# IMPACTOS ÉTICOS DA TECNOLOGIA NO CONTEXTO CONTÁBIL EMPRESARIAL: DESAFIOS DA PRIVACIDADE E SEGURANÇA DE DADOS

Laura Loranny Santana Arouche[1]
Sadi Tenente dos Santos Júnior[2]
Dra. Verçulina Firmino dos Santos[3]

## RESUMO

Este artigo tem como objetivo geral analisar os impactos éticos gerados pela tecnologia no contexto contábil empresarial, relacionados à privacidade e segurança de dados. Com o avanço tecnológico, as empresas têm adotado sistemas contábeis digitais e automatizados, o que, embora traga benefícios como a eficiência e a precisão, também levanta preocupações éticas significativas. Quanto aos procedimentos operacionais foram realizados uma pesquisa bibliográfica e um estudo de caso múltiplo, em que foram analisadas três empresas que sofreram violação de dados. Em relação a natureza, a pesquisa é qualitativa, e quanto aos objetivos é descritiva. O estudo aborda os principais desafios enfrentados pelos profissionais da contabilidade, como a proteção de informações sensíveis e o cumprimento das normas éticas em um ambiente digital cada vez mais vulnerável a ameaças cibernéticas. A pesquisa destaca a importância de implementar práticas robustas de segurança da informação e de promover uma cultura organizacional que valorize a ética no uso da tecnologia, visando garantir a integridade e a confiança nas práticas contábeis. A pesquisa revelou que os principais impactos enfrentados pelas empresas que tiveram os dados violadas foram a perda de confiança dos clientes, questionamentos sobre governança e segurança, risco reputacional, implicações legais e regulatórias, impacto na confiança dos colaborados e implicações para o setor de consultoria.

**Palavras-chave:** Tecnologia, impactos, ética contábil, privacidade de dados, segurança de dados.

## ABSTRACT

This article has the general objective of analyzing the ethical impacts generated by technology in the business accounting context, related to privacy and data security. With technological advancement, companies have digital and automated accounting systems, which, although it brings benefits such as efficiency and accuracy, also raises important ethical questions. Regarding operational procedures, a literature search and a multiple case study were carried out, in which three companies that suffered data breaches were highlighted. In terms of nature, the research is qualitative, and in terms of objectives, it is descriptive. The study addresses the main challenges faced by accounting professionals, such as protecting sensitive information and complying with ethical standards in a digital environment increasingly vulnerable to cyber threats. The research highlights the importance of implementing robust information security practices and promoting an organizational culture that values ethics in the use of technology, ensuring integrity and trust in accounting practices. A survey revealed that the main impacts faced by companies that had their data breached were the loss of customer trust, questions about governance and security, reputational risk, legal and regulatory implications, impact on employee trust and implications for the consulting sector.

**Keywords:** Technology, impacts, accounting ethics, data privacy, data security.

---

[1] Acadêmico do Curso de Ciências Contábeis da UFRR.
[2] Acadêmico do Curso de Ciências Contábeis da UFRR.
[3] Orientadora - Profa. do Curso de Ciências Contábeis da UFRR.

# 1 INTRODUCÃO

A revolução tecnológica que caracteriza o século XXI tem transformado profundamente diversas áreas do conhecimento e prática profissional, e a contabilidade não é exceção. A incorporação de tecnologias avançadas e processos automatizados no contexto contábil empresarial tem possibilitado um aumento significativo na eficiência, precisão e agilidade na execução de tarefas rotineiras, ao mesmo tempo em que cria novas oportunidades para a análise de dados e tomada de decisões estratégicas. No entanto, essa transformação digital também traz à tona um conjunto de desafios éticos que precisam ser cuidadosamente examinados e compreendidos.

Nesse sentido, Silva (2023) destaca que a prática contábil tem passado por transformações profundas nas últimas décadas, impulsionada pela crescente incorporação de tecnologias avançadas, em que essas inovações têm proporcionado ganhos significativos em termos de eficiência, precisão e acessibilidade das informações financeiras. E, Farias e Monteiro (2024) ressaltam que o uso dessas tecnologias também levanta questões sobre a confiabilidade dos dados, a transparência dos processos automatizados e a responsabilidade ética dos profissionais contábeis, isto é, trouxe à tona uma série de desafios éticos, especialmente no que diz respeito à privacidade e segurança dos dados.

A contabilidade lida com informações extremamente sensíveis, incluindo dados financeiros pessoais e corporativos, que, se expostos ou mal utilizados, podem causar danos significativos. Portanto, entender que a segurança desses dados é, uma prioridade, e garanti-los em um ambiente altamente automatizado e interconectado é uma tarefa complexa que requer uma abordagem multidisciplinar e a implementação de medidas de segurança robustas (Costa; Melo; Soares, 2015).

Diante deste cenário, este estudo busca responder à seguinte questão: quais os impactos éticos causados pela tecnologia no contexto contábil empresarial, relacionados à privacidade e a segurança de dados?

O objetivo geral deste estudo é analisar os impactos éticos gerados pela tecnologia no contexto contábil empresarial, relacionados à privacidade e segurança de dados. Para tanto, os objetivos específicos são: (1) identificar as principais tecnologias utilizadas no contexto contábil empresarial e como afetam privacidade e segurança dos dados; (2) investigar as principais teorias que fornecem uma base para a tomada de decisões morais na área de contabilidade; (3) verificar os principais desafios éticos enfrentados pelos profissionais contábeis devido à adoção de tecnologia, relacionados à privacidade e segurança de dado; (4)

analisar casos de violação de privacidade e segurança de dados no contexto contábil empresarial. Para alcançar esses objetivos adotou-se os procedimentos metodológicos a seguir descritos.

Em relação a natureza, a pesquisa é qualitativa, pois, esse tipo de abordagem permitirá uma análise detalhada dos impactos e dos desafios éticos da tecnologia no contexto contábil. Quanto aos níveis ou objetivos, a pesquisa é descritiva, utilizada para descrever características dos casos estudados e os impactos e desafios éticos.

Foi realizada revisão da literatura sobre as tecnologias utilizadas no contexto contábil, seus impactos na privacidade e segurança de dados, e os desafios éticos associados. A pesquisa bibliográfica foi feita por meio de fontes secundárias, que incluíram livros, artigos acadêmicos, publicações em revistas especializadas e material técnico sobre segurança de dados no setor contábil, cuja seleção foi feita com base na relevância e atualidade.

As unidades de análise foram compostas por três casos reais, cuja seleção se deu com base em relevância e impacto e por ser três das maiores empresas contábeis que enfrentaram incidentes significativos de violação de dados: Deloitte, DBO USA e Pricewaterhouse Coopers (PwC). Os dados sobre os incidentes foram acessados por meio de bases de dados acadêmicas, como *Google Scholar*, *Scopus* e *Web of Science*, e por meio de relatórios oficiais divulgados pelas empresas envolvidas e órgãos reguladores, publicações acadêmicas, notícias, análise de decisões judiciais e documentos legais.

Este estudo, ao analisar os impactos éticos gerados por essas inovações tecnológicas no contexto contábil, visa preencher uma lacuna significativa na literatura acadêmica, em que as implicações éticas da tecnologia ainda não foram plenamente exploradas.

Para a academia, a pesquisa oferece uma oportunidade de aprofundar o entendimento sobre as novas dinâmicas éticas que surgem com a digitalização das práticas contábeis. Além disso, contribui para a discussão sobre a necessidade de atualização e adaptação dos códigos de ética profissional para contemplar os desafios impostos pelas novas tecnologias.

Para os discentes, a investigação proporciona uma visão crítica sobre a responsabilidades ética associada ao uso de tecnologias emergentes no ambiente empresarial. Ao fomentar uma reflexão sobre a importância da privacidade e da segurança de dados, o estudo também prepara os futuros profissionais para lidar com os desafios éticos que provavelmente encontrarão em suas carreiras.

Por fim, para a sociedade, a pesquisa é relevante na medida em que a proteção da privacidade e a segurança de dados são questões de interesse público. À medida que as empresas coletam e processam volumes cada vez maiores de informações sensíveis, é fundamental que

esses dados sejam geridos de forma ética e responsável. Este estudo, ao abordar os impactos éticos da tecnologia no campo contábil, contribui para a construção de práticas empresariais mais seguras e alinhadas com os valores éticos fundamentais, promovendo assim a confiança e a transparência nas relações entre empresas, profissionais e a sociedade.

A estrutura do trabalho está organizada em 5 capítulos: o primeiro traz a introdução que apresenta o contexto geral, o problema, o objetivo geral e os objetivos específicos, os procedimentos metodológicos, a justificativa e a estrutura do trabalho. O segundo aborda sobre as tecnologias utilizadas no contexto contábil empresarial e como afetam a privacidade e segurança dos dados contábeis. O terceiro trata sobre os fundamentos da ética na prática contábil, enfatizando as teorias éticas aplicadas à contabilidade, os desafios éticos relacionados a privacidade e a segurança de dados. O quarto apresenta os casos de violação de dados e analisa os resultados, destacando os impactos e desafios éticos enfrentados pelas empresas objetos de estudo. O quinto e último, apresenta as considerações finais com as inferências dos autores.

## 2 TECNOLOGIAS UTILIZADAS NO CONTEXTO CONTÁBIL EMPRESARIAL

A crescente complexidade das operações empresariais, aliada à demanda por maior precisão e eficiência, tem impulsionado a adoção de diversas tecnologias na contabilidade. Essas inovações não apenas otimizam processos, mas também transformam a maneira como os profissionais contábeis desempenham suas funções, ampliando o escopo de suas atividades e introduzindo novas responsabilidades, especialmente em relação à gestão ética de dados e à segurança da informação (Ferreira, 2021).

Nessa direção, Farias e Monteiro (2024) destacam que a importância da tecnologia na prática contábil não pode ser subestimada, uma vez que ela tem revolucionado a forma como os profissionais contábeis executam suas funções. A introdução de sistemas automatizados e ferramentas avançadas trouxe uma nova dimensão à contabilidade, permitindo maior precisão, eficiência e capacidade de análise de dados em tempo real, além de permitirem aos contadores a concentração nas tarefas mais estratégicas, analíticas e nas operações rotineiras que são executadas por meio das maquinas de software.

Observa-se que a automação engloba diversas tecnologias, que vão desde os sistemas de gerenciamento financeiro integrados até ferramentas de auditoria automatizadas, permitindo que ocorra a redução dos erros humanos, associada a aceleração dos processos contábeis e a melhoria na conformidade com as regulamentações financeiras. Segundo Almeida e Saraiva (2024), isso tem sido um passo importante para a modernização do setor, proporcionando aos

profissionais contábeis os recursos necessários para lidar com a crescente complexidade dos negócios contemporâneos. Contudo, essas tecnologias, por mais sofisticadas que seja, ainda precisam de melhorias, pois, afetam a segurança dos dados contábeis de tal forma, que expõe informações consideradas sensíveis pelas empresas, por exemplo.

A seguir, são destacadas algumas das principais tecnologias que, atualmente, podem ser utilizadas no contexto contábil empresarial e como afetam a privacidade e a segurança dos dados contábeis.

Ferramentas como QuickBooks, Xero e SAP Concur oferecem soluções baseadas em nuvem que permitem o gerenciamento contábil remoto e em tempo real. Esses softwares automatizam tarefas como conciliação bancária, emissão de faturas e controle de despesas, além de proporcionar acessibilidade e colaboração entre diferentes usuários e nessa seara, Bomfim (2020), ressalta que a computação em nuvem é uma tecnologia que permite o armazenamento e acesso remoto a grandes volumes de dados, facilitando a colaboração e o compartilhamento de informações.

Todavia, para Reis et al. (2023), a acessibilidade aumentada também significa que os dados estão mais vulneráveis a ataques cibernéticos, e, diante disso, as empresas precisam implementar medidas de segurança robustas, como criptografia de dados e autenticação multifatorial, para proteger as informações contábeis armazenadas na nuvem.

Outro aspecto crítico, é ressaltado por Tadeu, Almeida e Gonçalves (2021) que aduzem que a conformidade regulatória é um aspecto crítico na utilização da computação em nuvem, pois diferentes jurisdições têm regulamentações específicas sobre a proteção de dados, a exemplo do General Data Protection Regulation – GDPR (Regulamento Geral de Proteção de Dados), na Europa, e da Lei Geral de Proteção de Dados – LGPD, no Brasil. Dessa forma, as empresas devem garantir que seus provedores de serviços em nuvem estejam em conformidade com essas regulamentações para evitar penalidades legais e proteger a privacidade dos dados de seus clientes e *stakeholders*.

A tecnologia *blockchain*, embora mais conhecida no contexto das criptomoedas, está ganhando espaço na contabilidade devido à sua capacidade de fornecer registros imutáveis e transparentes de transações financeiras. Essa tecnologia pode reduzir o risco de fraude, melhorar a rastreabilidade e simplificar auditorias. Tadeu, Almeida e Gonçalves (2021), destacam que, o *blockchain* é uma tecnologia emergente que tem um impacto significativo na privacidade e segurança dos dados contábeis e oferece um registro imutável e transparente de transações, o que pode aumentar a confiança e reduzir o risco de fraudes. Explicam que a contabilidade é transformada em algo mecanizado a partir da automação das tarefas complexas,

junto ao fornecimento de análises preditivas as quais identificam padrões e anomalias em grandes conjuntos de dados, auxiliando os contadores a detectar fraudes e tomar decisões informadas.

A privacidade dos dados, é considerada importante no uso do *blockchain*, pois, as identidades dos participantes são protegidas por meio de técnicas de anonimização. Mas, neste caso, é essencial equilibrar a transparência com a necessidade de proteger informações sensíveis, especialmente em contextos contábeis em que a confidencialidade é essencial. Assim, segundo Ferreira (2021), se juntados o *blockchain* e a Inteligência Artificial - IA pode-se automatizar a contabilidade e promover a identificação dos padrões e anomalias nos dados contábeis, ajudando a detectar fraudes e erros em tempo real. Porém, segundo Costa e Melo (2015), essas tecnologias levantam questões importantes sobre a privacidade dos dados, pois esses sistemas frequentemente dependem de grandes volumes de dados para treinar seus algoritmos.

Outro tipo de tecnologia utilizada no contexto contábil empresarial é a *Robotic Process Automation* – RPA (automação de processos robóticos). A RPA envolve o uso de *bots* para automatizar tarefas recorrentes e baseadas em regras, como o processamento de pagamentos. Isso libera tempo dos contadores para se concentrar em atividades mais estratégicas e analíticas.

Nessa direção, Silva (2023) ensina que a RPA envolve o uso de software para automatizar tarefas repetitivas e baseadas em regras, o que dentro do cenário contábil pode ser utilizada na automação dos processos como a entrada de dados, a conciliação bancária e a geração de relatórios financeiros, o que aumenta a eficiência e reduz os custos operacionais. Todavia, segundo Duarte (2022), em contrapartida, oferece desafios de segurança, o que torna essencial melhores configurações quanto aos *Bots* de RPA, que protegerão as empresas e os seus dados contra os dados não autorizados e manipulações indevidas, isto é, requer a adoção de medidas de segurança rigorosas, a fim de proteger os dados manipulados pelos robôs.

Outra tecnologia utilizada é a *big data*, conhecida como uma poderosa e atual ferramenta contábil, que segundo Silva (2023), permite a análise de grandes volumes de dados para identificar tendências e *insights*, e quanto a confiabilidade pode ser utilizada para realizar análises financeiras avançadas, detectar fraudes e prever tendências de mercado.

Mas, o processamento de grandes volumes de dados, conforme Heberle e Kônig (2023), também levanta preocupações éticas sobre a privacidade, a segurança e o consentimento dos dados, já que a coleta e análise de dados em larga escala podem infringir a privacidade dos indivíduos. Assim, quanto a essa e as demais tecnologias é necessário que ocorra a interação entre todas elas a fim de compreender a sua aplicação na prática contábil, junto a uma

abordagem equilibrada entre os usuários em questão. Nesse sentido, Lannes (2020) ressalta que se faz necessário à implementação de políticas de proteção de dados e conformidade com as regulamentações de privacidade, que são essenciais para garantir que os dados contábeis sejam processados de forma segura e ética.

Os sistemas Planejamento de Recursos Empresariais (ERP), é uma tecnologia que integram diversas funções empresariais, incluindo contabilidade, finanças, compras, e recursos humanos, em uma única plataforma. Eles permitem o processamento automatizado de transações financeiras, a geração de relatórios em tempo real e o monitoramento contínuo das atividades empresariais, facilitando a tomada de decisões informadas. Corroborando com tal assertiva, O'Leary (2000) ressalta que esses sistemas oferecem uma integração abrangente de processos empresariais, que facilita a eficiência organizacional ao reunir diversas funções em uma única plataforma, permitindo o monitoramento e controle contínuo das atividades empresariais.

O contexto contábil empresarial, também, pode contar com a automação de processos financeiros, as soluções de automação *Purchase to Pay* - P2P ( ) e *Order to Cash* - O2C ( ) ajudam a otimizar os ciclos de compras e recebíveis, respectivamente. Elas integram processos desde a emissão de ordens de compra até o pagamento de fornecedores, e desde a geração de pedidos até o recebimento de pagamentos, garantindo maior controle e eficiência nas operações financeiras. Assim, Monk e Wagner (2009) ao falar sobre essas soluções de automação, ressaltam a essencialidade dessas tecnologias quanto a otimização da gestão financeira, integrando processos para reduzir ineficiências e aumentar a visibilidade nos ciclos de compras e recebíveis.

Ferramentas como *Analytics* e *AuditBoard* - ACL permitem a automação de processos de auditoria e conformidade, garantindo que as empresas estejam em conformidade com as normas contábeis e regulatórias. Esses sistemas realizam análises contínuas dos dados financeiros para identificar possíveis desvios e irregularidades. À vista disso, Codesso et al. (2018), ressaltam que as ferramentas de auditoria como *Analytics* e *AuditBoard* (ACL) são fundamentais para a automação dos processos de conformidade e auditoria, permitindo que as empresas identifiquem desvios e garantam a conformidade regulatória por meio da análise contínua de dados.

Ferramentas de *Business Intelligence* - BI, como *Tableau* e *Power* BI, permitem que os contadores transformem dados financeiros brutos em *insights* acionáveis. A análise de dados automatizada facilita a visualização de tendências, a análise de desempenho financeiro e a criação de relatórios detalhados para a gestão. Dessa maneira, Wixom e Watson (2010)

explicam que as ferramentas de BI, como *Tableau* e *Power* BI, permitem aos contadores transformarem dados brutos em *insights* acionáveis, além de oferecerem suporte à tomada de decisão estratégica por meio da análise de grandes volumes de dados financeiros.

E, ainda, a Inteligência Artificial (IA) e o Aprendizado de Máquina (ML) são tecnologias utilizadas para analisar grandes volumes de dados financeiros, detectar padrões e anomalias, prever tendências e fornecer *insights* valiosos. Ferramentas como *chatbots* alimentados por IA também podem auxiliar na interação com clientes, automatizando respostas a consultas comuns e agilizando processos de atendimento, que de acordo com Davenport e Ronanki (2018) podem ser considerados como agentes transformadores da contabilidade, pois, permitem a análise avançada de grandes volumes de dados financeiros, automatizando a detecção de padrões e previsões, além de aprimorar a interação com clientes por meio de *chatbots* inteligentes.

Ante o exposto deduz-se, que essas tecnologias não apenas melhoram a eficiência e precisão das operações no contexto contábil empresarial, mas também levantam questões éticas significativas, especialmente em relação à privacidade e segurança dos dados financeiros sensíveis. O avanço dessas ferramentas exige dos profissionais contábeis uma atualização constante de seus conhecimentos técnicos e uma atenção redobrada às implicações éticas de sua utilização, garantindo que a inovação tecnológica seja aplicada de forma responsável e alinhada com os princípios éticos da profissão

## 3 FUNDAMENTOS DA ÉTICA NO CONTEXTO CONTÁBIL

A ética desempenha um papel fundamental em todas as profissões, sendo particularmente relevante no campo da contabilidade, em que a confiança e a integridade são fundamentais para a credibilidade das informações financeiras. Os fundamentos éticos na contabilidade não apenas guiam o comportamento dos profissionais, mas também asseguram que as práticas contábeis sejam conduzidas de forma justa, transparente e responsável, em benefício tanto das organizações quanto da sociedade (Sá, 2010).

No entanto, segundo Lima et al., (2015) o avanço tecnológico e a crescente complexidade dos ambientes de negócios trazem novos desafios éticos que requerem uma atenção especial, principalmente nas áreas de privacidade e segurança de dados. Para enfrentar esses desafios, é essencial que os contadores compreendam as teorias éticas que fundamentam a tomada de decisões em situações delicadas e complexas

As teorias éticas aplicadas à contabilidade, como a deontologia, o utilitarismo, da equidade moral ou da justiça e a ética da virtude, segundo Aranha; Martins (2005) oferecem diferentes perspectivas sobre como os profissionais devem se comportar diante de dilemas éticos.

No cenário atual, os desafios éticos na privacidade e segurança de dados são particularmente críticos. A manipulação de informações contábeis e a proteção de dados sensíveis exigem uma abordagem ética rigorosa para evitar práticas que possam comprometer a confiança e a segurança das partes envolvidas. A proteção contra a manipulação indevida de informações contábeis é essencial para manter a integridade das demonstrações financeiras e a confiança dos investidores e *stakeholders* (Seiblitz, 2021).

Neste contexto, esta seção explorará as teorias éticas aplicadas ao contexto contábil, os desafios específicos relacionados à privacidade e segurança de dados.

## 3.1 Teorias Éticas aplicadas à Contabilidade

As teorias éticas fornecem uma base para a tomada de decisões morais, especialmente em áreas que demandam alto grau de responsabilidade e confiança, como a contabilidade. Na prática contábil, essas teorias orientam os profissionais a manterem a integridade, transparência e a equidade em suas práticas, garantindo que as informações financeiras sejam apresentadas de maneira justa e verdadeira. Fornecem a base para decisões morais e profissionais, orientando na prática de suas responsabilidades (Sá, 2010).

Dentro desse contexto, é essencial compreender as principais teorias éticas que orientam a conduta dos contadores. A comprensão dessas bases teóricas é fundamental para uma análise crítica do Código de Ética Profissional do Contador e para a promoção de uma prática contábil que esteja alinhada com os mais altos padrões éticos. Portanto, a seguir são apresentadas as principais teorias éticas aplicadas ao contexto contábil.

Segundo Vázquez (2005), a teoria ética deontológica ou contratualista se baseia na ideia de que as ações morais devem ser avaliadas não apenas por suas consequências, mas também pelo cumprimento de deveres ou regras estabelecidas. A ética deontológica, fundamentada principalmente nas ideias de Immanuel Kant, foca no respeito a princípios morais universais, nos quais o valor de uma ação é determinado pela sua conformidade a um dever, independentemente dos resultados que ela possa gerar.

O aludido autor, destaca que, no contexto da abordagem deontológica ou contratualista, a moralidade é regida por normas preestabelecidas que guiam o comportamento dos indivíduos,

sendo menos flexível e focada em princípios absolutos ou em acordos sociais, ao contrário de teorias consequencialistas, como o utilitarismo, que focam nos resultados das ações.

A vertente deontológica contratualismo, sugere que as normas morais surgem de um acordo racional entre indivíduos que vivem em uma sociedade. Dessa forma, os princípios éticos são entendidos como compromissos que os membros de uma comunidade aceitam mutuamente para promover o bem-estar coletivo e garantir a justiça social. Nesse sentido, Lima et al., (2015), ressalta que no campo contábil, isso pode ser interpretado como o compromisso dos contadores em seguir as normas e códigos de ética estabelecidos pela profissão, que são aceitos coletivamente como guias para o comportamento adequado. A honestidade e a lealdade para com as normas profissionais e legais são fundamentais, e os contadores devem evitar qualquer comportamento que possa comprometer a integridade dos relatórios financeiros.

Nessa direção, Sá (2010) defende que o Código de Ética deve existir para assegurar que os profissionais atuem de maneira responsável, transparente e com integridade, protegendo o interesse público e garantindo a qualidade dos serviços prestados. O Código tem a função de orientar o comportamento dos profissionais, promovendo a ética nas relações interpessoais e no exercício da profissão. Ele também existe para reforçar a confiança do público nos profissionais, prevenindo condutas inadequadas ou antiéticas, e para promover a justiça e a equidade no ambiente de trabalho.

A ética utilitarista é uma teoria moral que orienta as ações com base no princípio de maximização da felicidade ou do bem-estar coletivo. De acordo com essa abordagem, uma ação é considerada moralmente correta se ela produzir o maior bem para o maior número de pessoas. O foco principal do utilitarismo está nos resultados ou nas consequências das ações, em vez de na intenção ou no cumprimento de deveres, como nas teorias deontológicas (Lima et al., 2015).

O utilitarismo é amplamente associado a filósofos como Jeremy Bentham e John Stuart Mill, que defendem que as ações devem ser avaliadas pela sua capacidade de promover o prazer e minimizar a dor. Portanto, o critério de julgamento ético no utilitarismo é baseado no cálculo das consequências, buscando sempre a maximização da utilidade, que se refere à promoção do bem-estar. Embora o utilitarismo ofereça uma maneira pragmática de tomar decisões, ele enfrenta críticas, especialmente em relação à dificuldade de prever todas as consequências de uma ação e à possibilidade de que, em alguns casos, possa justificar ações que violam direitos individuais em prol de um benefício coletivo maior. O utilitarismo, apesar de focar nos benefícios gerais, pode acabar justificando sacrifícios individuais em prol do bem coletivo, o que gera críticas e debates sobre suas implicações práticas e éticas (Lima et al., 2015).

Nessa direção, Aranha e Martins (2005) abordam a teoria utilitarista como uma corrente da ética que se preocupa com as consequências das ações. De acordo com essa visão, a moralidade de uma ação é julgada pelo seu resultado, sendo boa se produzir o maior bem para o maior número de pessoas. Os aludidos autores explicam que o utilitarismo é uma ética consequencialista, na qual o princípio básico é a maximização da felicidade ou bem-estar coletivo. Portanto, uma ação será considerada correta se seus efeitos levarem a um aumento do prazer ou a uma diminuição do sofrimento no maior número de indivíduos possível.

Lima et al., (2015), ressaltam que aplicada à contabilidade, essa teoria sugere que as decisões devem ser orientadas para gerar o maior benefício para o maior número de pessoas. Por exemplo, ao fornecer informações financeiras, o contador deve considerar os impactos de suas ações não apenas para os investidores ou clientes, mas também para a sociedade em geral, buscando minimizar os danos e maximizar os benefícios sociais.

A teoria da equidade moral, também, frequentemente chamada de teoria da justiça, especialmente quando se refere aos princípios formulados por filósofos como John Rawls. Rawls (1971), em sua obra "Uma Teoria da Justiça", descreve a equidade moral como uma forma de justiça distributiva, em que o objetivo é garantir que as instituições sociais e econômicas proporcionem uma distribuição justa de bens e oportunidades, considerando as desigualdades naturais e sociais.

Além disso, essa teoria pode ser referida como justiça equitativa ou justiça distributiva, focando na distribuição justa de recursos e benefícios dentro de uma sociedade, garantindo que as diferenças sejam tratadas de forma justa, levando em conta as necessidades e circunstâncias individuais. Nesse sentido, a teoria da justiça, busca a distribuição justa e equitativa dos benefícios e encargos e é outra abordagem ética relevante para a contabilidade, pois, segundo Moreira (2021), os contadores devem garantir que suas práticas promovam a justiça e a equidade, evitando discriminação e favorecimento.

De acordo com Marques (2017), a teoria ética da equidade moral está centrada na ideia de justiça e imparcialidade nas relações sociais e econômicas. Marques argumenta que essa teoria propõe que as ações devem ser julgadas com base na equidade, ou seja, no tratamento justo e igualitário para todas as partes envolvidas, levando em consideração as circunstâncias e necessidades individuais. A equidade moral busca equilibrar as condições de justiça em situações em que há desigualdade, visando garantir que os indivíduos tenham acesso a oportunidades justas e a um tratamento imparcial. Isso significa que, em vez de aplicar regras universais de forma rígida, a equidade moral requer uma análise contextual, em que as

condições e necessidades específicas de cada indivíduo ou grupo são consideradas para garantir um resultado justo.

Em suma, a teoria ética da equidade moral ou da justiça defende que, para uma ação ser considerada eticamente correta, deve levar em conta não apenas a igualdade formal, mas também as condições que garantam um tratamento justo e equitativo para todos.

A teoria ética da virtude, de acordo com Oliveira e Malinowski (2016), se destaca por seu foco no desenvolvimento do caráter moral e das virtudes individuais, em vez de apenas analisar as ações corretas ou suas consequências. Para os aludidos autores, essa abordagem ética enfatiza a importância de cultivar hábitos e disposições virtuosas que permitam ao indivíduo agir moralmente de maneira natural e constante, conduzindo a uma vida moralmente satisfatória. Ressaltam que, na ética da virtude, a moralidade não é apenas uma questão de seguir regras ou maximizar o bem-estar, como nas abordagens deontológica e utilitarista, respectivamente.

A ética da virtude também é conhecida como ética eudaimonista. Oliveira e Malinowski (2016) discutem que a ética da virtude, influenciada por pensadores como Aristóteles, está profundamente conectada à noção de eudaimonia, ou felicidade plena, que é atingida quando o indivíduo vive uma vida de virtude e realiza seu potencial humano. Os referidos autores apontam que essa abordagem valoriza a educação moral e o desenvolvimento contínuo das virtudes ao longo da vida como um caminho para a excelência ética. Isto é, na ética da virtude, o foco está no desenvolvimento do caráter moral e das virtudes, em vez de regras ou consequências das ações. Trata-se de cultivar qualidades como coragem, justiça, temperança e sabedoria, para que o indivíduo possa viver uma vida moralmente boa e atingir a eudaimonia.

No contexto contábil, essa teoria enfatiza a importância de desenvolver virtudes como honestidade, justiça, prudência e coragem. Um contador virtuoso é aquele que, além de seguir as regras, age com integridade e busca sempre o melhor interesse de todas as partes envolvidas, cultivando uma reputação de confiabilidade e ética ao longo de sua carreira.

Oliveira e Malinowski (2016), corrobora com tal assertiva quando ensinam que a ética das virtudes, que se concentra no desenvolvimento de qualidades morais como honestidade, integridade e justiça, é relevante para a contabilidade, pois, incentiva os profissionais contábeis a cultivar essas virtudes em suas práticas diárias, garantindo que suas ações estejam alinhadas com os mais altos padrões éticos.

Assim, conforme Seiblitz (2021), cada uma dessas teorias oferece uma perspectiva individual sobre a ética na contabilidade e os profissionais poderão usá-las em conjunto para guiar suas ações. Elas contribuem para promoverem a conformidade com os demais

regulamentos, e fortalecerem a confiança dos *stakeholders* quanto a integridade das informações financeiras, o que é particularmente importante em um ambiente de negócios no qual a transparência e a responsabilidade são essenciais para a construção de relações de confiança. Essas teorias, juntamente com a educação ética disseminadas nos locais de trabalho, por meio de cursos, treinamentos e *workshops*, farão com que os profissionais da área contábil tenham mais desenvoltura e aumentem a sua compreensão sobre a aplicação dos códigos de conduta nas suas práticas diárias.

Segundo Iguma (2020), a ética na contabilidade está intimamente ligada à responsabilidade social corporativa (RSC), pois, as empresas são incentivadas a adotar práticas contábeis que não só atendam às exigências legais, mas que também promovam o bem-estar social e ambiental. Isso inclui a transparência na divulgação de informações financeiras, a responsabilidade na gestão dos recursos e o compromisso com a sustentabilidade, que, em conjunto com a educação ética fará com que ocorra a adesão à códigos de conduta e a compreensão da sua essencialidade no contexto contábil atual.

Diante do exposto, infere-se que essas teorias éticas não são mutuamente exclusivas e muitas vezes se complementam na prática contábil. Um contador ético deve ser capaz de avaliar cada situação de maneira crítica, utilizando essas teorias como guias para tomar decisões que não apenas cumpram as normas legais, mas que também promovam o bem-estar social, a justiça e a confiança pública no sistema financeiro.

## 3.2 Desafios Éticos Relacionados a Privacidade e a Segurança de Dados

Na era digital, a contabilidade enfrenta desafios éticos cada vez mais complexos, especialmente no que diz respeito à privacidade e à segurança de dados. Com a crescente dependência de tecnologias da informação e a digitalização de processos contábeis, os profissionais da área são frequentemente confrontados com dilemas relacionados à proteção de informações sensíveis. A privacidade e a segurança de dados se tornam aspectos determinantes, pois os contadores lidam com informações financeiras confidenciais, que podem incluir desde detalhes pessoais de clientes até transações corporativas sigilosas (Duarte, 2022).

Nesse sentido, esta seção discute os principais desafios éticos enfrentados pelos profissionais contábeis na era digital, com foco na privacidade e segurança de dados, destacando a importância de práticas responsáveis e seguras para mitigar riscos e preservar a ética profissional.

Um dos principais desafios é garantir que essas informações sejam tratadas com a máxima confidencialidade, respeitando as normas e regulamentos, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na Europa, que impõem rígidas diretrizes sobre o tratamento de dados pessoais. Essas leis estabelecem requisitos rigorosos para a coleta, armazenamento e uso de dados pessoais, e as empresas contábeis devem garantir que suas práticas estejam em conformidade. A não conformidade pode resultar em penalidades severas e danos à reputação, sendo essencial que os profissionais contábeis estejam bem informados sobre as exigências legais e implementem políticas de conformidade eficazes para evitar tais consequências (Ferreira et al., 2017; Moreira, 2021).

O uso de tecnologias emergentes, como a inteligência artificial e a *big data* apresentam desafios éticos relacionados a privacidade de dados, tendo-se em vista que essas tecnologias frequentemente requerem acesso a grandes volumes de dados para funcionar de maneira eficaz. Nessa direção, Rosa et al. (2020) alertam que o uso inadequado ou excessivo de dados pode levar a preocupações com a privacidade, e os profissionais contábeis devem garantir que o uso dessas tecnologias seja feito de maneira ética, com o devido respeito à privacidade dos indivíduos e à integridade dos dados.

Além disso, a segurança cibernética é um componente crítico na proteção da privacidade de dados. Os profissionais de contabilidade devem estar vigilantes contra ameaças como *hackers* e vazamentos de dados, que podem comprometer a integridade das informações. Isso requer uma constante atualização em termos de conhecimento técnico e de práticas de segurança, e o desenvolvimento de uma cultura organizacional que priorize a proteção de dados. Portanto, os desafios éticos na privacidade e segurança de dados na contabilidade exigem que os profissionais da área mantenham um compromisso contínuo com a ética, a conformidade legal e a segurança, garantindo que as informações sob sua responsabilidade sejam tratadas de maneira íntegra e responsável.

Nessa lógica, segundo Ceolato (2019), a privacidade de dados é um dos principais desafios éticos enfrentados pelos profissionais de contabilidade na era digital, provocado pelo aumento da digitalização e da automação de grandes volumes de dados financeiros e pessoais, coletados, além da sua armazenagem, o que elevou o risco de violações de privacidade. Isso ocorreu devido à uma interconexão global que facilita tanto o compartilhamento quanto a sua vulnerabilidade, ressaltando a responsabilidade ética dos profissionais contábeis em proteger essas informações contra acessos não autorizados e uso indevido, garantindo a confidencialidade e a integridade das informações.

Um dos principais riscos de privacidade no contexto contábil empresarial é a violação de dados, em que informações sensíveis podem ser expostas devido a ataques cibernéticos ou falhas de segurança. E, consoante Whitman e Mattord (2018), a proteção contra essas ameaças, exige a implementação de medidas robustas de segurança, como criptografia de dados, *firewalls* e autenticação multifatorial e além disso, a formação contínua dos profissionais em práticas de segurança cibernética é essencial para manter a proteção dos dados, uma vez que as ameaças estão em constante evolução.

Jesus, Sarmento e Duarte (2018) ressaltam que a transparência é um princípio ético fundamental na proteção da privacidade de dados, e, também, argumentam que as empresas contábeis devem ser transparentes sobre as práticas de coleta e uso de dados, informando claramente aos clientes como seus dados serão utilizados e protegidos. Pois, a falta de transparência pode minar a confiança dos clientes e levar a percepções negativas sobre a empresa, o que torna a comunicação clara e aberta sobre a privacidade de dados essencial para manter a confiança e a reputação empresarial.

Conforme Seiblitz (2021), os sistemas automatizados contábeis oferecem benefícios como eficiência operacional e redução de erros humanos, mas, apresentam vulnerabilidades de segurança significativas. Desse modo, a possibilidade de ataques cibernéticos é uma das principais preocupações, pois *hackers* podem explorar falhas nos sistemas para acessar dados sensíveis, resultando em perdas financeiras e danos à reputação das empresas. Contudo, tal problema pode ser mitigado por meio das atualizações de *software* que são primordiais para que falhas sejam corrigidas e diferentes sistemas sejam repensados a fim de não criarem vulnerabilidades na transferência de dados, especialmente se medidas de segurança como criptografia não forem implementadas corretamente.

Matias (2021), alude que a configuração inadequada dos sistemas automatizados também pode expor dados a riscos, pois tais configurações permitem que atacantes explorem facilmente os sistemas. Torna-se essencial, portanto, que os administradores de Tecnologia da Informação - TI configurem corretamente os sistemas, seguindo as melhores práticas de segurança e garantindo que apenas usuários autorizados tenham acesso aos dados sensíveis. Nessa questão, o fator humano continua sendo uma das maiores vulnerabilidades nos sistemas automatizados, pois os erros humanos, como a criação de senhas fracas ou o descuido ao compartilhar informações confidenciais, podem comprometer a segurança dos sistemas. No entanto, se a empresa adotar práticas relacionas a formação contínua dos colaboradores, quanto a segurança cibernética e a criação de uma cultura de segurança, esses problemas serão mitigados.

Os desafios éticos na privacidade e na segurança de dados também podem surgir em situações de conflito de interesse. Conforme exemplifica Duarte (2022), um contador poder enfrentar pressões para compartilhar informações confidenciais com terceiros, como autoridades fiscais ou parceiros de negócios. Logo, deve-se avaliar cuidadosamente os requisitos legais e éticos, buscando um equilíbrio entre a transparência e a proteção da privacidade dos clientes, o que pode ser auxiliado pela tomada de decisões informada e pelo aconselhamento jurídico.

Nesse sentido, a ética na privacidade de dados envolve a minimização de dados, ou seja, a coleta e retenção apenas das informações necessárias para fins específicos. Mancebo (2022) explica que a retenção excessiva de dados pode aumentar o risco de violações de privacidade e complicar a conformidade com regulamentações de proteção de dados, devendo os profissionais contábeis adotarem tais práticas a fim de garantir que apenas as informações essenciais sejam coletadas e armazenadas para reduzir esses riscos.

A formação e a sensibilização sobre a privacidade e a segurança de dados são fundamentais para promover uma cultura ética nas empresas contábeis. Para tanto, Iguma (2020) sugere que programas de treinamento contínuo podem ajudar os profissionais a se manterem atualizados sobre as melhores práticas e as mudanças nas regulamentações. Também, podem contribuir para a criação de uma cultura organizacional, a qual valorize a privacidade e a ética e incentive comportamentos responsáveis e proporcione a redução de risco de violações, promovendo um ambiente de trabalho mais seguro e consciente.

Outra alternativa relevante para a redução de risco de violação de dados é a auditoria regular das práticas de privacidade de dados. Pois, de acordo com Heberle e König (2023), é uma das práticas que identifica as vulnerabilidades e que ajudam a identificar áreas de melhoria, além de implementar medidas corretivas para fortalecer a proteção de dados. Também, fornece uma avaliação independente da conformidade e das práticas de segurança, aumentando a confiança dos clientes e partes interessadas na empresa e nos seus processos de proteção de dados.

Os desafios éticos na privacidade e na segurança de dados também incluem a gestão adequada dos sistemas automatizados utilizados na contabilidade, pois, considera-se que os sistemas automatizados aumentam a eficiência e reduzem erros humanos, mas trazem riscos significativos de violação de privacidade. Tal assertiva, é corroborada pelos ensinamentos de Matias (2021), que aduz que a vulnerabilidade a ataques cibernéticos e a gestão inadequada de permissões de acesso são riscos críticos que devem ser gerenciados com políticas e procedimentos rigorosos para garantir a segurança dos dados coletados e armazenados. A

violação de privacidade pode ocorrer, por exemplo, por meio de vazamentos de dados para empresas desconhecidas ou bases como a *dark web*.

Ainda, a integração de diferentes sistemas automatizados pode criar pontos fracos na segurança, especialmente durante a transferência de dados entre sistemas. Em relação a isso, Whitman e Mattord (2018) destacam que a criptografia de dados durante a transmissão é essencial para proteger as informações contra interceptações e usos maliciosos. Também, um dos pilares, para que isso não ocorra, é a utilização de técnicas relacionadas à atualização regular dos *softwares*, que protege os sistemas contra novas ameaças e garante que as medidas de segurança estejam sempre atualizadas.

Além disso, as regulamentações de proteção de dados, como o GDPR e a LGPD, impõem obrigações de notificação em caso de violação de dados. A esse respeito, Ferreira (2017) e Moreira (2021) enfatizam que, em caso de violação que comprometa a privacidade dos dados, as empresas devem informar rapidamente as autoridades competentes e aos indivíduos afetados. Também, devem adotar a implementação de procedimentos de resposta a incidentes e a realização de treinamentos regulares para os funcionários, pois são medidas essenciais para cumprir essas exigências e proteger a reputação da empresa. Assim, a implementação de medidas de segurança robustas, a conformidade com regulamentações, a transparência nas práticas de dados e a formação contínua são essenciais para proteger a privacidade dos dados, o que garante o enfrentamento dos desafios, junto a garantia de confiança e integridade da profissão.

Ao longo desta seção, foi possível identificar que os desafios éticos relacionados à privacidade e à segurança de dados na contabilidade são complexos e multifacetados, exigindo dos profissionais contábeis uma atenção redobrada e um comprometimento rigoroso com os princípios éticos. A proteção de dados pessoais, conforme estabelecido pelas legislações vigentes, não é apenas uma questão de conformidade legal, mas também uma responsabilidade ética fundamental que envolve a confiança depositada pelos clientes e a integridade da profissão. Além disso, a crescente digitalização dos processos contábeis intensifica a necessidade de uma gestão cuidadosa e segura dos dados, impondo novos desafios que demandam atualização contínua dos profissionais e a adoção de práticas tecnológicas seguras. Portanto, a ética na privacidade e na segurança de dados não deve ser vista como um obstáculo, mas como um imperativo que fortalece a credibilidade e a reputação do contador em um ambiente cada vez mais pautado pela transparência e pela segurança da informação.

# 4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Nesta seção, são analisados casos notórios de violação de dados que ocorreram no contexto contábil empresarial, com foco nos impactos e desafios éticos que esses incidentes suscitaram. São examinados três casos de grande repercussão: a invasão dos sistemas da Deloitte; o vazamento de dados na BDO USA; e, o vazamento de dados na PricewaterhouseCoopers (PwC).

Esses casos não apenas evidenciam falhas significativas na proteção de informações sensíveis, mas também levantam questões profundas sobre a responsabilidade ética das organizações na gestão e proteção de dados. A análise busca revelar como a negligência ou inadequação das práticas de privacidade e de segurança de dados pode comprometer a confiança pública, resultar em graves consequências financeiras, legais e na reputação e colocar em xeque a integridade ética das empresas. São examinados aspectos como as consequências e as medidas adotadas pelas empresas, comparando os resultados com a literatura existente para verificar a consistência das descobertas e identificar possíveis lacunas ou novas perspectivas.

## 4.1 Caracterização da Empresa Deloitte

A Deloitte é uma das maiores e mais renomadas empresas de serviços profissionais do mundo, oferecendo uma ampla gama de serviços, incluindo auditoria, consultoria, assessoria financeira, gestão de riscos e serviços fiscais. Ela faz parte das chamadas *Big Four*, um grupo das quatro maiores empresas de auditoria e consultoria globais, ao lado da PwC, EY e KPMG (Carvalho, 2022).

A história da Deloitte remonta ao século XIX. A empresa foi fundada em 1845 por William Welch Deloitte, em Londres, Reino Unido. William Deloitte foi o primeiro a ser nomeado auditor independente de uma empresa pública, o Great Western Railway, o que estabeleceu uma base sólida para a reputação da empresa em auditoria e contabilidade (Lima, 2022).

Inicialmente focada em serviços de auditoria, a Deloitte expandiu suas operações ao longo dos anos, incorporando serviços de consultoria, assessoria financeira e tributária. A empresa cresceu substancialmente, tanto organicamente quanto por meio de fusões e aquisições. Uma das mais notáveis foi a fusão em 1989 com a firma Touche Ross, resultando na criação da Deloitte & Touche, um marco importante que fortaleceu ainda mais sua presença global (Carvalho, 2022; Lima, 2022).

Com o tempo, a Deloitte continuou a expandir sua presença em diferentes mercados ao redor do mundo, adotando uma abordagem inovadora e adaptando-se às mudanças nas

demandas do mercado. A empresa foi pioneira em muitas práticas de auditoria e consultoria e começou a integrar novas tecnologias em seus serviços, o que lhe permitiu se destacar em um ambiente de negócios cada vez mais competitivo.

Atualmente, a Deloitte opera em mais de 150 países, empregando cerca de 415.000 profissionais. A empresa se organiza como uma rede de firmas-membro independentes, que operam sob o nome Deloitte, mas cada uma mantém sua própria estrutura legal e governança e a sua missão é ajudar seus clientes a enfrentar desafios complexos e encontrar oportunidades em meio às mudanças do mercado. Seus valores fundamentais incluem integridade, compromisso com a qualidade, diversidade, inclusão e responsabilidade social. A empresa tem um forte foco em inovação e continua a investir em novas tecnologias para melhorar seus serviços e manter-se à frente no mercado global (Barros, 2017).

Em fim, a Deloitte é uma gigante global no setor de serviços profissionais, com uma longa história de crescimento e inovação. Sua capacidade de adaptar-se às mudanças e desafios do mercado, ao mesmo tempo em que mantém um compromisso com a qualidade e a ética, continua a solidificar sua posição como líder em seu campo.

### 4.1.1 Impactos e desafios éticos enfrentados pela Deloitte

Apesar de seu sucesso e influência global, a Deloitte, como qualquer grande organização, também enfrentou desafios e controvérsias ao longo de sua história. Casos de violações de dados, como revelada em 2017, destacam os desafios éticos e operacionais que empresas deste porte enfrentam, especialmente em um mundo cada vez mais digitalizado.

Conforme Maragno e Cordeiro (2022), a empresa passou por um ataque de *hackers*, que conseguiram acessar informações confidenciais de clientes da empresa ao explorar uma falha no seu sistema. Tal fato provocou a exposição das informações sensíveis de várias grandes corporações, incluindo planos de negócios, detalhes financeiros e estratégias internas, levantando preocupações sérias sobre a sua capacidade de proteger os dados de seus clientes, especialmente considerando seu papel como consultora em segurança cibernética para outras empresas.

Após a revelação da violação, conforme Forquilha (2017) a empresa passou por uma reação intensa, a qual caracterizou a perda da confiança na capacidade da empresa de proteger dados confidenciais. Foi questionada e levantada a suspeita por alguns clientes quanto as práticas internas da instituição relacionadas à seguridade. A empresa foi criticada por não ter implementado medidas de segurança básicas, como a autenticação multifator, que, de acordo

com Barboza et al. (2018), é imprescindível para a proteção de dados que poderia ter evitado o acesso não autorizado aos sistemas de *e-mail*, o que sublinhou a ironia de uma empresa de consultoria em segurança cibernética, por ser vítima de uma violação de dados devido à falha em adotar suas próprias recomendações de segurança.

Respondendo ao incidente, a Deloitte adotou diversas medidas voltadas à mitigação do impacto e à restauração da confiança dos clientes. Contratou especialistas em segurança cibernética para reforçar seus sistemas e realizou diversas auditorias internas para identificar e corrigir vulnerabilidades. Porém, Wheeler (2019), considera que o dano à reputação da empresa foi significativo, pois, houve o questionamento dos clientes quanto a eficácia dos serviços de segurança cibernética oferecidos pela Deloitte, levando a uma perda de contratos em um setor em que a confiança é essencial. Barboza et al. (2018), ressaltam que a confiança é um ativo essencial em serviços de consultoria, e a perda dessa confiança pode ter efeitos duradouros, como ocorreu nesse caso, em que os clientes demoraram a confiar novamente na empresa, provocando não somente desgaste na imagem, mas, também perda financeira.

Carnevalli (2020) ressalta que o impacto financeiro da violação foi substancial. A Deloitte por ser uma empresa global com uma base financeira robusta, conseguiu absorver parte do impacto sem sofrer uma queda significativa em suas operações, porém, enfrentou custos elevados para resolver o incidente, incluindo gastos com a implementação de novas medidas de segurança, auditorias e o gerenciamento de crises. Além disso, foi alvo de processos judiciais de clientes afetados pela violação, aumentando ainda mais os custos financeiros e de reputação.

Nesse caso, a violação também trouxe à tona a necessidade de uma cultura corporativa que priorize a segurança cibernética em todos os níveis. A Deloitte foi criticada por não ter promovido uma cultura interna forte de segurança, o que pode ter contribuído para a falha na adoção de medidas preventivas, sublinhando a importância de não apenas ter as ferramentas certas, mas também de garantir que todos os funcionários estejam cientes e comprometidos com as melhores práticas de segurança. À vista disso, Kaplan et all (2015) ressaltam que em relação à uma abordagem holística relacionada à segurança cibernética, inclui tanto a tecnologia quanto cultura organizacional, fatores essenciais para que não ocorram violações de dados.

Em resposta ao incidente, foram adotadas abordagens mais transparentes, como comunicação de forma aberta com os clientes sobre as medidas que estavam sendo tomadas para prevenir futuras violações. Essa transparência ajudou a mitigar parte do dano à sua reputação, embora o processo de reconstrução da confiança seja lento e contínuo. Os esforços de educação e treinamento em segurança cibernética também foram intensificados, tanto

internamente quanto para seus clientes, buscando recuperar sua posição como líder confiável em segurança (Carnevalli, 2020).

Este caso, demonstra que nenhuma empresa, independente do seu tamanho ou expertise, está imune a violações de dados. A empresa aprendeu que a segurança cibernética deve ser uma prioridade constante, com vigilância contínua e adaptação às novas ameaças. Dessa forma, Perazzolli et al., (2022) ressaltam que a capacidade de uma empresa de responder rapidamente e de forma eficaz a uma violação é fundamental para minimizar o impacto e recuperar a confiança do público, destacando assim, a importância de uma abordagem proativa e integrada à segurança cibernética, em que tecnologia, processos e cultura corporativa trabalham juntos para proteger informações sensíveis.

Em suma, o caso de violação de dados na Deloitte evidencia como até mesmo as maiores e mais respeitadas empresas podem ser vulneráveis a ataques cibernéticos com consequências significativas. O incidente não só expôs falhas na segurança das informações, mas também trouxe à tona importantes desafios éticos, especialmente em relação à confiança depositada pelos clientes e à responsabilidade da empresa em proteger dados confidenciais. A análise desse caso sublinha a necessidade crítica de as empresas adotarem práticas robustas de segurança e reforçarem seus compromissos éticos, a fim de prevenir violações futuras e mitigar os riscos associados. Além disso, destaca-se a importância de uma resposta transparente e responsável diante de tais incidentes, para preservar a integridade da empresa e manter a confiança do mercado e da sociedade.

A análise desse caso sublinha a necessidade crítica de as empresas adotarem práticas robustas de segurança e reforçarem seus compromissos éticos para prevenir violações futuras e mitigar os riscos associados., destacando-se a importância de uma resposta transparente e responsável diante de tais incidentes para preservar a integridade da empresa e manter a confiança do mercado e da sociedade.

## 4.2 Caracterização da Empresa BDO USA

A BDO USA, LLP é uma das principais empresas de contabilidade e consultoria nos Estados Unidos, parte da rede internacional BDO Global. A BDO Global foi fundada em 1963 como uma aliança entre várias firmas de contabilidade nacionais, buscando expandir sua presença internacionalmente. A sigla BDO inicialmente significava *Binder Dijker Otte*, uma referência aos nomes de seus fundadores originais em diferentes países (Miranda, 2018).

Nos EUA, a história da BDO remonta a 1910, quando o contador Seidman Leonard B. fundou a Seidman & Seidman em Nova York. Durante grande parte de sua história, a empresa operou sob o nome Seidman & Seidman, mas posteriormente adotou o nome BDO USA para alinhar-se com a marca global (BDO USA, 2024).

A BDO USA, conforme Miranda (2018) se destacou ao longo das décadas por oferecer serviços de auditoria, consultoria tributária, serviços de *advisory* e de *compliance* regulatório. A empresa tem se posicionado como uma fornecedora de serviços especializada em médias empresas, embora também atenda grandes corporações. Ela ganhou reputação por seu enfoque personalizado e pelo uso estratégico de tecnologia para oferecer soluções inovadoras.

Com sede em Chicago, a BDO USA tem mais de 70 escritórios no país e faz parte de uma rede global presente em mais de 160 países. A empresa continua a crescer por meio de fusões e aquisições, e, pela expansão de suas ofertas de serviços, especialmente em áreas de consultoria tecnológica e financeira (BDO USA, 2024).

A BDO USA é reconhecida pela sua experiência em setores como saúde, tecnologia, varejo, entre outros, e continua sendo uma das maiores firmas de contabilidade nos Estados Unidos, com um compromisso contínuo com a inovação e a excelência no atendimento ao cliente.

### 4.2.1 Impactos e desafios éticos enfrentados pela BDO USA

A BDO USA enfrentou uma série de impactos e desafios éticos, muitos dos quais são comuns a grandes empresas de auditoria. O vazamento de dados na BDO USA ocorreu em 2017**.** Na época, a empresa sofreu uma violação de segurança cibernética que resultou no acesso não autorizado a informações sensíveis, conforme Forquilha (2017). Esse incidente destacou a importância crescente de segurança de dados, especialmente em empresas de serviços profissionais que lidam com informações confidenciais de clientes.

O vazamento de dados da BDO USA em 2017 representou um marco significativo para a empresa, não apenas pela violação de segurança, mas também pelo conjunto de consequências que se seguiram e, ao abordar tais impactos éticos e financeiros do incidente, é importante considerar a análise de autores que discutem as repercussões de tal evento na confiança e na reputação da empresa (BDO USA, 2023).

A reputação da BDO USA sofreu um golpe severo devido ao vazamento, pois, ao que tange a relação de confiança e confidencialidade com a exposição dos dados sensíveis, houve o comprometimento destas, acarretando na quebra de parcerias, que antes eram fortes, no

momento do incidente passaram a ser reconsideradas, o que levou a empresa a um declínio significativo nos negócios, que junto ao dano à reputação foi difícil de reverter, exigindo um esforço contínuo de reconstrução da confiança junto aos *stakeholders* (BDO USA, 2023). Nesse sentido, Covey (2006) aduz que a confiança é a base das relações comerciais e, uma vez abalada, pode levar anos para ser restaurada, exigindo esforços contínuos e uma estratégia de comunicação transparente. Conforme destacado pela própria BDO USA (2023), a violação resultou em custos diretos significativos, estimados em cerca de US$ 4,35 milhões, incluindo gastos com mitigação, ações judiciais e notificações de clientes, que são partes elementares da resposta a um vazamento de dados e não se limitando apenas ao aspecto financeiro. A BDO também enfrentou perdas indiretas, como a perda de contratos e a diminuição da clientela, uma vez que a confiança do mercado foi abalada. À vista disso, a análise de Argenti (2009) sobre a confiança nas relações empresariais ressalta que, em um ambiente competitivo, a confiança é um ativo intangível vital, e sua perda pode levar a consequências duradouras.

A questão da confidencialidade foi central para o incidente. Com a BDO lidando com informações financeiras e pessoais, a violação aumentou o risco de fraudes e roubo de identidade. Nesse sentido, Schneier (2015) discute sobre os riscos associados à coleta, armazenamento e exposição de dados pessoais e financeiros, ressaltando como isso pode comprometer a segurança de indivíduos e organizações, aumentando as chances de fraudes e roubo de identidade.

A questão da confidencialidade dos dados também foi um ponto crítico no incidente, devido ao fato da BDO lidar com uma grande quantidade de informações financeiras e pessoais de clientes, pois a exposição desses dados aumentou o risco de fraudes e roubo de identidade. A própria BDO Canadá (2023) afirmou que, devido ao fato, a relação de confiança entre a empresa e seus clientes foi comprometida e em resposta, a empresa adotou medidas rigorosas de segurança cibernéticas e revisou políticas internas para mitigar os danos e garantir a proteção contínua das informações dos clientes. Tais medidas vão ao encontro do pensamento de Maiwald (2004), que destaca que a adoção de políticas de segurança não apenas ajuda a mitigar danos após um incidente, mas também atua como uma estratégia proativa para restaurar a confiança do cliente.

Com relação às implicações regulatórias, a BDO foi submetida a uma vigilância mais intensa, exigindo a implementação de medidas de segurança robustas, que, de acordo com que Sundfeld (2023) aborda em seus estudos, pode-se observar que a conformidade regulatória não é apenas uma exigência legal, mas uma forma de restabelecer a confiança no mercado. Isso

resultou em um aumento da carga regulatória, forçando a empresa a realizar auditorias internas mais frequentes e detalhadas.

Ademais, o dualismo entre auditoria e consultoria apresenta desafios éticos contínuos, como a independência dos auditores, que é um fator fundamental à empresa e a BDO, como outras grandes firmas, deve garantir que seus auditores mantenham a imparcialidade, o que vai ao encontro do pensamento de Lopes (2002), que afirma que o tempo prolongado de prestação de serviços pode criar uma relação de dependência, levantando preocupações sobre a qualidade das auditorias e a responsabilidade em identificar irregularidades financeiras.

A qualidade das auditorias está diretamente relacionada à ética profissional dos auditores e, nesse sentido, as negligências podem resultar em consequências significativas, tanto éticas quanto legais, como ocorreu com a BDO. Nessa direção, Werhane e Freeman (1997) aduzem que precisará de uma abordagem robusta para a gestão da ética corporativa, a fim de preservar a confiança pública em seus serviços, pois a sua capacidade em responder a esses desafios éticos e operacionais será crucial para sua sustentabilidade e sucesso no futuro.

Nesse contexto, a pressão competitiva em um mercado global pode levar a concessões éticas, em que as empresas frequentemente enfrentam o dilema de equilibrar a retenção de clientes e a conformidade com as normas éticas, conforme apontado por Gonçalves (2012).

Quanto aos incidentes regulatórios, após o vazamento, a BDO USA (2023), foi submetida a uma vigilância mais intensa por parte dos órgãos reguladores, que exigiram a implementação de medidas de segurança mais robustas e a conformidade com normas mais rigorosas, o que resultou em um aumento significativo na carga regulatória, com a necessidade de realizar auditorias internas frequentes e detalhadas para garantir o cumprimento das novas exigências.

A sua resposta ao incidente envolveu a implementação de uma série de medidas corretivas, já que além de revisar suas políticas de segurança cibernética, a empresa investiu em novas tecnologias para reforçar suas defesas contra ataques futuros, o que incluiu a realização de treinamentos aos funcionários a fim de aumentar a conscientização sobre segurança e a adoção de práticas mais rigorosas de gerenciamento de dados.

A BDO USA enfrentou desafios operacionais e financeiros adicionais como resultado do incidente. Teve que lidar com a perda de clientes, a necessidade de reestruturar suas operações internas e os custos associados à mitigação e à prevenção de futuros incidentes, o que apenas não afetou a lucratividade da empresa, mas, também impactou na sua posição competitiva no mercado.

O ambiente competitivo em que a BDO opera pode gerar pressões para reter clientes e expandir os negócios. Essa pressão pode, em alguns casos, levar a concessões éticas, como flexibilizar normas de auditoria ou ser complacente com práticas questionáveis para agradar a clientela.

Como uma empresa global, a BDO também enfrentou o desafio ético de garantir que suas práticas de governança estejam alinhadas com padrões elevados, independentemente da jurisdição. Cada país tem suas próprias regulamentações e expectativas éticas, o que pode criar um ambiente desafiador para manter a conformidade ética global.

A transformação digital traz oportunidades, mas também riscos éticos. A BDO, ao integrar tecnologias como *big data* e inteligência artificial em seus serviços, enfrentou e enfrenta o desafio de garantir que a privacidade e a segurança dos dados dos clientes sejam protegidas, além de evitar vieses nas análises.

Para responder a esses desafios, segundo Nico Fourie, diretor nacional de TIC da BDO, (citado por Watchguard, s/d) a empresa implementou o modelo extensível de segurança cibernética da Panda Security, que inclui o *Panda Adaptive Defense* 360 (AD360) e os módulos adicionais *Advanced Reporting Tool* (ART) e *Panda Patch Management*. Ele ressalta que a abordagem multiferramentas da Panda Security fornece visibilidade aumentada e geração de relatórios holística, permitindo identificar lacunas em nossa segurança que anteriormente não conheciam. Antes de implementar o AD360, a BDO tinha uma solução baseada em assinaturas que não detectava e bloqueava ameaças avançadas e *malware* de dia zero. Depois do AD360, a BDO está protegida contra os ataques sem *malware* ou arquivos.

Esses desafios mostram como a BDO, assim como outras empresas globais de auditoria, precisa de uma abordagem robusta para a gestão da ética corporativa, a fim de preservar a confiança pública em seus serviços.

### 4.3 Caracterização da Empresa PricewaterhouseCoopers (PwC)

A PwC é uma das maiores firmas de serviços profissionais do mundo, fazendo parte do grupo conhecido como *Big Four*, que reúne as quatro maiores empresas globais de auditoria e consultoria. A PwC foi formada em 1998, após a fusão entre Price Waterhouse e Coopers & Lybrand, ambas com longa tradição no setor (PwC, 2024).

A origem da Price Waterhouse remonta a 1849, quando Samuel Lowell Price fundou sua firma de contabilidade em Londres. Já a Coopers & Lybrand começou em 1854, com a criação da firma de William Cooper, também no Reino Unido. As duas empresas seguiram

trajetórias distintas, tornando-se influentes em auditoria, contabilidade e consultoria, até decidirem se unir (PwC, 2024).

Atualmente, a PwC está presente em mais de 150 países, oferecendo uma vasta gama de serviços, como auditoria, consultoria tributária, assessoria empresarial e de riscos. A empresa é reconhecida por sua atuação em mercados globais, sua experiência em diversos setores econômicos e seu compromisso com a responsabilidade corporativa e sustentabilidade (PwC, 2024).

### 4.3.1 Impactos e desafios éticos enfrentados PwC

O vazamento de dados na PwC, uma das maiores firmas globais de auditoria e consultoria, expôs a complexidade dos desafios enfrentados por grandes corporações na proteção de informações sensíveis e enfrentou desafios particularmente complexos em termos de conformidade regulatória, dado que opera em diversas jurisdições ao redor do mundo, cada uma com suas próprias regras e exigências de proteção de dados, além de garantir a conformidade com essas regulamentações, foi um processo complicado e oneroso, exigindo a implementação de políticas e procedimentos abrangentes que pudessem ser aplicados uniformemente em todas as suas operações (Infosecurity Magazine, 2023).

A gestão da cadeia de suprimentos também representou um desafio significativo para a PwC, dado que a empresa depende de uma vasta rede de parceiros e fornecedores para realizar suas operações, tinha-se a certeza de que qualquer falha na segurança desses parceiros poderia comprometer a integridade dos dados da PwC, fato que de acordo com a PwC (2021), destacou a necessidade de uma supervisão mais rigorosa e de avaliações contínuas das práticas de segurança adotadas pelos fornecedores.

Outro grande desafio enfrentado pela empresa, foi a proteção de dados sensíveis que, por ser uma empresa que lida com grandes volumes de informações confidenciais, ela tem a responsabilidade de garantir que esses dados estejam sempre protegidos, contudo o vazamento demonstrou que mesmo as medidas de segurança mais avançadas podem falhar diante de ataques cibernéticos sofisticados e diante disso, a resposta da PwC, como citada pela Infosecurity Magazine (2023), voltou-se à implementação de um plano de resposta abrangente, incluindo a notificação dos clientes afetados e uma investigação detalhada para determinar a origem e o impacto do vazamento.

Outra resposta dada pela empresa, envolveu uma revisão profunda de suas políticas internas de segurança e conformidade, já que ela foi forçada a adotar uma abordagem mais

proativa, implementando controles mais rigorosos de acesso aos dados, criptografia avançada e monitoramento contínuo de atividades suspeitas, que de acordo com Prazeres (2019) levou-a ao investimento de tecnologias relacionadas à segurança cibernética de ponta a ponta a fim de prevenir posteriores violações.

Quanto aos desafios operacionais, Prazeres (2019), ressalta que a empresa possuiu problemas relacionados ao vazamento de dados, aos quais voltaram-se a reestruturação de suas operações internas, a fim de que melhorassem a segurança cibernética e garantissem a conformidade contínua com as regulamentações internacionais, fato que que geraram interrupções nas operações além dos custos adicionais pelos serviços.

Por fim, o incidente teve um impacto negativo na confiança dos clientes, já que muitos questionaram a capacidade da empresa de proteger suas informações, levando alguns a reconsiderar suas parcerias e diante disso, conforme Carvalho (2022) a empresa reconheceu a necessidade de fortalecer sua cultura de segurança interna, além de garantir que todos os funcionários estivessem cientes das melhores práticas de segurança e da importância da proteção de dados sensíveis.

Esse caso demonstra a importância crítica de uma abordagem integrada e proativa em relação à segurança cibernética, tanto para proteger os dados contra ameaças externas quanto para garantir a conformidade com as normas regulatórias internacionais e junto a isso, enfatizam a necessidade de uma supervisão rigorosa e contínua das práticas de segurança de parceiros e fornecedores para evitar que vulnerabilidades externas comprometam a integridade dos dados de uma organização (Barbosa et al., 2016).

## 5 CONSIDERAÇÕES FINAIS

A análise dos impactos éticos gerados pela tecnologia no contexto contábil empresarial revelou um cenário complexo, em que a integração de novas ferramentas tecnológicas, embora potencialize a eficiência e a precisão das operações contábeis, também traz à tona significativos desafios relacionados à privacidade e à segurança de dados.

O estudo identificou as principais tecnologias utilizadas no ambiente contábil: as ferramentas QuickBooks, Xero e SAP Concur que oferecem soluções em nuvem; tecnologia *blockchain* que tem a capacidade de fornecer registros imutáveis e transparente de transações; sistemas de EPA, que envolve o uso de *bots* para automatizar tarefas recorrentes; sistemas de ERP, que integra diversas funções empresariais; P2P e O2C, que são soluções de automação que ajudam a otimizar os ciclos de compras e recebíveis, respectivamente; ACL, ferramentas

que permitem a automação de processos de auditoria e conformidade; BI, que permitem que os contadores transformem dados financeiros em *insights* acionáveis; AI e ML, tecnologias utilizadas para analisar grandes volumes de dados financeiros, detectar padrões e anomalias entre outros. Também, evidenciou que, embora essas ferramentas sejam fundamentais para a modernização da prática contábil, elas também ampliam a exposição a riscos cibernéticos.

Os impactos sobre a privacidade e segurança de dados se manifestam de forma evidente, principalmente em função da quantidade massiva de informações sensíveis processadas e armazenadas digitalmente. A investigação mostrou que, à medida que as tecnologias se tornam mais sofisticadas, também se intensificam as ameaças de violações de dados, exigindo que os profissionais contábeis adotem uma postura ética e vigilante, além de medidas de segurança robustas.

A análise de casos emblemáticos de violações de privacidade, como os das empresas Deloitte, BDO USA e PwC trouxe à tona as graves consequências que esses incidentes podem ter, não apenas para as organizações, mas também para a confiança do público e o bem-estar dos indivíduos cujos dados foram comprometidos. Esses casos, ilustram a urgência de um compromisso ético por parte das empresas e dos profissionais contábeis, no sentido de proteger as informações sob sua custódia e de implementar políticas e práticas que previnam futuras violações.

Verificou-se que os impactos causados nas aludidas empresas foram de diversas ordens, incluindo financeiros, legais, de reputação e operacionais.

Os financeiros foram: perda de receita, pois o vazamento de dados resultou na perda de clientes e contratos futuros, especialmente em mercados em que a confiança e a segurança de informações são fundamentais; multas e Penalidades, uma vez que as empresas enfrentaram multas regulatórias pesadas impostas por autoridades de proteção de dados, por não cumprirem os requisitos de segurança; custos de remediação, as empresas precisaram investir pesadamente em medidas de correção, como a implementação de novas tecnologias de segurança, serviços de monitoramento de crédito para vítimas de vazamentos, e custos legais associados.

Impactos legais: processos judiciais, uma vez que os vazamentos de dados levaram a processos de clientes, investidores e indivíduos cujas informações foram comprometidas; investigações regulamentares, pois as empresas objeto de estudo são frequentemente monitoradas por agências reguladoras, e a violação de dados desencadeou investigações mais amplas sobre sua práticas de segurança; obrigação de notificação, já que as leis de cada país, obrigam as empresas a notificar todos os indivíduos afetados pela violação de dados, o que pode gerar ainda mais complicações e custos.

Impactos na Reputação: perda de confiança, visto que a confiança é um ativo essencial para empresas de auditoria e consultoria. Os vazamentos de dados resultaram na perda de credibilidade perante os clientes, acionistas e o público em geral, levando a uma deterioração da marca; perda de clientes, as empresas perderam contratos importantes, uma vez que clientes podem optar por outras firmas que considerem mais seguras; danos à imagem pública, pois a gravidade dos vazamentos e a maneira como as empresas responderam geram impacto negativo sobre a marca.

As empresas, também, sofreram impacto operacional, tendo que aumentar os investimentos em cibersegurança, pois após os vazamentos, precisarão investir ainda mais em segurança cibernética, desde a contratação de profissionais até a compra de soluções tecnológicas mais avançadas.

O desafio ético reside na obrigação dos contadores de garantir que todas as medidas de segurança apropriadas sejam implementadas e mantidas para proteger as informações de possíveis acessos não autorizados. Isso inclui o uso de tecnologias de criptografia, controles de acesso rigorosos e práticas de gestão de risco cibernético. Além disso, os contadores devem se manter constantemente atualizados sobre as melhores práticas de segurança da informação para mitigar novos riscos à medida que surgem.

Observou-se que, para mitigar os riscos éticos associados à tecnologia, é fundamental que os contadores estejam continuamente atualizados sobre as melhores práticas de segurança e que as empresas invistam em soluções tecnológicas alinhadas aos princípios éticos da profissão contábil.

Esses incidentes destacam a importância de uma abordagem holística à segurança de dados, que não depende apenas de tecnologia avançada, mas também, de uma cultura corporativa que priorize a ética, a governança e a constante atualização de práticas de segurança.

Assim, as medidas corretivas adotadas por essas empresas após as violações, embora importantes, mostraram que a recuperação da confiança do público e do mercado é um processo árduo e muitas vezes insuficiente para reverter os danos causados pela falta de preparo e prevenção.

Por fim, este estudo ressalta a necessidade de uma abordagem ética e responsável na adoção de tecnologias e automação no contexto contábil, com foco na proteção da privacidade e segurança de dados. É imperativo que as organizações invistam continuamente em capacitação e em soluções tecnológicas avançadas, ao mesmo tempo em que estabeleçam e reforcem diretrizes éticas claras, para mitigar os riscos associados e garantir a integridade e a confiança na prática contábil empresarial.

## 6 REFERÊNCIAS

ALMEIDA, Francisco José; SARAIVA, Piedley Macedo. O homem e os novos cenários corporativos na era digital: um estudo prático aplicado a área contábil. ID *on line*. **Revista de psicologia**, v. 18, n. 71, p. 117-129, 2024. Disponível em: https://idonline.emnuvens.com.br/id/article/view/3992. Acesso em: 10.maio.2024.

ARANHA, M. L. A.; MARTINS, H. P. **Temas de filosofia.** São Paulo: Moderna, 2005.

ARGENTI, Paul A. **Corporate communication**. 6. ed. New York: McGraw-Hill, 2009.

BARBOSA, Guilherme Augusto Ruani et al. Segurança da informação: a proteção contra o vazamento de dados e sua importância para as empresas privadas. **Revista Eletrônica e-Fatec, v. 6, n. 1, p. 10-10, 2016.** Disponível em: https://pesquisafatec.com.br/ojs/index.php/efatec/article/view/105. Acesso em: 30.ago.2024.

BARBOZA, Eudes da Silva et al. **Autenticação multifatorial em hardware para o processo de assinatura digital da NF-e**. 2018. Dissertação de Mestrado. Universidade Federal de Pernambuco. Disponível em: https://repositorio.ufpe.br/handle/123456789/32403. Acesso em: 06.jul.2024.

BARROS, Thiago de Sousa. As falhas da Deloitte na auditoria contábil e financeira : um estudo das fraudes do banco Panamericano. **Revista de Administração e Negócios da Amazônia,** v. 9, n. 4, set./dez, 2017. Disponível em: https://repositorio.ufop.br/handle/123456789/10693. Acesso em: 08 set. 2024.

BDO CANADA. **Strategies for combatting data breaches.** 2023. Disponível em: https://www.bdo.ca. Acesso em: 4.set.2024.

BDO USA. **Prepare now to get ahead of SEC cybersecurity rules.** 2023. Disponível em: https://www.bdo.com/insights/prepare-now-to-get-ahead-of-sec-cybersecurity-rules. Acesso em: 4.set.2024.

BOMFIM, Vanessa Cantuaria. Os avanços tecnológicos e o perfil do contador frente à era digital. **Revista Trevisan**, v. 18, n. 173, p. 60 à 78-60 à 78, 2020. Disponível em: https://rtrevisan.emnuvens.com.br/revistatrevisan/article/download/74/63. Acesso em: 20.maio.2024.

CARNEVALLI, Kalil. **Instituições financeiras:** tendências e tecnologias. São Paulo, SP: Haikai Editora, 2020.

CARVALHO, Maria Eduarda Rodrigues de. **Big Data:** como a datificação está impactando a trabalho publicitário? Uma análise da atuação profissional na empresa Deloitte Digital. 2022. 75 f. Monografia (Graduação em Comunicação Social) – Curso de Graduação em Comunicação Social/Publicidade e Propaganda, Instituto de Cultura e Arte, Universidade Federal do Ceará, Fortaleza, 2022. Disponível em:https://repositorio.ufc.br/handle/riufc/68607. Acesso em: 20 set.2024.

CEOLATO, Renata Varela. **Análise bibliométrica de artigos da área de sistemas de informação contábil e suas contribuições relacionadas à aplicação de tecnologias**

**emergentes na contabilidade.** 2019. Trabalho de Conclusão de Curso, Universidade Federal do Rio Grande do Sul. Faculdade de Ciências Econômicas. Curso de Ciências Contábeis. Disponível em: https://lume.ufrgs.br/handle/10183/198557. Acesso em: 30.maio.2024.

CODESSO, Mauricio Mello et al. Continuous audit model: data integration framework. **Revista Contemporânea de Contabilidade**, v. 15, n. 34, p. 144-157, 2018. Disponível em: https://www.redalyc.org/journal/762/76261661008/76261661008.pdf. Acesso em: 28.ago.2024.

COSTA, Geovani Alves; MELO, Maurílio Alves; SOARES, Carlos Alberto de Souza. Ética profissional: um desafio para o contador na era digital. **II Congresso UFERSA de Contabilidade**, 8-10 de maio, 2015. Disponível em: https://contabeis.ufersa.edu.br/wp-content/uploads/sites/33/2014/09/II-Congresso-UFERSA-de-Contabilidade-Anais-20151.pdf#page=182. Acesso em: 10.maio.2024.

COVEY, S. M. R.. **The speed of trust:** the one thing that changes everything. New York: Free Press, 2006.

DAVENPORT, T. H.; RONANKI, R. **Artificial intelligence for the real world.** Harvard Business Review, 2018.

DUARTE, João Pedro Teixeira. **A adoção de tecnologias emergentes pelos profissionais de contabilidade**. 2022. Tese de Doutorado. Instituto Politécnico do Porto (Portugal). Disponível em: https://search.proquest.com/openview/ec591724df47b1f6479619e87b4605cf/1?pq-origsite=gscholar&cbl=2026366&diss=y. Acesso em: 12.jun.2024.

FARIAS, Joao Paulo Cristian; MONTEIRO, Tiago da Costa. **Os impactos da implementação da inteligência artificial na contabilidade:** uma análise dos aspectos técnicos e éticos. 2024. Disponível em: https://bdta.ufra.edu.br/jspui/handle/123456789/3702. Acesso em: 06.maio. 2024.

FERREIRA, Sofia da Silva. **Digital accountant:** competências e o papel do contabilista na era digital. 2021. Tese de Mestrado. Instituto Superior de Contabilidade e Administração do Porto. Mestrado em Contabilidade e Finanças, 2021. Disponível em: https://recipp.ipp.pt/handle/10400.22/19183. Acesso em: 10.maio.2024.

FERREIRA, Juliana Tupan. **O Papel das joint ventures no modelo chinês de desenvolvimento econômico e o crescimento da indústria de high technology:** o caso da Lenovo**.** 2017. Trabalho de Conclusão de Curso (Bacharelado em Relações Internacionais) – Faculdade de Relações Internacionais, Universidade Federal da Grande Dourados, Dourados, MS, 2017. Disponível em: https://repositorio.ufgd.edu.br/jspui/handle/prefix/3046. Acesso em: 20.jul.2024.

FERREIRA, Tiago Janes et al. Automação contábil: tecnologia em contabilidade sob a ótica da teoria institucional. **XI Congresso Anpcont,** de 3 -6 de junho de 2017, 2017. Disponível em: https://www.anpcont.org.br/pdf/2017/CCG650.pdf. Acesso em: 19.mai.2024.

FORQUILHA, Paulo dos Santos. **Utilização dos accruals como medida de manipulação dos resultados das empresas em Angola:** estudo exploratório. 2017. Dissertação de

Mestrado. Universidade Aberta (Portugal). Disponível em: https://search.proquest.com/openview/3db2f7404e33f1cbe6a8d4142cbe7cb7/1?pq-origsite=gscholar&cbl=2026366&diss=y. Acesso em: 10.ago.2024.

GONÇALVES, Eduardo A.. **Ética empresarial**: fundamentos, desafios e perspectivas. São Paulo: Saraiva, 2012.

HEBERLE, Éder Luís; KÖNIG, Jaqueline Grutzmann. Inteligência artificial e a robotização de tarefas para o aumento de eficiência em escritório de contabilidade. **RAGC**, v. 11, n. 45, 2023. Disponível em: https://www.revistas.fucamp.edu.br/index.php/ragc/article/view/2876. Acesso em: 20.mar.2024.

IGUMA, Marcio Kawahara. **Big data analytics e a evolução das práticas de auditoria interna:** um estudo sobre os antecedentes da aceitação e adoção da tecnologia no setor privado brasileiro. 2020. Tese de Doutorado. Universidade de São Paulo. Disponível em: https://www.teses.usp.br/teses/disponiveis/12/12136/tde-19032020-152236/en.php. Acesso em: 19.jun.2024.

INFOSECURITY MAGAZINE**. Data privacy week:** US data breaches surge. 2023 Sees 78% Increase. 2023. Disponível em: https://www.infosecurity-magazine.com. Acesso em: 4.set.2024.

JESUS, Tânia Alves; SARMENTO, Manuela; DUARTE, Manuela. Ética e responsabilidade social. **Dos Algarves: Tourism, Hospitality & Management Journal**, n. 29, p. 3-30, 2018. Disponível em: http://www.dosalgarves.com/index.php/dosalgarves/article/view/109. Acesso em: 31.mar.2024.

Kaplan, J. M. et all.. **Beyond cybersecurity**: protecting your digital business. Hoboken, NJ: Wiley, 2015.

LANNES, Yuri Nathan da Costa**. Nova privacidade no Brasil e os impactos jurídicos e econômicos**: uma análise do *big data* e da responsabilidade empresarial. 2020. Trabalho de Conclusão de Curso, Universidade Mackenzie, 2020. Disponível em: https://dspace.mackenzie.br/handle/10899/26476. Acesso em: 20.jun.2024.

LIMA, Maria Eduarda Barbosa et al. Ética em contabilidade: um estudo sobre a percepção dos discentes acerca da ética profissional. **Revista de Gestão e Contabilidade da UFPI**, v. 1, n. 2, 2015. Disponível em: http://www.atena.org.br/revista/ojs-2.2.3-08/index.php/GECONT/article/view/2294. Acesso em: 30.mai.2024.

LIMA, Bruno Ribeiro de. **Uma análise acerca dos principais assuntos de auditoria de empresas do setor financeiro brasileiro.** 2022. 20 f. Trabalho de Conclusão de Curso (Graduação em Ciências Contábeis) – Universidade Federal de Uberlândia, Uberlândia, 2022. Disponível em: https://repositorio.ufu.br/handle/123456789/34341. Acesso em: 30.mai.2024.

LOPES, Shiley R.. **Auditoria independente**: objetivos e responsabilidades. São Paulo: Atlas, 2002.

MAIWALD, E.. **Fundamentals of network security**. New York: McGraw-Hill, 2004.

MANCEBO, Víctor Oroña Claussen. **Tecnologias digitais e mudanças no escopo de atividades e funções da controladoria**. 2022. Tese de Doutorado. Universidade de São Paulo. Disponível em: https://www.teses.usp.br/teses/disponiveis/12/12136/tde-16032023-205740/en.php. Acesso em: 19.mar.2024.

MARAGNO, Lucas Martins Dias; CORDEIRO, Nadieli. A influência do lócus de comprometimento e do estilo ético no whistleblowing de auditores independentes. **Revista de Contabilidade e Organizações**, v. 16, p. e185317-e185317, 2022. Disponível em: https://www.revistas.usp.br/rco/article/view/185317. Acesso em: 14.ago.2024.

MARQUES, J. R. **Teoria da equidade.** 2017.

MATIAS, Rita Santos. **O uso da inteligência artificial:** o caso das empresas cotadas no PSI-20.2021. Tese de Doutorado, Universidade de Coimbra, 2021. Disponível em: https://comum.rcaap.pt/handle/10400.26/39017. Acesso em: 24.fev.2024.

MIRANDA, Catarina Vicente.**Impacto da auditoria interna na externa numa empresa multinacional: um estudo de caso**. 2018. Dissertação de Mestrado. Instituto Politécnico de Lisboa, Instituto Superior de Contabilidade e Administração de Lisboa. Disponível em http://hdl.handle.net/10400.21/16208. Acesso em: 10 set. 2024.

MONK, E.; WAGNER, B. **Concepts in enterprise resource planning.** Cengage Learning, 2009.

MOREIRA, Raiane Gomes. A tecnologia da informação no avanço da contabilidade. **Revista Farol**, v. 13, n. 13, p. 24-39, 2021.Disponível em: http://revista.farol.edu.br/index.php/farol/article/view/308. Acesso em: 19.mar.2024.

O'LEARY, D. E. **Enterprise resource planning systems:** systems, life cycle, electronic commerce and risk. Cambridge University Press, 2000.

OLIVEIRA, Diego Bianchi; MALINOWSKI, Carlos Eduardo. A importância da tecnologia da informação na contabilidade gerencial. **Revista de administração**, v. 14, n. 25, p. 3-22, 2016. Disponível em: http://revistas.fw.uri.br/index.php/revistadeadm/article/view/1596. Acesso em: 18.jun.2024.

PERAZZOLLI, Juliana Vieira Pereira et al. Deficiências das auditorias externas sediadas no BRICS: uma análise dos relatórios de inspeção do Public Company Accounting Oversight Board-PCAOB. In: **USP International Conference in Accounting**. Universidade Federal de Minas Gerais, 2022. Disponível em: https://repositorio.ufmg.br/handle/1843/60121. Acesso em: 06.jul.2024.

PRAZERES, Raquel Sofia Baptista dos. **Da gestão do conhecimento à inteligência competitiva:** o caso da PwC Portugal. Tese de mestrado em Ciências da Documentação e Informação. Universidade de Lisboa, 2019. Disponível em: https://repositorio.ul.pt/handle/10451/41725. Acesso em: 01.set.2024.

PWC. **Companies may be overlooking the riskiest cyber threats of all.** 2021. Disponível em: https://www.pwc.com/gx/en/issues/data-privacy-cybersecurity/companies-overlooking-riskiest-cyber-threats.html. Acesso em: 4.set.2024.

RAWLS, John. **Uma teoria da justiça.** Tradução de Almiro Pisetta e Lennita M. R. Esteves. São Paulo: Martins Fontes, 1997.

REIS, Patrícia Nunes Costa et al. Contabilidade estratégica e gestão de pessoas: os desafios na construção de profissionais éticos em tempos da indústria 4.0. In: **Congresso Brasileiro de Ciências e Saberes Multidisciplinares**. 2023. Disponível em: https://conferenciasunifoa.emnuvens.com.br/tc/article/view/990. Acesso em: 19.jun.2024.

ROSA, Reginaldo José et al. Tecnologias de contabilidade distribuídas (DLTS): evolução, diferenças, similaridades e vantagens. **Humanidades & Inovação**, v. 7, n. 9, p. 231-243, 2020. Disponível em: https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/2120. Acesso em: 12.jun.2024.

SÁ, A. L. **Ética profissional**. 9. ed. São Paulo: Atlas, 2010.

SCHNEIER, B.. **Data and goliath**: the hidden battles to collect your data and control your world. New York: W.W. Norton & Company, 2015.

SEIBLITZ, Mariana Hermes da Fonseca de Lossio. A importância da big data em finanças e contabilidade. **A importância do *big data* em finanças e contabilidade**, v. 39, 2021. Disponível em: https://pantheon.ufrj.br/handle/11422/15109. Acesso em: 19.mar.2024.

SILVA, Gabriel Nery. **Contabilidade 4.0**: as tendências tecnológicas que moldam o profissional contábil. 2023. Trabalho de Conclusão de Curso (graduação) — Universidade de Brasília, Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas, Departamento de Ciências Contábeis e Atuariais, 2023. Disponível em: https://bdm.unb.br/handle/10483/38289. Acesso em: 04.maio.2024.

STIGLITZ, Joseph; PIETH, Mark. Superando a economia paralela. **Análise nº 20/2017, Friedrich Ebert Stiftung Brasil**, 2017. Disponível em: https://library.fes.de/pdf-files/bueros/brasilien/13165.pdf. Acesso em: 13.ago.2024.

SUNDFELD, C. A.. **Direito administrativo e regulação econômica**. São Paulo: Malheiros Editores, 2017.

TADEU, Samuel; ALMEIDA, Naiara; GONÇALVES, Ariane. Contabilidade 4.0, a tecnologia a favor dos contadores na era digital. **Revista Projetos Extensionistas**, v. 1, n. 1, p. 146-153, 2021.Disponíiel em: https://periodicos.fapam.edu.br/index.php/RPE/article/view/342. Acesso em: 10.maio.2024.

VÁZQUEZ, A. S. **Ética**. São Paulo: Civilização Brasileira. 2005.

WERHANE, Patricia. H.; FREEMAN, R. E.. **Business ethics**: the state of the art. New York: Oxford University Press, 1997.

WHEELER, Alina. **Design de identidade da marca**: guia essencial para toda a equipe de gestão de marcas. Bookman, 2019.

WHITMAN, M.; MATTORD, H. **Principles of information security**. Cengage Learning, 2018.

WIXOM, B. H.; WATSON, H. J. The BI-Based Organization**. International Journal of Business Intelligence Research**, 2010. Disponível em: https://www.igi-global.com/article/based-organization/38937. Acesso em: 03.set.2024.