarat, S., & Shah, N. A. (2017). An Analytical Study on Role of Trade Association for Women Entrepreneurship and Their Capacity Building. *Journal of Gender Studies*, *15*(1), 175–198. https://doi.org/10.46568/pjgs.v15i1.134

Teffé, C. A. S. de, & Tepedino, G. (2020). O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil*, *25*(03), 83–116. https://rbdcivil.emnuvens.com.br/rbdc/article/view/521

Theophilo, C. R., & Martins, G. de A. (2016). *Metodologia Da Investigação Cientifica* (3ª). Atlas.

Yin, R. K. (2017). *Case Study Research and Applications: Design and Methods* (6º ed). Sage Publications, Inc.

Zandona, A. C., & Argiles, A. V. (2019). Incidente de segurança: O vazamento de dados de clientes do Banco Inter sob a perspectiva da Lei 13.709/2018. *REVISTA JUSTIÇA & SOCIEDADE*. https://www.metodista.br/revistas/revistas-ipa/index.php/direito/article/view/771

APÊNDICE A – Protocolo de Entrevistas

O protocolo de entrevistas aplicado aos respondentes possui os seguintes passos:

Passo 1. Realizar a introdução sobre o pesquisador e a pesquisa a ser feita;

Passo 2. Descrever como a coleta de dados será realizada;

Passo 3. Ressaltar a preocupação da confidencialidade e privacidade dos entrevistados. Explicar como os dados coletados serão mantidos no anonimato;

Passo 4. Iniciar as questões (Apêndice B);

Passo 5. Questionar se há alguma outra observação que será relevante para o estudo;

Passo 6. Finalizar a entrevista.

APÊNDICE B – Questionário

Conteúdo: Privacidade

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

Conteúdo: 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?

Conteúdo: Comunicação

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

Conteúdo: Preparação para a LGPD

#	**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?