SemeAd 2025
XXVIII Seminários em Administração

10, 11, 12, 13 e 14 de novembro de 2025
ISSN 2177-3866

PERCEPÇÃO DOS ALUNOS DE CIÊNCIAS CONTÁBEIS SOBRE SEGURANÇA DA INFORMAÇÃO E SUA RELAÇÃO COM A PRÁTICA CONTÁBIL

JOÃO BATISTA BOSCAINI
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL (UFRGS)

GIOVANA SORDI SCHIAVI
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL (UFRGS)

VITOR MORAES
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL (UFRGS)

PERCEPÇÃO DOS ALUNOS DE CIÊNCIAS CONTÁBEIS SOBRE SEGURANÇA DA INFORMAÇÃO E SUA RELAÇÃO COM A PRÁTICA CONTÁBIL

1 INTRODUÇÃO

O avanço da tecnologia e a crescente digitalização de processos têm proporcionado benefícios significativos tanto na esfera pessoal quanto profissional (Laudon & Laudon, 2022). A disseminação de dispositivos conectados, o armazenamento em nuvem e a automação de tarefas contábeis otimizam operações e possibilitam maior eficiência na análise e no compartilhamento de informações (Faria, Maçada & Kumar, 2017). No contexto contábil, a informatização tem facilitado a organização e o acesso a dados financeiros, reduzindo erros e agilizando a tomada de decisões, tornando-se um pilar essencial para o exercício da profissão (Laudon & Laudon, 2022).

Com esse crescimento exponencial no volume de dados circulando em meios digitais, surgem também preocupações relacionadas à segurança da informação (Laudon & Laudon, 2022). Vazamentos, acessos indevidos e ataques cibernéticos podem comprometer dados sensíveis, causando prejuízos financeiros, danos reputacionais e implicações legais para indivíduos e organizações (ISACA, 2013). O Brasil está entre os países líderes em ataques cibernéticos, conforme apontado pelo Norton Cybersecurity Insights Report (2017). Além disso, a dependência de sistemas digitais torna as informações contábeis alvos potenciais para fraudes, espionagem e ataques hackers (Abu-Musa, 2003).

Diante desse cenário, diversos marcos legais foram estabelecidos para regulamentar a segurança da informação e a proteção de dados pessoais. No contexto internacional, destaca-se o Regulamento Geral sobre a Proteção de Dados (GDPR), da União Europeia, que influenciou a criação de legislações semelhantes em outras nações (International Telecommunication Union, 2009). No Brasil, a Lei Geral de Proteção de Dados (LGPD) impõe diretrizes sobre o tratamento e a proteção de informações pessoais, exigindo que empresas e profissionais adotem medidas adequadas de segurança (Brasil, 2018). Além da legislação, práticas como auditorias especializadas, implementação de sistemas de proteção, treinamentos corporativos e a conscientização sobre boas práticas digitais são fundamentais para minimizar riscos (Kruger & Kearney, 2008).

No campo da contabilidade, a proteção de dados assume relevância ainda maior, visto que os profissionais são responsáveis por informações críticas, como balanços patrimoniais, demonstrações contábeis e declarações fiscais (Ribeiro et al., 2020). O acesso indevido a esses dados pode gerar impactos significativos para clientes e empresas, exigindo que os profissionais contábeis adotem práticas de segurança da informação alinhadas às exigências legais e às melhores práticas do mercado (Herath, 2011). Dessa forma, a implementação de protocolos eficazes de proteção se torna essencial para garantir conformidade regulatória e preservar confiança de clientes nos serviços contábeis (CFC, 2024).

Embora a segurança da informação seja frequentemente tratada como uma questão técnica, seu gerenciamento envolve também aspectos estratégicos e organizacionais (Knapp *et al*., 2009). Contadores não devem apenas depender de soluções tecnológicas externas, mas sim assumir um papel ativo na implementação e na supervisão das práticas de proteção de dados (Sarder & Haschak, 2019). Dessa forma, a segurança da informação deve ser vista como um elemento essencial da gestão contábil, e não apenas como uma responsabilidade delegada a setores de tecnologia ou terceiros (Knapp et al., 2009).

Entretanto, pesquisas indicam que, apesar do reconhecimento da importância da segurança da informação, há um distanciamento dos profissionais contábeis em relação à sua aplicação prática (Boss et al., 2022). O estudo de Ribeiro et al. (2020) aponta que contadores compreendem os riscos associados à proteção de dados, mas ainda se sentem inseguros sobre

como implementá-la em seu cotidiano profissional. Diante disso, torna-se relevante ampliar a discussão para o contexto acadêmico, investigando como a segurança da informação tem sido abordada na formação dos futuros contadores (Boss et al., 2022). A escolha da Universidade Federal do Rio Grande do Sul (UFRGS) como campo de estudo se justifica pela presença de disciplinas voltadas para sistemas contábeis, permitindo analisar como os alunos percebem esse tema e o impacto da formação na preparação para os desafios do mercado.

Nesse contexto, esta pesquisa busca responder à questão: **Qual é a percepção dos alunos de Ciências Contábeis da UFRGS sobre segurança da informação e sua relação com a prática contábil?** O objetivo geral é analisar a percepção dos alunos de Ciências Contábeis da UFRGS sobre segurança da informação e sua relação com a prática contábil, identificando lacunas de conhecimento e desafios na aplicação da segurança da informação no âmbito contábil. Os objetivos específicos incluem: (i) avaliar o nível de familiaridade dos estudantes com os princípios da segurança da informação e a LGPD; (ii) identificar as principais dificuldades enfrentadas na adoção de práticas de proteção de dados; e (iii) examinar a influência das disciplinas de sistemas na formação dos alunos sobre esse tema.

A relevância desta pesquisa reside na necessidade de aproximar a segurança da informação da prática contábil, contribuindo para a capacitação dos futuros profissionais em um cenário cada vez mais digital e regulamentado (Boss et al., 2022). Além disso, os resultados fornecem subsídios para aprimorar a formação acadêmica e auxiliar na implementação de estratégias que integrem a proteção de dados como uma competência essencial na contabilidade. Dessa forma, este estudo busca gerar impacto tanto no meio acadêmico quanto na prática profissional, incentivando uma maior conscientização e preparo para lidar com desafios relacionados à segurança da informação.

2 REFERENCIAL TEÓRICO

Nesta seção, apresenta-se o referencial teórico que embasa esta pesquisa, abordando conceitos fundamentais e práticas relacionadas à segurança da informação, bem como sua aplicabilidade no contexto contábil. Inicialmente, são discutidos os conceitos essenciais de segurança da informação, sua evolução ao longo do tempo e as principais tecnologias associadas ao tema, como criptografia, inteligência artificial (IA), internet das coisas (IoT) e sistemas integrados de gestão (ERP). De forma complementar, são abordadas regulamentações sobre proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados (LGPD), além das boas práticas adotadas pelas empresas para garantir a segurança das informações.

Na sequência, trata-se da importância da segurança da informação no setor contábil, considerando o grande volume de dados sensíveis manipulados pelos profissionais da área. São exploradas as vulnerabilidades específicas desse setor, as medidas adotadas para mitigar riscos e a necessidade de que a segurança da informação seja incorporada tanto na prática profissional quanto na formação acadêmica dos futuros contadores.

2.1 SEGURANÇA DA INFORMAÇÃO E SUAS PRÁTICAS

A segurança da informação pode ser definida como o conjunto de práticas, processos e tecnologias voltadas para a proteção de dados contra acessos não autorizados, modificações indevidas ou destruição acidental (International Telecommunication Union, 2009). Seu objetivo principal é garantir confidencialidade, integridade e disponibilidade das informações, princípios da gestão segura de dados no ambiente digital (ISO/IEC 27001, 2013).

O conceito de segurança da informação evoluiu à medida que as tecnologias de processamento e armazenamento de dados foram se desenvolvendo (Sarder & Haschak,

2019). Com a digitalização de processos empresariais, tornou-se essencial implementar medidas que assegurem a proteção das informações contra ameaças como ataques cibernéticos, fraudes e espionagem corporativa (Laudon & Laudon, 2022). O Brasil está entre os países mais visados para crimes cibernéticos, o que reforça a importância da adoção de medidas robustas para minimizar riscos (Norton Cybersecurity Insights Report, 2017).

A evolução da segurança da informação acompanha os avanços tecnológicos e organizacionais. Inicialmente, a preocupação estava centrada na proteção física de documentos e dados armazenados em servidores locais. Com a digitalização crescente, surgiram soluções como bancos de dados criptografados, inteligência artificial (IA) para monitoramento de ameaças, internet das coisas (IoT) para controle de acessos, sistemas integrados de gestão (ERP) e computação em nuvem para armazenamento seguro (Faria, Maçada & Kumar, 2017). Essas tecnologias auxiliam na automatização da segurança e na detecção precoce de anomalias, tornando os processos mais eficientes (ISACA 2013).

Diante da crescente complexidade do ambiente digital, novas regulamentações foram criadas para garantir a proteção dos dados pessoais e empresariais. No contexto internacional, destaca-se o Regulamento Geral sobre a Proteção de Dados (GDPR), implementado pela União Europeia, que influenciou legislações em diversos países (International Telecommunication Union, 2009). No Brasil, a Lei Geral de Proteção de Dados (LGPD), Lei n.º 13.709/2018, estabelece diretrizes para o tratamento adequado de informações pessoais, exigindo que empresas adotem práticas de segurança específicas para evitar vazamentos e acessos indevidos (Brasil, 2018).

Além das regulamentações, as empresas têm adotado diversas boas práticas para garantir a proteção dos dados e mitigar riscos relacionados à segurança da informação. Entre as principais medidas, destaca-se o uso da criptografia, um método essencial para proteger a integridade das informações armazenadas e transmitidas digitalmente, garantindo que apenas usuários autorizados possam acessá-las (Knapp et al., 2009). Outra estratégia amplamente utilizada é a autenticação multifator, que adiciona camadas extras de segurança ao processo de login, dificultando o acesso não autorizado aos sistemas (Kruger & Kearney, 2008).

Além dessas medidas, as organizações têm investido no monitoramento contínuo dos sistemas, utilizando inteligência artificial para detectar padrões suspeitos e prevenir possíveis ataques cibernéticos (Faria, Maçada & Kumar, 2017). A implementação de políticas de *backup* e recuperação de desastres também é fundamental para evitar a perda irreparável de dados em casos de falhas técnicas ou ataques ransomware (ISO/IEC 27001, 2013).

No entanto, nenhuma dessas medidas é eficaz sem a conscientização e o treinamento dos colaboradores, uma vez que falhas humanas continuam sendo uma das principais causas de incidentes de segurança da informação (Kruger & Kearney, 2008). A capacitação dos funcionários para identificar ameaças, como *phishing* e engenharia social, é crucial para reduzir vulnerabilidades e garantir uma cultura organizacional voltada à segurança dos dados.

Com essa crescente demanda por segurança, novas funções especializadas surgiram dentro das empresas, como analista de segurança da informação, engenheiro de cibersegurança e especialista em governança de TI, se tornaram essenciais para garantir a conformidade com as normas e minimizar vulnerabilidades (ISACA, 2013). No entanto, a segurança da informação não deve ser tratada apenas como uma questão tecnológica, mas também como uma responsabilidade gerencial. Mesmo empresas que não possuem um setor de TI estruturado precisam estabelecer políticas e procedimentos para a gestão da segurança da informação (Sarder & Haschak, 2019). Dessa forma, a governança de TI deve ser incorporada à cultura organizacional, promovendo a integração entre diferentes setores para garantir um ambiente digital seguro Ribeiro et al. (2020). Nesse sentido, a segurança da informação constitui um campo dinâmico, que evolui constantemente para acompanhar ameaças emergentes, exigindo tanto investimento tecnológico quanto políticas eficazes de

gestão — especialmente em setores que lidam com dados sensíveis, como a contabilidade, tema aprofundado na seção seguinte.

2.2 SEGURANÇA DA INFORMAÇÃO NA ÁREA CONTÁBIL

A contabilidade é uma área que lida diretamente com um grande volume de informações sensíveis, incluindo dados financeiros, patrimoniais e fiscais de empresas e indivíduos (Herath, 2011). O acesso indevido ou vazamento dessas informações pode gerar impactos significativos, como fraudes, prejuízos financeiros e sanções legais (CFC, 2024). Assim, a segurança da informação contábil é mais do que uma necessidade operacional, mas um fator estratégico para a credibilidade dos serviços prestados (Herath, 2011).

O profissional contábil atua diariamente com informações detalhadas sobre transações financeiras, folha de pagamento, tributos e planejamento estratégico de empresas (Ribeiro et al. 2020). Como essas informações são armazenadas digitalmente em sistemas contábeis, são alvos de ataques cibernéticos, que podem comprometer a integridade e confidencialidade dos dados (Abu-Musa, 2003). Segundo Ribeiro et al. (2020), muitos profissionais contábeis reconhecem a importância da segurança da informação, mas sentem dificuldades na sua aplicação prática, reforçando a necessidade de capacitação e medidas preventivas.

A Lei Geral de Proteção de Dados (LGPD) também impacta diretamente os escritórios contábeis, pois determina que qualquer organização que armazene ou processe dados pessoais deve garantir sua segurança e transparência no tratamento das informações (Brasil, 2018). Isso significa que os contadores precisam adotar políticas de proteção de dados, controle de acessos, criptografia e medidas de conformidade legal para evitar penalidades e proteger a privacidade dos clientes (Cots; Oliveira, 2018).

Para mitigar riscos e fortalecer a proteção dos dados contábeis, diversas práticas vêm sendo amplamente adotadas no setor. Uma das principais medidas é a utilização de softwares contábeis seguros, que incorporam criptografia de dados e *backups* automáticos, garantindo maior proteção contra acessos indevidos e falhas técnicas (Knapp et al., 2009). Além disso, a implementação de um controle rigoroso de acessos tem sido essencial para assegurar que apenas profissionais autorizados possam manipular informações sensíveis, reduzindo a exposição a fraudes e vazamentos (ISO/IEC 27001, 2013).

Outra prática fundamental é a política de segurança interna, que estabelece diretrizes claras para o armazenamento, compartilhamento e descarte de informações contábeis, assegurando conformidade com normas e regulamentações vigentes (Herath, 2011). Além disso, a realização de auditorias periódicas permite identificar possíveis vulnerabilidades nos sistemas contábeis, possibilitando ajustes preventivos antes que falhas possam ser exploradas por agentes mal-intencionados (Sarder & Haschak, 2019).

Por fim, a educação e a conscientização de profissionais contábeis sobre boas práticas de segurança da informação são essenciais para minimizar riscos. Muitos ataques cibernéticos exploram falhas humanas, como o desconhecimento sobre *phishing*, engenharia social e senhas fracas, tornando essencial a capacitação contínua desses profissionais para que identifiquem ameaças e adotem medidas preventivas (Knapp et al., 2009).

Além das práticas organizacionais, a formação acadêmica do contador deve evoluir para abranger o tema da segurança da informação. Atualmente, as Diretrizes Curriculares Nacionais (DCN) para o curso de Ciências Contábeis já incorporam conteúdos relacionados a tecnologia e sistemas de informação (Brasil, 2024), mas ainda há lacunas entre conhecimento teórico e aplicação prática (Ribeiro et al. 2020). A UFRGS, por exemplo, inclui disciplinas voltadas para sistemas contábeis, trabalhando essa temática contemporânea; entretanto, dados apontam que a abordagem sobre segurança da informação pode ser ampliada para preparar futuros contadores para os desafios do mercado digital (Ribeiro et al., 2020).

A falta de percepção da segurança da informação como uma responsabilidade gerencial também é um desafio (ISACA 2013). Muitas empresas veem a proteção de dados apenas como um custo adicional, e não como um investimento essencial para a continuidade do negócio (Sarder & Haschak, 2019). No entanto, com o crescimento das ameaças digitais e as exigências regulatórias, torna-se fundamental que os contadores assumam um papel ativo na gestão da segurança da informação, garantindo que seus clientes e empregadores adotem medidas adequadas de proteção (Herath, 2011).

Dessa forma, a segurança da informação na contabilidade deve ser encarada não apenas como uma questão técnica, mas também como uma estratégia gerencial que impacta diretamente a confiabilidade dos serviços contábeis (Knapp et al., 2009). O fortalecimento da educação acadêmica, a implementação de boas práticas e o alinhamento às regulamentações vigentes são aspectos essenciais para que os profissionais contábeis possam atuar com mais segurança e eficiência em um cenário digital cada vez mais desafiador (Ribeiro et al., 2020).

3 PROCEDIMENTOS METODOLÓGICOS

Esta pesquisa busca responder à seguinte questão: Qual é a percepção dos alunos de Ciências Contábeis da UFRGS sobre segurança da informação e sua relação com a prática contábil? O objetivo geral é analisar a percepção dos alunos de Ciências Contábeis da UFRGS sobre segurança da informação e sua relação com a prática. Para alcançar esse objetivo, a pesquisa adotou abordagens qualitativas e quantitativas, caracterizando-se como descritiva. A principal técnica de coleta de dados foi a utilização de grupos focais, complementada por observação participante e questionários aplicados antes e depois das atividades propostas.

As unidades de análise foram os alunos matriculados em disciplinas de sistemas de informações gerenciais da UFRGS. A coleta de dados deu-se por meio de grupos focais, uma técnica qualitativa que reúne pequenos grupos de participantes para discutir temas específicos, permitindo a obtenção de *insights* profundos sobre suas percepções e experiências (BEUREN, 2003), de questionários e de observação participante. Para a contextualização da coleta de dados entre os alunos, foi desenvolvida uma aula e uma atividade sobre segurança da informação, a qual foi aplicada durante aulas de sistemas de informação gerenciais, no semestre de 2025/1. Os alunos foram divididos em três grupos, cada um responsável por analisar e resolver um estudo de caso relacionado ao tema. Antes da aula e da atividade, foi aplicado um questionário para avaliar a percepção inicial dos alunos sobre segurança da informação, seu comportamento em relação ao tema, experiência profissional na área e práticas adotadas em suas empresas. Após a atividade, outro questionário foi aplicado para verificar mudanças na percepção dos alunos e avaliar a eficácia da atividade proposta. Além disso, questionamentos foram feitos a cada grupo, buscando a percepção deles sobre a temática em análise, a partir de grupos focais. Por fim, a observação participante foi realizada durante toda a atividade, registrando interações, discussões e comportamentos dos alunos.

Os instrumentos de coleta de dados incluíram roteiros de condução dos grupos focais, roteiro de observação e questionários estruturados. A elaboração desses instrumentos foi baseada nos artigos previamente analisados, que abordam metodologias semelhantes e oferecem diretrizes para a construção de ferramentas de pesquisa eficazes (Boss et al., 2022; Ribeiro et al., 2020). Os roteiros e questionários foram submetidos à validação por dois profissionais acadêmicos especializados em sistemas contábeis, garantindo sua adequação e relevância para os objetivos do estudo.

A coleta de dados ocorreu em abril de 2025, envolvendo 34 alunos participantes de disciplinas de Sistemas de Informação Gerencial. Para a realização dos grupos focais, os alunos foram divididos em três grupos, porém não foi registrado o quantitativo exato de participantes em cada grupo, uma vez que a dinâmica priorizou a discussão coletiva e a

rotação dos integrantes entre as atividades propostas. Os questionários foram disponibilizados via Google Forms, permitindo a coleta e organização automatizada das respostas. Os dados coletados foram exportados para planilhas do Microsoft Excel para realização da análise quantitativa. Já dados qualitativos, oriundos dos grupos focais e das notas de observação, estes foram gravados, transcritos e registrados manualmente pelo pesquisador em documento de texto, captando as interações, percepções e reflexões dos alunos ao longo da atividade.

Para a análise dos dados, foram empregadas técnicas de estatística descritiva simples, visando sumarizar e descrever as respostas obtidas nos questionários pré e pós-atividade. As observações registradas durante os grupos focais e as respostas qualitativas das perguntas realizadas no grupo focal foram submetidas à análise de conteúdo, identificando categorias e padrões emergentes (Bardin, 2011), a partir de construções teóricas definidas a priori, que possam fornecer uma compreensão aprofundada das percepções e comportamentos dos alunos em relação à segurança da informação no contexto contábil.

4 ANÁLISE DOS DADOS

Esta seção apresenta a análise dos dados coletados na pesquisa, que buscou analisar a percepção dos alunos do curso de Ciências Contábeis da Universidade Federal do Rio Grande do Sul (UFRGS) sobre segurança da informação e sua relação com a prática contábil, identificando lacunas de conhecimento e desafios na aplicação da segurança da informação no âmbito contábil. A análise foi conduzida a partir das informações obtidas em dois momentos distintos: inicialmente, por meio de um questionário aplicado antes da atividade de grupo focal, com o objetivo de mapear o perfil dos participantes, seu nível de familiaridade com os conceitos de segurança da informação e LGPD, bem como as dificuldades percebidas na adoção de práticas de proteção de dados; e, posteriormente, por meio de um questionário aplicado após a atividade, além de perguntas qualitativas durante o grupo focal, buscando compreender a influência das disciplinas de sistemas na formação dos alunos sobre o tema.

Dessa forma, os dados são apresentados e discutidos de acordo com os três objetivos específicos da pesquisa, que consistem em: (i) avaliar o nível de familiaridade dos estudantes com os princípios da segurança da informação e a LGPD; (ii) identificar as principais dificuldades enfrentadas na adoção de práticas de proteção de dados; e (iii) examinar a influência das disciplinas de sistemas na formação dos alunos sobre esse tema. A seguir, os resultados são organizados conforme cada um desses objetivos, permitindo uma análise estruturada e alinhada às questões de pesquisa que nortearam este estudo.

4.1 CARACTERIZAÇÃO DA AMOSTRA

A amostra deste estudo é composta por alunos de disciplinas de sistemas de informações gerenciais, do curso de Ciências Contábeis da Universidade Federal do Rio Grande do Sul (UFRGS). Participaram da pesquisa 34 estudantes, que responderam ao questionário pré-atividade, aplicado no contexto da aula sobre segurança da informação e proteção de dados. A análise demográfica da amostra revela uma predominância de jovens adultos entre 20 e 25 anos, padrão compatível com o perfil esperado de estudantes de graduação em formação inicial. Apesar de ligeira maioria masculina (55,88%), a distribuição etária é semelhante entre os gêneros. Em termos de atuação profissional, 52,94% dos respondentes afirmaram atuar na área contábil, 41,17% em outras áreas e 5,89% declararam estar exclusivamente dedicados aos estudos. Entre os que atuam na contabilidade, destaca-se a presença em escritórios contábeis (27,78%), seguida por consultoria financeira, auditoria e departamentos internos (16,67% cada), refletindo diversidade nas experiências dos alunos.

Quanto às funções desempenhadas, a posição de estagiário é a mais frequente (20,59%), seguida por cargos técnicos como analista contábil (14,71%), auditor e assistente (ambos com 8,82%). Um aspecto relevante é que 47,07% dos alunos indicaram exercer "outras funções", o que aponta para um perfil profissional heterogêneo, que pode incluir atividades administrativas, comerciais ou fora da contabilidade propriamente dita. No que se refere à formação acadêmica, a maioria dos estudantes (88,23%) está cursando sua primeira graduação, enquanto 11,77% já possuem diploma em outra área, indicando presença de alunos em processo de requalificação profissional.

A análise da amostra revela um grupo predominantemente formado por estudantes jovens, com idades entre 20 e 25 anos, e uma proporção relativamente equilibrada em termos de gênero, com leve predominância do público masculino. Observa-se que mais da metade dos respondentes já atuam na área contábil, especialmente em escritórios de contabilidade, consultorias, auditorias e departamentos contábeis de empresas, o que oferece uma visão prática relevante sobre o tema investigado. As funções ocupadas pelos participantes indicam, em sua maioria, profissionais em processo de formação ou início de carreira, o que torna ainda mais pertinente a investigação sobre sua percepção quanto à segurança da informação e à LGPD. O fato de que a ampla maioria dos alunos está cursando sua primeira graduação também reforça a importância de compreender como o tema da segurança da informação está sendo abordado durante a formação acadêmica, especialmente considerando o avanço das tecnologias, das demandas regulatórias e dos riscos digitais associados à prática contábil.

4.2 AVALIAÇÃO DO NÍVEL DE FAMILIARIDADE DOS ESTUDANTES COM SEGURANÇA DA INFORMAÇÃO E LGPD

Esta subseção apresenta os resultados obtidos com relação ao primeiro objetivo específico da pesquisa, que consiste em avaliar o nível de familiaridade dos estudantes com os conceitos de segurança da informação, LGPD e práticas associadas à proteção de dados. A avaliação foi realizada por meio de um conjunto de perguntas aplicadas no questionário pré-atividade, nas quais os participantes foram convidados a indicar, em uma escala de 1 a 5, seu grau de familiaridade com diferentes tópicos relacionados à segurança da informação.

Os itens avaliados incluíram aspectos conceituais, práticos e normativos, como (i) o conceito de segurança da informação, (ii) o conceito e a aplicabilidade da Lei Geral de Proteção de Dados (LGPD), (iii) estratégias para mitigação de riscos e práticas de proteção de dados, (iv) a relação entre segurança da informação e as atribuições do profissional contábil, e (v) a percepção sobre a responsabilidade do contador na adoção de medidas de proteção de dados. A seguir, a Tabela 3 apresenta a síntese com as médias obtidas para cada item avaliado, seguido da análise descritiva dos resultados.

Tabela 3 – Grau de familiaridade dos estudantes

Item Avaliado	Média
Grau de familiaridade com o conceito de segurança da informação	3,24
Grau de familiaridade com o conceito e aplicação da LGPD	3,18
Grau de familiaridade com estratégias de mitigação de riscos e proteção de dados	3,00
Grau de entendimento sobre a responsabilidade do contador na proteção de dados	2,91
Grau de familiaridade com práticas de segurança aplicadas à contabilidade	2,56

Fonte: Elaborado pelo autor com base nos dados.

Os resultados obtidos, sintetizados na Tabela 3, revelam um panorama intermediário em relação ao grau de familiaridade dos estudantes com os temas de segurança da informação e proteção de dados aplicados à prática contábil. O primeiro item analisado, "**Grau de familiaridade com o conceito de segurança da informação**", apresentou a maior média

entre os itens avaliados, com 3,24. Isso indica que os alunos possuem um conhecimento básico a intermediário sobre o conceito de segurança da informação. Esse resultado demonstra que, embora o tema seja relativamente conhecido, ele ainda não faz parte de uma compreensão consolidada entre os estudantes. Esse dado dialoga com o apontado por Ribeiro et al. (2020), que identificaram que os profissionais da contabilidade reconhecem a importância do tema, mas ainda apresentam dificuldades em aprofundar sua compreensão técnica e prática. Isso também reforça os apontamentos de Laudon e Laudon (2022), que destacam que a segurança da informação, apesar de fundamental no contexto empresarial, nem sempre é tratada como um tema prioritário fora dos setores especializados em TI.

Já o segundo item avaliado, "**Grau de familiaridade com o conceito e aplicação da LGPD**", apresenta uma média de 3,18, reforçando a percepção de um conhecimento superficial ou básico sobre a legislação. Considerando que a LGPD impacta diretamente a atuação dos profissionais contábeis, especialmente pela manipulação constante de dados pessoais de clientes, esse resultado evidencia uma lacuna formativa preocupante. Como discutido por Cots e Oliveira (2018) e refletido no estudo de Ribeiro et al. (2020), o desconhecimento dos princípios da legislação pode gerar riscos operacionais e legais para os profissionais e para as organizações.

O terceiro item, "**Grau de familiaridade com estratégias de mitigação de riscos e proteção de dados**", apresentou média de 3,00, indicando que os alunos possuem uma percepção inicial sobre essas práticas, mas sem um aprofundamento técnico ou aplicado. Este dado está alinhado às discussões de Kruger e Kearney (2008), que destacam que, embora as estratégias de segurança sejam amplamente difundidas no meio tecnológico, sua apropriação pelos setores não técnicos, como a contabilidade, ainda é limitada. O resultado também reforça o apontamento de Herath (2011), que defende que a segurança da informação deve ser vista não apenas como uma questão técnica, mas também como uma prática gerencial, o que ainda é pouco explorado no contexto contábil.

O quarto item avaliado, "**Grau de entendimento sobre a responsabilidade do contador na proteção de dados**", apresentou uma média de 2,91, considerada baixa. Esse resultado sugere que os estudantes têm dificuldades em compreender seu papel enquanto profissionais responsáveis pela proteção de dados no exercício da contabilidade. Esse cenário reflete uma percepção ainda equivocada de que a segurança da informação seria uma responsabilidade restrita às áreas de tecnologia, e não uma competência também ética, legal e gerencial dos contadores. Essa interpretação limitada já foi destacada por Knapp et al. (2009) e por Sarder e Haschak (2019), que defendem a necessidade de os profissionais, independentemente de sua formação técnica, assumirem uma postura ativa na gestão dos riscos relacionados à segurança da informação.

Por fim, o item "**Grau de familiaridade com práticas de segurança aplicadas à contabilidade**" apresentou a menor média entre os itens avaliados, 2,56, refletindo uma baixa familiaridade dos alunos quando a segurança da informação é contextualizada diretamente na prática contábil. Esse resultado evidencia que, embora haja algum nível de conhecimento sobre segurança da informação, esse saber não é automaticamente associado às atividades rotineiras da contabilidade. Esse achado dialoga com o estudo de Boss et al. (2022), que defendem a inserção de conteúdos de cibersegurança nos currículos de Ciências Contábeis como estratégia para combater essa lacuna formativa, preparando os futuros profissionais para lidar com desafios contemporâneos relacionados à segurança da informação.

De forma geral e consolidada, os resultados indicam que os estudantes possuem um nível de familiaridade que varia entre básico e intermediário em relação aos conceitos de segurança da informação e LGPD. Observa-se que, embora reconheçam os termos e tenham noções gerais sobre o tema, há uma lacuna significativa quando essas práticas são relacionadas diretamente ao contexto contábil. Os menores índices de familiaridade estão

justamente ligados à aplicação prática da segurança da informação na contabilidade e à compreensão da responsabilidade do contador na proteção dos dados, o que revela que o tema, embora presente de forma conceitual, ainda não é suficientemente aprofundado durante a formação acadêmica. Esses achados reforçam a necessidade de ampliar e aprofundar a abordagem do tema tanto nas disciplinas do curso quanto no desenvolvimento profissional dos futuros contadores, preparando-os para atuar em um cenário cada vez mais dependente de dados e regido por legislações como a LGPD.

4.3 PRINCIPAIS DIFICULDADES NA ADOÇÃO DE PRÁTICAS DE PROTEÇÃO DE DADOS

Esta subseção apresenta os resultados relacionados ao segundo objetivo específico da pesquisa, que busca identificar as principais dificuldades enfrentadas pelos alunos na adoção de práticas de proteção de dados, tanto na percepção acadêmica quanto na vivência profissional. A coleta foi realizada por meio de um conjunto de itens de múltipla escolha, nos quais os participantes puderam selecionar mais de uma alternativa, indicando os fatores que consideram desafiadores na adoção de práticas relacionadas à segurança da informação e à conformidade com a LGPD no ambiente organizacional. A Tabela 4 apresenta a síntese com a frequência das respostas obtidas.

Tabela 4 – Grau de dificuldade na adoção de práticas de proteção de dados

Dificuldade Apontada	Frequência Absoluta (n)	Frequência Relativa (%)
Utilizo práticas básicas de cibersegurança a partir do que conheço e utilizo para fins pessoais	10,00	20,83%
Minha empresa adota apenas práticas básicas e conhecidas de segurança da informação para as atividades desempenhadas	9,00	18,75%
Minha atividade é mais operacional e menos estratégica, não envolvendo pensar na segurança da informação	9,00	18,75%
Não busco me atualizar sobre esses temas	5,00	10,42%
Minha empresa terceiriza a segurança da informação e eu apenas sigo o que é recomendado	4,00	8,33%
Minha empresa não adota nenhuma prática estruturada de segurança da informação	3,00	6,25%
Minha empresa não tem uma área interna ou responsável de TI que suporte e oriente práticas de segurança da informação	3,00	6,25%
Segurança da informação nunca foi um problema nem ameaça para a minha empresa	2,00	4,17%
Minha empresa não acredita que será impactada por questões de segurança da informação	1,00	2,08%
Minha empresa não busca se atualizar sobre esses temas	1,00	2,08%
A segurança da informação não é uma prioridade na empresa	1,00	2,08%
A segurança da informação é tão somente uma fonte a mais de custo para a empresa	0,00	0,00%
Não percebo impacto direto da segurança da informação no meu trabalho	0,00	0,00%
Outras dificuldades (especificar: _____)	0,00	0,00%

Fonte: Elaborado pelo autor com base nos dados.

Os dados obtidos revelam um cenário em que as dificuldades estão divididas entre questões estruturais, operacionais e perceptivas. A dificuldade mais apontada foi "**Utilizo práticas básicas de cibersegurança a partir do que conheço e utilizo para fins pessoais**", com 20,83% das respostas. Este dado demonstra que, na ausência de diretrizes institucionais claras ou de uma cultura organizacional voltada para segurança, muitos alunos recorrem aos seus conhecimentos pessoais, aplicando práticas que, embora úteis, podem ser insuficientes

no contexto corporativo. Esse comportamento reflete uma lacuna tanto na formação profissional quanto na atuação das organizações em promover capacitação e políticas robustas de segurança da informação (Kruger & Kearney, 2008; Ribeiro et al., 2020).

Em segundo lugar, empatadas com 18,75%, aparecem as dificuldades relacionadas a duas questões: "**Minha empresa adota apenas práticas básicas e conhecidas de segurança da informação**", e "**Minha atividade é mais operacional e menos estratégica, não envolvendo pensar na segurança da informação**". Esses dados vão ao encontro da literatura sobre a percepção limitada de profissionais contábeis sobre segurança da informação. Eles reconhecem sua importância, mas, muitas vezes, a veem como responsabilidade de setores técnicos, ou então acreditam que, por estarem em funções operacionais, não têm participação direta no processo (Knapp et al., 2009; Herath, 2011; Sarder & Haschak, 2019).

Além das dificuldades de natureza operacional, os dados revelam obstáculos relacionados tanto ao comportamento individual dos alunos quanto às condições institucionais das organizações onde atuam. No plano individual, 10,42% dos participantes apontaram que "não buscam se atualizar sobre esses temas", o que, embora menos frequente, evidencia uma lacuna formativa importante. Essa falta de atualização pode ser reflexo de desinteresse, baixa sensibilização ou mesmo dificuldade de acesso a conteúdos técnicos, o que contribui para a manutenção de práticas frágeis no ambiente profissional.

No plano organizacional, observam-se barreiras estruturais. Um total de 8,33% dos respondentes indicou que empresas terceirizam a segurança da informação, limitando envolvimento às orientações recebidas. Outros 6,25% afirmaram ausência de práticas estruturadas de proteção de dados, e o mesmo percentual declarou a inexistência de áreas internas de TI responsáveis por orientar essas ações. Esses achados reforçam que a não existência de uma cultura organizacional voltada à segurança da informação, especialmente em empresas de menor porte, restringe o engajamento dos profissionais contábeis nas decisões estratégicas sobre o tema (Laudon & Laudon, 2022; Ribeiro et al., 2020).

Apesar desses desafios, alguns dados indicam um cenário parcialmente positivo. Itens como "a segurança da informação não é uma prioridade" ou "é apenas mais um custo" receberam baixíssima frequência (2,08% ou 0%), o que sugere que os alunos reconhecem a relevância do tema, mesmo diante das limitações operacionais. Essa percepção, embora ainda não convertida em prática efetiva, é um indicativo de abertura para o desenvolvimento de competências em segurança da informação.

Os dados evidenciam que as principais dificuldades na adoção de práticas de proteção de dados estão associadas à falta de estrutura organizacional, à ausência de uma cultura de segurança da informação, à dependência de terceiros e à percepção limitada sobre o papel do contador nesse processo. Além disso, percebe-se que muitos profissionais em formação ainda se posicionam de maneira operacional e passiva frente às questões de segurança, sem se perceberem como agentes ativos na gestão dos riscos relacionados às informações sensíveis. Os resultados reforçam a importância de fortalecer tanto a formação acadêmica, por meio de disciplinas que tratem mais diretamente do tema, quanto a conscientização sobre a segurança da informação como uma competência essencial do profissional contábil.

4.4 PERCEPÇÃO DOS ALUNOS SOBRE A INFLUÊNCIA DA DISCIPLINA NA COMPREENSÃO DA SEGURANÇA DA INFORMAÇÃO

Esta seção apresenta os resultados relacionados ao terceiro objetivo específico da pesquisa, que consiste em examinar a influência de disciplinas de sistemas de informações gerenciais na formação dos alunos quanto à segurança da informação e à proteção de dados. A análise baseia-se nos dados obtidos por meio da atividade prática realizada em sala de aula, estruturada em grupos, a partir da aplicação dos grupos focais e de um questionário com

escala Likert de 7 pontos, que avaliou a percepção dos estudantes sobre os impactos da atividade na sua compreensão sobre o tema, conforme metodologia de Boss et al. (2022).

A atividade foi organizada em três momentos principais: (i) análise de estudos de caso reais sobre incidentes de segurança da informação, (ii) discussão em grupo focal sobre percepções e experiências dos alunos, e (iii) questionário pós-atividade. Os estudantes foram divididos em três grupos, cada um responsável por analisar um caso prático relacionado a ataques cibernéticos e seus impactos financeiros, operacionais e reputacionais para as empresas envolvidas. No Quadro 1 a seguir, insere-se breve contexto dos casos analisados.

Quadro 1 – Descrição dos casos analisados em aula

Grupos	Descrição dos casos
Grupo 1	Migração de sistema com ataque hacker: O caso envolvia uma empresa que, durante a migração de dados para um sistema em nuvem, sofreu um ataque devido a uma brecha de segurança. O grupo destacou, além da falha tecnológica, a falta de comunicação eficaz da empresa sobre o incidente e os desafios de mensurar os impactos financeiros decorrentes. Também foi ressaltada a importância de os profissionais contábeis estarem preparados para lidar com esses efeitos, principalmente em termos de provisões e reporte contábil.
Grupo 2	Vazamento não comunicado formalmente: O ataque foi descoberto apenas durante uma renovação de licença vencida, e a comunicação feita pela empresa foi considerada vaga e tardia, ocorrendo por meio de um vídeo no YouTube e um número de call center. O grupo destacou o alto custo financeiro do incidente (cerca de R$ 4 milhões) e refletiu sobre a negligência da empresa na resposta, bem como a necessidade de contabilizar perdas, provisões e custos decorrentes do evento.
Grupo 3	Caso Target (EUA): O grupo apresentou o famoso caso da Target, onde uma empresa terceirizada, por meio de um ataque de *phishing*, proporcionou acesso a dados de cartões de crédito dos clientes. O grupo enfatizou a resposta lenta da empresa, os impactos financeiros elevados (estimados em US$ 500 milhões) e os desafios na reconquista da confiança dos clientes. Foram discutidos também os reflexos contábeis relacionados a provisões para contingências, custos operacionais e perdas reputacionais.

Fonte: Elaborado pelo autor com base nos dados.

Após a realização da atividade prática, que envolveu o estudo de casos citados, foram realizadas as discussões em grupo focal, para se compreender a percepção dos alunos sobre a influência da disciplina e dos conteúdos trabalhados. As percepções compartilhadas revelam um cenário que combina lacunas formativas e limitações estruturais, tanto no ambiente acadêmico quanto no profissional. Um dos aspectos que mais chamou atenção foi o relato de que, para muitos alunos, a aula representou o primeiro contato aprofundado com o tema no ambiente acadêmico. Isso evidencia que, mesmo em um curso que contempla disciplinas voltadas para sistemas de informação, como é o caso da UFRGS, a abordagem sobre segurança da informação ainda não vinha sendo tratada de forma aplicada e contextualizada para a realidade da contabilidade. Este achado está alinhado aos estudos de Ribeiro et al. (2020) e Boss et al. (2022), que já alertavam para a necessidade de inserir temas relacionados à cibersegurança de forma estruturada no currículo dos cursos de Ciências Contábeis, como forma de preparar os futuros profissionais para os desafios impostos pelo ambiente digital.

Do ponto de vista do mercado de trabalho, os relatos também demonstraram que a maioria dos alunos percebe um baixo espaço para discutir segurança da informação dentro das organizações onde atuam. Essa constatação reflete um problema cultural já discutido por Herath (2011) e Knapp et al. (2009), que destacam que, especialmente em pequenas e médias empresas, os temas relacionados à segurança da informação costumam ser tratados como responsabilidade exclusiva de áreas técnicas, como TI, sendo negligenciados pelos setores administrativos, financeiros e contábeis. A ausência de uma cultura organizacional voltada para a proteção de dados foi reforçada por outro dado relevante: poucos alunos relataram ter participado da elaboração, revisão ou análise de contratos que incluíssem cláusulas específicas sobre proteção de dados pessoais. Este dado é especialmente preocupante, considerando que, segundo a Lei Geral de Proteção de Dados (Brasil, 2018), a formalização

de políticas, contratos e termos de responsabilidade sobre o tratamento de dados não é apenas uma boa prática, mas uma obrigação legal das empresas e dos profissionais.

As percepções sobre as práticas adotadas nas empresas também corroboram a fragilidade desse cenário. Cerca de metade dos alunos relatou que existe algum nível de controle interno nas organizações, como o uso de senhas, bloqueio de acessos ou realização de *backups* básicos. Contudo, tais práticas são, em geral, isoladas e não fazem parte de uma política estruturada de segurança da informação. Esse comportamento organizacional, segundo Kruger e Kearney (2008), é bastante comum em empresas que não possuem uma governança informacional madura, em que a segurança é tratada como ação pontual ou reativa, e não como estratégia preventiva e integrada aos processos de negócio. Essa ausência de estrutura se reflete, inclusive, na falta de treinamentos específicos: a maioria dos alunos afirmou nunca ter recebido qualquer capacitação formal sobre segurança da informação, seja no ambiente acadêmico, seja no ambiente corporativo, o que está em consonância com as preocupações apontadas por Ribeiro et al. (2020) e Sarder e Haschak (2019).

Um dos relatos mais expressivos e que ilustra de forma contundente os riscos associados à negligência na segurança da informação foi apresentado por um aluno que vivenciou, em sua trajetória profissional, a perda completa de dados de três empresas, ocasionada por uma falha em um software terceirizado utilizado por um escritório contábil. O impacto foi tão severo que levou ao encerramento definitivo das atividades do escritório, evidenciando na prática os efeitos devastadores que a falta de medidas adequadas de proteção de dados pode gerar. Esse caso ilustra, de forma concreta, o que é discutido por Laudon e Laudon (2022), que destacam que falhas nos sistemas de informação não comprometem apenas processos operacionais, mas podem afetar diretamente a continuidade e a sobrevivência das organizações no mercado.

De forma geral, os relatos e discussões ocorridos durante a atividade evidenciaram que, até aquele momento, os alunos possuíam uma compreensão limitada não apenas sobre os conceitos técnicos da segurança da informação, mas também sobre sua própria responsabilidade profissional no tratamento e na proteção de dados sensíveis. Entretanto, também ficou evidente que a atividade proporcionou uma mudança significativa na percepção dos alunos, que passaram a entender de forma mais clara os impactos financeiros, operacionais, legais e reputacionais decorrentes de incidentes de segurança, além de reconhecerem a necessidade de desenvolver uma atuação mais proativa, consciente e alinhada às boas práticas de governança da informação. Esse resultado reforça a importância de que temas como segurança da informação, proteção de dados e cibersegurança sejam tratados de forma transversal em cursos de Ciências Contábeis, não como uma competência acessória, mas como uma competência central e indispensável para a prática contábil no contexto atual.

Por fim, foi aplicado um questionário com escala Likert de 1 (discordo totalmente) a 7 (concordo totalmente), com o objetivo de medir o quanto os alunos perceberam que a atividade contribuiu para sua formação e compreensão dos temas de segurança da informação e LGPD. Os resultados podem ser observados na Tabela 5.

Tabela 5 – Impacto da atividade na formação e compreensão de segurança da informação e LGPD

Afirmações Avaliadas	Média
O material da atividade era realista	6,79
A atividade foi um exercício de aprendizagem útil	6,59
A atividade me ajudou a entender possíveis ameaças à infraestrutura de segurança cibernética	6,44
Eu recomendaria ao professor usar esta atividade em aulas futuras	6,41
Foi interessante ler essa atividade	6,38
A atividade me ajudou a entender como as organizações podem responder a violações significativas de segurança	6,24
A atividade me ajudou a identificar como contadores gerenciais podem responder a violações	6,06
A atividade me ajudou a identificar como contadores financeiros podem responder a violações	6,00

A atividade me ajudou a entender quais divulgações ao cliente são necessárias após violações	5,94
A atividade me ajudou a identificar como auditores internos e externos podem responder a violações	5,62
A atividade me ajudou a entender quais divulgações de demonstrações financeiras são necessárias após violações	5,56

Fonte: Elaborado pelo autor com base nos dados.

As médias obtidas demonstram que os alunos avaliaram a atividade como extremamente relevante, realista e útil para sua formação profissional. O item com maior média foi "**O material da atividade era realista**" (6,79), seguido por "**A atividade foi um exercício de aprendizagem útil**" (6,59), indicando que o uso de casos práticos contribuiu significativamente para o engajamento dos estudantes e a consolidação dos conteúdos, em linha com os apontamentos de Boss et al. (2022) sobre a eficácia de metodologias ativas no ensino de cibersegurança aplicada à contabilidade. O entendimento sobre **ameaças cibernéticas** também obteve uma avaliação bastante elevada (6,44), reforçando que a atividade proporcionou uma visão clara dos riscos enfrentados pelas organizações. Além disso, os alunos atribuíram médias igualmente expressivas aos itens "**Eu recomendaria ao meu professor usar esta atividade em aulas futuras**" (6,41) e "**Foi interessante ler essa atividade**" (6,38), evidenciando tanto o nível de interesse quanto a percepção de valor acadêmico atribuído à proposta. Os itens que trataram da compreensão dos **papéis dos profissionais da contabilidade frente às violações de segurança cibernética** tiveram resultados ligeiramente mais baixos, porém ainda positivos, como no caso da **atuação dos contadores gerenciais** (6,06) e **contadores financeiros** (6,00), indicando que, embora a atividade tenha sido eficaz, há espaço para aprofundar o entendimento sobre as responsabilidades específicas de cada função. Por outro lado, os itens que exigem maior conexão entre os incidentes de segurança e as práticas contábeis, especialmente no que se refere às obrigações de reporte e transparência, foram os que obtiveram as menores médias: **divulgação ao cliente** (5,94), **atuação dos auditores internos e externos** (5,62) e **divulgações nas demonstrações financeiras** (5,56). Esses resultados indicam que os alunos encontram mais dificuldade em compreender como as falhas de segurança impactam diretamente os processos contábeis e os deveres de comunicação com stakeholders, reforçando a necessidade de aprofundar esses tópicos nas atividades acadêmicas e na formação contábil, para que os futuros profissionais estejam preparados não apenas para reconhecer os riscos, mas também para endereçá-los corretamente dentro das exigências legais e dos princípios da governança corporativa.

Os resultados, tanto quantitativos quanto qualitativos, evidenciam que a atividade foi eficaz na sensibilização e conscientização dos alunos sobre segurança da informação. As falas do grupo focal demonstraram um cenário de baixa preparação, tanto no ambiente acadêmico quanto nas empresas onde atuam, o que ficou corroborado pelos dados do questionário. A avaliação positiva da atividade confirma que, quando abordado de forma prática, o tema se torna mais compreensível e relevante para os futuros contadores.

Esses achados estão alinhados ao que defende a literatura, especialmente autores como Boss et al. (2022) e Ribeiro et al. (2020), que destacam que a segurança da informação precisa ser tratada como uma competência essencial na formação do contador, e não apenas como um tema técnico restrito às áreas de TI. A atividade proposta na disciplina demonstrou ser uma estratégia eficaz para aproximar os alunos dos temas de segurança da informação e proteção de dados, contextualizando-os na prática contábil. Ficou evidente que atividades que simulam situações reais, associadas à discussão reflexiva em grupo, potencializam a compreensão dos alunos sobre os riscos, impactos e responsabilidades da profissão contábil diante de incidentes cibernéticos. Dessa forma, reforça-se a importância de que a formação acadêmica dos contadores inclua, de maneira sistemática, conteúdos de segurança da informação como parte integrante das competências profissionais exigidas no cenário atual.

5 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo principal analisar a percepção dos alunos do curso de Ciências Contábeis da Universidade Federal do Rio Grande do Sul (UFRGS) sobre segurança da informação e sua relação com a prática contábil. A pesquisa foi motivada pela constatação, presente na literatura, de que, embora os profissionais contábeis reconheçam a importância da segurança da informação, ainda demonstram insegurança quanto à sua aplicação prática no contexto organizacional. Para tanto, foram desenvolvidas atividades de caráter prático, envolvendo grupos focais e a aplicação de questionários em disciplinas de sistemas de informações gerenciais, ofertadas no curso de Ciências Contábeis da UFRGS.

Os resultados obtidos permitiram compreender, em primeiro lugar, que os alunos possuem um nível de familiaridade entre básico e intermediário com os conceitos de segurança da informação e da Lei Geral de Proteção de Dados (LGPD). Embora demonstrem conhecimento dos termos e reconheçam sua relevância, os participantes revelaram dificuldades na aplicação desses conceitos à realidade contábil, especialmente no que se refere à gestão de riscos, elaboração de provisões contábeis e à compreensão dos impactos financeiros decorrentes de incidentes cibernéticos.

A análise das principais dificuldades apontou que fatores como a ausência de uma cultura organizacional voltada à segurança, a falta de estrutura nas empresas, o distanciamento do tema na prática profissional e uma visão limitada sobre o papel estratégico do contador figuram entre os principais entraves à adoção de práticas eficazes de proteção de dados. Esses achados reforçam as discussões teóricas que destacam a segurança da informação não apenas como um desafio tecnológico, mas como um tema de gestão e governança, que deve ser integrado às atividades contábeis.

Por fim, os resultados demonstraram que a atividade prática desenvolvida na disciplina contribuiu significativamente para a ampliação da percepção dos alunos sobre a importância da segurança da informação no exercício da contabilidade. As discussões em grupo e a análise de casos reais proporcionaram aos estudantes uma compreensão mais concreta dos riscos e das implicações financeiras e operacionais associadas a falhas na proteção dos dados. A avaliação positiva da atividade, em caráter quantitativo e qualitativo, evidencia que metodologias ativas, que aproximam a teoria da prática, são altamente eficazes para o desenvolvimento dessa competência no contexto da formação contábil.

Diante dos resultados, este estudo contribui, tanto para o meio acadêmico quanto para a prática profissional, ao evidenciar a necessidade de incorporar, de forma estruturada, temas relacionados à segurança da informação na formação dos futuros contadores. A pesquisa demonstra que o desenvolvimento de competências em segurança da informação deve ser tratado como um elemento essencial da formação profissional, especialmente diante de um cenário em que a digitalização de processos contábeis é crescente e as exigências regulatórias, como a LGPD, impõem responsabilidades significativas aos profissionais e às organizações.

Além disso, a pesquisa reforça que o contador não deve se posicionar apenas como um usuário passivo dos sistemas de informação, mas sim como um agente ativo na gestão de riscos, na elaboração de controles, na proteção de dados e na preservação da integridade e da confiabilidade das informações contábeis. Trata-se de uma mudança de mentalidade que pode fortalecer tanto o posicionamento estratégico do profissional contábil quanto a resiliência das organizações frente aos desafios da era digital.

Como limitações deste estudo, destaca-se o fato de a pesquisa ter sido conduzida com uma amostra restrita aos alunos da UFRGS, o que limita a generalização dos resultados para outras instituições ou contextos. Além disso, o instrumento adotado, embora adequado aos

objetivos da pesquisa, não permite uma análise aprofundada sobre determinadas variáveis, como diferenças entre perfis profissionais ou impactos de experiências anteriores.

Diante disso, sugere-se que futuras pesquisas ampliem a amostra, incluindo alunos de diferentes instituições ou profissionais já atuantes no mercado, bem como aprofundem a análise sobre a efetividade de disciplinas que abordem segurança da informação na formação contábil. Além disso, investigações que explorem o desenvolvimento de competências específicas, como a elaboração de políticas de proteção de dados ou a atuação do contador na gestão de crises de segurança, podem trazer contribuições para academia e mercado.

6 USO DE IAG NESTA PESQUISA

Para a revisão gramatical e a estruturação do texto, foram utilizadas as Inteligências Artificiais Generativas ChatGPT GPT-4o e DeepSeek-V3. Assim, o escopo de utilização de tais ferramentas limitou-se ao auxílio para melhor comunicação da pesquisa.

REFERÊNCIAS

ABU-MUSA, A. A. **The Perceived Threats to the Security of Computerized Accounting Information Systems.** Journal of American Academy of Business, Cambridge, v. 3, 2003.

BARDIN, Laurence. **Análise de conteúdo**. Lisboa: Edições 70, 2011.

BOSS, SCOTT R. *et al*. **Accountants, Cybersecurity Isn't Just for "Techies": Incorporating Cybersecurity into the Accounting Curriculum**. Issues in Accounting Education, 2022.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018. Lei de proteção de dados pessoais**. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. **RESOLUÇÃO CNE/CES Nº 1, de 27 de março de 2024. Institui as Diretrizes Curriculares Nacionais do Curso de Graduação em Ciências Contábeis, bacharelado**. Brasília, DF. Disponível em: http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=257031-rces001-24&category_slug=marco-2024&Itemid=30192.

CARVALHO, P. H. S. *et al*. **A percepção de estudantes do curso de Ciências Contábeis acerca do futuro da contabilidade com o avanço da automação dos processos.** Trabalho de Conclusão de Curso, Universidade Federal de Minas Gerais, 2020.

CONSELHO FEDERAL DE CONTABILIDADE (CFC). **Norma Brasileira de Contabilidade – NBC 28**. Brasília: CFC, 2024.

COTS, M.; OLIVEIRA, R. **Lei Geral de Proteção de Dados: aspectos teóricos e práticos. 1. ed.** São Paulo: Revista dos Tribunais, 2018.

FARIA, F.; MAÇADA, A.; KUMAR, K. **Modelo estrutural de governança da informação para bancos**. RAE-Revista de Administração de Empresas, v. 57, n. 1, p. 79-95, 2017.

HENRIQUE, Marcelo Rabelo et al. **A percepção dos estudantes de contabilidade da Faculdade Strong Business School sobre a aplicabilidade do blockchain na segurança da contabilidade**. Latin American Journal of Business Management, 2022.

HERATH, H. **Cybersecurity: An Emerging Area for Collaborative Post-Modern Management Accounting Research**. Journal of Cost Management, p. 14-26, 2011.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements**. Genebra: ISO, 2013.

INTERNATIONAL TELECOMMUNICATION UNION. **Understanding cybercrime: a guide for developing countries**. Technical report, 2009. Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

ISACA. **Information Security Governance: Guidance for Information Security Managers**. Rolling Meadows: ISACA, 2013.

ISACA. **COBIT 5: Transforming Cybersecurity. Guide Using COBIT 5**. Rolling Meadows: ISACA, 2013.

KNAPP, K. *et al*. **Information security policy: An organizational-level process model**. Computers & Security, v. 28, n. 7, 2009.

KRUGER, H. A.; KEARNEY, W. D. **Consensus Ranking – An ICT security awareness case study**. Computers & Security, v. 27, n. 1, p. 254-259, 2008.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais**. Bookman Editora, 2022.

BEUREN, Ilse Maria. **Como elaborar trabalhos monográficos em contabilidade: teoria e prática**. São Paulo: Atlas, 2003.

MADEIRA, A. C.; SOARES, S. V. **Segurança da informação na contabilidade e a importância da proteção dos dados contábeis**. Contribuciones a las Ciencias Sociales, 2024.

NORTON CYBERSECURITY INSIGHTS REPORT GLOBAL COMPARISON. **Norton, 2017**. Relatório interno.

RIBEIRO, R. et al. **Cibersegurança e segurança da informação contábil: uma análise da percepção do profissional contábil**. Revista de Auditoria Governança e Contabilidade, 2020.

SARDER, M. D.; HASCHAK, M. **Cyber security and its implication on material handling and logistics**. College-Industry Council on Material Handling Education, p. 1–18, 2019.