Revista de Educação e Pesquisa em Contabilidade
Journal of Education and Research in Accounting

Periódico de Publicação Contínua, digital e gratuito publicado pela Academia Brasileira de Ciências Contábeis | Disponível online em www.repec.org.br

REPeC, Brasília, v.19, 2025 | DOI: http://dx.doi.org/10.17524/repec.v19, e3430 | ISSN 1981-8610

Um olhar sobre o traço narcisista, a consciência sobre a segurança cibernética e custos de violação: um estudo com estudantes e profissionais da área contábil

Marcia Figueredo D'Souza
https://orcid.org/0000-0002-3196-5396

Juliana Ventura Amaral
https://orcid.org/0000-0001-7223-3848

Resumo

Objetivo: analisar a influência da consciência sobre segurança cibernética e do traço de personalidade narcisista na consciência sobre os custos de violação.

Método: pesquisa descritiva, de abordagem quantitativa, com duas coletas de dados por meio de um *survey*: uma com 262 alunos de Ciências Contábeis, outra com 166 profissionais da contabilidade. Houve aplicação de estatística descritiva e regressão logística.

Resultados: estudantes e profissionais têm dificuldade de classificar os custos de violação e informá-los nas demonstrações contábeis. A consciência sobre segurança cibernética habilita os profissionais a terem maior conhecimento para informar os impactos desses custos nas demonstrações contábeis e convicção sobre sua classificação. O excesso de confiança dos estudantes, com traços mais marcantes do narcisismo, propiciou relatos de maior consciência cibernética, contudo se negaram a reconhecer a dificuldade em classificar e informar os impactos desses custos nas demonstrações contábeis. Os profissionais apresentaram maior pontuação narcisista e confirmaram maior conhecimento para informar as violações dos custos nas demonstrações contábeis.

Contribuições: os achados contribuem com a literatura – as evidências empíricas sobre o tema são limitadas – e com o contexto profissional. Estimulam a reflexão nas empresas e instituições de ensino contábil para elaborar cursos e conteúdos específicos sobre segurança cibernética, a fim de habilitar os contadores ou aspirantes a contador a reconhecerem os impactos financeiros gerados pelos ataques cibernéticos.

Palavras-chave: Consciência sobre segurança cibernética. Custos de violação. Narcisismo.

Editado em Português e Inglês. Versão original em Português.

Rodada 1: Recebido em 9/10/2023. Aceito em 2/9/2024 por Bruna Camargos Avelino, Doutora (Editor assistente) e por Gerlando Augusto Sampaio Franco de Lima, Doutor (Editor). Publicado em 31/3/2025 Organização responsável pelo periódico: Abracicon.

1 Introdução

Na atualidade, as violações à segurança cibernética apresentam riscos contínuos e crescentes à medida que os sistemas em rede e a internet são mais utilizados. Essa situação passa a requerer mais atenção para as implicações contábeis de ataques perpetrados contra as organizações (Bakarich & Baranek, 2019), vez que os incidentes de segurança cibernética têm o potencial de impactar materialmente as demonstrações financeiras, interromper negócios catastroficamente e danificar reputações organizacionais (Boss *et al.*, 2022).

Boss *et al.* (2022) defendem que a consciência sobre segurança cibernética é fundamental no mundo dos negócios, sendo necessária para o sucesso de profissionais que lidam diretamente com os impactos e custos de violação de sistemas financeiros, especialmente os contadores. Segundo Allam *et al.* (2014), como os riscos e ameaças transformam-se e ficam cada dia mais especializados, a conscientização sobre segurança da informação implica um papel significativo na redução do risco de violações de segurança da informação.

O compartilhamento de conhecimento, a intervenção e a colaboração aumentam a consciência dos usuários, o que, por sua vez, influencia suas atitudes e comportamentos. A falta de consciência, negligência, distração, travessura, apatia e resistência dos usuários costumam ser os motivos das violações de segurança (Safa *et al.*, 2015).

Os ataques cibernéticos, cibercrimes e cibernegligência são assuntos recorrentes na atualidade, e a necessidade de conhecer seus impactos e efeitos materiais nas demonstrações contábeis justifica a inserção da cibersegurança nas disciplinas contábeis. Nessa concepção, Boss *et al.* (2022) desenvolveram estudos de caso com os quais abordaram as violações e seus reflexos nos relatórios financeiros, consequências tributárias, fiscais, gerenciais e de auditoria. Um dos casos debruça-se à classificação de custos relacionados a violações cibernéticas em custos diretos, custos indiretos e custos de oportunidade.

Lagazio *et al.* (2014) entendem que a classificação desses custos é importante para a visão geral do custo total de crimes cibernéticos. Os custos diretos são os gastos incorridos ao lidar com a violação após a detecção, incluindo a contratação de especialistas forenses e de escritórios de advocacia e a oferta de serviços de proteção de identidade às vítimas de violações. Os custos indiretos são os gastos relacionados com recursos internos (incluindo empregados), tempo, esforço e outros necessários para cobrir as perdas decorrentes da violação de dados. Os custos de oportunidade são os gastos gerados pela perda de oportunidades de negócios devido aos efeitos negativos de reputação. Segundo Anderson *et al.* (2013), a classificação e a mensuração dos custos são difíceis e subjetivas, devendo ser avaliadas tanto antes do dano esperado quanto depois de tomadas medidas de segurança. A consciência sobre tais custos também se mostra imperiosa no atual contexto de negócios.

Os custos são incorridos por ações propositais de violação à segurança cibernética executadas por diferentes partes. Os *hackers*, por exemplo, usam uma gama complexa de meios para perpetrar ataques cibernéticos, objetivando alterar a confidencialidade, integridade e disponibilidade das informações. Woo (2003) concluiu que é bastante provável que os *hackers* tenham atributos orientados pelo narcisismo e uma das suas características centrais é deixar marcas na tentativa de serem admirados.

Ora, o comportamento arriscado, de autoridade, autossuficiência, superioridade, exibicionismo, exploração, vaidade e senso de direito manifestados por indivíduos com altos traços narcisistas podem oferecer riscos à segurança cibernética. Os indivíduos narcisistas exibem sentimentos e atitudes de onipotência, com o intuito de explorar os outros e se sentirem merecedores de direitos e privilégios em relação àqueles. São intolerantes a críticas, por se considerarem autossuficientes e serem extremamente vaidosos (Raskin & Terry, 1988). Narcisistas envolvem-se em maus comportamentos porque são preocupados apenas com eles mesmos (Curtis *et al.*, 2018).

Baumeister *et al.* (2000) argumentam que pessoas com traços narcisistas, quando são questionadas ou contrariadas, tendem a violar a fonte de ameaça a fim de proteger seu ego. Logo, os narcisistas podem se sentir estimulados a violar o que enxergam como fonte de ameaça. Nesse particular, Jones (2022) estuda a psicologia das violações cibernéticas e as associa ao narcisismo, com a finalidade de encontrar maneiras de minimizar a eficácia e os danos causados pelos ataques.

Vale mencionar que o narcisismo é caracterizado por um senso geral de superioridade, grandiosidade, direito e domínio. Os narcisistas são altamente autocentrados, têm uma autovisão inflada e se correlacionam negativamente com a empatia (Maasberg *et al.*, 2020). Muitas vezes, eles se envolvem em comportamentos malévolos pelo senso de grandiosidade, direito e superioridade, não pelo desejo explícito de prejudicar ou impactar negativamente os outros. Os narcisistas não se importam com os impactos nos outros porque os veem como sem importância.

Avelino (2017) realizou um estudo amplo relativo à personalidade narcisista em estudantes de graduação de Ciências Contábeis e concluiu que níveis de traços de personalidade narcisista mais elevados culminam em maior probabilidade de autoavaliação otimista. Nesse sentido, é possível que tais traços também impactem a autopercepção do nível de consciência sobre custos de violação de estudantes e de profissionais dessa área.

Diante da contextualização apresentada, pretende-se elucidar o seguinte problema de pesquisa: **Qual a influência da consciência sobre segurança cibernética e do traço de personalidade narcisista na consciência sobre custos de violação, em profissionais e estudantes de Ciências Contábeis brasileiros?** Especificamente, objetiva-se verificar como a consciência sobre segurança cibernética e como os traços narcisistas de autossuficiência, excesso de confiança e ego inflado se refletem no reconhecimento de dificuldades sobre o reconhecimento dos custos dos impactos nas demonstrações contábeis, assunto complexo e emergente.

A investigação dessa relação oportuniza contribuições teóricas e práticas. Teóricas, por ampliar o debate sobre as temáticas objetos de estudo, uma vez que pesquisas prévias abordaram isoladamente o assunto de custos de violação enquanto outras exploraram os traços de personalidade, existindo uma lacuna de integração entre esses conceitos. Por exemplo, podem ser encontrados trabalhos que lançaram luz sobre a consciência acerca da segurança da informação (Safa *et al.*, 2015) e casos de ensino sobre consciência cibernética para aplicação nas áreas educacionais de negócios e contábil (Bakarich & Baranek, 2019; Boss *et al.*, 2022; Cram & D'Arcy, 2016; Janvrin & Wang, 2022; Reidenbach & Wang, 2021; Roohani & Zheng, 2019). Há ainda trabalhos que examinaram o posicionamento de contadores frente ao gerenciamento de riscos de segurança cibernética, consultoria e proteção (Eaton, Grenier, & Layman, 2019), a análise dos impactos econômicos e de custos causados por ataques cibernéticos no setor financeiro (Anderson *et al.*, 2013; Lagazio, Sherif, & Cushman, 2014; Silva, 2018) e a discussão sobre a relação entre ataques cibernéticos e traços de personalidades sombrias (Curtis *et al.*, 2018; Jones, 2022; Jones *et al.*, 2021; Maasberg *et al.*, 2020).

Ora, os traços de personalidade sombrios, como o narcisismo, impactam a percepção de autossuficiência, vaidade e ego e podem impedir a habilitação de estudantes e profissionais para a consciência sobre a segurança cibernética nas organizações. Os estudos prévios, contudo, não focaram ainda nessa relação.

No tocante às contribuições práticas, a aplicação empírica com estudantes e profissionais da área contábil possibilita a análise sobre a percepção, o conhecimento, as dificuldades e convicções acerca da segurança cibernética, apontando para a necessidade contínua da promoção de treinamentos e cursos sobre o assunto. Adicionalmente, este estudo é relevante e impacta a reflexão sobre o comportamento de estudantes e profissionais da contabilidade, entre eles professores e empresários, que utilizam a tecnologia e necessitam de segurança e confiabilidade da informação e comunicação, de sistemas e redes.

Se por um lado o custo de implantação de um sistema de segurança da informação é oneroso para as empresas, por outro, o custo de um ataque cibernético é ainda maior, sobretudo se as informações sequestradas proporcionarem perda de credibilidade e reputação para as empresas. Como afirmam Bakarich e Baranek (2019), as consequências negativas de um ataque cibernético excedem muito o custo da violação e podem incluir danos à reputação, aumento dos custos de proteção, litígios e riscos legais, aumento dos prêmios de seguro e diminuição do preço das ações e do valor do acionista.

2 Revisão da Literatura e Desenvolvimento das Hipóteses

2.1 Segurança cibernética

No Brasil, uma normatização robusta sobre segurança cibernética encontra-se em desenvolvimento. O Governo federal aprovou a Estratégia Nacional de Segurança Cibernética E-Ciber, publicada por meio do Decreto n.º 10.222, de 5/2/2020, que tem por objetivo estabelecer ações nacionais, na área da segurança cibernética.

A Resolução CVM n.º 35, de 26/5/2021, também faz recomendações sobre a adoção de um programa de segurança cibernética, que visa à identificação e avaliação dos riscos cibernéticos internos e externos, redução da vulnerabilidade da instituição contra ataques cibernéticos e procedimentos e controles internos adotados, sobretudo no tratamento e controle de dados de clientes, com a finalidade de "(...) desenvolver e implementar regras, procedimentos e controles internos adequados visando garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade dos dados e informações sensíveis" (p. 14).

Igualmente a Lei Geral de Proteção de Dados (Lei n.º 13.709, de 2018) traz em seu arcabouço recomendações de proteção sobre os direitos fundamentais de liberdade e de privacidade no tratamento de dados pessoais, inclusive nos meios digitais. Os ataques de *phishing*, negação de serviço em larga escala, vazamentos de informações privadas ou institucionais, espionagem cibernética e a interrupção de serviços são as principais violações dos sistemas e podem ser considerados como infrações perante essa lei.

2.2 Violação à segurança cibernética e seus custos

As violações à segurança cibernética trazem impactos contábeis, cumprindo destacar aqueles ressaltados por Boss *et al.* (2022) referentes aos custos de violação de ataques cibernéticos. Lagazio *et al.* (2014) classificam esses custos em diretos, indiretos e de oportunidade.

Gordon e Loeb (2006) definem os custos diretos como gastos oriundos de violações específicas de segurança. Já Boss *et al.* (2022) consideram os custos diretos como gastos incorridos ao lidar com a violação após a detecção, incluindo a contratação de especialistas forenses e de escritórios de advocacia e a oferta de serviços de proteção de identidade às vítimas de violações.

Os custos indiretos, por sua vez, embora sejam claramente causados pelo fato de que ocorreram violações, são mais genéricos. Eles englobam o custo das medidas para prevenir violações de segurança ou para treinar colaboradores para que adotem práticas de segurança (Núcleo de Informação e Coordenação do Ponto BR, 2020). Boss *et al.* (2022) trazem os custos indiretos como os gastos relacionados com recursos internos (incluindo empregados), tempo, esforço e outros necessários para cobrir as perdas decorrentes da violação de dados.

Por fim, os custos de oportunidade são os gastos gerados pela perda de oportunidades de negócios devido aos efeitos negativos de reputação. Englobam a perda de negócios devida ao aumento da rotatividade dos clientes, a perda de receita devida ao tempo de inatividade do sistema e o aumento do custo de aquisição de novos negócios devido à reputação diminuída (Boss *et al.*, 2022).

Boss *et al.* (2022) elaboraram um caso de ensino considerando a classificação dos custos de violação à segurança cibernética. Nessa vertente, Roohani e Zheng (2019) elaboraram 10 módulos de ensino, ilustrados por vídeos profissionais, com a finalidade de promover a educação em segurança cibernética para estudantes. Na mesma linha de pesquisa, Reidenbach e Wang (2021) apresentaram um estudo de caso direcionado a estudantes de Contabilidade, sobre a violação de dados operacionais da Heartland Payment, em 2008, com a finalidade de determinar os impactos contábeis imediatos e operacionais de longo prazo e a sustentabilidade da empresa.

Cram e D'Arcy (2016) propuseram introduzir um curso básico de Segurança da Informação que equilibrasse o conteúdo técnico fundamental sobre segurança da informação com o conteúdo gerencial que a profissão requer para valorização do trabalho na área de negócios. Em adição, Bakarich e Baranek (2019) desenvolveram um caso de ensino com base em uma situação real de uma empresa pública dos EUA que foi vítima de um esquema de *Business Email Compromise* (BEC).

Anderson *et al.* (2013) realizaram um estudo sistemático sobre os custos relacionados ao cibercrime. Os autores apresentaram a definição, por categoria, do que é e do que não é conhecido sobre custos diretos, indiretos e de defesa/proteção, que atendem às demandas do Reino Unido e em âmbito global. Pontuaram ainda que os custos indiretos e transitórios são mais onerosos, sobretudo porque "os crimes cibernéticos são globais e têm fortes externalidades".

Lagazio *et al.* (2014) desenvolveram um modelo multinível para compreender o impacto dos crimes cibernéticos no setor financeiro. Os resultados indicaram que relacionamentos dinâmicos fortes, entre fatores tangíveis e intangíveis, afetam o custo dos crimes cibernéticos, e ocorrem em diferentes níveis da sociedade e da rede de valor.

Silva (2018) investigou os impactos causados por ataques cibernéticos no setor financeiro no Brasil e desenvolveu uma metodologia de cálculo para conhecer os impactos dos custos no setor. Janvrin e Wang (2022) elaboraram um estudo apresentando uma estrutura contábil de mensuração da segurança cibernética. A proposta foi identificar as ameaças, os riscos, os eventos de segurança e suas implicações e desenvolver estratégias de respostas. Já Eaton *et al.* (2019) descreveram o posicionamento dos contadores frente ao gerenciamento de riscos de segurança cibernética e discutiram como as habilidades e competências dos contadores podem agregar valor em cada um dos cinco estágios do modelo proposto.

Em todos os estudos, pode-se perceber que a classificação e mensuração dos custos são difíceis e subjetivas. Anderson *et al.* (2013) defendem que, para a identificação dos custos ou benefícios de medidas de segurança, é necessário determinar o custo antes do dano esperado e depois de tomadas medidas de segurança. Portanto, faz-se necessário ter consciência sobre segurança cibernética.

2.3 Consciência sobre segurança cibernética

Shaw *et al.* (2009) definem a consciência sobre segurança cibernética como "o grau de compreensão dos usuários sobre a importância da segurança da informação e suas responsabilidades de exercer níveis suficientes de controle de informações para proteger os dados e redes da organização" (p. 92). Essa compreensão traz uma consciência da necessidade de assegurar a informação e essa necessidade, de acordo com Landwehr (2001), centra-se em três focos: proteção dos dados recebidos, armazenados e retransmitidos; garantia dos processos executados nesses dados; e proteção das propriedades físicas do sistema, como *backups*, *laptops* e impressões.

Safa *et al.* (2015) constataram que a conscientização sobre segurança, política de organização de segurança da informação, experiência e envolvimento em segurança da informação, atitudes em relação à segurança da informação, normas subjetivas, avaliação de ameaças e autoeficácia em segurança da informação têm um efeito positivo sobre o comportamento dos usuários.

A combinação de procedimentos e controles técnicos é imprescindível para a redução do risco de *hackeamento* de dados. Quando os usuários das informações têm o comportamento de ignorar procedimentos ou políticas de segurança e não os integram à cultura organizacional, o ambiente torna-se vulnerável e passível de invasões, sujeito à incidência dos custos de violação (Albrechtsen & Hovden, 2010; Safa *et al.*, 2015). Diante do exposto, é formulada a **Hipótese 1:** A consciência sobre segurança cibernética impacta a consciência sobre os custos de violação.

De modo específico, vale trazer que Allam *et al.* (2014) reforçam que a conscientização sobre segurança da informação implica um papel significativo na redução do risco de violações de segurança da informação. Por aumentar a consciência dos usuários, ela influencia suas atitudes e comportamentos. O comportamento dos usuários deve ser considerado um fator importante nesse domínio, já que a negligência, ignorância, falta de consciência, travessura, apatia e resistência dos usuários costumam ser os motivos das violações de segurança (Safa *et al.*, 2015). Em função desses argumentos, desmembram-se a hipótese em H1a: A consciência sobre segurança cibernética impacta negativamente a dificuldade de classificação dos custos de violação; H1b: A consciência sobre segurança cibernética impacta positivamente a convicção sobre os acertos de classificação dos custos de violação; e H1c: A consciência sobre segurança cibernética impacta positivamente o conhecimento sobre os impactos dos custos de violação nas demonstrações contábeis.

2.4 Segurança cibernética e traços de personalidade narcisista

Interessante pontuar que já há estudos (por exemplo, Curtis *et al.*, 2018; Maasberg *et al.*, 2020; Jones *et al.*, 2021) que abordaram a violação à segurança cibernética impactada pelos traços de personalidade. No entanto, esses estudos não abordam ainda o foco central desta pesquisa, que se refere aos custos de violação.

Curtis *et al.* (2018) investigaram a relação entre três traços de personalidade – maquiavelismo, narcisismo e psicopatia – e esforço de *phishing*, sucesso do ataque e suscetibilidade do usuário final a *e-mails* de *phishing*. Eles perceberam que os três traços de personalidade se relacionam ao esforço que eles colocam para escrever um *e-mail* de *phishing*, mas não preveem o sucesso do *phishing*. Já os usuários com altas pontuações dos traços preveem o sucesso dos *e-mails* de *phishing*. O narcisismo do usuário final associou-se a uma maior vulnerabilidade ao receber *e-mails* de *phishing*.

Maasberg *et al.* (2020) relacionaram traços narcisistas, maquiavelistas e psicopatas, com intenções de envolvimento em ameaça cibernética. Já Jones *et al.* (2021) desenvolveram duas pesquisas para conhecer o comportamento de indivíduos com traços de narcisismo, maquiavelismo e psicopatia, frente ao crime cibernético e observaram uma associação entre narcisistas e psicopatas a ataques cibernéticos de curto prazo.

O narcisismo merece destaque, pois é caracterizado por um senso geral de superioridade, grandiosidade, direito e domínio. Os narcisistas são altamente autocentrados, têm uma autovisão inflada e correlacionam-se negativamente com a empatia (Maasberg *et al.*, 2020). Eles se envolvem, às vezes, em comportamentos malévolos, pelo senso de grandiosidade, direito e superioridade do narcisista, não pelo desejo explícito de prejudicar ou impactar negativamente os outros. Os narcisistas não se importam com os impactos nos outros porque os veem como sem importância.

Para Campbell *et al.* (2011), o traço de personalidade narcisista pode ser compreendido por três componentes: o Eu, as relações interpessoais e as estratégias autorregulatórias. O Eu narcisista é caracterizado por positividade, especialidade, singularidade, vaidade, senso de direito e desejo de poder e estima.

Os relacionamentos narcisistas contêm baixos níveis de empatia e intimidade emocional e/ou são superficiais, podendo variar de emocionantes e envolventes a manipuladores e exploradores. As estratégias narcisistas direcionam para autovisões infladas, sendo que os narcisistas buscam oportunidades de atenção e admiração, gabam-se, roubam o crédito dos outros e jogam nos relacionamentos. No contexto específico contábil, Avelino e Lima (2017) averiguaram a concordância dos estudantes para a busca desenfreada pelo prazer, o que poderia corroborar o anseio por violações cibernéticas.

Jones (2022) estudou os traços de personalidade de narcisismo, maquiavelismo e psicopatia para compreender por que indivíduos com altos traços envolvem-se em crimes cibernéticos. No tocante ao narcisismo, o autor defendeu que eles podem se envolver nos ataques pela autoridade, excessiva confiança e grandiosidade. Entre outros resultados, ficou evidente que a simulação de fornecer versões mais leves de mensagens persuasivas pode proteger usuários finais, que são excessivamente confiantes, contra-ataques de *phishing*. Diante do exposto, acredita-se que a autoridade, a excessiva confiança e a grandiosidade dos narcisistas conduzam à **Hipótese 2:** O traço de personalidade narcisista influencia a consciência sobre os custos de violação. E especificamente, desmembram-se que H2a: Há maior probabilidade de os indivíduos com traços narcisistas mais marcantes relatarem menor dificuldade para classificar os custos de violação; H2b: Há maior probabilidade de os indivíduos com traços narcisistas mais marcantes relatarem maior convicção quanto aos acertos na classificação dos custos; e H2c: Há maior probabilidade de os indivíduos com traços narcisistas mais marcantes relatarem conhecer os impactos dos custos de violação nas demonstrações contábeis.

3. Procedimentos metodológicos

3.1 Abordagem, procedimento de coleta de dados e amostra da pesquisa

A abordagem metodológica teórico-empírica foi aplicada ao estudo descritivo, com abordagem quantitativa, para descrever e analisar o fenômeno objeto de investigação. O *survey* foi utilizado como estratégia de coleta de dados.

Para a coleta de dados, foi aplicado um questionário, na modalidade remota, via *link* do *form office* do *Microsoft teams*, enviado por *e-mail* para alunos de Ciências Contábeis cursando do 4º aos 8º semestres em universidades do território nacional e profissionais da contabilidade, incluindo professores, que participaram de um congresso científico em Contabilidade em 2022. As universidades acessadas abrangeram instituições públicas e privadas localizadas nos diversos estados brasileiros. O congresso científico acessado refere-se a um dos principais do Brasil, aquele promovido pela USP (Universidade de São Paulo), o XX *USP International Conference on Accounting*.

Dessa forma, a aplicação do instrumento foi realizada por acessibilidade, de outubro a dezembro de 2022, com a finalidade de capturar um número significativo e diversificado de indivíduos que se adequassem aos critérios da presente pesquisa. A aplicação da pesquisa foi autorizada pelo Comitê de Ética da Universidade Estadual da Bahia, sob o número 65415822.0.0000.0057, emitido pelo CAAE.

O questionário foi composto do Termo de Consentimento Livre e Esclarecido (TCLE); do perfil demográfico e social; do instrumento de mensuração do narcisismo NPI (Raskin & Hall, 1979; Raskin & Terry, 1988); e de questões para identificar a Consciência sobre Segurança Cibernética e a Consciência sobre Custos de Violação.

3.2 Constructos e variáveis da pesquisa

O constructo sobre a Consciência sobre Custos de Violação é considerado, neste estudo, como o constructo dependente. O instrumento de coleta baseou-se em um caso de ensino/simulação, adaptado do estudo de Boss *et al.* (2022), conforme Tabela 1.

Tabela 1

Consciência sobre Custos de Violação

Suponha que você seja o controller de uma empresa de grande porte. Você toma conhecimento que a empresa sofreu uma violação de segurança cibernética, a qual afetou vários servidores durante o período atual, além de expor dados bancários e informações financeiras relevantes da empresa e de clientes.
Uma empresa de segurança cibernética foi contratada para eliminar e evitar uma violação repetida. Mas você será responsável por mensurar o impacto financeiro da violação.
Tomando por base o contexto da violação cibernética, você foi desafiado a classificar alguns custos relativos à violação, em diretos (CD), indiretos (CI) e de oportunidade (CO), apresentados abaixo:

Custos de violação	CD	CI	CO
- Atividades forenses e investigativas relacionadas à violação			
- Treinamento de conscientização dos funcionários			
- Novos controles de segurança instalados, incluindo um novo firewall e software de detecção de intrusão			
- Multas regulatórias relacionadas à violação de segurança cibernética			
- Indenização às partes afetadas			
- Comunicações sobre o ocorrido, status e efeito da violação			
- Custos legais			
- Perda de receita com o tempo de inatividade do sistema			
- Perda de negócios devido a efeitos negativos de reputação			
- Redução nos lucros devido à perda de reputação			

Gostaríamos de ter seu feedback sobre as classificações acima:

Você teve dificuldade para classificar esses custos? ( ) Sim ( ) Não

Se for atribuir uma nota de 0 a 5, qual o seu grau de dificuldade? _____

Você tem plena convicção/confiança de que acertou mais que 70% das classificações, **sem qualquer tipo de consulta**? ( ) Sim ( ) Não

Se for atribuir uma nota de 0 a 5, qual o seu grau de convicção/confiança? _____

Suponha que um ano após a violação inicial de segurança cibernética, você toma conhecimento que a empresa enfrentará uma ação judicial relacionada à violação. Você saberia informar os impactos dos custos de violação nas demonstrações contábeis? ( ) Sim ( ) Não

Se for atribuir uma nota de 0 a 5, qual o seu grau de dificuldade? _____

Você considera importante a inserção de conhecimentos sobre segurança cibernética no currículo do curso de Ciências Contábeis, para habilitação profissional? ( ) Sim ( ) Não

Fonte: inspirada no estudo de Boss *et al.* (2022)

A partir da aplicação desse caso de ensino/simulação, três variáveis do constructo "Consciência sobre Custos de Violação" foram definidas, sendo binárias e qualitativas: Dificuldade para Classificar os Custos (DCC) (1 – Sim e 0 – Não); Convicção dos Acertos sobre as Classificações dos Custos (CACC) (1 – Sim e 0 – Não); e Conhecimento para informar os Impactos dos Custos de Violação nas Demonstrações Contábeis (CICVDC) (1 – Sim e 0 – Não).

Já como constructo independente, tem-se primeiramente a Consciência sobre Segurança Cibernética (ConsSegCibernética). Ela foi capturada mediante aplicação de nove assertivas do tipo *Likert* (1-5 pontos). Para mensuração e formação dos fatores, aplicou-se o teste estatístico Análise Fatorial. O instrumento composto por nove assertivas foi adaptado dos estudos de Safa *et al.* (2015) e Boss *et al.* (2022).

Tabela 2

Consciência sobre segurança cibernética

1- Estou ciente de um potencial ameaça à segurança.
2- Eu entendo o risco de incidentes de segurança cibernética das violações de segurança cibernética
3- Eu me mantenho atualizado em termos de conscientização sobre segurança da informação
4- Tenho conhecimento suficiente sobre o custo de violações de segurança cibernética.
5- Compartilho conhecimentos de segurança da informação para aumentar minha consciência
6- Tenho compreensão conceitual/teórica sobre segurança cibernética
7- Tenho conhecimento sobre os aspectos gerenciais e aspectos organizacionais da segurança da informação e como eles se relacionam aos tópicos gerais de contabilidade.
8- Tenho conhecimento sobre os procedimentos e controles internos adotados para efetuar o monitoramento contínuo em situações de ataque cibernético.
9- Tenho conhecimento sobre os aspectos éticos e legais da segurança cibernética e a responsabilidade do contador em cada uma dessas áreas.

Fonte: inspirada nos estudos de Safa *et al.* (2015) e Boss *et al.* (2022)

Tem-se também o constructo independente do Grau de Dificuldade para informar os Impactos dos Custos de Violação nas Demonstrações Contábeis (GDICVDC) elaborado em consonância ao estudo de Boss *et al.* (2022).

Finalmente, o outro constructo independente desta pesquisa refere-se à Presença de Traços de Personalidade Narcisista (PontosNARC) e foi composto de uma única variável, referente ao traço de personalidade narcisista. O instrumento de mensuração é o NPI, constituído por 40 assertivas que, segundo Paulhus e Jones (2015), é o instrumento que melhor captura isoladamente as características de grandiosidade, autossuficiência e o ego inflado do narcisismo subclínico. Esse instrumento foi validado nacionalmente por Magalhães e Koller (1994) e aplicado por Avelino (2017) em investigação na área contábil.

Raskin e Hall (1979) e Raskin e Terry (1988) desenvolveram um inventário de medição de traços de personalidade narcisista denominado NPI, cujas assertivas remetem aos fatores autoridade, autossuficiência, superioridade, exibicionismo, exploração, vaidade e senso de direito. O NPI é uma medida de escolha forçada com um par de declarações de características narcisistas e não narcisistas, em cuja mensuração é atribuído o valor 1 para declarações narcisistas e o valor 0 para declarações não narcisistas. As 40 assertivas são binárias, sendo que a mensuração é realizada pela somatória dos pontos, com o máximo de 40, gerando uma variável quantitativa.

Cabe aqui mencionar a inserção das variáveis gênero, faixa etária, semestre e atividade remunerada, para os estudantes e, adicionalmente, para os profissionais, atuação, tempo de experiência e formação. Essas variáveis foram inseridas como variáveis de controle do modelo investigado, por serem consideradas potencialmente influenciadoras nas interpretações e escolhas dos indivíduos, conforme enuncia Hambrick e Mason (1984). Os autores argumentam que características de raízes socioeconômicas, tais como idade, educação, ocupação na empresa, experiência funcional e posição financeira são consideradas importantes e complexas e possibilitam uma visão psicológica do comportamento humano. Hambrick (2007, p. 334) frisa que "[...] a personalidade, os valores e as experiências dos executivos influenciam fortemente suas interpretações, que por sua vez afetam suas escolhas".

Importa considerar que o coeficiente de confiabilidade do modelo investigado, medido pelo Alpha de Cronbach, foi de 0,710 para todas as variáveis inseridas em conjunto. Esses resultados indicam a consistência dos modelos em estudo.

3.3 Abordagem estatística

No que diz respeito à abordagem estatística, foram adotados: Estatística Descritiva (frequências, médias, desvio-padrão, valor máximo e valor mínimo), Análise Fatorial e Regressão Logística.

A estatística descritiva teve o intuito de resumir, descrever e compreender os dados da amostra em estudo. Já a Análise Fatorial teve o intuito de possibilitar a simplificação das variáveis da Consciência sobre Segurança Cibernética, haja vista a inspiração do instrumento original, sem uso integral do estudo base. Por fim, foi aplicada a regressão logística para verificar as relações entre as variáveis dependente e independentes e assim trazer evidência sobre a probabilidade de ocorrência de um evento, além de ser uma técnica adequada ao teste das hipóteses da pesquisa. As hipóteses desta pesquisa foram operacionalizadas mediante essa regressão, sendo desmembradas de acordo com as três variáveis do constructo dependente "Consciência sobre Custos de Violação".

Para a estimação do modelo de regressão logística, este estudo contou com equações específicas: para os estudantes e para os profissionais. As respostas das amostras foram divididas nas duas categorias binárias das variáveis dependentes, isto é, DCC – Com ou Sem Dificuldade para Classificar os Custos; CACC – Com ou Sem Convicção dos Acertos sobre as Classificações dos Custos; e CICVDC – Com ou Sem Conhecimento para Informar os Impactos dos Custos de Violação nas Demonstrações Contábeis.

Como variáveis independentes, foram incluídas as variáveis Consciência sobre Segurança Cibernética (CSC), Presença de Traços de Personalidade Narcisista (NARC) e Grau de Dificuldade para informar os Impactos dos Custos de Violação nas Demonstrações Contábeis (GDICVDC).

Para os estudantes, além das variáveis independentes, foram incluídas as variáveis de controle gênero, faixa etária, semestre e atividade remunerada. Essas variáveis foram inspiradas em estudos prévios como Allen, Fuller e Luckett (1998) e Avelino (2017). Na sequência, são trazidos os três modelos de equação deste estudo relativos aos estudantes.

$$DCC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 SEM_i + \beta_7 REM_i + \varepsilon_i$$

$$CACC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 SEM_i + \beta_7 REM_i + \varepsilon_i$$

$$CICVDC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 SEM_i + \beta_7 REM_i + \varepsilon_i$$

Para os profissionais, foram incluídas as variáveis de controle gênero, faixa etária, atuação, tempo de experiência e formação. As variáveis de controle foram inspiradas em estudos prévios, como os de Campbell *et al.* (20111) e Avelino (2017). Os três modelos de equação desta pesquisa relativos aos profissionais são trazidos na sequência.

$$DCC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 ATUA_i + \beta_7 EXP_i + \beta_7 FORM_i + \varepsilon_i$$

$$CACC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 ATUA_i + \beta_7 EXP_i + \beta_7 FORM_i + \varepsilon_i$$

$$CICVDC_i = \beta_0 + \beta_1 CSC_i + \beta_2 GDICVDC_i + \beta_3 NARC_i + \beta_4 GEN_i + \beta_5 ETARIA_i + \beta_6 ATUA_i + \beta_7 EXP_i + \beta_7 FORM_i + \varepsilon_i$$

4 Resultados

Como foram realizadas duas coletas, sendo uma com alunos de Ciências Contábeis e a outra com profissionais atuantes na área contábil, os resultados são inicialmente apresentados de forma individualizada e descritiva. Em seguida, esses resultados são discutidos e comparados, considerando-se, adicionalmente, os resultados de estudos anteriores.

4.1 Estudo 1: Perfil dos estudantes de Ciências Contábeis

A maioria dos estudantes pertence ao gênero feminino, tem faixa etária entre 18 e 25 anos, cursa entre o 6º e o 8º semestres, exerce atividade remunerada e é oriunda de instituição de ensino superior pública na região Nordeste.

De acordo com a Tabela 3, a pontuação máxima de acertos referentes à classificação dos custos foi de 80 pontos, e houve quem zerasse a classificação, sendo a média de 38,4 pontos. Sobre a pontuação dos traços do narcisismo, a amostra apresenta 11,79 pontos, de um máximo totalizando 40 pontos, com as maiores concordâncias para as assertivas: "Acho fácil manipular pessoas; gosto de sempre assumir a responsabilidade pelas minhas decisões; sou capaz de convencer as pessoas; serei um sucesso; e vejo-me como um bom líder".

Tabela 3
Estatística descritiva para a coleta com estudantes

	N	Mínimo	Máximo	Média	Desvio-padrão
Variáveis					
Pontuação Narcisismo	262	2	29	11,79	5,474
Total Acertos Classificação dos Custos	262	0	80	38,40	18,144
N válido (de lista)	262				

Fonte: desenvolvida pelos autores (2024).

Esses parâmetros confirmam que o fator formado consegue descrever satisfatoriamente a variação dos dados originais, o qual foi incorporado ao modelo estatístico. Na sequência, aplicou-se a regressão logística (Tabela 4), em função da natureza binária das variáveis dependentes. Adotou-se o método *Forward Wald,* para a inclusão das variáveis significantes e a exclusão das variáveis não significantes. Os resultados do teste qui-quadrado apresentaram a significância sig = ,000 conjunta dos coeficientes para os três modelos em estudo, possibilitando inferir que as variáveis inseridas no modelo são capazes de predizer com acurácia a investigação.

Tabela 4
Ajuste ao modelo de regressão logística para a coleta com estudantes

	Etapa	Verossimilhança de log -2	R quadrado Cox & Snell	R quadrado Nagelkerke
DCC	2	196,129	,076	,136
CACC	4	215,930	,223	,338
CIVCDC	2	252,440	,253	,353

Nota 1: Dificuldade para Classificar os Custos (DCC); Convicção dos Acertos sobre as Classificações dos Custos (CACC), Conhecimento para informar os Impactos dos Custos de Violação nas Demonstrações Contábeis (CIVCDC).

Fonte: desenvolvida pelos autores (2024).

Verifica-se que o modelo é adequado (-2LL), sendo menor que 1 para os três modelos. Com base no teste de Cox e Snell, verifica-se que 7,6%, 22,3% e 25,3% das variações ocorridas no *log* da razão de chance da probabilidade de ocorrência são explicados pelo conjunto de variáveis independentes sobre DCC, CACC e CIVCDC, respectivamente. O modelo estatístico é capaz de explicar 13,6%, 33,8% e 35,3% das variações registradas nas variáveis DCC, CACC e CIVCDC, respectivamente. A Tabela 5 traz os coeficientes, sinais e teste de Wald, trazendo somente aquelas variáveis que foram incluídas a partir da aplicação do Forward Wald.

Tabela 5
Coeficientes, Sinais e Teste de Wald para a coleta com estudantes

	Variáveis	Sinal esperado	Sinal encontrado	Coeficiente B	Coeficientes Exp(β)	Teste de Wald
						P-Value
DCC Modelo 1	Gênero		-	1,056	,348	,004
	GDICVDC		+	,507	1,660	,001
	Constante		+	,559	1,749	,320
CACC Modelo 2	CSC	+	+	,668	1,950	,001
	GDICVDC		-	,800	,449	,000
	Gênero		+	1,070	2,915	,002
	Semestre		-	,552	,576	,001
	Constante		+	4,651	104,705	,000
CIVCDC Modelo 3	CSC	+	+	,929	2,531	,000
	GDICVDC		-	,839	,432	,000
	Constante		+	1,933	6,911	000

Nota 1: Dificuldade para Classificar os Custos (DCC), Convicção dos Acertos sobre as Classificações dos Custos (CACC), Conhecimento para informar os Impactos dos Custos de Violação nas Demonstrações Contábeis (CIVCDC), Grau de Dificuldade para informar os Impactos dos Custos de Violação nas Demonstrações Contábeis (GDICVDC), Consciência sobre Segurança Cibernética (CSC).

Fonte: desenvolvida pelos autores (2024).

A análise individual dos parâmetros, pelo Modelo 1 da Tabela 5, evidencia que as variáveis GDICVDC tem sinal positivo, indicando que as variações positivas dessa variável concorrem para o aumento da probabilidade de os estudantes manifestarem dificuldade de classificar os custos. Já a variável Gênero apresentou sinal negativo, sinalizando que a dificuldade de classificar os custos diminui em função dessa variável.

No Modelo 2, as variáveis ConsSegCibernética e Gênero têm sinais positivos, revelando a probabilidade de que a convicção sobre os acertos é majorada com o aumento da consciência sobre segurança cibernética e em função do Gênero. De forma contrária, a convicção dos acertos diminui em função do semestre em curso e do GDICVDC.

Já no Modelo 3, o sinal do CSC foi positivo, permitindo a inferência de que existe a probabilidade de que o conhecimento para informar os impactos dos custos de violação nas demonstrações contábeis aumente em função da consciência sobre a segurança cibernética e diminua em função do GDICVDC.

Esses achados demonstram que, para os estudantes, uma maior consciência sobre segurança cibernética no geral impacta a consciência sobre os custos de violação. A única relação não observada refere-se à dificuldade para classificar os custos, talvez pelo estágio de formação que ainda se encontram os estudantes. Esse resultado alinha-se à defesa de Anderson *et al.* (2013) que, para a identificação dos custos de violação, faz-se necessário ter consciência sobre segurança cibernética. Já para os achados referentes aos traços narcisistas, não houve significância estatística, o que refuta expectativa de maior consciência pela autovisão de superioridade e grandiosidade, pontuada por Maasberg *et al.* (2020).

4.2 Estudo 2: Perfil dos profissionais da área contábil

A maioria dos profissionais é do gênero masculino, com faixa etária de 26 a 35 anos, ensino superior completo e atuação em empresa pública ou privada na região Sudeste. De acordo com a Tabela 6, a pontuação máxima de acertos, no que se refere à classificação dos custos, foi de 80 pontos, e houve quem zerasse a classificação, sendo a média de 44,7 pontos. Sobre a pontuação dos traços do narcisismo, a amostra apresenta 12,76 pontos, com as maiores concordâncias para as assertivas: "A modéstia não é meu forte; gosto de sempre assumir a responsabilidade pelas minhas decisões; sou uma pessoa segura; vejo-me como um bom líder; e tenho talento natural para influenciar as pessoas".

Tabela 6
Estatística descritiva para a coleta com profissionais

	N	Mínimo	Máximo	Média	Desvio-padrão
Profissionais					
Pontuação Narcisismo	166	2	32	12,76	6,559
Total Acertos Classificação dos Custos	166	0	80	44,70	19,530
N válido (de lista)	166				

Fonte: desenvolvida pelos autores (2024).

Na sequência, foi realizada a análise fatorial a fim de agrupar as questões constituintes da Consciência sobre Segurança Cibernética. Foi possível agrupar as assertivas, com a formação do fator Consciência sobre Segurança Cibernética (CSC). Vale mencionar que, na análise fatorial para definição desse fator, para os estudantes, o teste de Bartlett evidenciou que o modelo em estudo é estatisticamente significativo (sig. < 0,00) e o KMO, que representa o grau de explicação dos dados a partir do fator encontrado, que foi de 86,8%. O *eigenvalue* assumiu valor de 4,592, responsável por 51,026% da variância explicada. Para os profissionais, o teste de Bartlett apresentou sig. < 0,00 e o KMO foi de 0,717. O *eigenvalue* assumiu valor 3,822, responsável por 42,467%, da variância explicada.

Finalmente, aplicou-se a regressão logística pelo método *Forward Wald* (Tabela 7).

Tabela 7
Ajuste ao modelo de regressão logística para a coleta com profissionais

	Etapa	Verossimilhança de log -2	R quadrado Cox & Snell	R quadrado Nagelkerke
DCC	3	169,222	,128	,187
CACC	2	153,796	,084	,132
CICVDC	4	136,539	,376	,518

Fonte: desenvolvida pelos autores (2024).

Verifica-se que os resultados do teste qui-quadrado apresentaram a significância sig = ,000 conjunta dos coeficientes, para os três modelos em estudo. O modelo é adequado (-2LL) menor que 1 para os três modelos. O teste de Cox e Snell apresentou que 12,8%, 8,4% e 37,5% das variações ocorridas são explicados pelo conjunto de variáveis independentes sobre DCC, CACC e CICVDC, respectivamente; e o modelo estatístico é capaz de explicar 18,7%, 13,2% e 51,8% as variações registradas nas variáveis DCC, CACC e CICVDC, nessa ordem. Já a Tabela 8 traz os coeficientes, sinais e teste de Wald, apresentando somente aquelas variáveis que foram incluídas a partir da aplicação do Forward Wald.

Tabela 8

Coeficientes, sinais e teste de Wald para a coleta com profissionais

	Variáveis	Sinal esperado	Sinal encontrado	Coeficiente B	Coeficientes Exp(β)	Teste de Wald
						P-Value
DCC Modelo 1	CSC	-	-	,430	,651	,038
	GDICVDC		+	,299	1,348	,027
	Gênero		-	1,176	,308	,008
	Constante		+	,898	2,455	,139
CACC Modelo 2	CSC	+	+	,699	2,012	,002
	TempoExp		+	,248	1,282	,027
	Constante		-	2,250	,105	,000
CICVDC Modelo 3	NARC	+	+	,118	1,125	,001
	CSC	+	+	1,103	3,012	,000
	GDICVDC		-	1,110	,329	,000
	Formação		+	2,319	10,169	,003
	Constante		-	3,322	,036	,041

Nota 1. Dificuldade para Classificar os Custos (DCC), Convicção dos Acertos sobre as Classificações dos Custos (CACC), Conhecimento para informar os Impactos dos Custos de Violação nas Demonstrações Contábeis (CIVCDC), Grau de Dificuldade para informar os Impactos dos Custos de Violação nas Demonstrações Contábeis (GDICVDC), Consciência sobre Segurança Cibernética (CSC), Pontuação de Traços Narcisistas (NARC).

Fonte: desenvolvida pelos autores (2024).

A análise individual dos parâmetros, pelo Modelo 1 da Tabela 8, evidencia que a variável CSC tem sinal negativo, indicando que a variação negativa dessa variável concorre para o aumento da probabilidade de os profissionais manifestarem dificuldade de classificar os custos. Contrariamente, o GDICVDC apresentou sinal positivo.

No Modelo 2, a CSC e tempo de experiência apresentou sinal positivo, apontando para a probabilidade de que a convicção sobre os acertos aumente com o aumento da consciência sobre segurança cibernética e da experiência dos profissionais.

E no Modelo 3, o Narcisismo, a CSC e a Formação apresentaram sinais positivos, permitindo inferir que existe a probabilidade de que o conhecimento para informar os impactos dos custos de violação nas demonstrações contábeis aumente em função dessas variáveis e diminua em função do GDICVDC.

Esses achados demonstram que para os profissionais uma maior consciência sobre segurança cibernética impacta plenamente a consciência sobre os custos de violação, o que mais uma vez vai ao encontro do argumento de Anderson *et al.* (2013), referente à necessidade da consciência sobre segurança cibernética para a identificação dos custos de violação. Os achados referentes aos traços narcisistas mais uma vez, no geral, não demonstraram significância estatística, o que novamente refuta a expectativa pontuada por Maasberg *et al.* (2020) de maior consciência pela autovisão de superioridade e grandiosidade. Em diferença aos estudantes, todavia, os profissionais com mais traços narcisistas mostraram conhecer mais os impactos dos custos de violação nas demonstrações contábeis do que os profissionais com menos traços.

5 Discussão

Para dar início à discussão, cabe apresentar a Tabela 9 com a decisão sobre as hipóteses de pesquisa formuladas neste trabalho.

Tabela 9
Decisão Hipótese da pesquisa

Hipóteses	Variável dependente	Variável independente	Decisão	
			Estudantes	Profissionais
Hipótese 1: A consciência sobre segurança cibernética impacta a consciência sobre os custos de violação.			**Parcialmente rejeitada**	**Não rejeitada**
H1a: A consciência sobre segurança cibernética impacta negativamente a dificuldade de classificação dos custos de violação.	DCC	CSC	Rejeitada	Não rejeitada
H1b: A consciência sobre segurança cibernética impacta positivamente a convicção sobre os acertos de classificação dos custos de violação.	CACC	CSC	Não rejeitada	Não rejeitada
H1c: A consciência sobre segurança cibernética impacta positivamente o conhecimento sobre os impactos dos custos de violação nas demonstrações contábeis.	CIVCDC	CSC	Não rejeitada	Não rejeitada
Hipótese 2: O traço de personalidade narcisista influencia a consciência sobre os custos de violação.			**Rejeitada**	**Parcialmente rejeitada**
H2a: Há maior probabilidade de os indivíduos com traços narcisistas mais marcantes relatarem menor dificuldade para classificar os custos de violação.	DCC	NARC	Rejeitada	Rejeitada
H2b: Há maior probabilidade de os indivíduos com traços narcisistas mais marcantes relatarem maior convicção quanto aos acertos na classificação dos custos.	CACC	NARC	Rejeitada	Rejeitada
H2c: Há maior probabilidade de os indivíduos com traços narcisistas mais marcantes relatarem conhecer os impactos dos custos de violação nas demonstrações contábeis.	CIVCDC	NARC	Rejeitada	Não rejeitada

Fonte: desenvolvida pelos autores (2024).

Os resultados apresentados merecem atenção para a área contábil. A dificuldade de classificar os custos de violação e de conhecimento para informar os custos de violação nas demonstrações contábeis e a ausência de convicção sobre os acertos de classificação dos custos foram percebidas pelos estudantes e profissionais da amostra em estudo. Embora os profissionais tenham pontuado mais que os estudantes na classificação dos custos de violação, a média ficou abaixo de 50 pontos, entre os 100 totais. A falta de cultura em segurança cibernética, de habilitação e de conhecimento de grande número de brasileiros conectados ao mundo digital mostra que a sociedade brasileira não está preparada para o uso das ferramentas digitais com os cuidados adequados relativos à segurança cibernética (Decreto n.º 10.222, de 2020).

Esses achados também ratificam os argumentos de Boss *et al.* (2022) sobre o fato de a consciência cibernética ser um tópico importante que, no contexto prático da área contábil, produzirá profissionais mais bem informados. Nessa concepção, defendem que a cibersegurança seja vista não como um "acréscimo" ou "outro" assunto na contabilidade, mas como parte integrante da contabilidade. Curiosamente, apesar do aumento da ênfase regulatória e profissional, a maioria dos currículos de contabilidade limita a cobertura de segurança cibernética à disciplina Sistemas da Informação Contábeis.

Ao analisar a disposição para o traço narcisista, os profissionais demonstraram mais aproximação, confirmando a pouca modéstia e maior segurança em suas escolhas. Já os estudantes com o traço mais intenso revelaram que é fácil manipular as pessoas. Contudo, ambos os integrantes dos dois grupos informaram que se veem como bons líderes e gostam de assumir a responsabilidade por suas decisões. Infere-se, portanto, que a autossuficiência, a vaidade e o ego inflado desse traço se revelaram entre os pesquisados, o que pode implicar o despreparo para lidar com as ameaças cibernéticas, tão contínuas e cada vez mais complexas, na atualidade. Esse resultado é parcialmente corroborado pelos achados de Avelino e Lima (2017), segundo os quais os estudantes de Ciências Contábeis informaram com maior intensidade que se veem como bons líderes.

Ao analisar a consciência sobre segurança cibernética dos pesquisados, tanto os estudantes quanto os profissionais, que apresentaram maior consciência cibernética, revelaram maior convicção sobre os acertos de classificação dos custos e conhecimento para informar os impactos nas demonstrações contábeis. Os profissionais demonstraram, adicionalmente, menor dificuldade para classificar e informar o impacto dos custos nas demonstrações contábeis.

Esses achados estão em consonância com os de Safa *et al.* (2015) ao comprovarem que profissionais com conscientização sobre segurança relacionam-se com boas atitudes dos usuários; e também com os achados de Boss *et al.* (2022) sobre a percepção dos estudantes, que revelaram a subjetividade da classificação e a dificuldade de mensuração dos custos de violação. Anuíram que os conteúdos devem ser trabalhados ao longo das disciplinas, tal como o resultado do presente estudo, no qual 80,2% dos respondentes concordaram com a inserção dos conteúdos nos currículos de cursos de Ciências Contábeis.

Esses achados também reforçam os argumentos de Reidenbach e Wang (2021) sobre a importância da aplicação de casos de ensino nos cursos de Contabilidade por oportunizar aos estudantes a prática de situações reais e concretas, podendo desenvolver e aplicar as habilidades adquiridas e o pensamento crítico para avaliação das decisões tomadas pela empresa, por auditores externos e acionistas.

Ademais, os achados alinham-se à defesa de Boss *et al.* (2022) de que tópicos de segurança cibernética introduzidos, enfatizados e integrados ao conteúdo dos cursos em todo o currículo, oportunizarão um grande benefício para os estudantes de Contabilidade e futuros profissionais. Os autores não defendem a mudança de foco do ensino contábil de todas as disciplinas, mas incitam a discussão, também alvo dos estudos de Roohani e Zheng (2019), sobre a complementação do currículo atual de Contabilidade, a fim de equipar os estudantes com conhecimentos e habilidades suficientes para avaliarem o risco de segurança cibernética e aprenderem sobre os controles para mitigar esses riscos, dados os recentes e contínuos incidentes de segurança cibernética.

Finalmente, no que se refere aos traços de narcisismo, de forma particular, cabe trazer que os profissionais mais narcisistas somente exibiram maiores chances de relatar sobre conhecer os impactos das violações nas demonstrações contábeis. O gênero, o tempo de experiência e a formação também se destacaram nos resultados da amostra dos profissionais, enquanto o gênero e o semestre em curso também se destacaram na amostra dos estudantes, confirmando o pressuposto da Teoria dos Altos Escalões (Hambrick & Mason, 1984; Carpenter *et al.*, 2004) de que os fatores sociais e demográficos influenciam as escolhas dos indivíduos.

A nem maior nem menor consciência dos custos de violação pelos índividuos com mais traços narcisistas (ausência de significância estatística) traz a reflexão de que, mesmo que os respondentes com maiores disposições para o traço narcisista tenham percebido o desconhecimento sobre os assuntos, eles não reconheceriam suas fragilidades, confirmando seu comportamento de superioridade, grandiosidade e a visão inflada de suas capacidades, conforme pontuam Maasberg *et al.* (2020) e Raskin e Terry (1988).

6 Conclusão

As violações cibernéticas expõem a confidencialidade e a integridade das informações financeiras no meio organizacional. Por vezes, os ataques são facilitados pela falta de consciência do risco de compartilhar informações da conta, de baixar softwares da internet, anotar senhas em papel e abrir e-mails de origem duvidosa (Safa *et al.*, 2015).

Este estudo propôs a análise da influência dos traços narcisistas no que tange à consciência sobre segurança cibernética e os custos de violação, com estudantes e profissionais da contabilidade. Os resultados evidenciaram que tanto estudantes quanto profissionais sentiram dificuldade de classificar os custos de violação e informar os custos de violação nas demonstrações contábeis, fato constatado pelo total de acertos de classificação dos custos não superar 50 pontos.

Pela literatura, era esperado o resultado de que a consciência sobre segurança cibernética habilitaria os estudantes e profissionais a terem maior conhecimento para informar os impactos dos custos de violação nas demonstrações contábeis e convicção sobre a classificação desses custos. Confirmou-se a probabilidade de estudantes e profissionais com consciência cibernética relatarem maior convicção quanto aos acertos de classificação e de reconhecimento dos impactos dos custos nas demonstrações contábeis.

Sobre o traço narcisista, os profissionais apresentaram maior pontuação e confirmaram maior conhecimento para informar as violações dos custos nas demonstrações contábeis. Os demais resultados não mostraram ser impactados pela personalidade narcisista.

Assim, esses resultados respondem ao problema de pesquisa, demonstrando que, sim, a consciência sobre segurança cibernética influencia a consciência sobre os custos de violação com os profissionais e estudantes de Contabilidade pesquisados. Os resultados também demonstram que o traço de personalidade narcisista não impacta tão fortemente quanto esperado o nível de consciência dos custos de violação, ao passo que tão somente o conhecimento para informar as violações dos custos nas demonstrações contábeis mostrou-se mais expressivo em profissionais narcisistas.

Os resultados contribuem com a área científica da Contabilidade, sobretudo, na reflexão sobre a influência dos traços de personalidade narcisista no comportamento de estudantes e profissionais, além de permitirem a análise individualizada e também comparativa da percepção, do conhecimento, das dificuldades e das convicções sobre a segurança cibernética e dos impactos dos custos de violação nas demonstrações contábeis.

Também joga luz às instituições de ensino para inserção de conceitos sobre a segurança cibernética, de forma mais assertiva, nas ementas das disciplinas do curso de Ciências Contábeis, tais como Contabilidade Geral, Gerencial e de Custos, Controladoria, Administração Financeira, Orçamento Empresarial, Análise das Demonstrações Contábeis e Auditoria, o que oportunizará maior segurança em reconhecer os impactos dos ataques nas demonstrações contábeis, como também promoverá atividades extracurriculares para o ensino aprendizagem sobre esse assunto emergente e impactante.

Os achados despertam a atenção também dos professores para se capacitarem frente a esse novo contexto, bem como para a implementação e aplicação de casos de estudos concretos que oportunizem aos estudantes a se comportarem em situações de violação, tal como o presente estudo. Ademais, chama a atenção de empresários para a importância de investirem na implantação de um sistema de segurança da informação, que, embora tenha um alto custo, terá um impacto financeiro menor que o custo de um ataque cibernético, sobretudo, se as informações sequestradas, proporcionarem perda de credibilidade e reputação para as empresas.

Espera-se que os resultados provoquem uma reflexão nas instituições de ensino contábil e nas empresas, com a finalidade de introduzirem treinamentos e conteúdos mais específicos sobre segurança cibernética nas disciplinas dos cursos de Contabilidade, de forma contextualizada com outras matérias curriculares, para habilitar os aspirantes contadores a reconhecerem os impactos financeiros gerados pelos ataques cibernéticos e os custos de recuperação das empresas.

O estudo apresenta limitações, sobretudo relacionadas à amostra e à análise comportamental, e não clínica, dos traços narcisistas, e também à análise desse comportamento autossuficiente, vaidoso e autocentrado, que não reconhece fragilidades e a necessidade de buscar novas habilidades e competências para o exercício profissional.

Sugere-se, para pesquisas futuras, ampliar o espectro amostral, a aplicação de novos casos de ensino inspirados nos estudos estrangeiros e o aprofundamento do debate a respeito da inserção dos conteúdos sobre segurança cibernética e os impactos para os registros contábeis, nas resoluções que normatizam o ensino contábil nacional e internacional.

Referências

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432-445.

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: a victim of operational pressures. *Computers & Security, 42*, 56-65.

Allen, J., Fuller, D., & Luckett, M. (1998). Academic integrity: behaviors, rates and attitudes of business students toward cheating. *Journal of Marketing Education, 20*(1), 41-52.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M. J. van, Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In Böhme, R. (eds). *The Economics of Information Security and Privacy*. Springer, Berlin, Heidelberg. (pp. 265-300). https://doi.org/10.1007/978-3-642-39498-0_12

Avelino, B. C. (2017). Olhando-se no espelho: uma investigação sobre o narcisismo no ambiente acadêmico. [Tese de doutorado, Universidade de São Paulo]. Biblioteca Digital. https://doi.org/10.11606/T.12.2017.tde-06042017-165713

Avelino, B. C., & Lima, G. A. S. F. (2017). Narcisismo e desonestidade acadêmica. *Revista Universo Contábil, 13*(3), 70. doi:10.4270/ruc.2017319

Bakarich, K. M., & Baranek, D. (2019). Something phish-y is going on here: a teaching case on business email compromise. *Current Issues in Auditing, 14*(1), A1-A9.

Baumeister, R. F., Bushman, B. J., & Campbell, W. K. (2000). Self-esteem, narcissism, and aggression: does violence result from low self-esteem or from threatened egotism? *Current Directions in Psychological Science, 9*, 26-29.

Boss, S. R., Gray, J., & Janvrin, D. J. (2022). Accountants, cybersecurity isn't just for "techies": incorporating cybersecurity into the accounting curriculum. *Issues in Accounting Education, 37*(3), 73-89.

Campbell, W. K., Hoffman, B. J., Campbell, S. M., & Marchisio, G. (2011). Narcissism in organizational contexts. *Human Resource Management Review, 21*(4), 268-284.

Carpenter, M. A., Geletkanycz, M. A., & Sanders, G. M. (2004). Upper echelons research revisited: antecedents, elements and consequences of top management team composition. *Journal of Management*, *30*(6), 749-778.

Cram, W. A., & D'Arcy, J. (2016). Teaching information security in business schools: current practices and a proposed direction for the future. *Communications of the Association for Information Systems*, *39*(1), 3.

Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: patterns of attack and vulnerability. *Computers in Human Behavior, 87*, 174-182.

Decreto n. 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, *13*(2), C1-C9.

Gordon, L. A., & Loeb, M. P. (2006). *Managing cybersecurity resources: a cost-benefit analysis* (Vol. 1). New York: McGraw-Hill.

Hambrick, D. C. (2007). Upper echelons theory: an update. *Academy of Management Review, 32*(2), 334-343.

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: the organization as a reflection of its top managers. *Academy of Management Review, 9*(2), 193-206.

Janvrin, D. J., & Wang, T. (2022). Linking cybersecurity and accounting: an event, impact, response framework. *Accounting Horizons, 36*(4), 67-112.

Jones D. N. (2022). Shadows behind the keyboard: dark personalities and deception in cyberattacks. *Proceedings of the 2022 ACM International Workshop on Security and Privacy Analytics (IWSPA '22)*, April 27, 2022, Baltimore, MD, USA. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3510548.3519379

Jones, D. N., Padilla, E., Curtis, S. R., & Kiekintveld, C. (2021). Network discovery and scanning strategies and the dark triad. *Computers in Human Behavior*, *122*, 106799.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security*, *45*, 58-74.

Landwehr, C. E. (2001). Computer security. *International Journal of Information Security, 1*(1), 3-13.

Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Maasberg, M., Slyke, C. Van, Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM, 63*(12), 64-80.

Magalhães, M., & Koller, S. H. (1994). Relação entre narcisismo, gênero e gênero. *Arquivos Brasileiro de Psicologia, 46*(3/4), 77-93.

Núcleo de Informação e Coordenação do Ponto BR. (2020). *Segurança digital: uma análise da gestão de riscos em empresas brasileiras* [livro eletrônico]. Comitê Gestor da Internet no Brasil. https://www.nic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf

Paulhus, D. & Jones, D. (2015). *Measures of dark personalities*. In Boyle, G. J., Saklofske, D. H., & Matthews, G. (Eds.). *Measures of personality and social psychological constructs* (pp. 562-594). Elsevier. 10.1016/B978-0-12-386915-9.00020-6

Raskin, R., & Hall, C. S. (1979). A narcissistic personality inventory. *Psychological Reports*, *45*, 590.

Raskin, R., & Terry, H. (1988). A principal-components analysis of the narcissistic personality inventory and further evidence of its construct validity. *Journal of Personality and Social Psychology, 5*4(5), 890-902.

Reidenbach, M., & Wang, P. (2021). Heartland payment systems: cybersecurity impact on audits and financial statement contingencies. *Issues in Accounting Education*, *36*(2), 93-109.

Resolução CVM n. 35, de 26 de maio de 2021. Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários. https://conteudo.cvm.gov.br/legislacao/resolucoes/resol035.html

Roohani, S. J. & Zheng, X. (2019). Using ten teaching modules and recently publicized data-breach cases to integrate cybersecurity into upper-level accounting courses. In Calderon, T. G. (Ed.). *Advances in accounting education: teaching and curriculum innovations*. (Vol. 23), Emerald Publishing Limited, Bingley (pp. 113-125). https://doi.org/10.1108/S1085-462220190000023007

Safa, N. S., Sookhak, M., Solms, R. Von, Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Silva, W. R. (2018). *Análise econômica dos impactos de ataques cibernéticos*. [Dissertação de Mestrado, Faculdade de Economia, Administração e Contabilidade da Universidade de Brasília]. Repositório Aberto da Universidade de Brasília. http://repositorio.unb.br/handle/10482/34838

Woo, H-J. (2003). *The hacker mentality: exploring the relationship between psychological variables and hacking activities.* Dissertação [Doutorado em Filosofia, University of Georgia].

Anexo 1 – Extrato original do trabalho de Boss *et al* (2022) usado como inspiração para definição do constructo "Consciência sobre Custos de Violação"

1. Identify which of the following expenses are direct vs indirect vs lost opportunity costs.

Expense	Direct costs	Indirect costs	Lost opportunity costs
Forensic and investigative activities related to breach			
Penetration testing to ensure vulnerabilities addressed			
Costs associated with issuing new accounts / credit cards			
Employee awareness training			
Installed new security controls including a new firewall and intrusion detection software			
Added a new IT position, chief information security officer			
Regulatory fines related to cybersecurity breach			
Compensation to affected parties			
Communications regarding status and effect of breach			
Loss of customers			
Legal costs			
Public relations costs			
Credit monitoring costs			
Lost revenue from system downtime			
Lost business due to negative reputation effects			
Shortfall in profits due to loss of reputation			

2. Which of these costs are easiest to measure? Why?

3. Which of these costs are most difficult to measure? Why?

4. When could you measure (or estimate) each cost? Why?