UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
CURSO DE CIÊNCIAS CONTÁBEIS

Henrique Gabbi Bittencourt

CONTRIBUIÇÕES DA AUDITORIA INDEPENDENTE PARA A GESTÃO DE RISCOS RELACIONADOS À LEI GERAL DE PROTEÇÃO DE DADOS

Santa Maria, RS
2023

Henrique Gabbi Bittencourt

CONTRIBUIÇÕES DA AUDITORIA INDEPENDENTE PARA A GESTÃO DE RISCOS RELACIONADOS À LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Ciências Contábeis, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Bacharel em Ciências Contábeis**.

Orientador: Prof. Dr. Vinícius Costa da Silva Zonatto

Santa Maria, RS
2023

Henrique Gabbi Bittencourt

CONTRIBUIÇÕES DA AUDITORIA INDEPENDENTE PARA A GESTÃO DE RISCOS RELACIONADOS À LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Ciências Contábeis, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Bacharel em Ciências Contábeis**.

Aprovado em 13 de julho de 2023.

_____
Vinícius Costa da Silva Zonatto, Dr. (UFSM)
(Presidente/Orientador)

_____
Ana Paula Fraga, Msc. (UFSM)
(Avaliadora)

_____
Cláudia de Freitas Michelin, Dra. (UFSM)
(Avaliadora)

Santa Maria, RS
2023

RESUMO

CONTRIBUIÇÕES DA AUDITORIA INDEPENDENTE PARA A GESTÃO DE RISCOS RELACIONADOS À LEI GERAL DE PROTEÇÃO DE DADOS

AUTOR: Henrique Gabbi Bittencourt
ORIENTADOR: Prof. Dr. Vinicius Costa da Silva Zonatto

Esta pesquisa tem por objetivo analisar as contribuições da auditoria independente para a gestão de riscos em LGPD. Deste modo, foi realizado um estudo de múltiplos casos, de natureza descritiva e abordagem qualitativa dos dados. Por meio de três trabalhos de auditoria independente realizados em programas de LGPD, em empresas que haviam implementado este programa a mais de um ano, foram analisados os planejamentos e programas de auditoria aplicados pelos auditores, bem como, os riscos identificados por esta aplicação e as quantificações percentuais destes eventos, o que possibilitou a identificação de oportunidades de melhoria e a sugestão de planos de ação por parte dos auditores. Os resultados da aplicação da metodologia proposta demonstram que a auditoria independente, por meio da NBC TA 500, viabilizou a estruturação de um plano adequado de planejamento de atividades para os trabalhos realizados, bem como definiu adequadamente um conjunto de procedimentos de auditoria aplicados no trabalho realizado pelos auditores. Verificou-se que a execução dos trabalhos realizados encontra embasamento teórico na NBC TA 300, apresentando sua conformidade. Sendo assim, é possível aferir que, ao quantificar percentualmente os riscos de exposição à LGPD, os auditores utilizaram os preceitos da NBC TA 315 para sua aplicação. Em relação aos casos analisados, verificou-se que todas as organizações apresentam algum nível de exposição a riscos relacionados a LGPD. Pôde-se concluir que a auditoria independente contribui para a estruturação de uma metodologia de gestão de riscos adequada, referente aos itens recomendados para proteção de dados pela Lei Geral de Proteção de Dados (LGPD). Os resultados da pesquisa realizada, apontam para o fato de que, por meio das suas normas técnicas, a auditoria independente contribui diretamente para todo o processo de formalização dos trabalhos de auditoria em gestão de riscos de LGPD, o qual permite a identificação e análise adequada dos eventos que representam riscos a organização auditada. Assim, esta pesquisa contribui para o avanço da literatura sobre gerenciamento de riscos relacionados a LGPD, ao fornecer novas evidências a respeito dos papéis da auditoria independente no processo de gestão de riscos, bem como ao destacar como a existência de fragilidades na estrutura de controle pode resultar em infrações relacionadas a referida Lei.

Palavras-chave: Auditoria Independente. Gestão de Riscos. LGPD.

ABSTRACT

INDEPENDENT AUDIT'S CONTRIBUTIONS TO RISK MANAGEMENT RELATED TO THE GENERAL LAW ON DATA PROTECTION

AUTHOR: Henrique Gabbi Bittencourt
ADVISOR: Prof. Dr. Vinicius Costa da Silva Zonatto

This research aims to analyze the contributions of independent audit to risk management in LGPD. Thus, a multiple case study was conducted, descriptive in nature and qualitative approach to data. By means of three independent audit works carried out in LGPD programs, in companies that had implemented this program more than a year before, the audit planning and programs applied by the auditors were analyzed, as well as the risks identified by this application and the percentage quantifications of these events, which enabled the identification of improvement opportunities and the suggestion of action plans by the auditors. The results of the application of the proposed methodology show that independent auditing, by means of the NBC TA 500, enabled the structuring of an adequate plan of activity planning for the work performed, as well as adequately defined a set of auditing procedures applied in the work performed by the auditors. It was verified that the execution of the work carried out finds theoretical grounding in the NBC TA 300, presenting its conformity. Thus, it is possible to assess that, when quantifying the percentage of exposure risks to the LGPD, the auditors used the precepts of NBC TA 315 for their application. Regarding the cases analyzed, it was found that all organizations present some level of exposure to risks related to the LGPD. It was possible to conclude that independent auditing contributes to the structuring of an adequate risk management methodology, regarding the items recommended for data protection by the General Law of Data Protection (LGPD). The results of the research point to the fact that, through its technical standards, independent auditing contributes directly to the whole process of formalizing the audit work in risk management of the LGPD, which allows the identification and proper analysis of the events that represent risks to the audited organization. Thus, this research contributes to the advancement of the literature on risk management related to the LGPD, by providing new evidence about the roles of independent auditors in the risk management process, as well as highlighting how the existence of weaknesses in the control structure can result in violations related to this law.

Keywords: Independent Auditing. Risk Management. LGPD.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

CRC – Conselho Regional de Contabilidade

CVM – Comissão de Valores Mobiliários

GDPR – General Data Protection Regulation

LGPD – Lei Geral de Proteção de Dados

NBC TA – Normas Brasileiras de Contabilidade da Auditoria Independente

TI – Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Esta seção apresenta a introdução que contempla a contextualização inicial do tema estudado, a questão problema, os objetivos, justificativas e contribuições do estudo. Por fim, finaliza com a apresentação da estrutura do trabalho.

1.1 APRESENTAÇÃO DO TEMA

Nos últimos anos, o Brasil vem sendo submetido a uma série de iniciativas legais ligadas ao combate à corrupção e a proteção de dados pessoais. Uma destas regulamentações está relacionada à edição da Lei nº 12.846/2013, denominada Lei Anticorrupção Brasileira, a qual dispõe sobre a possibilidade de responsabilização objetiva, no âmbito civil e administrativo, de empresas que praticam atos lesivos contra a administração pública (SILVEIRA, 2015).

Em linha com a Lei Anticorrupção Brasileira, foi editada no ano de 2018 a Lei nº 13.709, conhecida como a Lei Geral de Proteção de Dados (LGPD), a qual, segundo Pinheiro (2023), surgiu para acompanhar o desenvolvimento do modelo de negócios da economia digital, objetivo o qual é complementado pela análise do teor desta Lei (BRASIL, 2018, p. 1). Ainda, Pinheiro (2023) comenta que o seu propósito também é de dispor “sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado”.

Ao analisar a LGPD sob o enfoque das pessoas jurídicas, verifica-se que estas devem adequar os seus processos de gestão para que possam atender às premissas dispostas no artigo 7º desta Lei. Desta forma, conforme explicam Nakamura, Formigoni Filho e Ide (2019), para o sucesso nas ações de tratamento de dados pessoais, é necessária a implementação de práticas de gestão de riscos específicas para este fim.

A gestão de riscos, quando analisada de forma ampla, contribui também para os processos de governança e gerenciamento das organizações, pois seus resultados contribuem diretamente para os processos de planejamento e tomada de decisão, pois, suas práticas perpassam todas as ações e processos organizacionais, as quais, inevitavelmente, estão sujeitas a diversos tipos de riscos (HOPKIN, 2018).

Haja vista, neste amplo alcance da gestão de riscos no ambiente empresarial evidencia-se que esta também pode ser aplicada aos processos de proteção de dados

pessoais, pois a LGPD pode apresentar diversos riscos de infração aos seus artigos. Demetzou (2019) comenta que da legislação que trata da proteção de dados pessoais é possível extrair informações para identificação de riscos, fato este que permite seu efetivo gerenciamento.

Para este gerenciamento de riscos no âmbito da LGPD, torna-se necessária a adoção de instrumentos que possam operacionalizar esta gestão, o que ocorre por meio da aplicação de procedimentos e ferramentas de gestão. Conforme explicam Bromiley et al. (2015), as empresas devem abordar todos os seus riscos de forma abrangente e coerente, ao invés de gerenciá-los individualmente, fato este que reforça a utilização de meios que permitam este tratamento de forma ampla.

Pesquisas na área de gestão de riscos apresentam alguns exemplos de ferramentas que podem ser utilizadas neste processo, citando como benefícios alcançados pelas organizações, além do ganho de conformidade um melhor desempenho. O estudo de Webwe e Diehl (2016) identificou doze instrumentos que podem contribuir nesta gestão, dentre os quais, pode-se destacar a infraestrutura tecnológica, a cultura de consciência de risco, o controle interno, o mapeamento do risco, a estruturação de um sistema adequado de comunicação interna, auditoria, quantificação do risco, gestão do conhecimento, entre outros.

Os resultados desta pesquisa apontaram para o fato que dentre as ferramentas identificadas mais usualmente utilizadas pelas organizações estão relacionadas ao controle interno e a auditoria, sendo que esta última foi caracterizada como uma ferramenta eficaz na gestão de riscos (WEBWE; DIEHL,2016). A importância da auditoria na gestão de riscos também pode ser observada em suas etapas de aplicação. Conforme a pesquisa de Byrnes et al. (2018), as etapas de execução da auditoria iniciam com uma avaliação dos riscos, com a determinação de escopo e objetivos, culminando com a construção de um plano de auditoria.

Assim sendo, esta estruturação da auditoria, a qual engloba, dentre outras características, a avaliação de riscos, permite a esta técnica influenciar diretamente os processos de gestão de riscos, pois sua aplicação e seus resultados possibilitam o entendimento de um conjunto de dados sob uma visão macro da organização, característica esta que pode auxiliar na gestão de riscos (AJAO; OLAMIDE; ETEMITOPE, 2016).

Estas características da auditoria evidenciadas na literatura também podem ser visualizadas nas normas brasileiras e internacionais de auditoria independente, como,

por exemplo, na NBC TA 00, que determina que a auditoria deverá estabelecer um conjunto de normas sobre planejamento, programas e procedimentos, práticas estas que combinadas com o disposto na NBC TA 315 (R2), que trata sobre a avaliação dos riscos de distorção relevante, confirmam a aderência da utilização da auditoria como ferramenta capaz de contribuir para os processos de gestão de riscos.

Neste sentido, com base no exposto, verifica-se que em contextos de LGPD, a gestão de riscos é instrumento fundamental e pode ser operacionalizada com ferramentas como a auditoria independente, pois esta e seus processos demonstram aderência aos conceitos de gestão de riscos em LGPD, podendo contribuir para a identificação de eventos que possam representar riscos ao cumprimento desta norma, o que implica em infração e penalização das organizações.

Desta forma, como demonstrado anteriormente e, considerando a importância do tema, depreende-se que a atuação da auditoria independente, por meio da estruturação de processos adequados à gestão de riscos, pode contribuir para a observância aos aspectos legais recomendados pela LGPD. Assim, com base no contexto apresentado, a presente pesquisa identificou o seguinte problema: Como a auditoria independente pode contribuir para os processos de gestão de riscos referentes à LGPD?

O objetivo central deste estudo consiste em analisar as contribuições da auditoria independente para a gestão de riscos em LGPD. Como objetivos específicos definidos para responder ao objetivo geral, foram estabelecidos os seguintes: a) Descrever os planejamentos e procedimentos utilizados em auditorias de gestão de riscos em LGPD; b) Identificar riscos de infração à LGPD por meio da aplicação dos planejamentos e procedimentos de auditoria nos casos analisados; e, c) Avaliar (percentualmente) os graus de risco de infração à LGPD e seus planos de ação.

A realização deste trabalho se justifica por alguns elementos. Quanto ao aspecto acadêmico científico, este trabalho contribui diretamente para as pesquisas nas áreas de auditoria e gestão de riscos de LGPD, haja vista que ao analisar as principais revistas e publicações sobre o tema, observam-se poucos estudos relacionando essas temáticas, bem como o fato de que as bibliografias pesquisadas não contemplam estudos de auditoria envolvendo LGPD sob a configuração proposta por este trabalho, lacuna teórica explorada nesta pesquisa. Dessa forma, este trabalho poderá servir como referência para futuras pesquisas, produzindo novos conhecimentos sobre o tema.

Quanto ao aspecto prático, no âmbito do ensino e sua aplicação, justifica-se a realização desta pesquisa pelo fato de que sua execução permitirá colocar em prática os assuntos teóricos e os estudos realizados em sala de aula, principalmente no que tange as disciplinas de auditoria e controladoria, contribuindo diretamente para a formação acadêmica, sob o ponto de vista teórico e prático.

Quanto ao aspecto empresarial e social, para as empresas que implementam um programa de proteção de dados, a justificativa deste trabalho se dá pela busca de evidências que permitem compreender como a adoção de tais práticas refletem na conformidade legal em relação aos aspectos recomendados pela LGPD. Assim, reforça a necessidade de identificação de oportunidades de melhoria contínua, visando o aprimoramento de tais práticas de gestão (DEMETZOU, 2019).

Do mesmo modo, mediante o auxílio da auditoria independente, torna-se possível melhor compreender como as práticas de segurança de dados pessoais são avaliadas por atores externos à organização, os quais emitirão parecer sobre o quão oportunos são os procedimentos adotados para tratar de maneira correta e adequada os riscos identificados relacionados à LGPD. Assim, sob uma ótica da auditoria independente, a atuação do auditor assume a função de subsidiar, por meio de suas ferramentas, a aplicação de um programa estruturado de proteção de dados, de modo que este se torne mais robusto à organização (BYRNES et al., 2018).

Por fim, é importante considerar que a validação de um conjunto de procedimentos recomendados por uma pesquisa científica permite um estudo mais aprofundado de tais aspectos, uma vez que esse está centrado na ideia de melhor adaptar processos de trabalho, para que se evitem incidentes, vazamentos e acessos indevidos, sem necessidade explícita de dados pessoais, e/ou a incidência de penalização para a organização.

1.2 ESTRUTURA DO TRABALHO

Esta pesquisa está estruturada em cinco seções. Na primeira, são apresentadas as informações necessárias a contextualização do tema, problema, objetivos, justificativas e contribuições da pesquisa, além da estrutura do trabalho. Em um segundo momento, por meio do referencial teórico, descrevem-se, detalhadamente, os principais conceitos envoltos neste trabalho, dentre eles, àqueles

responsáveis pela sustentação da estrutura do mesmo (LGPD, auditoria e gestão de riscos).

Na terceira seção, são demonstrados os procedimentos metodológicos adotados para a realização da pesquisa. Inicialmente, define-se o delineamento da pesquisa, para que se entenda mais precisamente suas classificações metodológicas, seguido da descrição dos casos selecionados e os sujeitos envolvidos na pesquisa, bem como, são apresentados o constructo da pesquisa e as unidades de análise. Na sequência, descrevem-se os procedimentos de coleta e de análise dos dados adotados. Por fim, finaliza-se a seção abordando as limitações do estudo.

Já, na quarta seção da pesquisa, busca-se apresentar os resultados obtidos. Inicialmente, promove-se a apresentação dos trabalhos analisados. Na sequência, no intuito de atingir o primeiro objetivo, avaliou-se o conjunto de elementos a serem utilizados pela auditoria independente em trabalhos ligados à gestão de riscos em LGPD. Após, mediante aplicação prática deste método de análise, buscou-se identificar os riscos aos quais as organizações analisadas estão expostas. Desta forma, ao final, os riscos identificados foram mensurados com base no seu grau de exposição e planos de ação foram atribuídos individualmente, levando em consideração o caráter específico de cada setor e seu respectivo grau de exposição.

Na quinta seção da pesquisa, apresentam-se as conclusões do trabalho realizado, evidenciando quais foram as contribuições da auditoria independente para o processo de gestão de riscos em LGPD. Em seguida, sugerem-se recomendações para pesquisas futuras a respeito do tema. Ademais, são inseridas, ao final deste trabalho, a listagem de referências utilizadas para embasamento teórico e legal do estudo.

2 REFERENCIAL TEÓRICO

Neste capítulo, são apresentados os principais conceitos relacionados as temáticas centrais tratadas neste trabalho que envolvem os seguintes temas: Lei Geral de Proteção de Dados (LGPD) e Gestão de Riscos e Auditoria.

2.1 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Conforme Botelho (2020), a era digital trouxe diversas fragilidades, no que tange a privacidade dos dados pessoais dos indivíduos. A exemplo disto, pode-se citar o momento em que são realizadas ações envolvendo cadastros e *logins* em redes e páginas virtuais, pelos usuários de tais serviços, mediante a comunicação de seus dados pessoais.

Neste sentido, no intuito de proteger os dados pessoais dos seus cidadãos, diversos países iniciaram processos de regulamentações específicas sobre o tema, como no Brasil, com o advento da publicação da Lei Geral de Proteção de Dados (LGPD). Para tanto, utilizou-se como exemplo uma referência de Lei que disserta sobre a proteção de dados em países constituintes da União Europeia, os quais estão sob os regimentos da GDPR (*General Data Protection Regulation*), aprovada no ano de 2016, com seus objetos e objetivos descritos a seguir:

> - O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
> - O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.
> - A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais (GDPR, Art. 1º, 2016).

Analogamente, no intuito de se adequar às premissas das regulamentações supracitadas, na data de 14 de agosto de 2018, o Brasil sancionou a Lei nº 13.709/2018, também conhecida como LGPD, cuja vigência e conteúdo, além de assegurar o tratamento de dados pessoais em todo o território brasileiro, também facilita continuamente as relações comerciais com outros países do exterior, tendo em

vista que proporciona uma maior confiabilidade no compartilhamento de dados, principalmente no que se refere à segurança de contratos.

Diante disso, desde sua entrada em vigor, em setembro de 2020, a LGPD vem trazendo impactos à diversos modelos de negócios, fazendo com que as organizações não apenas adotem, mas também reforcem suas medidas de segurança físicas, lógicas e técnicas em seus ambientes operacionais, no intuito de garantir segurança aos dados pessoais dos titulares de dados (pessoas físicas) em qualquer hipótese de tratamento dos seus dados pessoais. Esta orientação explícita é definida pela própria Lei nº 13.709/2018, que estabelece que:

> “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”, deve estar segura sob o controle da organização (BRASIL, 2018).

Portanto, tendo em vista que a implementação da LGPD é um programa que envolve a análise de riscos e vulnerabilidades, bem como todo o seu processo a ser seguido (identificação, mensuração e estratégias de solução), trata-se como indispensável a gestão de riscos em programas eficazes de proteção de dados, para a observância dos aspectos regulatórios estabelecidos na referida norma, uma vez que, a não observância de seus preceitos pode resultar em penalização da organização.

Frente a este contexto, o qual exige que as organizações adotem práticas de proteção de dados pessoais com base na LGPD, observa-se que é inevitável a adoção de práticas de gestão capazes de identificar e oferecer um tratamento adequado a presença de riscos de exposição identificados na organização. Isto porque, o descumprimento a tais aspectos, resulta em penalidades a organização, decorrentes da não observância às recomendações estabelecidas por esta legislação.

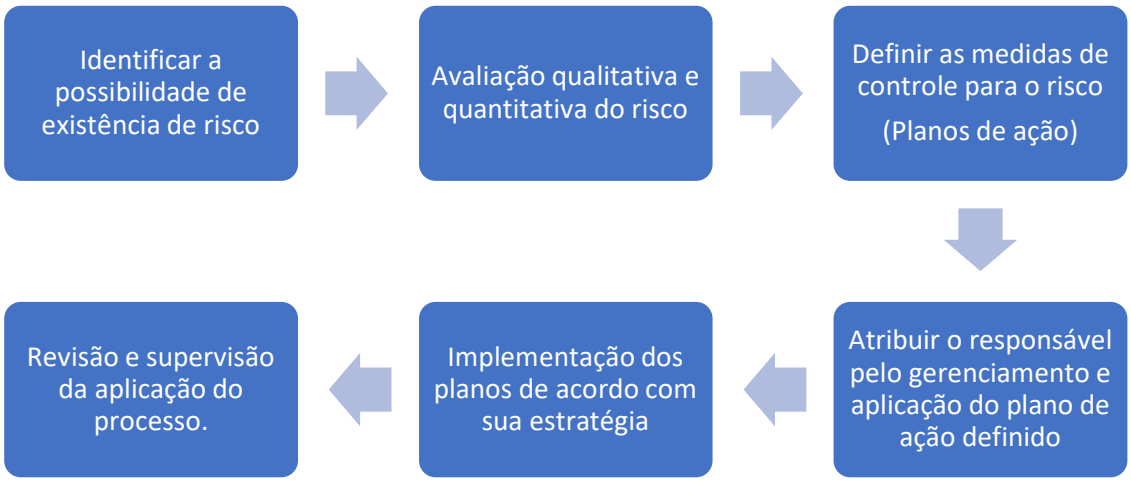
Por esta razão, o processo de gestão de riscos de proteção de dados pessoais é aplicado por meio de ferramentas adequadas de identificação, mensuração e tratamento das exposições identificadas.

2.2 GESTÃO DE RISCO

Conforme Assi (2021), o conceito de gerir riscos se concentra em identificar e planejar a aplicação dos recursos da organização de maneira que sejam utilizados da forma mais adequada e, concomitantemente, que os responsáveis por sua gestão identifiquem características nos seus processos rotineiros que possam ser consideradas futuras ameaças ao êxito da empresa em atingir seus objetivos. Por esta razão, é evidente que a relação entre os conceitos de gestão de riscos e as práticas de gestão estão diretamente ligados aos benefícios proporcionados pelas atividades e princípios utilizados pela auditoria independente, na promoção do aperfeiçoamento do ambiente de controle interno estabelecido na empresa.

De acordo com Namazian e Eslami (2011), para que uma gestão de riscos tenha um resultado de fato e cumpra seu objetivo final de maneira eficaz, deve apresentar 6 passos, como demonstrado na Figura 1.

FIGURA 1 - Processo de gestão de risco



Fonte: elaborada pelo autor (2023), baseado em Namazian e Eslami (2011).

Mediante a aplicação das ferramentas de gestão de riscos, o processo de gestão de riscos, inicia-se na etapa de identificação da possibilidade da existência de

riscos na organização. Em se observando tal fato, o processo prossegue com as avaliações qualitativas e quantitativas do risco a que a organização está exposta. Em seguida, em decorrência desta avaliação, verificam-se os planos de ação definidos/sugeridos com medidas que servirão para a mitigação dos riscos expostos. Na quarta etapa, são atribuídos os responsáveis pelo gerenciamento de cada um destes riscos, para que a aplicação do plano de ação sugerido ocorra de maneira prática e efetiva (NAMAZIAN; ESLAMI, 2011).

Assim, na etapa seguinte, é possível avaliar o conjunto de alternativas existentes, de modo que se possa identificar as estratégias que serão implementadas para cada risco identificado e o setor ao qual este se refere. Por fim, após a execução das etapas apresentadas, finaliza-se o processo de gerenciamento de riscos com a revisão e supervisão de sua aplicação (NAMAZIAN; ESLAMI, 2011). Esta avaliação é necessária para que se possa observar se as práticas de gestão instituídas estão proporcionando o retorno desejado, sendo estas capazes de reduzir os níveis de exposição da organização (ZONATTO; BEUREN, 2010).

Deste modo, pode-se inferir que, após a caracterização das etapas de um processo de gestão de riscos, é necessário analisar a forma como este processo foi (ou será) executado e quais as ferramentas que foram (ou serão) aplicadas para a determinação do resultado da referida gestão (COSO, 2007). A não observância de tais aspectos pode induzir os gestores a uma avaliação inadequada dos riscos aos quais a organização está exposta. Logo, pode refletir negativamente nas operações dela (COSO, 2004).

Diante de tal preocupação, dois aspectos destacam-se como meios relevantes para a gestão de riscos, sendo estes o contexto de análise das ferramentas de gestão de riscos e a avaliação da matriz de probabilidade e impacto.

2.2.1 Ferramentas de gestão de risco

Entende-se por ferramentas de gestão de riscos todos os meios utilizados por algum responsável que execute o trabalho de análise, seja ele colaborador interno, como nos casos referentes a auditoria interna ou por profissionais terceirizados, para os casos de auditoria externa (independente) (OLIVEIRA JÚNIOR; GOMES; VASCONCELLOS MACHADO, 2015).

Segundo Longo (2012), as organizações estão envolvidas em um ambiente de mercado que, por seu forte caráter de competitividade entre aqueles que estão inseridos, apenas a avaliação e entendimento sobre valores dos seus ativos intangíveis não são mais suficientes para o seu crescimento escalar. Dessa forma, ressalta-se a importância das empresas possuírem mecanismos de controle adequados, para que possam proporcionar a gestão de riscos diante dos eventos a que a organização poderá estar exposta envolvendo sua atividade de negócios.

Sabe-se que o processo de gerenciamento de riscos, conforme evidenciado na seção anterior, é um caminho a ser seguido envolvendo diversas etapas. Portanto, podem ser utilizados diversos mecanismos de controle para sua formalização, sendo eles diferentes uns dos outros, a depender da etapa que está sendo realizado o gerenciamento (identificação, mensuração ou definição de estratégia) e dos tipos de eventos que a organização está exposta.

Assim, ressalta-se que na etapa intermediária (identificação, avaliação e resposta aos riscos), a mensuração adequada dos eventos que representam riscos ao negócio é determinante para que os gestores possam identificar a forma mais adequada de como proceder para responder a estes eventos. Isto porque é após a identificação dos eventos que organização está exposta, que os gestores deverão atuar para avaliar a severidade de tais eventos, sua probabilidade de ocorrência e potencial de impacto (ZONATTO; BEUREN, 2010), razão pela qual deverão definir como serão respondidos tais eventos.

Portanto, é neste momento que o grau médio de exposição é definido, para que a empresa tenha conhecimento de quanto, em valores percentuais, àqueles riscos identificados poderão influenciar a sua atividade, tanto de maneira individual (aos departamentos/unidades), quanto de maneira geral (processos globais). Assim, para a efetivação da gestão de riscos, destaca-se que é necessária a adoção de um conjunto de ferramentas de gestão capaz de instrumentalizar este processo (COSO, 2007).

Uma vez que é necessário identificar estes riscos, para que possam ser mensurados e tratados, não é possível definir uma solução única para o seu tratamento, o que deve ser realizado diante das circunstâncias identificadas em cada ambiente organizacional (ZONATTO; BEUREN, 2010). Desta forma, embora atuem em um mesmo ambiente, organizações podem estar expostas a riscos distintos

(COSO, 2004). Nesta linha, o estudo de Webwe e Diehl (2016, p. 41), identificou doze diferentes instrumentos que podem contribuir nesta gestão, sendo estes:

> Infraestrutura tecnológica, cultura de consciência de risco, controle interno, mapeamento do risco, apólice de seguro, sistema de comunicação interna, auditoria, quantificação do risco, gestão do conhecimento, modelos VaR (*Value at Risk*) e o emprego dos métodos de simulação Monte Carlo e Bayesian como técnicas de medição de riscos operacionais.

Segundo estes autores, dentre as diferentes ferramentas de gestão de riscos possíveis de serem utilizadas pelas empresas, estão o controle interno e a auditoria, sendo esta (auditoria) caracterizada como uma ferramenta eficaz na gestão de riscos (WEBWE; DIEHL,2016). Desta forma, para a realização deste trabalho, busca-se inferir sobre as contribuições da auditoria especificamente nos processos de gestão de riscos relacionados a LGPD.

2.2.2 Gestão de riscos em LGPD

A gestão de riscos em LGPD consiste no auxílio as organizações na estruturação de práticas de gestão adequadas a proteção de dados. Como partes indissociáveis, a gestão de riscos e a LGPD, decorrem de práticas alinhadas instituídas com o propósito de assegurar o correto cumprimento da legislação aplicada, sem a incidência de penalização a organização (DEMETZOU, 2019).

Assim sendo, pode-se afirmar que não se tem como realizar um programa completo e eficaz de adequação as recomendações estabelecidas pela LGPD para a correta proteção de dados, sem que uma gestão de riscos apropriada seja realizada, com a adoção de ferramentas necessárias ao estabelecimento de um ambiente efetivo de controle de riscos, instituído na organização com o propósito de fortalecer o ambiente de controle interno e reduzir a exposição da organização aos riscos do negócio. Para tanto, torna-se necessário o envolvimento da alta gestão e de profissionais especializados, com conhecimento e expertise para tratar esta temática (COSO, 2004).

Quando se aborda a temática de gestão de riscos, deve-se destacar, concomitantemente, a função que a auditoria independente possui nestes processos, tendo em vista que, para uma implementação completa em programas de LGPD, muitas premissas, como o seguimento de um programa de controle de dados e a

adoção de ferramentas de controle adequadas, são necessárias para a identificação de lacunas e eventos que representam riscos para o negócio. Esta é uma das atribuições da auditoria, identificadas na literatura (BYRNES et al., 2018).

De maneira prática, como disposto na Lei nº 13.709/2018 (LGPD), em seu artigo 5º, inciso XVII, a exigência e grau de importância de que o risco seja gerenciado, tendo seu detalhamento exposto no denominado Relatório de Impacto à Proteção de Dados Pessoais (RIPD), é uma exigência legal aplicada às organizações. Conforme esta norma, a:

> "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 (BRASIL, 2018)", devem ser asseguradas pelo responsável pelo gerenciamento da informação.

Sendo assim, nota-se que a gestão de riscos em LGPD nada mais é do que um dos processos de gestão instituído, que está dentro de um cronograma completo de programas de LGPD, que é utilizado para proteger os dados manuseados na organização. Deste modo, a acurácia de tal sistema de controle pode ser aferida e seus benefícios podem ser maximizados se os procedimentos da auditoria independente utilizados para sua avaliação forem capazes de assegurar a efetividade do sistema de controle estabelecido.

É por esta razão que se entende que a auditoria pode contribuir para a efetividade de tais mecanismos de controle, visto que, a *expertise* e os conhecimentos existentes por parte dos auditores, para a estruturação de programas de conformidade legal, são capazes de contribuir para o gerenciamento adequado das informações processadas pelas empresas.

2.3 AUDITORIA E PROGRAMA DE TRABALHO

A auditoria se apresenta como um instrumento relevante para aumentar o grau de confiança das informações elaboradas e divulgadas pelas organizações. De acordo com Crepaldi (2019, p. 4), isto ocorre porque a auditoria, "valendo-se de normas e padrões de natureza técnica e ética claramente determinados, [...] torna-se elemento fundamental no sistema de informações, medição de desempenho e

prestação de contas da administração". Portanto, sua atuação agrega valor às empresas.

Além disso, percebe-se a importância da auditoria, pois ela é capaz de perpassar diversas etapas do processo de gestão empresarial, que vai desde seus processos operacionais e de mensuração de resultados, até a divulgação destes para terceiros e as partes interessadas. Em conformidade a este contexto, visualiza-se também a definição de asseguração apresentada na NBC TA 00, que versa sobre a Estrutura Conceitual para Trabalhos de Asseguração. Segundo esta norma, o:

> trabalho de asseguração é o trabalho no qual o auditor independente visa obter evidências apropriadas e suficientes para expressar sua conclusão, de forma a aumentar o grau de confiança dos usuários previstos sobre o resultado da mensuração ou avaliação do objeto, de acordo com os critérios que sejam aplicáveis.

Observa-se no conceito apresentado, a importante função da auditoria que consiste em aumentar o grau de confiança dos usuários. Importante destacar que a auditoria em momento algum proporciona segurança absoluta aos diferentes usuários das informações contábeis utilizadas pela organização. Busca assegurar um grau de segurança que seja aceitável aos seus diferentes *stakeholders* (CREPALDI, 2019).

Este fato reforça a atual importância da auditoria, onde os auditores não podem garantir que os relatórios divulgados pelas organizações estejam completamente livres de distorções. Contudo, espera-se que estes profissionais utilizem integralmente as normas de auditoria e que possuam conhecimento necessário ao aplicar procedimentos razoáveis, capaz de lhes proporcionar um grau de conforto ao opinar sobre as informações contábeis e financeiras (VOLAREVIĆ; VAROVIĆE, 2018).

Outro aspecto observado nas orientações apresentadas pela NBC TA 00 está relacionado a utilização do termo de asseguração para se referir a auditoria. Segundo a norma, no trabalho de asseguração razoável, o auditor independente reduz o risco do trabalho para um nível aceitavelmente baixo, nas circunstâncias do trabalho como base para a sua conclusão. Assim, ao reduzir o risco do trabalho a um nível aceitavelmente baixo, a asseguração razoável passa a se configurar como um trabalho de auditoria, onde o auditor emite uma opinião positiva. Por esta razão, a importância da emissão de seu parecer aos diferentes usuários de tais informações (CREPALDI, 2019).

Em contextos de auditoria, a NBC TA 00 também apresenta o termo asseguração limitada, a qual o auditor independente reduz o risco do trabalho para um nível que é aceitável, mas que ainda é maior do que para um trabalho de asseguração razoável. No entanto, a asseguração limitada não se configura em um trabalho de auditoria, mas tão somente de revisão, onde é emitida uma opinião negativa. O Quadro 1 apresenta as principais diferenças entre ambos os aspectos.

QUADRO 1 – Comparativo entre asseguração razoável e limitada

Tipo de Asseguração	Classificação	Risco	Opinião
Razoável	Auditoria	Aceitavelmente Baixo	Positiva
Limitada	Revisão	Aceitável nas Circunstâncias do Trabalho	Negativa

Fonte: Elaborado pelo autor, baseado na NBC TA 00 (2023).

Como pode-se verificar, o trabalho do auditor é desenvolvido visando assegurar condições para que este possa emitir uma opinião favorável das informações analisadas, visto que, por meio desta, torna-se possível assegurar, em um nível de riscos relativamente baixo, a possibilidade de que problemas não identificados possam resultar em distorções destas informações. Portanto, quando da realização da auditoria e da emissão de opinião positiva, este profissional estará assegurando, em alguma medida, que os itens avaliados apresentam riscos aceitáveis (baixos).

De modo geral, os serviços de auditoria podem ser desenvolvidos em nível interno (auditor interno) e externo (auditor independente). Este trabalho enfatiza os papéis de trabalho e as contribuições do auditor independente, nos processos de gestão de riscos de programas de proteção de dados. Assim, torna-se importante compreender as principais diferenças entre ambos os tipos de auditoria, seja interna ou externa (LINS, 2017). O Quadro 2 apresenta um comparativo entre auditoria externa e interna, destacando suas principais diferenças.

QUADRO 2 – Comparativo entre auditoria externa e a interna

ELEMENTOS	AUDITORIA EXTERNA	AUDITORIA INTERNA
SUJEITO	Profissional Independente	Profissional Interno
AÇÃO E OBJETO	Exame das demonstrações financeiras	Exame dos controles operacionais
FINALIDADE	Expressar uma opinião e assegurar a veracidade das demonstrações financeiras	Promover melhorias nos controles operacionais
RELATÓRIO PRINCIPAL	Relatório da Auditoria	Recomendações de controle interno e eficiência administrativa
GRAU DE INDEPENDÊNCIA	Mais amplo	Menos amplo
INTERESSADOS NO TRABALHO	A empresa e público em geral (terceiros)	A empresa
RESPONSABILIDADE	Profissional, civil e criminal	Trabalhista
NÚMERO DE ÁREAS COBERTAS PELO EXAME DURANTE UM PERÍODO	Maior	Menor
INTENSIDADE DOS TRABALHOS EM CADA ÁREA	Menor	Maior
CONTINUIDADE DO TRABALHO	Periódico	Contínuo

Fonte: Adaptado de Crepaldi (2019).

Com base no Quadro 2 apresentado, evidenciam-se várias diferenças entre os dois tipos de auditoria, sendo que cabe destacar que uma das principais que demarcam a atuação dos profissionais da auditoria no âmbito interno e externo, refere-se à independência do auditor. Esta característica pode ser explicada pelo fato de que a independência do auditor pode ser afetada com base na natureza da relação entre a empresa auditada e seu auditor (RAMZAN; AHMED; RAFAY, 2020).

No caso da auditoria externa, foco desta pesquisa, esta relação não possui vínculo de dependência empregatícia, fato que, de modo geral, acontece na relação entre o auditor e a auditada em trabalhos de auditora interna, reforçando o impacto da natureza da relação na independência do auditor (RAMZAN; AHMED; RAFAY, 2020). Por esta razão, como proposto para a realização desta pesquisa, busca-se identificar, sob a perspectiva da auditoria externa (ou independente), a avaliação da gestão de riscos de LGPD das organizações estudadas, assumindo-se a premissa de que sua

atuação pode contribuir para a melhoria dos processos de gestão destas empresas, com vistas a redução da exposição da organização a tais riscos.

2.3.1 Planejamento de Auditoria

Para tanto, é necessário que o auditor seja capaz de definir adequadamente os principais temas relacionados à execução de um trabalho de auditoria a ser realizado. No caso proposto, um programa de auditoria em proteção de dados, um dos aspectos observados neste trabalho. Conforme explica Crepaldi (2019), a execução da auditoria passa, inicialmente, pela elaboração de um planejamento adequado, ou seja, a definição de uma estratégia de trabalho.

Crepaldi (2019) explica que, o planejamento da auditoria envolve a definição de estratégia global para o trabalho e o desenvolvimento de plano de auditoria. Nesta mesma linha, a NBC TA 300 apresenta a definição de que um planejamento adequado é benéfico para a auditoria de várias maneiras, inclusive para:

> - auxiliar o auditor a dedicar atenção apropriada às áreas importantes da auditoria;
> - auxiliar o auditor a identificar e resolver tempestivamente problemas potenciais;
> - auxiliar o auditor a organizar adequadamente o trabalho de auditoria para que seja realizado de forma eficaz e eficiente;
> - auxiliar na seleção dos membros da equipe de trabalho com níveis apropriados de capacidade e competência para responderem aos riscos esperados e na alocação apropriada de tarefas;
> - facilitar a direção e a supervisão dos membros da equipe de trabalho e a revisão do seu trabalho;
> - auxiliar, se for o caso, na coordenação do trabalho realizado por outros auditores e especialistas.

Ademais, no que tange às premissas relacionadas ao planejamento da auditoria, Oliveira (2015, p. 44-45) afirma que:

> o planejamento pode ser considerado como um guia no processo de auditoria, cujo objetivo é facilitar as ações posteriores, para que transcorra de maneira certa e sem maiores transtornos, uma vez que o auditor terá de maneira antecipada a descrição dos passos vindouros, uma vez que terá conhecimento dos passos a serem executados.

Assim sendo, evidencia-se a importância do planejamento da auditoria, tendo em vista sua característica de nortear os trabalhos desde sua etapa preliminar até a

elaboração do relatório final com a opinião do auditor. Portanto, deve ser elaborado, como ponto de partida para a execução do trabalho a ser realizado.

2.3.2 Programa da Auditoria

Após a definição da estratégia de auditoria, torna-se necessária a elaboração do programa de trabalho, onde deverão constar as formas de execução do planejamento. No entendimento de Attie (2018, p. 294), o programa de auditoria é o "plano de ação voltado para orientar e controlar a execução dos exames de auditoria e sua aplicação", o qual pode apresentar as seguintes vantagens:

> • estabelecer a forma adequada de realização dos trabalhos;
> • as considerações feitas pelo auditor para a determinação de seu trabalho;
> • controlar o tempo despendido na realização do trabalho;
> • a sequência lógica de realização do trabalho; e
> • evidência dos trabalhos e quaisquer modificações ocorridas em relação ao original (ATTIE, 2018, p. 294).

O programa de auditoria, também conhecido como plano de auditoria, demonstra as características da organização do trabalho de auditoria, bem como seus controles e registro dos resultados da aplicação dos procedimentos. Este fato demonstra que o plano é mais detalhado que o planejamento, visto que os aspectos como natureza, época e extensão dos procedimentos de auditoria são minuciosamente descritos nesse documento (RIBEIRO; RIBEIRO, 2017).

Do mesmo modo, outro aspecto importante a ser observado é que o programa de auditoria também contribui para a delegação das atividades para a equipe de trabalho, pois ao determinar os procedimentos aplicáveis ao trabalho a ser realizado, pode-se indicar o número de horas e os membros da equipe que serão responsáveis pela aplicação destes procedimentos. Desta forma, torna-se possível organizar as atividades a serem executadas e definir a força de trabalho e atribuições necessárias designadas a cada membro da equipe de auditores envolvidos.

2.3.3 Procedimentos de Auditoria

Após a análise do programa de auditoria, são definidos os procedimentos de auditoria a serem adotados no trabalho a ser realizado. Neste caso, observa-se que no documento elaborado (programa de auditoria), já constam os procedimentos de auditoria que serão aplicados para execução do trabalho. Assim sendo, com base na NBC TA 00, verifica-se que ao desenvolver o programa de auditoria, os procedimentos a serem adotados devem ser determinados conforme: a natureza, época e da extensão, bem como dependem do julgamento profissional do auditor, os quais podem variar de um serviço para outro.

Conforme explica Crepaldi (2019, p. 218):

> Os procedimentos de auditoria são técnicas para obtenção de evidências suficientes e adequadas para fundamentação da opinião. Abrangem testes de observância e substantivos. São o conjunto de técnicas que permitem ao auditor obter evidências ou provas suficientes e adequadas para fundamentar sua opinião sobre as demonstrações contábeis auditadas e abrangem os testes de observância e os testes substantivos.

Os procedimentos contextualizados acima configuram-se em uma vasta lista de ações aplicadas pelos auditores, com vistas a obter evidencias para a formação de sua opinião. Como exemplos de procedimentos a serem adotados, destacam-se os apresentados por Alves (2017, p. 102), sendo estes: “exame físico, confirmação, documentos originais, cálculos, escrituração, investigação, inquérito, registro auxiliares, correlação e observação”.

A NBC TA 00 (p. 18), estabelece que a combinação de procedimentos é tipicamente utilizada para obter tanto a asseguração razoável como a asseguração limitada e pode incluir: “inspeção; observação; confirmação; recálculo; reexecução; procedimentos analíticos e indagação”. Com base nas constatações que envolvem os procedimentos de auditoria é possível identificar que estes se configuram como as ferramentas necessárias à execução da auditoria os quais devem estar presentes no processo de planejamento dos trabalhos e descritos no programa de auditora.

2.3.4 Matriz de probabilidade x impacto no âmbito da auditoria

Por fim, quando da realização da auditoria e da avaliação dos riscos a que a organização está exposta, torna-se necessário promover sua valoração. Desta forma, a utilização da auditoria em ambientes de gestão de riscos, encontra suporte em sua própria estruturação, pois, dentre suas etapas, observa-se que a realização da auditoria passa pela avaliação dos riscos, determinação de escopo e objetivos, culminando com a construção de um plano de auditoria, capaz de quantificar a exposição da organização a estes eventos (BYRNES et al., 2018).

Neste sentido, este processo de avaliação de riscos previsto na auditoria pode ser materializado por meio da aplicação da matriz de probabilidade e impacto, a qual constitui-se uma prática de gestão que permite avaliar o efeito da ocorrência de determinado evento nas operações desenvolvidas pela empresa (OLIVEIRA JÚNIOR; GOMES; VASCONCELLOS MACHADO, 2015).

No que tange as particularidades da matriz de probabilidade x impacto, ressalta-se como ponto principal o seu objetivo, o qual se concentra na obtenção do grau de exposição do risco identificado. Esta avaliação é realizada por meio da identificação do produto resultante da observação entre probabilidade (P) de ocorrência e impacto (I), ou seja, GE (Grau de Exposição) = P (Probabilidade) x I (Impacto) (GAUDÊNCIO; SCHRAMM; SILVA, 2019).

Segundo Gaudêncio, Schramm e Silva (2019), a importância do entendimento da correlação entre estas duas variáveis (P e I) está na compreensão da classificação dos riscos com maior grau de confiabilidade e precisão, tendo em vista que este fato se aplica ao caso em que, geralmente, os gestores realizam uma análise intuitiva do risco, que conta apenas com uma perspectiva unilateral (apenas probabilidade ou apenas o impacto da ocorrência do risco identificado). Desta forma, torna-se possível apurar, com maior acurácia, a severidade deste evento.

Neste contexto, verifica-se que a matriz de risco é uma ferramenta eficiente utilizada amplamente para classificar e mensurar riscos de processos, determinando as prioridades de tratamento destes, sempre com o foco de contribuir para o processo de tomada de decisão (BAYBUTT, 2018). Portanto, as características de avaliação (probabilidade e impacto) analisadas na matriz de risco demonstram sua aderência às etapas de execução da auditoria, em especial àquela ligada a avaliação dos riscos, visto que o conjunto de exposições identificados precisam ser adequadamente

mensurados para que a organização possa avaliar se estes devem ser tratados e como proceder para mitigá-los.

Diante do exposto, considerando a importância do tema e o potencial de contribuição da auditoria independente na avaliação dos processos de gestão de riscos em LGPD, busca-se, com a execução desta pesquisa, a partir da realização de um estudo de múltiplos casos, demonstrar como a auditoria independente pode contribuir com os processos de gestão de riscos ligados à LGPD, motivação pela qual se propõe a realização deste estudo.

3 MÉTODO E PROCEDIMENTOS DA PESQUISA

Esta seção apresenta os procedimentos metodológicos definidos para a realização desta pesquisa. Em um primeiro momento, por meio do delineamento da pesquisa, busca-se caracterizá-la, levando-se em consideração suas tipologias específicas. Na sequência, são determinados os casos selecionados para a realização do estudo, bem como os sujeitos envolvidos e o constructo da pesquisa. Por fim, evidenciam-se os procedimentos de coleta e análise de dados e as limitações do trabalho.

3.1 DELINEAMENTO DA PESQUISA

Considerando os objetivos da pesquisa, essa se caracteriza como descritiva, pois o estudo considerou, para atingir seus objetivos, a descrição resultante da análise de dados de casos reais, relacionados ao tema central investigado no estudo. Conforme Gil (2008, p. 42), “as pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis”.

Quanto aos procedimentos observados, o trabalho se caracteriza como um estudo de casos múltiplo, realizado por meio de análise documental, entrevistas e visitação com observação *in loco*. No seu primeiro aspecto, trata-se como um estudo de casos múltiplos, pois são analisados dados provenientes de casos de 3 (três) empresas diferentes, o que possibilita uma abrangência maior para a análise de questões comuns observadas diante dos resultados individuais.

Yin (2010) entende que o estudo de caso se constitui um método de investigação adequado, quando se busca observar em um estudo de um ou mais casos, no momento em que um fenômeno contemporâneo acontece e dentro da lógica do seu ambiente, como sua incidência ocorre. No caso proposto, os procedimentos de um programa de proteção de dados relacionados a aplicação da LGPD.

Quanto a abordagem da pesquisa, essa se classifica como qualitativa, haja vista que neste tipo de pesquisa, as análises no que se refere ao conteúdo tratado, são mais aprofundadas e específicas, fato considerado inerente ao estudo proposto. Evidencia-se que este tipo de análise objetiva entender com maior precisão pontos e detalhamentos que um estudo denominado quantitativo não aborda, considerando

seu teor mais superficial (RAUPP; BEUREN, 2006). Para sua interpretação, utilizou-se da análise de conteúdo, como proposto por Bardin (2016). Segundo a autora, “a análise do conteúdo é um conjunto de instrumentos metodológicos em constante aperfeiçoamento, que se aplicam a discursos (conteúdos e continentes) extremamente diversificados” (BARDIN, 2016, p. 15).

As fontes de coleta de dados utilizadas nesta pesquisa são análise documental, entrevistas e visitação com observação *in loco*. Quanto ao aspecto documental, utiliza-se tal fundamento no intuito de atingir os objetivos específicos estabelecidos pelo estudo, uma vez que as análises realizadas por meio de estudos de casos requerem a observância de múltiplas fontes de evidências, como a análise de documentos, a observação direta *in loco* e a realização de entrevistas. Deste modo, mediante as etapas de coleta e análises dos dados e resultados encontrados, será possível demonstrar quais são as contribuições da auditoria independente para o fortalecimento dos processos de gestão de riscos, de acordo com a LGPD.

Os dados coletados e documentos analisados referem-se a registros, documentos internos, relatórios gerenciais e práticas instituídas na organização em estudo. As entrevistas realizadas, de maneira não estruturada, visaram coletar informações para que fosse possível confirmar se as recomendações da LGPD estavam sendo observadas, bem como para identificar quais fragilidades existem no ambiente de controle interno da organização, relacionadas a esta temática. Uma síntese das principais questões utilizadas é apresentada no Roteiro de Entrevistas elaborado e anexo a este trabalho.

Do mesmo modo, as observações *in loco* permitiram confirmar tais apontamentos, identificados, de maneira particular, em cada ambiente (caso analisado). Assim, diante deste conjunto de procedimentos adotados, tem-se maior consistência na avaliação realizada, de modo que se possa emitir uma opinião adequada sobre os níveis de exposição da organização, aos possíveis riscos identificados no trabalho realizado.

3.2 SELEÇÃO DOS CASOS E SUJEITOS DA PESQUISA

Para a realização deste trabalho, inicialmente identificou-se na cidade de Santa Maria/RS, uma empresa de auditoria que houvesse realizado trabalhos específicos

em programa de LGPD. Assim, foram analisados os sítios da *internet* de empresas de auditoria desta cidade.

Como critérios de seleção para a definição de uma organização, foram selecionadas empresas que possuem registro na CVM (Comissão de Valores Mobiliários), haja vista que este registro demonstra o grau de maturidade e qualidade dos serviços prestados por estas empresas. O resultado da pesquisa realizada apontou para duas organizações com estas características.

Em seguida, ao selecionar essas duas empresas, foi possível verificar que somente uma destas executa trabalhos ligados à LGPD, fato este que motivou um contato inicial com uma das diretoras da empresa, por meio do e-mail divulgado no sitio institucional da organização. Após dois dias, a empresa retornou e aceitou se reunir com o pesquisador, gerando a apresentação dos propósitos da pesquisa e as demandas necessárias para sua execução.

De posse do esclarecimento de dúvidas apresentadas, relacionadas aos procedimentos éticos a serem adotados (apresentados no Termo de Consentimento Livre e Esclarecido e no Termo de Confidencialidade elaborados e anexados a este trabalho), para que se possa manter a confidencialidade dos dados a serem acessados e analisados, obteve-se a aceitação por parte da empresa de auditoria para a realização desta pesquisa. Do mesmo modo, recebeu-se a indicação de alguns dos trabalhos realizados recentemente, com aplicação de programas de LGPD, para que se possa avaliar os mais adequados aos propósitos deste trabalho. Assim, foram selecionados 3 (três) diferentes casos, sob a condição de que nenhum nome das empresas envolvidas fosse divulgado no trabalho.

Após as reuniões iniciais realizadas com os responsáveis pela empresa de auditoria, foram solicitados os papéis de trabalho dos referidos serviços, de modo que fosse possível analisar tais documentos. Os papéis de trabalho analisados estão relacionados a três trabalhos que foram executados em empresas que possuíam prazo de implementação de programas de LGPD semelhantes. Por esta razão, apresentam um contexto adequado para a realização de inferências relacionadas a resposta aos objetivos desta pesquisa.

Em seguida, após acessar os documentos solicitados, o pesquisador verificou que os três trabalhos estavam aptos a serem objeto de pesquisa, haja vista que a partir destes, é possível aplicar o mesmo método proposto pela pesquisa, bem como

todos tinham o mesmo escopo de trabalho e seus prazos de implementação estavam alinhados.

Os sujeitos envolvidos na pesquisa, além do próprio pesquisador, foram os auditores que realizaram as auditorias disponibilizadas para a pesquisa, os quais, por meio de entrevistas informais, não estruturadas, forneceram detalhes sobre o planejamento, procedimentos e a execução dos serviços de auditoria. Também, estes mesmos profissionais viabilizaram o acesso ao sistema de auditoria da empresa, para que o pesquisador pudesse observar o conjunto dos trabalhos realizados nas três organizações analisadas.

Adicionalmente, procedeu-se ainda a investigação *in loco* das soluções implementadas. Neste momento, foi possível acompanhar e dirimir dúvidas sobre o processo de planejamento e execução da auditoria realizada, assim como da elaboração e aplicação do programa de proteção de dados em LGPD e da exposição destas organizações aos riscos identificados.

3.3 CONSTRUCTO DA PESQUISA E UNIDADES DE ANÁLISE

Diante dos propósitos deste estudo, os constructos da pesquisa e unidades de análise definidos para a realização deste trabalho são apresentados no Quadro 3.

QUADRO 3 – Constructos da pesquisa e unidades de análise

Constructos da Pesquisa	**Definição Operacional**	**Unidade de Análise**
Programa de Auditoria	Refere-se ao programa de trabalho elaborado para a auditoria realizada com o objetivo de identificar a qualidade e eficácia dos programas de proteção de dados em LGPD avaliados.	- Planejamento de auditoria em LGPD; - Procedimentos de auditoria em LGPD.
Identificação de Riscos de Infração à LGPD	Refere-se a identificação e análise de eventos que representam riscos ao cumprimento das normas estabelecidas pela LGPD para a estruturação de programas de proteção de dados.	- Identificação de eventos que representam riscos à LGPD; - Avaliação dos eventos que representam riscos à LGPD.
Avaliação de Riscos de Infração à LGPD e definição de planos de ação	Refere-se a identificação de respostas aos eventos identificados como fontes de riscos a proteção de dados, que permitem a elaboração de um plano de ação para mitigação de sua ocorrência.	- Identificação de alternativas de resposta aos eventos que representam riscos à LGPD; - Elaboração de plano de ações para resposta aos eventos que representam riscos à LGPD.

Fonte: Elaborado pelo autor (2023).

Parte-se da avaliação inicial do programa de auditoria elaborado, bem como a identificação de sua adequação, considerando seu propósito de inferir sobre a qualidade e eficácia dos programas de proteção de dados em LGPD avaliados. Neste caso, constituem-se as principais unidades de análise descritas neste programa: o planejamento das atividades e os procedimentos de auditoria adotados.

Decorrente de sua aplicação, a seguir avalia-se o conjunto de eventos identificados e classificados como potenciais riscos de infração à LGPD. As unidades de análise deste item referem-se à identificação e análise de eventos que representam riscos ao cumprimento das normas estabelecidas pela LGPD para a estruturação de programas de proteção de dados.

Assim, ao final desta avaliação, torna-se possível estabelecer os planos de ação (terceira unidade de análise), caracterizados como as respostas definidas (e recomendadas) pelo auditor, como possíveis soluções a serem implementadas, para a redução de exposição da organização aos riscos identificados.

3.4 PROCEDIMENTOS DE COLETA DOS DADOS

Inicialmente, conforme as descrições observadas no capítulo referente a seleção dos casos e unidades de análise, foi selecionada a empresa de auditoria a qual foi a responsável pela disponibilização dos três casos analisados ao longo do trabalho realizado. Destaca-se que, desde a escolha da empresa de auditoria responsável pelos trabalhos até a finalização da análise por parte do pesquisador, foram adotados todos os procedimentos éticos de pesquisa, necessários a assegurar o anonimato da identificação dos participantes e dados analisados.

Assim, foram estabelecidos como procedimentos éticos para esta pesquisa: a) não identificação do participante da pesquisa; b) a não identificação da organização em que atua; c) o tratamento consolidado dos dados; d) a possibilidade de desistência de participar da pesquisa a qualquer momento, sem a necessidade de apresentação de qualquer justificativa; e, e) o uso dos dados coletados para fins de elaboração deste trabalho e a produção de artigos derivados.

Mediante esta definição inicial, buscou-se promover a coleta de dados a partir de múltiplas fontes de evidências, como a análise de documentos disponibilizados pela organização (registros, documentos internos, relatórios gerenciais, programa de auditoria e práticas instituídas na organização em estudo), além de entrevistas não

estruturadas realizadas com os auditores responsáveis pela execução dos trabalhos de LGPD (3 profissionais). Adicionalmente, procedeu-se observações *in loco*, a fim de que fosse possível confirmar tais apontamentos, identificados de maneira particular em cada ambiente (caso analisado), bem como esclarecer eventuais dúvidas sobre os dados analisados.

O período de coleta de dados compreendeu os meses de setembro a dezembro de 2022. A partir utilização deste conjunto de procedimentos adotados, foi possível uma compreensão completa e adequada de informações necessárias a realização desta pesquisa, de modo que fosse possível a apresentação de inferências e conclusões sobre os propósitos deste trabalho.

3.5 PROCEDIMENTOS DE ANÁLISE DOS DADOS

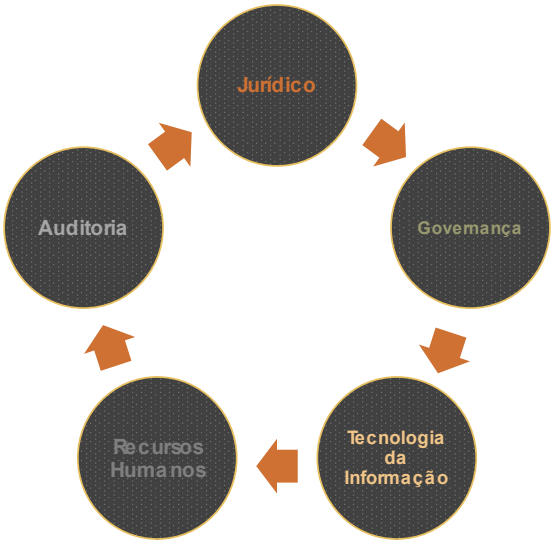
No que se refere aos procedimentos de análise, os dados coletados foram analisados por meio de uma abordagem qualitativa, mediante a análise do seu conteúdo e significado. De a cordo com Bardin (2016, p. 42), a análise de conteúdo consiste em:

> [...] um conjunto de técnicas de análise das comunicações visando obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) destas mensagens.

Para tanto, foram observadas as três etapas da técnica de análise de conteúdo recomendada por Bardin (2016), sendo estas: (1) pré-análise; (2) exploração do material e tratamento dos resultados; e, (3) inferência e a interpretação. Desta forma, sob uma visão geral, a análise dos dados teve início no primeiro momento do acesso aos documentos disponibilizados pela empresa de auditoria. A seguir, para que as informações acessadas pelo pesquisador pudessem ser delimitadas e ajustadas aos moldes do tema proposto, buscou-se identificar as áreas utilizadas pelos auditores, no momento da execução do programa de proteção de dados. Por fim, inferiu-se sobre as exposições identificadas nos casos analisados, bem como a forma de tratamento recomendada a estes eventos.

As áreas consideradas pelos auditores para a elaboração do programa de auditoria e a determinação dos procedimentos de auditoria a serem adotados nos trabalhos realizados são apresentadas na Figura 2.

FIGURA 2 - Áreas consideradas para planejamento e para os procedimentos



Fonte: Elaborado pelo autor (2023).

De posse desta definição, na sequência foi realizado um estudo cruzado, onde foi identificada a justificativa e fundamentação legal para a avaliação dos riscos em programas de proteção de dados, com base no disposto pela Lei nº 13.709/2018 (LGPD). A síntese dos apontamentos realizados é apresentada no Quadro 4.

QUADRO 4 – Cruzamento entre áreas e seus fundamentos legais

Áreas	**Fundamento Legal na Lei 13.709/2018 (LGPD)**
Jurídico	Artigo 7º, Inciso I; Artigo 7º, Inciso V; Artigo 42º
Governança	Artigo 50º, § 2º, Inciso I
Tecnologia da informação (TI)	Artigo 1º
Recursos Humanos (RH)	Artigo 6º
Auditoria	Artigo 46º

Fonte: Elaborado pelo autor (2023).

De posse destas informações, para a execução da pesquisa, foram utilizados os planejamentos e procedimentos de auditoria padronizados pelos auditores e

utilizados nos três trabalhos de auditoria estudados. Com vistas a demonstrar os resultados extraídos dos papéis de trabalho disponibilizados pelos auditores, foi elaborado um Quadro (5) demonstrativo, composto de uma coluna com as informações relacionadas ao planejamento da auditoria, outra coluna com a especificação da área a ser auditada, e, por fim, uma coluna com a descrição dos procedimentos de auditoria previstos pelos auditores, para cada atividade a ser realizada. O Quadro 5 apresenta a síntese destas informações.

QUADRO 5 - Planejamentos e procedimentos de auditoria

Código	Planejamento	Área	Procedimentos
1.1	Auditar os Testes de intrusão em sistemas e redes *(pentest)*	Tecnologia da Informação	**Inspecionar** os relatórios técnicos de teste de vulnerabilidades realizado pelo profissional de segurança da informação
1.2	Adequar juridicamente, com base na LGPD, os contratos ativos	Jurídico	**Inspecionar** as cláusulas dos contratos selecionados
1.3	Identificar os riscos operacionais	Auditoria e Governança	**Indagar** gerentes e colaboradores a respeito das práticas do seu cotidiano que envolvam o tratamento de dados pessoais
1.4	Auditar o programa de proteção de dados após sua implementação	Auditoria	**Recalcular** o grau de exposição ao risco após aplicação do plano de ação sugerido
1.5	Analisar os efeitos da implementação do canal de solicitação de dados no *site*	Auditoria e Governança	**Comparar** o efeito/comportamento das solicitações de dados antes e depois da implementação do mesmo
1.6	Analisar as políticas de privacidade e proteção de dados	Auditoria e Governança	**Inspecionar** se as políticas de privacidade estão de acordo com os princípios básicos de proteção de dados
1.7	Verificar o nível de adequação à LGPD da rede de prestadores de serviços e fornecedores por meio do manual *Due Diligence*	Auditoria e Governança	**Confirmar** com terceiros (operadores dos dados) de que estes possuem requisitos básicos de segurança para tratar os dados do controlador de maneira legítima
1.8	Adequar e formalizar às condutas internas, a serem	Recursos Humanos	**Reexecutar** os princípios evidenciados no manual de conduta, a fim de que

	adotadas pelos colaboradores, com os devidos princípios de proteção de dados		estes estejam, concomitantemente, de acordo com a LGPD e com os processos específicos da empresa

Fonte: Elaborado pelo autor (2023).

Quanto aos procedimentos de auditoria, verificou-se que os auditores consideraram os constantes na NBC TA 00, ou seja, inspeção; observação; confirmação; recálculo; reexecução; procedimentos analíticos; e, indagação. Deste modo, o plano de auditoria elaborado mostra-se adequado para a realização dos testes necessários, sendo possível a identificação dos níveis de exposição destas organizações (os três casos analisados), a riscos existentes em seus programas de proteção de dados em LGPD.

3.6 LIMITAÇÕES DA PESQUISA

Esta pesquisa apresenta algumas limitações que não permitem a generalização de seus resultados. Inicialmente, trata-se de um estudo de casos (três), portanto, representa observações em particular do contexto analisado. Do mesmo modo, está sujeito a interpretações e percepções dos auditores e delineadores do programa de proteção de dados. Assim, em outros contextos analisados, tais fatores podem fornecer evidências de outros fatores de influência da gestão de riscos em programas de LGPD.

Do mesmo modo, esta pesquisa avaliou um programa em específico, adequado a um conjunto de cinco componentes de análise (apresentados no Quadro 5). Desta forma, a avaliação de outros componentes irá resultar em observações distintas e específicas dos níveis de exposição das organizações, a existência de riscos em programas de LGPD. Quanto ao método, há de se considerar que a coleta de dados ocorreu por meio de entrevistas e o relato de percepções, o que também pode representar uma limitação (pelo viés) destes achados.

Contudo, acredita-se que o rigor metodológico adotado oferece o suporte necessário para que se possa apresentar observações e conclusões sobre a pesquisa realizada. Os resultados encontrados, são apresentados a seguir.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Nesta seção são apresentados os resultados da pesquisa, com base nos objetivos delimitados para a realização deste trabalho. Primeiramente, será apresentado uma breve descrição dos três casos auditados. Em seguida, mediante a aplicação do programa de auditoria evidenciado no Quadro 5, procedeu-se a descrição e análise dos planejamentos e procedimentos de auditoria utilizados pelos auditores nos trabalhos realizados, ligados à gestão de riscos em LGPD (primeira contribuição da auditoria independente identificada nesta pesquisa).

De posse destas informações, na sequência, foi identificado os riscos a que as organizações auditadas estão expostas, por meio da aplicação dos planejamentos e procedimentos de auditoria utilizados e a identificação de fragilidades em seu ambiente de controle interno relacionado à gestão de riscos em LGPD (segunda contribuição da auditoria independente identificada neste estudo). Por fim, avaliou-se os riscos de infração relacionados à LGPD, com base nos seus graus de exposição identificados e a análise dos seus planos de ação sugeridos (terceira contribuição da auditoria independente identificada neste trabalho).

4.1 APRESENTAÇÃO DOS CASOS ANALISADOS

A empresa de auditoria contatada para a realização desta pesquisa, foi a Vision Auditoria Ltda., registrada no conselho regional de contabilidade (CRC) e na comissão de valores mobiliários (CVM), localizada na cidade de Santa Maria RS.

Fundada no ano de 1995, possui 28 anos de atuação no mercado, sendo que nos cinco primeiros anos teve uma atividade regionalizada. A partir do ano de 2001 passou para uma expansão nacional, atuando nos estados do: Rio Grande do Sul, Santa Catarina, Paraná, São Paulo, Rio de Janeiro, Minas Gerais, Mato Grosso, Mato Grosso do Sul, Bahia, Piauí, Tocantins, Maranhão, Pará, Rondônia e Distrito Federal, totalizando 14 Estados atendidos e o Distrito Federal.

Atualmente a organização desenvolve trabalhos de auditoria independente nas áreas contábil, operacional, *compliance* e LGPD, além de auditoria interna e *due diligence*. Ainda, realiza trabalhos de consultoria em temas ligados à área de governança, tributária, laudos de PPA (*price purchase alocation*) e avaliação de empresas (*valuation*).

Para execução da pesquisa e aplicação da metodologia proposta, foram utilizados três trabalhos de auditoria em LGPD, realizados pela empresa de auditoria. O primeiro trabalho se refere a uma auditoria realizada no programa de LGPD de uma concessionária de máquinas agrícolas, fundada ha mais de 45 anos, com matriz localizada no estado do Maranhão, a qual havia implementado o programa de proteção de dados há 14 meses.

O segundo trabalho analisado se refere a uma auditoria realizada no programa de LGPD de uma indústria de produtos lácteos, fundada ha mais de 20 anos, com matriz localizada no estado do Rio Grande do Sul, a qual havia implementado o programa há 15 meses. Por fim, o terceiro trabalho analisado se refere a uma auditoria realizada no programa de LGPD de um clube social, localizado no estado do Rio Grande do Sul, o qual também havia implementado o seu programa de proteção de dados há 15 meses.

4.2 DESCRIÇÃO DOS PLANEJAMENTOS E PROCEDIMENTOS DE AUDITORIA UTILIZADOS PELOS AUDITORES NOS TRABALHOS LIGADOS À GESTÃO DE RISCOS EM LGPD

Para responder ao primeiro objetivo específico estabelecido para esta pesquisa, por meio da análise de conteúdo, foi realizada uma análise descritiva dos planejamentos e procedimentos de auditoria utilizados pelos auditores para a execução dos trabalhos realizados nas três empresas estudadas.

Observou-se que os auditores aplicaram o mesmo planejamento e procedimentos de auditoria elaborados para as três empresas analisadas, os quais estão apresentados no Quadro 5 (no capítulo da metodologia, na seção de descrição dos procedimentos de análise dos dados). Durante as entrevistas realizadas, os auditores justificaram que aplicaram o mesmo modelo para as empresas auditadas, pelo fato de que estas encontravam-se em estágio semelhante quanto ao prazo de implementação do seu programa de proteção de dados (entre 14 e 15 meses). Sendo assim, torna-se adequado seu uso para a análise e observações realizadas sobre a eficácia do programa de proteção de dados elaborado.

De acordo com o plano de trabalho elaborado, na primeira análise realizada (descrita no código 1.1), foram definidos, no planejamento de auditoria, a necessidade de realização dos testes de intrusão em sistemas e redes. Estes testes são realizados

por meio de procedimentos que visam inspecionar os relatórios técnicos de teste de vulnerabilidades, os quais, geralmente, são realizados nestas organizações pelos profissionais de segurança da informação.

Na segunda análise realizada (descrita no código 1.2), procedeu-se a avaliação da adequação jurídica dos contratos ativos firmados por estas organizações, com colaboradores, prestadores de serviço, fornecedores e clientes. Neste momento, buscou-se inspecionar a estrutura formalizada de cada um destes documentos, de modo a se verificar eventual ausência de cláusulas de proteção de dados específicas às finalidades individuais.

Concluída esta avaliação, a seguir foi realizada a identificação dos riscos operacionais de cada um dos negócios (como descrito no código 1.3). Para tanto, são analisados os resultados de entrevistas executadas pelos auditores com os gerentes e colaboradores da empresa, a respeito das práticas de gestão adotadas em seu cotidiano que envolvam o tratamento de dados pessoais.

O quarto item avaliado (descrito no código 1.4), consistiu na realização da auditoria do programa de proteção de dados adotado, após sua efetiva implementação em cada um dos casos analisados. Neste momento, torna-se possível executar a revisão do programa de proteção de dados no que tange a identificação e análise dos aspectos que apresentam eventuais fragilidades e implicam na identificação de riscos. É nesta etapa que são calculados os níveis (grau) de exposição ao risco, tornando possível identificar o conjunto de alternativas existentes para sua mitigação, as quais, são consideradas para a elaboração do plano de ação sugerido.

A quinta avaliação realizada (descrita no código 1.5), consiste na análise dos efeitos da implementação do canal de privacidade, destinado aos titulares de dados (pessoas físicas) que possuem relações com a empresa. Neste momento, são comparados os efeitos/comportamento das solicitações de dados antes e depois da implementação deste canal, utilizando os mesmos critérios de determinação de prazos definidos e aplicados para a avaliação do item 1.4, levando-se em consideração a particularidade de cada empresa, seu negócio e seu respectivo programa de LGPD.

Após esta avaliação, torna-se possível avaliar a pertinência e adequação das políticas de privacidade de dados instituídas na organização (código 1.6). Esta análise visa identificar se as orientações institucionais e as práticas de gestão instituídas, estão de acordo com os princípios básicos de proteção de dados recomendados pela

LGPD. Na descrição das políticas de privacidade e proteção de dados apresentadas, leva-se em consideração a estrutura e o conteúdo que este tipo de documento necessita possuir, bem como sua adequação aos itens observados e avaliados como necessários para serem incorporados no referido documento.

Na sétima etapa da avaliação realizada (descrita no código 1.7) busca-se, por meio da aplicação de um manual/questionário (manual de *Due Diligence*), verificar o nível de adequação à LGPD, da rede de prestadores de serviços e fornecedores. A partir desta avaliação, procura-se confirmar com terceiros (os operadores dos dados), se estes possuem os requisitos básicos de segurança para tratar os dados do controlador de maneira segura e legítima.

Por fim, na última etapa da avaliação (apresentada no código 1.8), foi realizado o planejamento de ações visando a adequação e formalização das condutas internas a serem adotadas pelos colaboradores, em virtude de eventuais exposições identificadas. Neste momento, observa-se as fragilidades identificadas e os devidos princípios de proteção de dados recomendados pela LGPD, para que se possam sugerir adequações visando alcançar a conformidade recomendada pela LGPD, diante dos processos específicos desenvolvidos na organização.

Com base nas análises realizadas, nesta etapa da pesquisa, foi possível identificar que o programa de auditoria elaborado para a realização da auditagem dos programas de proteção de dados dos três casos analisados é adequado, estando em conformidade com as normas de auditoria aplicadas (NBC TA 300 e NBC TA 500), bem como as recomendações estabelecidas pela Lei nº 13.709, conhecida como a Lei Geral de Proteção de Dados (LGPD). Estes resultados mostram a importância da organização das atividades por parte do auditor, delimitada, inicialmente, pelo programa de auditoria elaborado e a descrição adequada do planejamento de ações a serem realizadas, assim como os procedimentos recomendados para esta avaliação.

A auditoria permite a avaliação adequada da estrutura de controle da empresa (CREPALDI, 2019). Portanto, atua de maneira preventiva, como um mecanismo de controle que contribui para a eficácia dos mecanismos de controle interno instituídos na organização. É por meio de um planejamento adequado (OLIVEIRA, 2015) que são delimitados os elementos chaves, objeto de avaliação, os quais, a partir da delimitação dos procedimentos mais adequados, serão auditados para aferir sua conformidade legal e operacional (CREPALDI, 2019).

No contexto da LGPD, é possível checar se o conjunto de princípios, a política e os procedimentos de proteção de dados adotados por estas empresas, estão resultando efetivamente na proteção de dados de seus clientes e fornecedores, de modo que a organização possa alcançar a conformidade no tratamento dos dados manuseados. Esta é uma preocupação sobre o tema, destacada em estudos anteriores, como Nakamura, Formigoni Filho e Ide (2019) e Pinheiro (2021), que explicam que, para o êxito no estabelecimento de ações de tratamento de dados pessoais, é necessária a implementação de práticas adequadas de gerenciamento de riscos, que, por meio do plano de auditoria apresentado, é contemplado na etapa de execução deste trabalho, visto que este é um dos elementos de análise (planos de ação) realizados pela auditoria.

Portanto, pode-se inferir que, ao promover esta avaliação, a auditoria contribui para o fortalecimento do ambiente de controle interno destas organizações, assim como para o estabelecimento de um programa eficiente de proteção de dados, capaz de avaliar e delimitar como deve ocorrer o tratamento de exposições que podem representar riscos à organização.

4.3 IDENTIFICAÇÃO DOS RISCOS POR MEIO DA APLICAÇÃO DOS PLANEJAMENTOS E PROCEDIMENTOS DE AUDITORIA

Após a etapa de análise inicial realizada, referente aos planejamentos e procedimentos de auditoria adotados para a avaliação da efetividade dos programas de proteção de dados dos três casos analisados e visando responder ao segundo objetivo específico estabelecido para esta pesquisa, procedeu-se a identificação dos riscos de infração à LGPD a que estas organizações estão expostas.

Para tanto, foram utilizadas as informações coletadas a partir da aplicação das etapas dos planejamentos e procedimentos de auditoria descritos nos códigos: 1.1 (testes de intrusão em sistemas e redes), 1.2 (adequação dos contratos ativos), 1.3 (identificação de riscos operacionais), 1.6 (políticas de privacidade e proteção de dados) e 1.7 (adequação à LGPD da rede de prestadores de serviços e fornecedores) do plano de trabalho elaborado. Os itens descritos nos códigos 1.4 (auditagem do programa de proteção de dados após sua implementação) e 1.5 (efeitos da implementação do canal de solicitação de dados) não permitem a identificação de riscos, haja vista que, mesmo que possuam planejamento e procedimentos

estabelecidos, estes não foram aplicados no momento da execução dos trabalhos de auditoria realizados.

Sendo assim, a partir de tais definições, com base na aplicação dos procedimentos apresentados para cada um destes itens e por meio da inspeção documental dos arquivos digitais das auditorias executadas, foi possível realizar a identificação de riscos de infração à LGPD, a qual cada uma destas organizações está exposta. A síntese dos resultados encontrados é apresentada a seguir.

4.3.1 Identificação de riscos na empresa concessionária de máquinas agrícolas

O Quadro 6 apresenta a síntese dos resultados encontrados para a análise da identificação dos tipos de riscos que a empresa concessionária de máquinas agrícolas está exposta, considerando o seu programa de proteção de dados implementados.

QUADRO 6 – Riscos identificados na empresa concessionária de máquinas agrícolas

(continua)

Código	Resultados	Riscos	Categoria do risco
1.1	Protocolo/Serviço: *OpenSSH* 6.6.1; Porta: 22; A versão utilizada do *OpenSSH* é bastante antiga (ano 2014)	Muitas vulnerabilidades foram descobertas e podem ser exploradas por invasores	TI Infraestrutura
1.1	Protocolo/Serviço: *Pure FTPd*; Porta: 21. O *FTP* é um protocolo bastante antigo de transferência de arquivos.	Como a autenticação no serviço é realizada apenas com usuário e senha, um ataque de força bruta a fim de conseguir obter credenciais de um usuário é facilitado	TI Infraestrutura
1.2	Contratos ativos com prestadores de serviços e fornecedores, não adequados à LGPD	Responsabilização da empresa no caso de vazamento ou incidente com dados pessoais.	Jurídico
1.3	Não possuem termo de consentimento do cliente para uso de imagem de clientes em mídias sociais impressas.	Utilização indevida da imagem do cliente sem seu devido consentimento	Marketing

(conclusão)

Código	Resultados	Riscos	Categoria do risco
1.3	Orçamentos de vendas de peças, com dados de clientes, ficam armazenados e expostos no balcão dos vendedores	Risco de terceiros acessar indevidamente os dados.	Peças
1.3	Utilizam *notebooks* pessoais para prestação do serviço técnico, envolvendo, inclusive, coleta e manutenção de dados pessoais do cliente	Risco de extravio ou vazamento dos dados dos clientes.	Serviços
1.6	A concessionária não disponibiliza os meios de contato do Encarregado de Proteção de dados aos titulares na sua Política de privacidade	Exposição da empresa diante da inconformidade com o artigo 18 da LGPD, o qual trata dos direitos assegurados ao titular de dados	Documentos Internos
1.7	Com base na análise da aplicação do questionário *Due Diligence*, observou-se que um prestador de serviços de TI terceirizado não possui segurança devida para tratar os dados da concessionária	Em caso de vazamento de dados por parte de terceiros, a controladora dos dados (concessionária responsável) poderá ser responsabilizada	Documentos Internos
1.8	80% da equipe da concessionária afirmou não ter acessado e recebido o manual de conduta da mesma	Risco de os colaboradores executar atividades que infrinjam a LGPD	Documentos Internos

Fonte: elaborado pelo autor (2023).

Em relação ao programa de proteção de dados utilizado pela empresa concessionária de máquinas agrícolas, pode-se inferir que ele está estruturado de maneira adequada e contempla a identificação de medidas necessárias à proteção dos dados manuseados. Trata-se de um documento formal elaborado, disponibilizado e acessível a todos os usuários da informação processada que envolvem, em alguma medida, o tratamento de dados pessoais.

Tais definições denotam a preocupação da organização com o atendimento as exigências recomendadas pela LGPD, para a proteção de dados pessoais. De acordo com Demetzou (2019), a proteção de dados pessoais tem início com a compreensão de seus usuários sobre os cuidados que precisam ser adotados para o manuseio destas informações. Quando isto ocorre, além da preocupação, se tem o comprometimento destas pessoas com o tratamento de tais informações, o que corrobora para a efetividade do programa de proteção de dados instituídos na organização. Em contrapartida, a não adoção de tal postura, pode implicar em problemas de não conformidade, as quais podem implicar em infrações à organização.

Embora a concessionária auditada apresente um programa formal de proteção de dados, a partir da análise realizada, observa-se que a estrutura de controle avaliada ainda apresenta algumas fragilidades. Como pode-se verificar a partir dos resultados apresentados no Quadro 7, a entidade apresenta exposições relacionadas aos serviços prestados pela infraestrutura de rede (TI) mantida na organização. Do mesmo modo, verificou-se que alguns contratos analisados ainda não dispõem da inclusão de cláusulas de proteção de dados, que compartilham a preocupação com o zelo e a responsabilidade pela manipulação destas informações, entre as partes relacionadas.

No setor de *marketing* da organização, verificou-se que nem todas as ações desenvolvidas estão amparadas com a coleta (formal) do termo de consentimento do cliente para uso de sua imagem em mídias sociais impressas da empresa. Do mesmo modo, no setor de peças, verificou-se a existência de documentos e registros internos utilizados (com informações pessoais), que ficam expostos de maneira indevida (como nos balcões de atendimento).

Em relação aos serviços prestados, verificou-se o uso de equipamentos pessoais (como *notebooks*) para a prestação de serviços técnicos, a partir dos quais são coletadas e armazenadas informações pessoais, que apresentam dados sensíveis do cliente (como a identificação do seu CPF). Embora possam facilitar o registro das informações e a prestação de serviços, requerem a adoção de políticas e filtros de segurança em tecnologia da informação que impedem o acesso a determinados *sites* e programas, o que, por se tratar de um equipamento de uso particular e pessoal, nem sempre é observado.

Por fim, verificou-se nesta organização, fragilidades relacionadas ao uso e manuseio de alguns documentos internos que são utilizados para os registros

institucionais e a prestação de serviços. Porém, também requerem precaução quanto ao seu uso, em virtude a exposição de dados regulados pela LGPD.

De modo geral, pode-se verificar que a identificação de tais riscos permite a organização, prospectar alternativas para o seu tratamento, de modo que possa minimizar seus eventuais efeitos negativos nas suas operações. Neste caso, riscos decorrentes de penalidades aplicadas pela LGPD. Conforme explica Assi (2021), gerir riscos, consiste em identificar e aplicar recursos da organização, para que tais ameaças posam ser atenuadas, de modo que o sistema de controle interno adotado possa ser consolidado. Assim sendo, a partir destas informações e sua avaliação (apresentada no tópico 4.4.2 deste trabalho), é possível delimitar como a empresa concessionária estará respondendo a cada um destes eventos.

4.3.2 Identificação de riscos na indústria de produtos lácteos

O Quadro 7 apresenta a síntese dos resultados encontrados para a análise da identificação dos tipos de riscos que a indústria de produtos lácteos está exposta, considerando o seu programa de proteção de dados implementados.

QUADRO 7 – Riscos identificados na indústria de produtos lácteos

(continua)

Código	Resultados	Riscos	Categoria do risco
1.1	Serviço/Protocolo: *RTSP*, porta: 631, os dados transmitidos podem ser capturados por um usuário não autenticado	Risco de ataques e vazamento de dados	TI Infraestrutura
1.1	Serviço/Protocolo: *Printer*, porta: 515, essa porta é constantemente utilizada por vários vírus (*eg. MscanWorm, lpdw0rm e Ramen*). Podem ser realizados ataques de negação de serviço, roubo de informações e manipulação da impressora	Risco de ataques, vazamentos e sequestro do banco de dados	TI Infraestrutura

(conclusão)

Código	Resultados	Riscos	Categoria do risco
1.2	Contratos ativos com colaboradores não adequados à LGPD	Vulnerabilidade de defesa judicial em caso de processos trabalhistas	Jurídico
1.3	Não há prazo de armazenamento definido para os currículos	Despadronização dos processos referentes à segurança estabelecidos pela LGPD	Recursos Humanos
1.3	Eventualmente, ocorre acesso remoto ao computador do setor	Risco de extravio ou vazamento dos dados pessoais contidos na pasta do setor	Fiscal
1.3	Todos os colaboradores do setor possuem acesso a todos os cadastros no sistema	Risco de acessos aos dados sem uma finalidade fim justificada e necessária	Financeiro
1.6	A empresa não informa quais dados são coletados e suas respectivas finalidades que serão utilizadas, no momento do cadastro do cliente (coleta)	Exposição da empresa diante da inconformidade com o primeiro item do artigo 6º da LGPD, o qual trata dos princípios a serem seguidos em atividades de tratamento de dados pessoais	Documentos Internos
1.7	-	-	-
1.8	A empresa não dispõe de um tópico sobre coleta e gestão de dados dos seus colaboradores no seu manual de conduta, não expondo situações que serão coletados os consentimentos dos mesmos	Compartilhamentos de dados e uso de imagem indevidos; risco da empresa ser penalizada por não ter evidenciado previamente as finalidades pretendidas	Documentos Internos

Fonte: elaborado pelo autor (2023).

Diante do segundo caso analisado, o qual se refere às particularidades do programa de proteção de dados adotado pela indústria de produtos lácteos, notou-se que este também tem sua adequação bem estruturada e formalizada de acordo com as premissas da LGPD. No entanto, conforme abordado pela própria Lei, deve-se proceder com a avaliação de riscos à segurança dos dados no momento que as práticas cotidianas envolvidas na rotina do negócio possam gerar riscos.

A observação realizada demonstra que a indústria trata como indispensável o acompanhamento dos processos da sua rotina que possam gerar riscos aos seus pilares de segurança da informação. Tal fato está de acordo com Nakamura, Formigoni Filho e Ide (2019), os quais ressaltam que para o sucesso nas ações de tratamento de dados pessoais, é necessária a implementação de práticas de gestão de riscos específicas para este fim. Sendo assim, verifica-se que tais pontos de sucesso podem ser notados quando a equipe de um setor se envolve na gestão de riscos do seu departamento, o que traz uma maior precisão nos resultados pretendidos. No entanto, em caso de não acompanhamento periódico dos riscos identificados, a indústria estará exposta a fragilidades que poderão tornar-se penalizações mais graves com base nas sanções previstas pela LGPD.

Diante do que se visualiza no Quadro 7, entende-se, por meio de sua análise técnica e legal, que os resultados evidenciados se caracterizam como riscos. Em um primeiro momento, verificou-se que a indústria possui fragilidades em seus sistemas e redes, no que se refere ao setor de TI infraestrutura. Analogamente, verificou-se que a mesma possuía alguns dos seus contratos vigentes com colaboradores, em desacordo com as cláusulas de segurança e tratamento de dados por parte dos mesmos, fragilizando uma defesa judicial da indústria, em casos de processos trabalhistas que possam vir a ocorrer.

A este respeito, cabe ressaltar que, embora haja tal preocupação e a formalização contratual estabelece regras e penalidades para o tratamento inadequado de dados pessoais, a obrigação perante o seu tratamento é da empresa. Desta forma, torna-se importante a organização adotar um conjunto de medidas, como esta, que visa sensibilizar e mobilizar o seu quadro funcional, quanto a sensibilidade e relevância do tratamento adequado destes dados e informações.

Analisando os riscos enquadrados na categoria das indagações aos gerentes realizadas pelos auditores, observou-se que os currículos recebidos, dentro do

processo de recrutamento e seleção da empresa, não possuem um prazo de armazenamento definido, fato que acaba despadronizando as políticas básicas de segurança de informação da indústria. Já no que se refere ao setor fiscal, pôde-se notar que, eventualmente, colaboradores do próprio departamento acabam acessando remotamente as máquinas localizadas nos domínios da indústria, prática que traz riscos de extravio ou até mesmo vazamentos de dados pessoais contidos em arquivos, sistemas e pastas do setor.

Na linha que envolve a definição de política de acessos, observou-se que no setor financeiro da indústria os colaboradores envolvidos possuem acessos irrestritos aos cadastros no sistema. Esta prática gera um risco de acesso aos dados lá contidos de maneira indevida, sem justificativa e necessidade fundamentadas.

Ao final, no que se refere aos documentos formalizados do programa implementado, pôde-se constatar dois fatores de fragilidade para a indústria. O primeiro é relacionado à falta de informe das finalidades, dentro do contexto da política de privacidade estabelecida, da coleta dos dados que serão solicitadas no cadastro dos clientes, o que gera uma exposição à indústria aos princípios da Lei e fragilidades quanto à segurança de dados de terceiros em suas bases. Já o outro fator está relacionado ao manual de conduta, onde observa-se ausência de finalidades de coletas de dados dos funcionários da sua equipe, a exemplo da coleta e postagem de fotos particulares em redes sociais públicas da empresa, o que traz um risco de penalização em casos de processos judiciais por parte do titular dos dados.

Desta forma, trazendo-se à tona o objetivo da organização em se ter sucesso nas suas atividades, entende-se que a indústria de produtos lácteos preza pelo acompanhamento contínuo do seu processo de gestão de riscos, razão pela qual também adotou um programa de auditoria para avaliar suas práticas de proteção de dados adotadas. Conforme explica Longo (2012), organizações, ao estarem envolvidas em um ambiente de mercado de alta competitividade, precisam aprimorar suas práticas de gestão.

A adoção de práticas de gestão de riscos é uma das formas de aprimoramento de tais aspectos. Apenas a avaliação e entendimento sobre valores dos seus ativos intangíveis não são mais suficientes para o seu crescimento escalar (LONGO, 2012). É necessário o desenvolvimento de sua capacidade de identificação e resolução de problemas e fragilidades, as quais, se incidentes, podem resultar em perdas a organização. Assim sendo, a partir destas informações e sua avaliação (apresentada

no tópico 4.4.2 deste trabalho), é possível delimitar como a indústria analisada estará respondendo a cada um destes eventos.

4.3.3 Identificação de riscos no clube social

O Quadro 8 apresenta a síntese dos resultados encontrados para a análise da identificação dos tipos de riscos que o clube social está exposto, considerando o seu programa de proteção de dados implementados.

QUADRO 8 – Riscos identificados no clube social

(continua)

Código	Resultados	Riscos	Categoria do risco
1.1	A versão utilizada na porta 443 é a 7.5 possui 6 vulnerabilidades, dentre elas duas de nível crítico	O invasor pode executar códigos remotamente no servidor	TI Infraestrutura
1.1	O protocolo *FTP* não utiliza nenhum tipo de criptografia	O invasor pode ter acesso e visualizar o conteúdo das comunicações *FTP*	TI Infraestrutura
1.2	Contratos ativos com os associados não estão adequados à LGPD	Em caso de uso dos dados de maneira indevida o clube poderá ser penalizado	Jurídico
1.2	Contratos ativos com colaboradores não adequados à LGPD	Vulnerabilidade de defesa judicial em caso de processos trabalhistas	Jurídico
1.3	Médico, contratado como colaborador terceirizado, sem cláusula contratual específica de LGPD, tem acesso ao sistema com os dados sensíveis dos colaboradores	Vulnerabilidade de segurança dos dados pessoais sensíveis, bem como fragilidade contratual, no que tange responsabilização das partes, em caso de ocorrências inesperadas com vazamento de dados	Segurança do Trabalho
1.4	Compartilhamento de dados com a Unimed para concessão de beneficio de plano de saúde	Vulnerabilidade que gera a possibilidade de penalização pela LGPD, tendo em vista a não adequação contratual devida	Departamento Pessoal

(conclusão)

Código	Resultados	Riscos	Categoria do risco
1.5	Coleta informações por meio de entrevistas para elaboração de algumas matérias sem termo de consentimento documentado	Utilização indevida de informações pessoais, imagem e voz do associado sem seu devido consentimento	Jornalismo
1.6	O clube não é claro quanto ao informe dos prazos de armazenamento dos dados mantidos nos seus bancos	Despadronização dos processos referentes à segurança estabelecidos pela LGPD	Documentos Internos
1.7	50% dos prestadores de serviço, com contratos ativos, não passaram pela avaliação de risco de terceiros	Risco de que os terceiros não avaliados possam realizar tratamento inadequado com os dados de responsabilidade da empresa contratante	Documentos Internos
1.8.1	-	-	-

Fonte: elaborado pelo autor (2023).

No tocante ao programa de proteção de dados implementado e formalizado no clube social, pôde-se observar que este dispõe de documentações oficializadas em sua estrutura, principalmente àquelas direcionadas ao seu público de associados, como o caso da publicação de suas políticas de privacidade em seus meios sociais (*site* e redes sociais). Este fato demonstra que o clube não objetiva apenas o estrito cumprimento de normas estabelecidas pela LGPD, mas também se preocupa fortemente com a segurança dos dados pessoais dos seus titulares associados, tanto na transparência referente ao tratamento de dados pessoais de sua rede, quanto na gestão dos seus riscos de segurança da informação, onde estes estão armazenados.

Conforme explica Hopkin (2018), a gestão de riscos decorre de uma analisa integrada, sob uma visão ampla, que auxilia os gestores na identificação de conformidades e fragilidades nos processos de governança e gestão instituídos na organização. Quando desenvolvida de maneira adequada, protege os ativos da organização e contribui para o seu desenvolvimento. Nesta condição, além de

contribuir para a manutenção dos indicadores de conformidade da empresa, também contribui para a qualificação dos processos de tomada de decisão na entidade.

Da mesma forma que os casos anteriormente analisados, verificou-se que o clube social também possui vulnerabilidades nas suas estruturas referentes ao seu programa de proteção de dados formalizado. Diante do conteúdo inserido no Quadro 8, verifica-se, em um primeiro momento, dois riscos referentes ao setor de TI, ocasião em que se observam vulnerabilidades na infraestrutura das redes, o que, se não tratados da maneira correta, poderão gerar prejuízos à segurança dos dados, como vazamentos ou sequestros do banco de dados por invasores.

Diante da análise de mais dois riscos identificados, enquadrados na categoria jurídica, pôde-se observar que os contratos, tanto com associados quanto com colaboradores, ainda não estão completamente adequados com a inclusão de cláusulas necessárias específicas à sua finalidade, trazendo fragilidades tanto à segurança da informação dos dados, como em uma eventual necessidade de defesa judicial ao clube, em caso de solicitações dos envolvidos. No departamento responsável por questões relacionadas à segurança do trabalho, visualizou-se que o médico, cujo contrato se caracteriza como prestação de serviço terceirizada, acessa livremente os dados sensíveis coletados dos colaboradores do clube, sem uma cláusula de segurança e de responsabilidade no contrato, o que também traz ao clube social um risco de responsabilização à entidade em caso de hipóteses de vazamento de dados (independentemente da parte responsável).

Nesta mesma linha, observou-se também o fato dos dados pessoais dos colaboradores serem compartilhados com a Unimed, sem cláusulas contratuais específicas, referentes a proteção de dados com base na LGPD, evidenciando as responsabilidades das partes. No setor de jornalismo, verificou-se também que as entrevistas com os associados, realizadas no objetivo de elaboração de conteúdo próprio para matérias, as quais, posteriormente, serão publicadas na revista do clube e em redes sociais do mesmo, não estão amparadas com o devido consentimento do titular e o uso de sua voz nas mídias citadas, o que se caracteriza como um risco pela utilização indevida de dados por parte do controlador (clube).

Por fim, verificaram-se também fragilidades relacionadas às estruturas que compõem alguns documentos internos, os quais são tratados como papeis oficiais do programa de proteção de dados do clube. A primeira análise apontou que, referente a formalização das políticas de privacidade, não foi possível se evidenciar quais são os

prazos de armazenamento, por parte do clube, dos dados da sua rede de titulares, fato este que gera um risco ao mesmo, tendo em vista a falta de transparência e evidenciação pública desta hipótese de tratamento (armazenamento). Já o segundo apontamento realizado diz respeito à falta de avaliação do nível de adequação à LGPD e da adoção de ferramentas de segurança da informação no acesso de dados da metade dos prestadores de serviços contratados, o que possibilita um risco de que estes terceiros tratem os dados, de responsabilidade primária do clube, de maneira indevida e/ou sem ferramentas adequadas de segurança aos dados acessados, facilitando, por exemplo, um vazamento ou incidente com os dados pessoais.

Desta forma, diante dos detalhamentos evidenciados, ainda se observam vulnerabilidades na estrutura do programa de proteção de dados do clube, os quais precisam ser tratados para que ocorra a mitigação de sua probabilidade de ocorrência e impacto. Conforme Nakamura, Formigoni Filho e Ide (2019), para o sucesso nas ações de tratamento de dados pessoais, é necessária a implementação de práticas de gestão de riscos específicas para este fim. Estas práticas visam identificar fragilidades e como se proceder para tratar adequadamente a cada um dos eventos identificados. Parte-se da premisse de que não existe uma solução única para todos os problemas. Desta forma, cabe aos gestores identificar qual solução é a mais adequada para ser aplicada diante de tais apontamentos.

Neste contexto, a partir de sua implementação e com o decorrer dos meses, mediante o acompanhamento por parte dos responsáveis pelo programa, torna-se possível avaliar a eficácia das soluções implementadas, para o tratamento adequado dos dados coletados e armazenados pelo controlador. Sendo assim, a avaliação e encaminhamentos de novas ações, quando necessárias, devem continuamente ser colocadas em prática, para que o êxito completo na adequação à LGPD possa ser obtido pelo clube social. A partir destas informações, e sua respectiva avaliação (apresentada no tópico 4.4.3 deste trabalho), é possível compreender como o clube estará tratando cada um dos eventos destacados.

4.3.4 Análise conjunta dos resultados encontrados sob a ótica das contribuições da auditoria para a identificação de riscos

Como pode-se verificar a partir dos resultados apresentados para cada um dos casos analisados, a adoção de um programa de auditoria permitiu verificar a

existência de diferentes tipos de riscos de inconformidade relacionados à LGPD, em cada empresa. Estes resultados revelam que a auditoria é capaz de contribuir para identificação de fragilidades no ambiente de controle relacionado a adoção e uso de programas de proteção de dados. Do mesmo modo, para a identificação de riscos a que as organizações estão expostas.

Assim, é possível inferir que a auditoria pode contribuir para o fortalecimento das estruturas integradas de controle e proteção de dados, bem como para a delimitação de um programa formal de gerenciamento de riscos relacionados. Dentre as principais funções da auditoria está sua atuação nos processos de gestão de riscos, constituindo-se um mecanismo de controle eficaz para este fim (WEBWE; DIEHL, 2016). É a partir de sua execução que a auditoria apoiará os processos de gestão de riscos, por meio da identificação, avaliação e análise de eventos que possam representar riscos ao negócio (BYRNES et al., 2018).

Assim sendo, esta estruturação da auditoria, a qual engloba, dentre outras características, a avaliação de riscos, permite influenciar diretamente os processos de gestão de riscos instituídos em uma organização, de modo que possa agir para atenuar seus possíveis efeitos negativos (consequências). Isto ocorre quando, a partir de sua aplicação e seus resultados, a auditoria é capaz de proporcionar um melhor entendimento de um conjunto de dados processados que, sob uma visão macro da organização, permite um melhor entendimento de sua importância, consequências, e necessidade de tratamento (AJAO; OLAMIDE; ETEMITOPE, 2016).

Neste contexto, torna-se possível responder ao segundo objetivo específico estabelecido para esta pesquisa, uma vez que, por meio da aplicação dos planejamentos e procedimentos de auditoria nos casos analisados foi possível identificar sua exposição a riscos de infração à LGPD.

4.4 GRAUS DE EXPOSIÇÃO DOS RISCOS DE INFRAÇÃO À LGPD E PLANOS DE AÇÃO

Após as etapas de descrição dos planejamentos e procedimentos de auditoria e da apresentação dos riscos ligados a LGPD, e procurando responder ao terceiro objetivo específico estabelecido para esta pesquisa, foi realizada a avaliação (percentual) dos graus de exposição dos riscos identificados de infração à LGPD, estabelecendo-se os respectivos planos de ação para o seu tratamento.

Para tanto, inicialmente foi elaborada a matriz de riscos, definida por meio da aplicação de escalas de avaliação de probabilidade de ocorrência e impacto. Assim, o grau percentual de exposição aos riscos de cada um dos trabalhos de auditoria estudados foi apurado como demonstrado no Quadro 9.

QUADRO 9 – Escala de Risco utilizada na pesquisa

% de Risco	**Classificação**
Até 9,6%	Baixo
De 9,61% a 35,69%	Médio
De 35,7% a 63,89%	Alto
De 63,9% a 81%	Muito Alto

Fonte: elaborado pelo autor (2023).

A classificação do grau de exposição foi definida a partir de quatro classificações que envolvem níveis de exposição: baixo, médio, alto e muito alto. Aderiu-se o quadro no objetivo de que os riscos identificados pudessem ser mensurados com base em suas probabilidades e impactos, cujo valor resultante do produto destas variáveis possibilitou encontrar o valor do percentual de risco a que a organização está exposta e, a partir deste, classificar o evento diante de cada uma de suas particularidades (atribuição de métricas qualitativas com base em valores quantitativos). Esta etapa de análise vai ao acordo do entendimento de processo de gestão de risco estabelecido por Namazian e Eslami (2011), o qual, utilizando-se como base a referência apresentada na Figura 1 (página 14), recomenda a avaliação qualitativa e quantitativa de riscos, a qual caracteriza este processo como indispensável ao processo íntegro e completo de gestão de risco.

Nesta pesquisa, os níveis baixos de classificação indicam que o risco possui sua probabilidade de ocorrência baixa e/ou seu impacto, em caso de ocorrência, também baixo. Quando classificados em médios, os riscos começam a gerar um alerta um pouco maior para a organização, tendo em vista o fato de que, se não tratados a longo prazo, terão seus graus de exposição aumentados e mais graves. No que se refere a classificação de níveis altos de exposição, tem-se como entendimento que os riscos enquadrados nesta categoria deverão ser mitigados a curto prazo e com planos de ação e estratégias mais rígidas, bem como acompanhadas continuamente pelos responsáveis, observando seu alto grau de probabilidade de acontecimento e impacto

mais severo. Por fim, na classificação de riscos como níveis muito altos, significa que a organização apresenta exposição crítica a estes eventos e demanda intervenção imediata.

De acordo com Baybutt (2018), a matriz de risco é um meio eficiente de avaliação de grau de severidade de cada risco identificado na organização, auxiliando posteriormente na determinação de prioridades de tratamento, contribuindo diretamente para a tomada de decisão do responsável pela gestão. Deste modo, é necessária sua elaboração para que a organização tenha seus processos continuamente monitorados, assim como àqueles que se caracterizarem como riscos de exposição elevada, possam ser submetidos de maneira individual a um tratamento adequado, definidos a partir de um plano de ação específico.

Uma avaliação inadequada de tais eventos pode implicar em alguns problemas para a empresa, a exemplo de gastos desnecessários dispendidos para mitigação dos riscos ou para o pagamento de notificações decorrentes de autos de infração relatados. Por esta razão, é necessária a adoção de medidas viáveis ao tratamento de cada evento, determinada diante da avaliação realizada refere ao grau de severidade (ocorrência e impacto) do risco identificado. Sendo assim, por meio de seu tratamento, torna-se possível, não sua eliminação, mas a identificação de alternativas viáveis para uma menor exposição, o que atenua tais consequências (COSO, 2004).

A partir de tais definições e dos cálculos realizados, bem como seu enquadramento diante das escalas apresentadas no Quadro 9, foi possível inferir sobre o grau de exposição dos eventos identificados pelos auditores em cada um dos trabalhos executados. Os resultados encontrados são apresentados a seguir.

4.4.1 Graus de exposição e planos de ação da concessionária de máquinas agrícolas

O Quadro 10 apresenta a síntese dos resultados encontrados para a análise do grau de exposição dos riscos relacionados à LGPD que a concessionária de máquinas agrícolas está exposta. Da mesma forma, os respectivos planos de ação recomendados para a mitigação dos eventos que contribuem para tal exposição.

QUADRO 10 – Graus de exposição a riscos e planos de ação da concessionária de máquinas agrícolas

(continua)

Código	Resultado dos procedimentos	Riscos	Grau de risco %	Plano de ação
1.1	Protocolo/Serviço: *OpenSSH* 6.6.1; Porta: 22; A versão utilizada do *OpenSSH* é bastante antiga (ano 2014)	Muitas vulnerabilidades foram descobertas e podem ser exploradas por invasores	25% Médio	Atualizar para a versão mais recente: 8.9.
1.1	Protocolo/Serviço: *Pure FTPd*; Porta: 21. O *FTP* é um protocolo bastante antigo de transferência de arquivos.	Como a autenticação no serviço é realizada apenas com usuário e senha, um ataque de força bruta a fim de conseguir obter credenciais de um usuário é facilitado	25% Médio	Utilização do *Pure FTPD* permite que a comunicação seja realizada através do protocolo *TLS*, adicionando assim uma camada de segurança que originalmente o *FTP* não fornece.
1.2	Contratos ativos com prestadores de serviços e fornecedores, não adequados à LGPD	Responsabilização da empresa no caso de vazamento ou incidente com dados pessoais.	60% Alto	Adequar os contratos com cláusulas de proteção de dados específicas de acordo com a hipótese de tratamento e suas devidas necessidades.
1.3	Não possuem termo de consentimento do cliente para uso de imagem de clientes em mídias sociais impressas.	Utilização indevida da imagem do cliente sem seu devido consentimento	25% Médio	Fotos poderão ser compartilhadas apenas mediante coleta de consentimento do titular; assim, deve-se utilizar um termo, com a assinatura dele, para a hipótese especifica evidenciada.
1.3	Orçamentos de vendas de peças, com dados de clientes, ficam armazenados e expostos no balcão dos vendedores	Risco de terceiros acessar indevidamente os dados.	25% Médio	Fixar um aviso em cima dos balcões evidenciando que este tipo de documento não poderá ser exposto em ambientes de circulação geral.

(continua)

Código	Resultado dos procedimentos	Riscos	Grau de risco %	Plano de ação
1.3	Utilizam *notebooks* pessoais para prestação do serviço técnico, envolvendo, inclusive, coleta e manutenção de dados pessoais do cliente	Risco de extravio ou vazamento dos dados dos clientes.	42% Alto	Recomenda-se que a concessionária disponibilize dispositivos de domínio corporativo para toda sua equipe, bem como deverá cobrar dos colaboradores que os utilizem para assuntos relacionadas à organização.
1.6	A concessionária não disponibiliza os meios de contato do Encarregado de Proteção de dados aos titulares na sua Política de privacidade	Exposição da empresa diante da inconformidade com o artigo 18 da LGPD, o qual trata dos direitos assegurados ao titular de dados	64% Muito Alto	É altamente recomendado que a concessionária altere sua política imediatamente, atualizando esta com o contato do Encarregado responsável pelo programa.
1.7	Com base na análise da aplicação do questionário Due Diligence, observou-se que um prestador de serviços de TI terceirizado não possui segurança devida para tratar os dados da concessionária	Em caso de vazamento de dados por parte de terceiros, a controladora dos dados (concessionária responsável) poderá ser responsabilizada	70% Muito Alto	O contrato com o terceiro deve ser imediatamente ajustado com as cláusulas devidas de responsabilidade, em que este deverá se adequar as premissas básicas de segurança da informação para que se tenha um tratamento/acesso aos dados do terceiro de maneira lícita.

(conclusão)

Código	Resultado dos procedimentos	Riscos	Grau de risco %	Plano de ação
1.8	80% da equipe da concessionária afirmou não ter acessado e recebido o manual de conduta da mesma	Risco de os colaboradores executar atividades que infrinjam a LGPD	58,9% Alto	O manual de conduta já desenvolvido deverá ser disponibilizado nas redes internas, digitalmente, bem como em vias físicas, no momento da contratação do funcionário.

Fonte: Elaborado pelo autor (2023).

Como pode-se verificar a partir dos resultados apresentados no Quadro 10, a empresa concessionária de máquinas agrícolas está exposta a riscos que apresentam diferentes graus de severidade. De modo geral, nenhum dos eventos identificados é classificado como de baixa exposição, o que denota a importância de seu tratamento. Dos nove eventos avaliados, quatro foram classificados como de média exposição. Entre os demais, três apresentam alta exposição e apenas dois eventos são classificados como de muito alta severidade, os quais requerem atenção imediata.

Estes resultados revelam que a maior parte dos riscos da concessionária devem ser monitorados continuamente, principalmente os riscos enquadrados como médios e altos, para que não tenham seu grau de exposição agravado. Já os dois riscos de caráter de exposição muito alto devem ser mitigados imediatamente, estando elencados na primeira classe das prioridades de atuação por parte da gestão. A severidade de um evento quando identificada requer atenção imediata, uma vez que sua exposição pode impactar negativamente as atividades desenvolvidas pela empresa (COSO, 2004; ZONATTO; BEUREN, 2010).

No caso analisado, para fins de desenvolvimento e elaboração dos planos de ação recomendados, pôde-se verificar que cada risco foi discutido entre o auditor e a equipe interna da empresa concessionária, para que este fosse aplicado da maneira mais precisa possível, considerando-se cada uma de suas particularidades. Observou-se que, por motivos técnicos, os riscos referentes à infraestrutura de redes tiveram suas estratégias de mitigação provenientes do relatório de um auditor técnico de segurança da informação especializado.

Neste caso, torna-se necessário que a organização atue no sentido de contratar um profissional interno para atuar como responsável por tais atividades na empresa,

ou proceda a contratação de um profissional terceirizado, de modo que tais atividades sejam constantemente monitoradas. Em relação a ambos os eventos que apresentam maior grau de exposição, os planos de ação elaborados recomendaram, imediatamente, a necessidade de revisão e alteração da política de proteção de dados (e da política de privacidade de dados estabelecida na empresa), bem como, que todos os contratos firmados possam ser ajustados, com a inclusão de cláusulas devidas de responsabilidade, em que o contratado deverá se adequar as premissas básicas de segurança da informação para que se tenha um tratamento/acesso aos dados de terceiros de maneira lícita e adequada.

A adoção de tais ações contribuirá para a redução dos níveis de exposição da organização a estes riscos de infração relacionados a LGPD.

4.4.2 Graus de exposição e planos de ação da indústria de produtos lácteos

O Quadro 11 apresenta a síntese dos resultados encontrados para a análise do grau de exposição dos riscos relacionados a LGPD que a indústria de produtos lácteos está exposta, bem como os planos de ação recomendados para a mitigação dos eventos que contribuem para tal exposição.

QUADRO 11 – Graus de exposição a riscos e planos de ação da indústria de produtos lácteos

(continua)

Código	Resultado dos procedimentos	Riscos	Grau de risco %	Plano de ação
1.1	Serviço/Protocolo: *RTSP*, porta: 631, os dados transmitidos podem ser capturados por um usuário não autenticado	Risco de ataques e vazamento de dados	25% Médio	Verificar e utilizar uma rede privada para o tráfego desses dados e implantar criptografia na transmissão.
1.1	Serviço/Protocolo: *Printer*, porta: 515, essa porta é constantemente utilizada por vários vírus (*eg. MscanWorm, lpdw0rm e Ramen*). Podem ser realizados ataques de negação de serviço, roubo de informações e manipulação da impressora	Risco de ataques, vazamentos e sequestro do banco de dados	25% Médio	Utilizar um servidor de impressora e restringir acesso a este por meio de um *vlan*. Manter a porta 9100 para a *Internet* é uma boa prática. Também é importante manter os drivers dos dispositivos e drivers atualizados.

(continua)

Código	Resultado dos procedimentos	Riscos	Grau de risco %	Plano de ação
1.2	Contratos ativos com colaboradores não adequados à LGPD	Vulnerabilidade de defesa judicial em caso de processos trabalhistas	60% Alto	Adequar os contratos com cláusulas de proteção de dados específicas de acordo com a hipótese de tratamento e suas devidas necessidades, com base nas condutas de proteção de dados internas formalizadas pela empresa.
1.3	Não há prazo de armazenamento definido para os currículos	Despadronização dos processos referentes à segurança estabelecidos pela LGPD	35% Médio	O DPO e o Comitê Interno de Proteção de Dados devem definir um prazo de descarte para cada tipo de documento que contenha dados pessoais, sugere-se, que o prazo de armazenamento seja de, no máximo 3 anos.
1.3	Eventualmente, ocorre acesso remoto ao computador do setor	Risco de extravio ou vazamento dos dados pessoais contidos na pasta do setor	35% Médio	Tendo em vista que a existência deste risco está condicionada à uma necessidade da atividade, deve-se aceitar, considerando-se a boa-fé do colaborador e a adoção dos princípios de segurança disponibilizados no manual de conduta interno à proteção de dados da empresa.

(conclusão)

Código	Resultado dos procedimentos	Riscos	Grau de risco %	Plano de ação
1.3	Todos os colaboradores do setor possuem acesso a todos os cadastros no sistema	Risco de acessos aos dados sem uma finalidade fim justificada e necessária	15% Médio	O responsável pelo gerenciamento dos acessos ao sistema e pastas deverá proceder com as limitações aos colaboradores do departamento, de forma que estes só tenham acesso aos dados necessários à suas atividades.
1.6	A empresa não informa quais dados são coletados e suas respectivas finalidades que serão utilizadas, no momento do cadastro do cliente (coleta)	Exposição da empresa diante da inconformidade com o primeiro item do artigo 6º da LGPD, o qual trata dos princípios a serem seguidos em atividades de tratamento de dados pessoais	67,6% Muito Alto	Tendo em vista o alto grau de exposição do risco, deve-se inserir um tópico, imediatamente, na política de privacidade já desenvolvida, abordando as finalidades de coleta pretendidas.
1.8	A empresa não dispõe de um tópico sobre coleta e gestão de dados dos seus colaboradores no seu manual de conduta, não expondo situações que serão coletados os consentimentos dos mesmos	Compartilhamentos de dados e uso de imagem indevidos; risco da empresa ser penalizada por não ter evidenciado previamente as finalidades pretendidas	35,9% Alto	Ajuste do manual de conduta, evidenciando as hipóteses atuais em que se evidenciam necessidade explícita de coleta de consentimento do colaborador.

Fonte: elaborado pelo autor (2023)

Como pode-se verificar a partir dos resultados apresentados no Quadro 11, a indústria de produtos lácteos está exposta a riscos que apresentam diferentes graus de severidade. Nota-se, da mesma forma que no caso anterior analisado, que nenhum

dos eventos identificados é classificado como de baixa exposição, reforçando a importância de seu tratamento. Dos nove eventos avaliados, cinco foram classificados como de média exposição. Entre os demais, dois apresentam alta exposição e apenas um evento é classificado como de muito alta severidade.

Estes resultados revelam que a maior parte dos riscos identificados na indústria de produtos lácteos devem ser monitorados continuamente, principalmente os riscos enquadrados como médios, para que não tenham seu grau de exposição agravado e se tornem riscos com grau de exposição alto. Já os dois riscos de caráter de exposição alto, devem ser mitigados a curto prazo pela gestão, a fim de que se possa evitar possíveis penalizações legais. Quanto ao risco de caráter muito alto, este deve ter o seu plano de ação sugerido aplicado imediatamente.

Neste caso, foi recomendado que a organização estabeleça em seu programa de proteção de dados a definição adequada de quais dados são necessários para a realização adequada do cadastro dos clientes, e como estes dados devem ser tratados pelos usuários com acesso a esta informação. Esta adequação contribuirá para o alinhamento da política de privacidade de dados já desenvolvida pela empresa, e a sensibilização por parte dos usuários da informação da importância de seu cuidado com o acesso e manuseio de tais informações. A coleta de tais informações também permitirá a identificação da anuência do cliente, diante do cadastro das informações solicitadas, o que denota conformidade na política de coleta, tratamento e armazenamento de dados.

Desta forma, a partir da adoção de tais ações, torna-se possível promover a redução dos níveis de exposição elevada da organização, identificados especificamente nestes riscos de infração relacionados a LGPD.

4.4.3 Graus de exposição e planos de ação do clube social

O Quadro 12 apresenta a síntese dos resultados encontrados para a análise do grau de exposição dos riscos relacionados a LGPD que o clube social está exposto, e os respectivos planos de ação recomendados para a mitigação dos eventos que contribuem para tal exposição.

QUADRO 12 – Graus de exposição a riscos e planos de ação do clube social

(continua)

Código	Resultado dos procedimentos	Riscos	Grau de risco %	Plano de ação
1.1	A versão utilizada na porta 443 é a 7.5 possui 6 vulnerabilidades, dentre elas duas de nível crítico	O invasor pode executar códigos remotamente no servidor	49% Alto	Altamente recomendado atualizar para a versão atual (10.0).
1.1	O protocolo *FTP* não utiliza nenhum tipo de criptografia	O invasor pode ter acesso e visualizar o conteúdo das comunicações *FTP*	32% Médio	Utilizar um protocolo seguro para transferência de arquivos, como *SSH*, que incorpora o *SFTP* na qual é uma versão segura do protocolo *FTP.*
1.2	Contratos ativos com os associados não estão adequados à LGPD	Em caso de uso dos dados de maneira indevida o clube poderá ser penalizado	60% Alto	Adequar os contratos com cláusulas de proteção de dados específicas de acordo com a hipótese de tratamento e suas devidas necessidades.
1.2	Contratos ativos com colaboradores não adequados à LGPD	Vulnerabilidade de defesa judicial em caso de processos trabalhistas	60% Alto	Adequar os contratos com cláusulas de proteção de dados específicas de acordo com a hipótese de tratamento e suas devidas necessidades, com base nas condutas de proteção de dados internas formalizadas pelo clube.

(continua)

Código	Resultado dos procedimentos	Riscos	Grau de risco %	Plano de ação
1.3	Médico, contratado como colaborador terceirizado, sem cláusula contratual específica de LGPD, tem acesso ao sistema com os dados sensíveis dos colaboradores	Vulnerabilidade de segurança dos dados pessoais sensíveis, bem como fragilidade contratual, no que tange responsabilização das partes, em caso de ocorrências inesperadas com vazamento de dados	21% Médio	É altamente recomendado que seja estabelecido um contrato de prestação serviço, para haver um resguardo contratual em caso de ocorrências; além disso, sua elaboração já deve conter as devidas cláusulas de evidenciação para proteção de dados pessoais sensíveis.
1.3	Compartilhamento de dados com a Unimed para concessão de benefício de plano de saúde	Vulnerabilidade que gera a possibilidade de penalização pela LGPD, devido a não adequação contratual.	15% Médio	Inserção de cláusulas de LGPD no contrato com a entidade; deve-se, inclusive, prever contratualmente tal compartilhamento com o colaborador.
1.3	Coleta informações por meio de entrevistas para elaboração de algumas matérias sem termo de consentimento documentado	Utilização indevida de informações pessoais, imagem e voz do associado sem seu devido consentimento	21% Médio	No momento da coleta, deve-se coletar um consentimento (documentado ou gravado antes da entrevista) visando a asseguração formal do processo
1.6	O clube não é claro quanto ao informe dos prazos de armazenamento dos dados mantidos nos seus bancos	Despadronização dos processos referentes à segurança estabelecidos pela LGPD	45% Alto	O clube deve estabelecer uma política de armazenamento separada por tipo de dados, para que cada um tenha seus prazos legais ajustados dentro dos seus objetivos de retenção.

(conclusão)

código	Resultado dos procedimentos	Riscos	Grau de risco %	Plano de ação
1.7	50% dos prestadores de serviço, com contratos ativos, não passaram pela avaliação de risco de terceiros	Risco de que os terceiros não avaliados possam realizar tratamento inadequado com os dados de responsabilidade da empresa contratante	56,1% Alto	Aplicação imediata da avaliação com os terceiros em pendência, mediante questionário *Due Diligence.*

Fonte: elaborada pelo autor (2023).

Como pode-se verificar a partir dos resultados apresentados no Quadro 12, o clube social está exposto a riscos que apresentam diferentes graus de severidade. Novamente, não se observam riscos enquadrados a níveis de baixa exposição, ressaltando-se a necessidade dos seus tratamentos devidos. Contudo, neste caso analisado, também não se identifica a exposição da organização a níveis críticos, considerados como muito altos, o que denota uma preocupação adequada em relação a cuidados necessários ao estabelecimento de um programa efetivo de proteção de dados, visando a redução dos níveis de exposição da organização, a eventos críticos de riscos.

Estas evidências sugerem que a adoção de práticas de gestão de riscos está contribuindo para a mitigação dos riscos de infração relacionados ao não atendimento as recomendações estabelecidas pela LGPD. Contudo, não as elimina, como destacado na literatura (DEMETZOU, 2019). Isto ocorre porque, em alguma medida, todas as organizações estão expostas a riscos do negócio (COSO, 2004). Assim, diante da impossibilidade de sua eliminação, a preocupação dos gestores deve centrar-se em trazê-los a parâmetros aceitáveis, reduzindo seu potencial danoso a organização (COSO, 2007).

Dos nove eventos avaliados, quatro foram classificados como de média exposição. Os demais, caracterizam-se como eventos de alta exposição, e demandam atenção para serem adequadamente tratados. Em relação aos planos de ação recomendados, pôde-se verificar que a realização de investimentos em TI e a modernização de sistemas de controle de acesso, bem como a adequação de

contratos de associados, dos funcionários contratados e prestadores de serviços, e o estabelecimento de uma política de armazenamento de dados, separada por tipos de dados, para que cada usuário tenha acesso restrito e específico aos dados necessários ao desenvolvimento de suas atividades de trabalho, são as principais ações recomendadas.

Com isto, espera-se que a partir da adoção de tais ações, seja possível contribuir para a redução dos níveis de exposição da organização a estes riscos de infração relacionados a LGPD identificados no clube social.

4.4.4 Análise conjunta dos resultados encontrados sob a ótica das contribuições da auditoria para a avaliação dos graus de exposição a riscos

Diante dos três casos analisados, como pode-se verificar a partir dos resultados obtidos para a avaliação do grau de exposição e a elaboração dos planos de ação definidos para o seu tratamento, a adoção de um programa de auditoria permitiu a identificação da severidade de cada um dos eventos identificados. Para tanto, considerando-se as características e particularidades de cada evento e sua incidência em cada organização, foi possível avaliar sua probabilidade de ocorrência e impacto, o que permitiu a inferência da severidade do evento e suas consequências (danos).

Estes resultados revelam que a auditoria é capaz de contribuir para identificação dos graus de exposição a riscos em cada organização. Do mesmo modo, possibilita avaliar, diante de suas características e potencial de dano, a forma mais adequada e o período de tempo necessário para a intervenção e o seu tratamento. Conforme explicam Nakamura, Formigoni Filho e Ide (2019), o sucesso no estabelecimento de mecanismos de controle e tratamento adequado de dados perpassa pela capacidade da organização em identificar, avaliar e proceder o tratamento adequado de cada um dos eventos identificados como riscos do negócio.

Assim, embora a proteção de dados tenha início com a compreensão de seus usuários sobre a necessidade de adoção de cuidados para o manuseio destas informações, é a avaliação e o seu tratamento (respostas) que determinarão a eficácia das medidas corretivas implementadas (DEMETZOU, 2019). Deste modo, a partir da identificação de tais respostas, apresentadas nos respectivos planos de ação elaborados, não é possível avaliar imediatamente se a solução proposta é capaz de proporcionar os resultados esperados. Contudo, em um determinado período de

tempo, a partir de uma nova avaliação, é possível inferir se as alterações recomendadas e realizadas estão proporcionando o tratamento adequado de dados, manuseados em conformidade com o recomendado pela LGPD.

Este conjunto de procedimentos adotados para a realização de tais inferências também permitem identificar a aplicação por parte dos auditores da NBC TA 315, que dispõe sobre a identificação e a avaliação dos riscos de distorção relevante por meio do entendimento da entidade e do seu ambiente, onde estes promoverem uma avaliação dos riscos para entender o contexto de exposição de cada empresa auditada a LGPD, para que então, de posse destas informações, elaborassem os planos de ação. Isto foi observado nos casos analisados.

Diante do exposto, torna-se possível responder ao terceiro objetivo específico estabelecido para esta pesquisa, uma vez que, por meio das análises realizadas, foi possível avaliar (percentualmente) os graus de risco de infração relacionados à LGPD e estabelecer seus planos de ação para o tratamento destes eventos.

5 CONCLUSÕES E RECOMENDAÇÕES

Esta seção apresenta as conclusões do trabalho e as recomendações a estudos futuros.

5.1 CONCLUSÕES

Este estudo teve como objetivo central analisar as contribuições da auditoria independente para a gestão de riscos em LGPD. Desta forma, para atingir o mesmo, desenvolveram-se três objetivos específicos, os quais foram executados com base na metodologia definida para condução dessa pesquisa, caracterizada como um estudo descritivo, de múltiplos casos, realizado por meio de análise documental, entrevistas e visitação com observação *in loco*.

Por meio de três trabalhos de auditoria independente realizados em programas de LGPD, em empresas que haviam implementado este programa a mais de um ano, foram analisados os planejamentos e programas de auditoria aplicados pelos auditores (primeiro objetivo), bem como os riscos identificados por esta aplicação (segundo objetivo) e as quantificações percentuais destes eventos, o que possibilitou a identificação de oportunidades de melhoria e a sugestão de planos de ação por parte dos auditores (terceiro objetivo).

A partir da análise dos planejamentos e procedimentos de auditoria utilizados nos trabalhos ligados à gestão de riscos em LGPD, foi possível verificar que, previamente à elaboração dos planejamentos e procedimentos adotados, os auditores, com base nos artigos da LGPD, determinaram cinco áreas básicas de avaliação, sendo estas: jurídica, governança, TI, RH e auditoria, as quais foram contempladas com planejamentos e procedimentos de auditoria específicos para sua avaliação nos três casos analisados.

Com a execução desta análise, foi possível identificar que os procedimentos de auditoria aplicados pelos auditores são exatamente àqueles previstos na NBC TA 500, assim como, verificou-se que os auditores se valeram da NBC TA 300 para padronizar e organizar o trabalho de construção do planejamento das auditorias realizadas. Estes resultados demonstraram a contribuição da auditoria independente e suas normas para a identificação e gestão de riscos de infração relacionados à LGPD, os quais, se

considerados, permitirão o fortalecimento dos mecanismos de controle interno adotados pelas empresas estudadas.

A partir da identificação dos riscos de infração à LGPD encontrados por meio da aplicação dos planejamentos e procedimentos de auditoria definidos para cada caso analisado, foi possível verificar que os riscos são extraídos dos resultados da aplicação dos procedimentos de auditoria definidos pelos auditores na etapa de planejamento dos trabalhos. Do mesmo modo, que estes eventos representam fragilidades identificadas no ambiente de controle interno relacionado ao programa de proteção de dados instituído nestas organizações. Sendo assim, é possível observar que os auditores aplicam um planejamento e procedimentos delimitados com base no disposto pela LGPD, sendo este um eficiente plano de trabalho elaborado para a identificação de eventos que representam riscos de infração ao disposto nesta norma.

Verificou-se também que, mesmo que os procedimentos sejam padronizados, os resultados obtidos para cada empresa estudada foram divergentes, fato este que se justifica pelas diferentes atividades de negócio das empresas estudadas, concessionária, indústria de produtos lácteos e clube social, e os diferentes níveis de exposição apresentados, diante de suas estruturas de controle definidas para apoiar o programa de proteção de dados estabelecido. Os diferentes processos organizacionais existentes e pessoas envolvidas no tratamento destes dados, também determina os níveis de exposição destas organizações, a riscos relacionados a LGPD. Tanto no que se refere a funcionários que atuam no ambiente interno da organização, como prestadores de serviços, fornecedores e parceiros de negócio, que ao manterem alguma relação com a organização estudada, possuem acesso a um determinado grupo de informações.

Por fim, a demonstração dos graus percentuais de riscos existentes nas empresas estudadas, considerando os níveis de exposição dos riscos de infração à LGPD revelaram que estas organizações estão expostas a diferentes fatores, os quais, são caracterizados como eventos de média, alta e muito alta exposição. A matriz de risco de probabilidade x impacto desenvolvida pelos auditores para avaliar cada um dos riscos identificados nas empresas auditadas mostrou-se eficiente para este propósito, indicando ainda que os auditores se valeram da NBC TA 315 para avaliação destes riscos.

Para a elaboração da matriz de risco de probabilidade e impacto, os auditores aplicaram escalas padronizadas, as quais são utilizadas uniformemente para todas as

empresas auditadas. Consequentemente, permitem avaliar sua capacidade preditiva e acurácia para a avaliação da severidade destes eventos em diferentes casos. A este respeito, os resultados desta pesquisa também revelaram que para cada um dos riscos identificados, os auditores propuseram um plano de ação para que cada empresa auditada desenvolva ações necessárias a mitigação destes riscos.

Pôde-se concluir que a auditoria independente contribui para a estruturação de uma metodologia de gestão de riscos adequada, referente aos itens recomendados para proteção de dados pela Lei Geral de Proteção de Dados (LGPD). Os resultados da pesquisa realizada, apontam para o fato de que, por meio das suas normas técnicas, a auditoria independente contribui diretamente para todo o processo de formalização dos trabalhos de auditoria em gestão de riscos de LGPD, o qual permite a identificação e análise adequada dos eventos que representam riscos a organização auditada. A observância de tais práticas oportunizou as organizações avaliar suas estruturas de controle relacionadas ao programa de proteção de dados implementados, bem como da política de tratamento de dados pessoais instituída.

Assim, além de permitir esta avaliação, contribui para que a organização revise, organize, estruture e disponibilize novos procedimentos para execução de trabalhos, com o zelo necessário a resguardar o tratamento, manuseio e armazenamento de tais dados, sem incorrer em penalidades relacionadas a infração pelo não cumprimento das recomendações estabelecidas pela LGPD. No contexto da auditoria, os resultados encontrados revelam que, a partir da definição de um plano de trabalho adequado a este fim, a auditoria pode atuar para identificar riscos de infração à LGPD, bem como para avaliar seus efeitos (consequências), diante dos níveis de exposição avaliados, de modo que possa identificar e sugerir a adoção de práticas de gestão eficazes para que infrações e penalizações não ocorram, o que se constitui uma nova oportunidade de atuação para os auditores.

Por meio das suas normas técnicas, a auditoria independente contribui diretamente para todo o processo de formalização dos trabalhos de auditoria em gestão de riscos de LGPD, o qual permite a identificação e análise adequada dos eventos que representam riscos a organização auditada, o que reflete em conformidade legal. Diante do exposto, pode-se inferir que a auditoria independente contribui positivamente para o processo de gestão de riscos, atenuando a exposição das organizações a eventos críticos de riscos e contribuindo para o fortalecimento do seu ambiente integrado de gestão de riscos corporativos relacionados a LGPD.

Assim, esta pesquisa contribui para o avanço da literatura sobre gerenciamento de riscos relacionados a LGPD, ao fornecer novas evidências a respeito dos papéis da auditoria independente no processo de gestão de riscos, bem como ao destacar como a existência de fragilidades na estrutura de controle pode resultar em infrações relacionadas a referida Lei.

5.2 RECOMENDAÇÕES A ESTUDOS FUTUROS

A realização deste estudo evidenciou lacunas de pesquisa que poderão servir de base para realização de trabalhos futuros como a realização de um estudo sobre os resultados obtidos em futuras auditorias sobre o programa de proteção de dados, após sua implementação, e sobre os efeitos da implementação do canal de solicitação de dados no *site*, conforme previsto nos itens 1.4 e 1.5 do Quadro 6. Ainda poderão ser realizadas pesquisas para identificação sobre como as empresas auditadas conduziram o processo de mitigação de riscos por meio dos planos de ação dos auditores, onde poderá ser analisada a capacidade das empresas auditadas em tomar ações corretivas sobre riscos iminentes.

A análise de práticas de gestão de riscos relacionadas a LGPD também pode contribuir para a análise dos mecanismos de controle eficazes utilizados para minimizar tais exposições. Do mesmo modo, a avaliação de tais práticas pode contribuir para o entendimento dos fatores que atenuam os riscos de conformidade legal. Ao compreender as práticas de auditoria adotadas por diferentes empresas de auditoria e/ou auditores, pode-se inferir sobre a efetividade de sua atuação na definição dos processos de gestão de riscos de conformidade legal, como os relacionados a LGPD. Tais aspectos constituem-se importantes oportunidades de pesquisa para a realização de novos estudos.

REFERÊNCIAS

AJAO, Owolabi Sunday; OLAMIDE, Jayeoba Olajumoke; TEMITOPE, Ajibade Ayodeji. Evolution and development of auditing. **Unique Journal of Business Management Research**, v. 3, n. 1, p. 032-040, 2016.

ALVES, Aline. **Auditoria contábil avançada**. Porto Alegre: Sagah, 2017.

ASSI, Marcos. **Gestão de riscos com controles internos**. 2. ed. São Paulo: Saint Paul, 2021.

ATTIE, William. **Auditoria:** Conceitos e Aplicações, 7 ed.- São Paulo: Atlas: Grupo GEN, 2018.

BARDIN, Laurence. **Análise de conteúdo**. Tradução de Luís Antero Reto, Augusto Pinheiro. São Paulo: Edições 70, 2016.

BAYBUTT, Paul. Guidelines for designing risk matrices. **Process safety progress**, v. 37, n. 1, p.49-55, 2018. Disponível em: https://aiche.onlinelibrary.wiley.com/doi/abs/10.1002/prs.11905. Acesso em: 10 jan. 2023.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista Direitos Sociais e Políticas Públicas (Unifafibe)**, São Paulo, v. 8, n. 2, p. 18, 2020. Disponível em: https://apphotspot.com.br/wp-content/uploads/elementor/forms/Botelho,Marcos-C%C3%A9sar-A-LGPD-e-prote%C3%A7%C3%A3o-dados-crian%C3%A7as-e-adolescentes-artigo.pdf. Acesso em: 10 jan. 2023.

BRASIL. **Decreto 11.129, de 11 de julho de 2022.** Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Presidência da República Secretaria Geral. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11129.htm#art70. Acesso em: 10 jan. 2023.

_____. **Lei n. 12.846, de 01 de agosto de 2013.** Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Presidência da República Casa Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 10 jan. 2023.

_____. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Presidência da República Secretaria Geral. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jan. 2023.

_____. NBC TA 00 – Estrutura conceitual para trabalhos de asseguração. **Conselho Federal de Contabilidade**. Disponível em https://www.cosif.com.br/publica.asp?arquivo=nbcta01ind. Acesso em: 10 jan. 2023.

_____. NBC TA 300 – Planejamento da Auditoria de Demonstrações Contábeis. **Conselho Federal de Contabilidade**. Disponível em: https://cfc.org.br/tecnica/normas-brasileiras-de-contabilidade/nbc-ta-de-auditoria-independente/. Acesso em: 10 jan. 2023.

_____. NBC TA 315 (R2) – Identificação e Avaliação dos Riscos de Distorção Relevante por meio do Entendimento da Entidade e do seu Ambiente. **Conselho Federal de Contabilidade.** Disponível em: https://cfc.org.br/tecnica/normas-brasileiras-de-contabilidade/nbc-ta-de-auditoria-independente/. Acesso em: 10 jan. 2023.

_____. NBC TA 500 (R1) – Evidência de Auditoria. **Conselho Federal de Contabilidade.** Disponível em: https://www2.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2016/NBCTA500(R1)&_ga=2.121069452.545859551.1688429453-810522823.1673880433. Acesso em: 10 jan. 2023.

_____. Resolução CVM n. 23, de 25 de fevereiro de 2021. Dispõe sobre o registro e o exercício da atividade de auditoria independente no âmbito do mercado de valores mobiliários, define os deveres e as responsabilidades dos administradores das entidades auditadas no relacionamento com os auditores independentes. **Comissão de Valores Mobiliários.** Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cvm-n-23-de-25-de-fevereiro-de-2021-305408516. Acesso em: 10 jan. 2023.

BROMILEY, P.; MCSHANE, M.; NAIR; A.; RUSTAMBEKOV, E. (2015). **Enterprise risk management**: Reviw, critique, and research directions. Long range planning, 48 (4), 265-276.

BYRNES, Paul Eric; AL-AWADHI, Abdullah; GULLVIST, Benita; LIBURD, Ryan Teeter; WARREN JR, Donald; VASARHELYI, Miklos. Evolution of auditing: From the traditional approach to the future audit. In: **Continuous auditing: Theory and application**. Emerald Publishing Limited, 2018. p. 285-297.

COSO - Committee of Sponsoring Organization of the Treadway Commission. **Enterprise risk management:** integrated framework. New York, AICPA, 2004.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. **Gerenciamento de Riscos Corporativos:** Estrutura Integrada, 2007. Disponível em: https://auditoria.mpu.mp.br/pgmq/COSOIIERMExecutiveSummaryPortuguese.pdf. Acesso em: 17 maio 2023.

CREPALDI, Silvio Aparecido. **Auditoria Contábil** - Teoria e Prática. 6.ed. São Paulo: Atlas, 2019.

DEMETZOU, Katerina. Data Protection Impact Assessment: A tool for accountability and the unclarified concept of ‘high risk’in the General Data Protection Regulation. **Computer Law & Security Review**, v. 35, n. 6, p. 105342, 2019. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364918304357. Acesso em: 17 maio 2023.

GAUDÊNCIO, Marina Penazzi; SCHRAMM, Fernando; SILVA, Vanessa Batista de S. **Aplicação da matriz de probabilidade e impacto no gerenciamento de projetos em uma empresa de construção metálica.** *In:* XXXIX Encontro Nacional de Engenharia de Produção; 2019. Santos, São Paulo. Disponível em: https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=Aplica%C3%A7%C3%A3o+da+matriz+de+probabilidade+e+impacto+no+gerenciamento+de+projetos+em+uma+empresa+de+constru%C3%A7%C3%A3o+met%C3%A1lica&btnG. Acesso em: 10 jan. 2023.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

HOPKIN, Paul. **Fundamentals of risk management: understanding, evaluating and implementing effective risk management**. 2.ed. United States: Kogan Page Publishers, 2018.

LINS, Luiz dos Santos. **Auditoria:** uma abordagem prática com ênfase na auditoria externa. 4. ed. São Paulo, Atlas, 2017.

LONGO, Eduardo. The Knowledge Management Role in Mitigating opertional risk Synapsing. **Proceedings of the ECIC,(Stam C., ed)**, p. 314-320, 2012.

Manual de Dissertações e Teses da UFSM (Recurso eletrônico): **Estrutura e apresentação documental para trabalhos acadêmicos.** Universidade Federal de Santa Maria. Pró-reitoria de pós-graduação e pesquisa, Biblioteca da UFSM, Ed UFSM, Santa Maria, RS, 2021.Disponível em: <https://www.ufsm.br/app/uploads/sites/538/2021/12/MDT_UFSM_2021.pdf>. Acesso em 02 out. 2022.

NAKAMURA, Emilio; FORMIGONI FILHO, José Reynaldo; IDE, Marcos Cesar. Metodologia de Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais. *In*: WORKSHOP DE REGULAÇÃO, AVALIAÇÃO DA CONFORMIDADE E CERTIFICAÇÃO DE SEGURANÇA, 5., 2019, São Paulo. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019. p. 11-16. DOI: https://doi.org/10.5753/wrac.2019.14032. Disponível em: https://sol.sbc.org.br/index.php/wrac/article/view/14032. Acesso em: 17 jun. 2023.

NAMAZIAN, A.; ESLAMI, N. Operational risk management (ORM). **Australian Journal of Basic and Applied Sciences**, v. 5, n. 12, p. 3240-3245, 2011.

OLIVEIRA, Marcelo Knopf de. **A importância da matriz de riscos no planejamento da auditoria**. 2015, 89f. Dissertação (Mestrado em economia, modalidade profissionalizante com ênfase em controladoria). Programa de pós

graduação em economia. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015.

OLIVEIRA JÚNIOR, Antonio José Saraiva de; GOMES, Arnaldo Ribeiro; VASCONCELLOS MACHADO, Guilherme de. Metodologia de auditoria com foco em processo e risco. **Revista do TCU**, n. 132, p. 28-37, 2015. Disponível em: https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/249. Acesso em: 15 jun. 2023.

PINHEIRO, Patricia Peck Garrido. **Proteção de dados pessoais:** comentários à lei n. 13.709/2018 (LGPD). São Paulo, SP: Editora Saraiva, 2023. *E-book*. ISBN 9786555599480. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599480/. Acesso em: 17 jun. 2023.

RAMZAN, Muhammad; AHMED, Ishfaq; RAFAY, Abdul. Is Auditor Independence Influenced by Non-Audit Services? A Stakeholder's Viewpoint. **A Stakeholder's Viewpoint**, p. 388-408, 2020.

RAUPP, Fabiano Maury; BEUREN, Ilse Maria. Metodologia da pesquisa aplicável às ciências sociais. In: BEUREN, Ilse Maria (coord.). **Como elaborar trabalhos monográficos em contabilidade**: Teoria e prática. 3. ed. São Paulo, Atlas, 2006. 97p.

RIBEIRO, Osni Moura; RIBEIRO, Juliana Moura. **Auditoria fácil**. 2.ed. São Paulo: Saraiva Educação SA, 2017.

SILVEIRA, Renato de Mello Jorge. **Compliance, direito penal e lei anticorrupção**, São Paulo, SP: Editora Saraiva, 2015. *E-book*. ISBN 9788502622098. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502622098/. Acesso em: 17 jun. 2023.

UNIÃO EUROPEIA. Regulamento 2016/679, de 27 de abril de 2016. **Regulamento Geral Sobre a Proteção de Dados.** 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/ PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em: 10 jan. 2023

WEBWE, Elson Luciano; DIEHL, Carlos Alberto. Gestão de riscos operacionais: um estudo bibliográfico sobre ferramentas de auxílio. **Revista de Contabilidade do Mestrado em Ciências contábeis da UERJ**, Rio de Janeiro, v. 19, n. 3, 2016. Disponível em: http://atena.org.br/revista/ojs-2.2.3-06/index.php/UERJ/article/viewArticle/2837. Acesso em: 17 maio 2023.

VOLAREVIĆ, Hrvoje; VAROVIĆ, Mario. Internal model for IFRS 9-Expected credit losses calculation. **Ekonomski pregled**, v. 69, n. 3, p. 269-297, 2018.

YIN, R. K. **Estudo de caso:** planejamento e métodos. Porto Alegre: Bookman, 2010.

ZONATTO, Vinícius Costa da Silva; BEUREN, Ilse Maria. Categorias de riscos evidenciadas nos relatórios da administração de empresas brasileiras com ADRs.

RBGN: Revista Brasileira de Gestão de Negócios, São Paulo, v. 12, n. 35, p. 141-155, 2010. Disponível em: http://dx.doi.org/10.5329/RECADM.20100902001. Acesso em: 10 jan. 2023.

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Título do Estudo: CONTRIBUIÇÕES DA AUDITORIA INDEPENDENTE PARA A GESTÃO DE RISCOS RELACIONADOS À LEI GERAL DE PROTEÇÃO DE DADOS
Pesquisadores responsáveis: Henrique Gabbi Bittencourt (Orientado) e Prof. Dr. Vinícius Costa da Silva Zonatto (Orientador)
Instituição/Departamento: Universidade Federal de Santa Maria (UFSM) / Departamento de Ciências Contábeis (DCC)
Área do Conhecimento/Curso: Ciências Sociais Aplicadas / Ciências Contábeis (abordagem comportamental)
Endereço postal completo: Av. Roraima n° 1000, Prédio 74C, Sala 4343. CEP.: 97105-900, Camobi - Santa Maria/RS
Contatos E-mail: henriquegabbi01@gmail.com ou viniciuszonatto@gmail.com
Local da Coleta: Vision Auditoria Ltda.

Prezado(a) Participante:

Você está sendo convidado(a) a participar da pesquisa intitulada “CONTRIBUIÇÕES DA AUDITORIA INDEPENDENTE PARA A GESTÃO DE RISCOS RELACIONADOS À LEI GERAL DE PROTEÇÃO DE DADOS”, que tem por objetivo “analisar as contribuições da auditoria independente para a gestão de riscos em LGPD”. Este documento contém todas as informações necessárias sobre a pesquisa que está sendo realizada. Sua colaboração neste estudo será de muita importância para nós. Sendo assim, consideramos importante prestarmos alguns esclarecimentos antes de convidá-lo a participar da pesquisa, respondendo voluntariamente aos questionamentos que lhe são apresentados, se assim desejar, bem como permitindo acesso a documentação necessária a realização do estudo proposto.

Em relação aos elementos de análise desta pesquisa, torna-se importante ressaltar que o propósito deste trabalho está relacionado a identificação de “como a auditoria independente pode contribuir para os processos de gestão de riscos referentes à Lei Geral de Proteção de Dados (LGPD). No contexto dos papéis de trabalho dos auditores, busca-se descrever e analisar os planejamentos e procedimentos utilizados em auditorias de gestão de riscos em LGPD, para que se possa compreender como ocorrem as auditorias realizadas com esta temática. A seguir, busca-se identificar os riscos de infração à LGPD por meio da aplicação dos planejamentos e procedimentos de auditoria nos casos analisados, de modo que se possa compreender como os programas de proteção de dados são estruturados e quais eventos representam riscos (fragilidades) para a estrutura de controle das organizações. Por fim, espera-se ainda avaliar (percentualmente) os graus de risco de infração à LGPD identificados em cada caso analisado, bem como identificar, a partir de suas recomendações, como são estruturados os planos de ação elaborados e recomendados para cada evento (risco) identificado.

Portanto, o nível de análise desta pesquisa são os relatórios de auditoria elaborados a partir de três casos auditados, sendo o nível de análise os programas de proteção de dados (e os apontamentos realizados pela auditoria em relação a estes programas em cada relatório elaborado/auditoria realizada.

Considera-se que os benefícios dessa pesquisa estão relacionados a um maior conhecimento sobre a percepção de auditores em relação as contribuições da auditoria independente para a gestão de riscos em LGPD. Em contrapartida, o risco a que você estará submetido(a) ao participar desta pesquisa está relacionado a um possível desconforto e cansaço devido ao tempo despendido no esclarecimento de dúvidas relacionadas a auditoria realizada, e a coleta de informações necessárias a realização deste Trabalho de Conclusão de Curso.

Se você tiver alguma consideração ou dúvida sobre a ética da pesquisa, entre em contato:
Comitê de Ética em Pesquisa - Cidade Universitária - Bairro Camobi - Av. Roraima, nº 1000, Reitoria, 2º andar - CEP: 97.105.900 - Santa Maria - RS. Telefone: (55) 3220-9362 - Fax: (55) 3220-8009. E-mail: comiteeticapesquisa@smail.ufsm.br. Web: www.ufsm.br/cep.

Esclarecimentos informados:

Informamos que a pesquisa aplicada é regida pelos princípios gerais relativos: (i) ao consentimento informado; (ii) a preocupação em não prejudicar as pessoas e as entidades em que elas trabalham; e, (iii) o compromisso em manter a confidencialidade das pessoas e da entidade. Assim, os seguintes procedimentos foram adotados para assegurar a confidencialidade dos participantes da pesquisa:

a) O respondente participará da pesquisa voluntariamente, se assim desejar;
b) Não haverá nenhuma compensação financeira para sua participação, e também não haverá custos para você participar;
c) O respondente terá liberdade de desistir ou de interromper a colaboração nesta pesquisa no momento em que desejar, sem necessidade de qualquer explicação;
d) A entrevista realizada não solicitará nenhuma identificação individual pessoal do participante ou da organização em que este atua;
e) Os dados coletados serão tratados de maneira consolidada;
f) Apenas os pesquisadores envolvidos terão acesso às informações coletadas e sem a identificação dos respondentes;
g) Ao preencher voluntariamente e entregar o instrumento de coleta de dados, o respondente concorda que sejam divulgados os resultados da pesquisa em publicações científicas; e,
h) Qualquer dúvida referente a pesquisa realizada pode ser esclarecida neste ou a qualquer momento com os pesquisadores responsáveis pela execução da pesquisa realizada, por meio de uma destas formas de contato: Telefone/WhatsApp (55) 99988-2698 e/ou e-mail: henriquegabbi01@gmail.com ou viniciuszonatto@gmail.com.

Declaração de ciência e aceite em participar da pesquisa:

Recebidas tais informações, se você desejar voluntariamente participar de nossa pesquisa, respondendo aos questionamentos apresentados (sem qualquer identificação pessoal), você declara:

a) ter recebido cópia assinada do Termo de Confidencialidade e do Termo de Consentimento Livre e Esclarecido Informado;
b) ter recebido todas as explicações e orientações necessárias ao esclarecimento de suas eventuais dúvidas particulares, se houverem;
c) estar ciente de que poderia ter deixado de participar da pesquisa a qualquer momento, sem qualquer explicação;
d) ter ciência de que os dados coletados serão tratados de maneira consolidada e utilizados única e exclusivamente na produção e divulgação de trabalhos acadêmicos; e,
e) concordar com os termos da pesquisa realizada.

Os pesquisadores declaram que as informações coletadas serão mantidas no Centro de Ciências Sociais e Humanas - CCSH, situado na Av. Roraima, nº 1000, Prédio 74C, Sala 4341 - Grupo de Pesquisas em Controladoria, Contabilidade Comportamental e Sistemas de Controle Gerencial (GPCCCSCG), CEP. 97.105.900, B. Camobi, Santa Maria - RS, sob a responsabilidade do Prof. Dr. Vinícius Costa da Silva Zonatto, por um período de 5 anos. Após esse período, os dados coletados serão destruídos.

Santa Maria/RS, ____ de _____ de 20__.

_____ _____

Henrique Gabbi Bittencourt Prof. Dr. Vinícius Costa da Silva Zonatto

_____

Assinatura do Participante da Pesquisa (opcional)

Se você tiver alguma consideração ou dúvida sobre a ética da pesquisa, entre em contato: Comitê de Ética em Pesquisa - Cidade Universitária - Bairro Camobi - Av. Roraima, nº 1000, Reitoria, 2º andar - CEP: 97.105.900 - Santa Maria - RS. Telefone: (55) 3220-9362 - Fax: (55) 3220-8009. E-mail: comiteeticapesquisa@smail.ufsm.br. Web: www.ufsm.br/cep.

TERMO DE CONFIDENCIALIDADE

Título do Estudo: CONTRIBUIÇÕES DA AUDITORIA INDEPENDENTE PARA A GESTÃO DE RISCOS RELACIONADOS À LEI GERAL DE PROTEÇÃO DE DADOS
Pesquisadores responsáveis: Henrique Gabbi Bittencourt (Orientado) e Prof. Dr. Vinícius Costa da Silva Zonatto (Orientador)
Instituição/Departamento: Universidade Federal de Santa Maria (UFSM) / Departamento de Ciências Contábeis (DCC)
Área do Conhecimento/Curso: Ciências Sociais Aplicadas / Ciências Contábeis (abordagem comportamental)
Endereço postal completo: Av. Roraima n° 1000, Prédio 74C, Sala 4343. CEP.: 97105-900, Camobi - Santa Maria/RS
Contatos E-mail: henriquegabbi01@gmail.com ou viniciuszonatto@gmail.com
Local da Coleta: Vision Auditoria Ltda.

Prezado(a) Participante:

Os pesquisadores proponentes deste projeto de pesquisa comprometem-se a assegurar a todas as pessoas participantes do estudo os esclarecimentos necessários a realização desta investigação, os quais podem ser obtidos pelos e-mails: henriquegabbi01@gmail.com ou viniciuszonatto@gmail.com ou pelo telefone (55) 99988-2698 (também WhatsApp). Do mesmo modo, os pesquisadores garantem aos indivíduos interessados em participar desta pesquisa a possibilidade de retirar seu consentimento de participação voluntária em nossa investigação a qualquer momento, sem a necessidade de apresentação de qualquer satisfação ou sem sofrer penalização alguma.

Fica assegurado a todos os indivíduos convidados a participar desta pesquisa o esclarecimento de que sua participação é voluntária e facultativa, bem como o seu direito de desistir de participar da pesquisa a qualquer momento, mesmo tendo iniciado a resposta aos questionamentos apresentados. Além disso, os pesquisadores também garantem a todos os potenciais participantes da pesquisa a confidencialidade dos dados dos participantes, através da apresentação deste Termo de Confidencialidade e a não identificação dos respondentes e das respostas obtidas.

Uma vez que a coleta de dados será realizada por meio de entrevistas e a análise de documentos disponibilizados, não haverá necessidade de identificação alguma dos respondentes ou da organização em que atuam, o que preserva sua privacidade e o sigilo de suas respostas. Os dados coletados são armazenados pelos pesquisadores sem qualquer identificação individual do respondente.

Adicionalmente, será assegurado aos participantes da pesquisa que os dados coletados serão tratados e analisados de maneira consolidada, preservando-se o sigilo e a privacidade dos sujeitos cujas informações serão estudadas, assegurando-se ainda que as informações coletadas serão utilizadas única e exclusivamente para a execução do projeto de pesquisa em questão, bem como, que os resultados desta pesquisa somente serão divulgados de forma anônima e consolidada, não sendo usadas quaisquer indicações que possam identificar o sujeito da pesquisa. As informações coletadas por meio das entrevistas realizadas servirão para a compreensão dos temas envoltos neste projeto, das práticas de auditoria adotadas e as questões relacionados aos elementos de análise que permitirão responder aos objetivos desta pesquisa. Portanto, não terão outra finalidade que não estas, e não serão divulgadas.

Se você tiver alguma consideração ou dúvida sobre a ética da pesquisa, entre em contato: Comitê de Ética em Pesquisa - Cidade Universitária - Bairro Camobi - Av. Roraima, nº 1000, Reitoria, 2º andar - CEP: 97.105.900 - Santa Maria - RS. Telefone: (55) 3220-9362 - Fax: (55) 3220-8009. E-mail: comiteeticapesquisa@smail.ufsm.br. Web: www.ufsm.br/cep.

Os pesquisadores declaram ainda ter conhecimento de que as informações pertinentes às técnicas do projeto de pesquisa somente podem ser acessadas por aqueles que assinaram o Termo de Confidencialidade, excetuando-se os casos em que a quebra de confidencialidade é inerente à atividade ou que a informação e/ou documentação já for de domínio público. Por fim, os pesquisadores declaram que as informações coletadas e tabuladas automaticamente em planilha eletrônica serão mantidas no Centro de Ciências Sociais e Humanas - CCSH, situado na Av. Roraima, nº 1000, Prédio 74C, Sala 4341 - Grupo de Pesquisas em controladoria, Contabilidade Comportamental e Sistemas de Controle Gerencial (GPCCCSCG), CEP. 97.105.900, B. Camobi, Santa Maria - RS, sob a responsabilidade do Prof. Dr. Vinícius Costa da Silva Zonatto, por um período de 5 anos. Após esse período, os dados coletados serão destruídos.

Santa Maria/RS, ____ de _____ de 20__.

_____	_____
Henrique Gabbi Bittencourt	Prof. Dr. Vinícius Costa da Silva Zonatto

Se você tiver alguma consideração ou dúvida sobre a ética da pesquisa, entre em contato: Comitê de Ética em Pesquisa - Cidade Universitária - Bairro Camobi - Av. Roraima, nº 1000, Reitoria, 2º andar - CEP: 97.105.900 - Santa Maria - RS. Telefone: (55) 3220-9362 - Fax: (55) 3220-8009. E-mail: comiteeticapesquisa@smail.ufsm.br. Web: www.ufsm.br/cep.

ROTEIRO DE ENTREVISTAS

Como são elaborados os planos (planejamentos e procedimentos) de auditoria para avaliação de programas de proteção de dados em LGPD?

Quais os principais cuidados que o auditor precisa ter para efetuar a auditoria em programas de proteção de proteção de dados em LGPD, de modo que possa apresentar recomendação com segurança razoável a organização auditada?

As organizações auditadas, que adotam programas formais de proteção de dados, adotam medidas suficientes para a gestão de riscos em LGPD?

Quais são as principais preocupações observadas nas auditorias realizadas em relação ao tratamento de dados em programas de proteção de dados em LGPD?

Quais são as principais fragilidades identificadas nas auditorias realizadas em relação a programas de proteção de dados em LGPD?

Quais os principais eventos que representam riscos a proteção de dados em LGPD?

Como a auditoria independente pode contribuir para a proteção de dados em LGPD?