UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

DEPARTAMENTO DE CIÊNCIAS CONTÁBEIS E ATUARIAIS

CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS

BARBARA HERMÍNIA VILA NOVA

RISCOS TECNOLÓGICOS À CONTABILIDADE: os impactos do cibercrime na atuação dos profissionais contábeis

Recife

2022

BARBARA HERMÍNIA VILA NOVA

RISCOS TECNOLÓGICOS À CONTABILIDADE: os impactos do cibercrime na atuação dos profissionais contábeis

Trabalho de Conclusão de Curso apresentado ao Curso de Ciências Contábeis da Universidade Federal de Pernambuco – UFPE, como requisito parcial para obtenção do grau de Bacharel em Ciências Contábeis.

Orientador (a): Miguel Lopes de Oliveira Filho

Recife

2022

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Nova, Barbara Hermínia Vila.
Riscos Tecnológicos à Contabilidade: os impactos do cibercrime na atuação dos profissionais contábeis / Barbara Hermínia Vila Nova. - Recife, 2022.
65 p. : il., tab.

Orientador(a): Miguel Lopes de Oliveira Filho
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Ciências Sociais Aplicadas, Ciências Contábeis - Bacharelado, 2022.
Inclui referências, apêndices.

1. Riscos Tecnológicos. 2. Cibersegurança. 3. Cibercrimes. 4. Contabilidade. 5. Invasões Cibernéticas. I. Oliveira Filho, Miguel Lopes de . (Orientação). II. Título.

600 CDD (22.ed.)

FOLHA DE APROVAÇÃO

BARBARA HERMÍNIA VILA NOVA

RISCOS TECNOLÓGICOS À CONTABILIDADE: os impactos do cibercrime na atuação dos profissionais contábeis

Trabalho de Conclusão de Curso apresentado ao Curso de Ciências Contábeis da Universidade Federal de Pernambuco – UFPE, como requisito parcial para obtenção do grau de Bacharel em Ciências Contábeis.

Aprovado em 08 de novembro de 2022.

BANCA EXAMINADORA

_____

Prof/a. Miguel Lopes de Oliveira Filho (Orientador)
Universidade Federal de Pernambuco

_____

Prof/a. Álvaro Pereira de Andrade (Avaliador/a)
Universidade Federal de Pernambuco

_____

Prof/a. Rodrigo Vaz Gomes Bastos (Avaliador/a)
Universidade Federal de Pernambuco

DEDICATÓRIA

Dedico este trabalho aos meus pais Elaine e Clewerson e aos meus avós Ana, Maria, Valdemiro e João, as pessoas que mais amo e que sempre estão a me apoiar nos meus sonhos e objetos, este trabalho é uma conquista nossa. Amo-vos.

AGRADECIMENTOS

Agradeço primeiramente a Deus a oportunidade de estar podendo concluir o curso de Ciências Contábeis, como também toda a ajuda nos estudos, toda força e firmeza para encarar as dificuldades que se apresentaram no meu caminho durante esses quatro anos, ao amado e bondoso pai, eu agradeço.

Agradeço ao Mestre que me guia e ilumina, enchendo meu coração de paz e amor, ao amigo fiel que tanto me guarnece e que está comigo em todos os momentos, eu agradeço.

Agradeço aos meus pais, amigos e familiares que me apoiaram e incentivaram na realização deste trabalho, grata pelas palavras de apoio, amor e carinho.

“Conhecereis a verdade e a verdade vos libertará.”

(JOÃO 8:32)

RESUMO

O presente trabalho teve por objetivo identificar os riscos tecnológicos que podem impactar na realização das atividades contábeis, desta forma conhecendo áreas de atuação contábil que podem auxiliar no combate aos crimes cibernéticos e como o tema é abordado aos graduandos e proposto nas grades curriculares das universidades. Ademais, foram apresentados os riscos pertinentes à contabilidade e as empresas, as formas e métodos utilizados por criminosos para conseguir acesso aos computadores, redes e sistemas, além de também evidenciar conhecimentos essenciais para prevenção de ameaças. Como metodologia utilizou-se o método de levantamento de dados, através de respostas ao questionário online disponibilizado aos alunos de graduação da Universidade Federal de Pernambuco (UFPE) pela plataforma *Google Forms* e pesquisa bibliográfica com análise dos planos de ensino do curso de contábeis nas nove Universidades Federais do Nordeste, assim apresentando uma abordagem qualitativa e quantitativa. Durante a pesquisa, realizou-se a análise dos dados, colhendo informações das disciplinas relacionadas à tecnologia da informação, por meio do sítio da universidade e projeto pedagógico do curso, desta forma evidenciando no resultado que todas as instituições possuem pelo menos uma disciplina relacionada ao tema e que a UFPE apesenta o melhor desempenho, além disso, também se apurou os resultados com o formulário online, no qual contém 18 questões e procurou saber a importância do tema aos graduandos, como também analisar os conhecimentos básicos que eles possuem sobre o assunto, assim o estudo mostrou que o tema é relevante aos alunos, mas que temas como técnicas antiforenses e tipos de malware precisam de melhor abordagem. De todo modo, o objetivo da pesquisa obteve êxito e conseguiu evidenciar os riscos técnicos que impactam nas atividades contábeis.

Palavras-chave: Riscos Tecnológicos, Cibersegurança, Cibercrimes, Contabilidade, Invasões Cibernéticas.

ABSTRACT

The present work aimed to identify the technological risks that can impact the performance of accounting activities, thus knowing areas of accounting activity that can help in the fight against cyber crimes and how the theme is addressed to undergraduates and proposed in the curricula of universities. In addition, the relevant risks to accounting and companies were presented, the ways and methods used by criminals to gain access to computers, networks and systems, in addition to also showing essential knowledge for preventing threats. As a methodology, the data collection method was used, through responses to the online questionnaire made available to undergraduate students at the Federal University of Pernambuco (UFPE) through the Google Forms platform and bibliographical research with analysis of the teaching plans of the accounting course in the nine Federal Universities of the Northeast, thus presenting a qualitative and quantitative approach. During the research, data analysis was carried out, collecting information from disciplines related to information technology, through the university website and the course's pedagogical project, thus showing in the result that all institutions have at least one discipline related to the theme and that UFPE has the best performance, in addition, the results were also calculated with the online form, which contains 18 questions and sought to know the importance of the theme to undergraduates, as well as to analyze the basic knowledge they have on the subject , so the study showed that the topic is relevant to students, but that topics such as anti-forensic techniques and types of malware need a better approach. In any case, the objective of the research was successful and managed to highlight the technical risks that impact accounting activities.

Keywords: Technological Risks, Cybersecurity, Cybercrimes, Accounting, Cyber Invasions.

.

LISTA DE QUADROS/TABELAS

LISTA DE GRÁFICOS/FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CD	Compact Disk
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CFC	Conselho Federal de Contabilidade
CID	Confidencialidade, Integridade e Disponibilidade
CNE/CES	Conselho Nacional de Educação/Câmara de Educação Superior
CPF	Cadastro da Pessoa Física
DIRJ	Declaração de Rendimentos da Pessoa Jurídica
DOJ	Department of Justice
DOS	Disk Operating System
DVD	Digital Versatile Disc
EAD	Educação a Distância
ERP	Enterprise Resource Planning
FEAAC	Faculdade de Economia, Administração, Atuária e Contabilidade
HDD	Hard Disk Drive
IES	Instituições de Ensino Superior
IFES	Instituto Federal de Ensino Superior
IOT	Internet das Coisas
IP	Internet Protocol (Protocolo de Internet)
ISAR	Intergovernmental Working Group of Experts on International Standards of Accounting and Reporting
LAN	Local Area Network
LGPD	Lei Geral de Proteção de Dados
MEC	Ministério da Educação
NBC PG	Normas Brasileiras de Contabilidade aplicada a todos os profissionais do segmento contábil
NBC TA	Normas Brasileiras de Contabilidade de auditoria independente de informação contábil histórica
NBC TP	Normas Brasileiras de Contabilidade referente a trabalhos de perícia contábil
NBR ISO/IEC	Normas Brasileiras correspondentes ao ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission)
NDE	Núcleo Docente Estruturante
ONU	Organização das Nações Unidas

PCAOB	Public Company Accounting Oversight Board
PSI	Política de Sistema de Informação
SI	Sistema de Informação
SOX	Lei Sarbanes Oxley
TA	Técnicas Antiforense
TI	Tecnologia da Informação
TOR	The Onion Router
UFAL	Universidade Federal de Alagoas
UFBA	Universidade Federal da Bahia
UFC	Universidade Federal do Ceará
UFMA	Universidade Federal do Maranhão
UFPB	Universidade Federal da Paraíba
UFPE	Universidade Federal de Pernambuco
UFPI	Universidade Federal do Piauí
UFRN	Universidade Federal do Rio Grande do Norte
UFS	Universidade Federal de Sergipe
UNCTAD	*United Nations Conference on Trade and Development*
VPN	Virtual Private Network

LISTA DE SÍMBOLOS

%	Porcentagem
*	Asterisco em forma de estrela

SUMÁRIO

1. INTRODUÇÃO

Muitos foram os avanços tecnológicos, econômicos e sociais desde a Primeira Revolução Industrial em 1780, atualmente a humanidade vivencia a Quarta Revolução Industrial, no qual Schwab (2016, p. 20) definiu como a revolução que "cria um mundo onde os sistemas físicos e virtuais de fabricação cooperam de forma global e flexível", assim compreende-se que o objetivo desta revolução é a "interação dos meios físicos, digitais e biológicos". Entre as características dessa nova fase mundial percebe-se o uso de tecnologias mais refinadas como a inteligência artificial, robótica, big data, internet das coisas (IoT) e integração dos sistemas. Assim, proporcionando maior rapidez, produtividade, qualidade e diminuição de custos às empresas.

Contudo, ao ponto que os avanços tecnológicos oferecem tantos benefícios às entidades e sociedade, muitos são os riscos que a falta de conhecimento e uso desses meios pode ocasionar, como o risco cibernético.

Segundo estudos do relatório de segurança da empresa Nozomi Networks (2021), o aumento de crimes de ransomware[1] foi de 116%. Desta forma, a pesquisa pretende explorar os riscos tecnológicos à contabilidade, assim procurando identificar as principais ameaças, os métodos de prevenção, como as áreas de atuação do contador podem cooperar no combate aos crimes cibernéticos e a importância do tema ser abordado durante a graduação.

Assim, procurou-se validar as hipóteses levantadas através de pesquisa bibliográfica analisando os planos de ensino das Universidades Federais do Nordeste e formulário online com os alunos de Ciências Contábeis da UFPE.

1.1. PROBLEMA DE PESQUISA

Segundo Albertin (2004), o uso da tecnologia da informação é um dos principais componentes do ambiente empresarial, no qual as empresas vêm utilizando a tecnologia e os meios tecnológicos em níveis estratégicos, como também operacionais para o melhor desempenho de suas atividades.

[1] É um tipo de software malicioso utilizado por cibercriminosos para infectar computadores e redes, no qual pode bloquear o acesso dos usuários e criptografar os dados.

Contudo, nos últimos anos percebe-se que o uso dessas tecnologias também pode ocasionar prejuízos e riscos a continuidade da empresa, como descreve o site da Forbes Tech sobre o levantamento da empresa Cybereason em 2021, no qual a maioria das organizações vítimas de ransomware vivenciaram um resultado negativo nos negócios, com "(...) perda de receita, danos à marca, cortes imprevistos de pessoas e até o encerramento das atividades. (...)". (TECH; 2021, p.01)

Com isso, é necessário que os profissionais contábeis mantenham-se atualizados e busquem por especializações na área de tecnologia, a fim de responderem à pergunta: Quais são os riscos tecnológicos que impactam nas atividades dos profissionais contábeis?

1.2. JUSTIFICATIVA

A tecnologia faz parte do passado, do presente e do futuro da profissão contábil, desta forma é imprescindível que os profissionais da área mantenham-se atualizados sobre os avanços tecnológicos e as vantagens que essas ferramentas possibilitam, como: agilidade nos processos, diminuição de falhas e retrabalho, além de melhorar a precisão e a qualidade dos serviços.

Contudo, pouco se discute sobre os riscos tecnológicos que os profissionais e as empresas, sendo de ramos diversos, estão enfrentando. O assunto é altamente relevante e precisa ser melhor apresentado aos contabilistas, visto que afeta uma característica importantíssima na contabilidade, a representação fidedigna, segundo o CPC[2] 00 (R2) item 2.13 "Para ser representação perfeitamente fidedigna, a representação tem três características. Ela é completa, neutra e isenta de erros. (...)", a literatura compreende que ter uma representação perfeita é uma raridade, contudo deve-se maximizar essas qualidades o tanto quanto possível.

Os riscos tecnológicos podem afetar a integridade das informações em decorrência da facilidade de acesso aos bancos de dados das empresas, no qual ao investirem na automatização dos processos, com uso de softwares e dispositivos autônomos, informações importantes as atividades da empresa são disponibilizadas nesses meios e viram alvos para ataques e invasões por cibercriminosos, que podem facilmente manipular as informações conforme suas intenções.

[2] Comitê de Pronunciamentos Contábeis

Além disso, segundo a empresa de consultoria alemã Roland Berger, o Brasil foi o 5° país com mais ataques cibernéticos em 2021, no qual só no primeiro trimestre houve 9,1 milhões de ocorrências, os hackers ao invadirem os sistemas integrados, softwares e meios de armazenamento de informações buscam por materiais sigilosos, assim objetivando aplicar novos golpes e fraudes com o uso desses dados, como também adquirir recursos financeiros através de chantagens e ameaças de divulgação.

Neste contexto, o estudo sobre os riscos tecnológicos à contabilidade, em decorrência do uso equivocado das ferramentas de automação dos processos é justificado pela necessidade do contador conhecer as ameaças que podem impactar suas atividades, como também fazer uso de áreas de atuação contábeis para investigar e combater as práticas criminosas.

1.3. OBJETIVOS

Essa pesquisa tem por objetivos descrever as influências dos avanços tecnológicos na ciência contábil e a importância de buscar conhecimentos nessa área para o aperfeiçoamento profissional.

1.3.1. Objetivo Geral

Identificar os principais riscos tecnológicos que podem impactar no objetivo da contabilidade, no qual compreende fornecer informações úteis a seus usuários para a tomada de decisões, ademais apontar áreas de atuação na contabilidade que podem auxiliar no combate as condutas criminosas.

1.3.2. Objetivos Específicos

De acordo com a proposta do objetivo geral, os objetivos específicos foram definidos:

I. Identificar os principais riscos tecnológicos, no qual os contabilistas e empresas estão sujeitos;

II. Estabelecer os principais conhecimentos necessários à prevenção de ameaças tecnológicas;
III. Avaliar áreas de conhecimento contábil que podem auxiliar no entendimento e investigação de cibercrimes;
IV. Verificar o plano de ensino das Universidades Federais do Nordeste e comparar ao modelo de currículo da ISAR/UNCTAD/ONU (2011) e minuta Proposta de Resolução (2022) do CFC; e
V. Averiguar a opinião dos alunos de Ciências Contábeis sobre a importância do tema e a necessidade de maior conhecimento do assunto para o futuro da profissão**.**

2. REFERENCIAL TEÓRICO

Conforme Trombetta e Trombetta (2016, p. 105) *apud* Coelho e Lins (2010), a contabilidade busca “informações precisas para proporcionar cada vez mais ganhos”, como também os reflexos sociais, políticos e econômicos da sociedade, desta forma sendo considerada por muitos autores uma ciência social aplicada, nesse contexto procura-se compreender como a contabilidade se desenvolveu até a informatização para então descrever os riscos tecnológicos que a impactam.

2.1 OS AVANÇOS TECNOLÓGICOS DA CONTABILIDADE

Os avanços tecnológicos impactam fortemente no desenvolvimento da contabilidade, no qual inicialmente desempenhava suas atividades de forma manual, como descreve no Código Comercial de 1850, art. 35, item 3, havia na época “os feitores, guarda-livros e caixeiros”, agentes auxiliares do comércio que realizavam a escrituração e contabilidade das empresas.

No século XX houve a introdução das máquinas de escrever portáteis e elétricas, no qual contribuíram no desenvolvimento econômico e social de escritórios, repartições públicas e nos setores de comércio e serviço, desta forma proporcionando maior rapidez e uniformidade da escrita (MOUTINHO, 2011).

Com o uso das máquinas de escrever a forma de desempenhar as atividades contábeis torna-se maquinizada / mecânica, no qual começaram a desenvolver máquinas com pequenos ajustes para a aplicação da tecnologia de reprodução decalcada[3], a fim de melhor atender aos serviços contábeis, assim construíram máquinas manuais para os lançamentos com uma única operação simultânea nos livros diário e razão. (CONSENZA; ROCCHI, 2014) Contudo com o desenvolvimento de computadores e redes de comunicação o uso desses equipamentos e sistemas entrou em desuso e a contabilidade passou a desenvolver suas funções de forma informatizada.

A informática no Brasil é compreendida em duas fases, sendo a primeira entre 1958 a 1970, no qual importava equipamentos de empresas multinacionais e a segunda a partir de 1974, com o estabelecimento de “bases e diretrizes de uma

[3] Método utilizado na contabilidade manual, em que usava um papel de carbono para transferir os lançamentos de uma folha á outra por pressão ou cópia.

política nacional de informática, e os meios de ação para implementá-la, com o contingenciamento das importações e a reserva de mercado na faixa dos minicomputadores". (MARCELINO, 1983, p. 1)

A política de fomento a informática contribuiu para maior adesão de equipamentos tecnológicos nas empresas e escritórios contábeis, assim tornando as atividades contábeis mais rápidas e eficientes, entre as vantagens que a informatização proporcionou tem-se: melhoria nos serviços prestados, aumento da produtividade, segurança das informações, facilidade no manuseio e modificações nos relatórios. (OLIVEIRA, 1997)

Além disso, com o desenvolvimento de softwares que auxiliam na execução das atividades contábeis a Receita Federal começa a adotar mudanças para a entrega da declaração de renda da pessoa jurídica, na época conhecida como DIPJ, no qual após o preenchimento das informações nos sistemas informatizados, gerava-se o arquivo, armazena-o em um disquete e entregava a Receita Federal, o mesmo procedimento também começou a ser desempenhado para as declarações de renda da pessoa física (HERNANDES, 2018, p. 39).

Assim, pode-se entender que a adesão aos processos informatizados no Brasil se deu por imposição da Receita Federal, em que ao ditar as regras para entrega do imposto de renda fez com que as empresas e escritórios contábeis se adequassem quanto aos sistemas tecnológicos, tornando-se imprescindível a continuação da entidade sem a informatização.

Atualmente, os escritórios contábeis para a realização das suas atividades necessitam de equipamentos de hardware e software, no qual conseguem proporcionar maior agilidade, qualidade e a automação dos processos, entre os elementos indispensáveis têm-se: os sistemas ERP (Enterprise Resource Planning), no qual centraliza todas as informações da empresa em um só aplicativo, assim facilitando o fluxo de dados, diminuindo erros e custos a entidade; armazenamento nas nuvens; e rede de computadores, como a LAN (Local Area Network) e a VPN (Virtual Private Network).

Além do uso de equipamentos e dispositivos intangíveis que auxiliam na execução das atividades, os profissionais precisam também se atualizar quanto aos meios de contato e interação com os clientes através de redes sociais, e-mail, WhatsApp corporativo e aplicativos para reuniões remotas.

2.2 RISCOS TECNOLÓGICOS QUE IMPACTAM A CONTABILIDADE E EMPRESAS

Segundo o relatório *Digital* 2022 *April Global Statshot* da Datareportal (2022), mais de 05 bilhões de pessoas no mundo têm acesso a Internet, ou seja, 63% da população total do planeta está online e tendo a oportunidade de acessar informações através da Internet. Contudo, proporcionalmente ao aumento de usuários online há também o crescimento de práticas criminosas no ambiente digital.

Os riscos e ameaças tecnológicas conseguem impactar as empresas através da identificação de vulnerabilidades que ela apresenta, conforme Turban *et al* (2010), as vulnerabilidades de sistemas de informação podem ser classificadas como não intencionais e intencionais, no qual os não intencionais podem ser de três tipos, sendo: erros humanos, riscos ambientais e falhas de sistema de computador.

Os erros humanos apresentam-se no projeto do hardware, na utilização de softwares, programação, coleta, entrada de dados, enfim os erros derivados da capacidade humana são os que mais contribuem para os problemas de controle e segurança das entidades.

Já os riscos ambientais podem ser de grande proporção, como terremotos, vulcões, inundações, no qual o meio, região onde a empresa está localizada sofre com algum fenômeno da natureza e os de pequena proporção, como incêndios, em que a fumaça, calor e água podem danificar os equipamentos e sistemas de informação. E as falhas de sistema de computador, que ocorrem por uso de materiais precários e com defeito, que funcionam de forma inadequada e causam a perda de informações pela empresa.

Quanto às vulnerabilidades intencionais, são brechas que os criminosos como *Hackers* ou mais precisamente *Crackers*[4]*,* podem encontrar nos sistemas de informação e rede das organizações, desta forma conseguindo acesso para a prática de crimes, que incluem:

> roubo de dados; uso indevido de dados (por exemplo, na manipulação de entradas); roubo de tempo de computador *mainframe*; roubo de equipamento e/ou programas; manipulação deliberada no tratamento, na

[4] Cracker é o nome técnico para hackers que usam seus conhecimentos negativamente, invadindo redes, violando sistemas.

> entrada, no processamento, na transferência ou na programação de dados; greves trabalhistas; revoltas ou sabotagem; dano malicioso a recursos de computador; destruição por vírus e ataques semelhantes; e abusos de computador diversos e fraude na Internet. (TURBAN et al, 2010)

Os riscos e crimes cibernéticos também se apresentam de outras formas, como por meio da espionagem industrial, em que o infrator busca obter informações, acesso a dados sigilosos das empresas, a fim de usufruir de vantagens financeiras, sociais e materiais. Esse tipo de risco, também pode ser caracterizado como estelionato, quando segue os requisitos de “obtenção de vantagem ilícita; causar prejuízo a outra pessoa; uso de meio de ardil, ou artimanha; enganar alguém ou levá-lo a erro”, de acordo com o Art. 171 do Decreto-Lei nº 2.848, de 07 de dezembro de 1940. (BRASIL, 1940)

Segundo Branco (2022), o roubo de identidades é também muito comum no meio digital, invadindo o banco de dados das empresas, os criminosos conseguem o Cadastro da Pessoa Física (CPF) e dados do cartão de crédito, como senhas e limite bancário dos clientes, assim põem em riscos a identidade e segurança das vítimas, no qual essas informações são usadas para extorsão, roubo, empréstimo indevido e podem ser comercializadas no mercado clandestino, como *Deep Web* e *Dark Web*.

Além disso, a adulteração de dados também é um crime que impacta grandemente as empresas, visto que por vezes é realizada por funcionários internos, assim com acesso aos documentos e softwares os infratores conseguem fraudar, alterar e/ou excluir dados existentes. (TURBAN, 2010) Desta forma, as informações passam a conter erros e parcialidade, podendo ferir a fidedignidade dos dados, principalmente financeiros.

Ademais, outros fatores de responsabilidade da empresa também proporcionam vulnerabilidades e má gestão da segurança da informação. Geralmente, a diretoria visando à segurança dos dados investe massivamente nos aspectos tecnológicos, como: vírus, computadores, Hackers e Internet. Contudo, não se relacionam a aspectos físicos e humanos, que também são essenciais para a garantia da seguridade. (SÊMOLA, 2003)

Além disso, segundo Sêmola (2003, p. 20) alguns “pecados” praticados podem afetar a empresa negativamente, como:

> Atribuir exclusivamente à área tecnológica a segurança da informação; Posicionar hierarquicamente essa equipe abaixo da diretoria; Definir investimentos subestimados e limitados à abrangência dessa diretoria; Elaborar planos de ação orientados à reatividade; Não perceber a interferência direta da segurança com o negócio; Tratar as atividades como despesa e não como investimento; Adotar ferramentas pontuais como medida paliativa; Satisfazer-se com a sensação de segurança provocada por ações isoladas; Não cultivar corporativamente a mentalidade de segurança; Tratar a segurança como um projeto e não como um processo. (SÊMOLA; 2003, p. 20)

Vale salientar, que esses pecados tendem a aumentar quando a empresa não mapeia, identifica as ameaças, riscos que podem vir a impactá-la, assim precisando de um serviço personalizado de gestão de segurança para garantir a qualidade do serviço, visto que cada empresa possui suas próprias características. (SÊMOLA, 2003)

Quanto aos impactos dos riscos tecnológicos à contabilidade, todo e qualquer fator que possa lesar as atividades operacionais da empresa afetam a contabilidade, principalmente quando visam o financeiro, que é o principal objetivo dos ataques cibernéticos.

Além disso, segundo Crepaldi (2010, p. 06) “o ato intencional de omissão ou manipulação de transações e operações, adulteração de documentos, registros, relatórios, informações de demonstrações contábeis (...)”, conforme a definição de fraude, também proporciona fragilidade às operações da empresa e resultam na contabilidade.

Visto que, de acordo com o CPC 00 (R2) os relatórios para fins gerais, como balanço patrimonial, demonstração do resultado, fluxo de caixa e outros, tem por objetivo fornecer informações úteis à “tomada de decisões referente à oferta de recursos à entidade”, além de apresentar características qualitativas fundamentais e de melhoria a garantir a representação fidedigna das informações.

2.2.1 Técnicas Antiforenses

As técnicas antiforenses (TA), segundo Melo (2018) são técnicas empenhadas para dificultar a identificação e investigação de dados periciais, assim apagando ou ocultando informações, ofuscando arquivos e ataques contra as ferramentas forenses. Além disso, são métodos também utilizados por aqueles que

desejam preservar a privacidade e destruir dados de forma segura, como: agentes da lei, jornalistas, pesquisadores, políticos e outros.

Hassan (2019, p. 263) descreve 05 (cinco) técnicas mais utilizadas, sendo: “técnica de ocultação de dados (esteganografia); técnica de destruição de dados (antirrecuperação); técnicas de criptografia; técnicas criptografia de anonimato; ataques diretos contra ferramentas de computação forense”.

A técnica de esteganografia visa ocultar a informação no arquivo hospedeiro sem danificar seu funcionamento, normalmente a técnica é empregada em imagens, vídeos, áudio, no qual armazena a mensagem de forma sútil e sem alterar sua estrutura, tamanho. (VECCHIA, 2019)

Um dos exemplos mais antigos de esteganografia são as mensagens por hieróglifos dos egípcios, no qual cada hieróglifo continha mensagens subliminares, como na Figura 01.

Figura 01: Hieróglifos

Fonte: Centro de Tecnologia – COPPE – GTA da UFRJ[5]

Já as técnicas de destruição de dados, são métodos usados para tornar impossível a recuperação das informações por meio das ferramentas especializadas. Existem três maneiras de destruir os dados, sendo: destruição física; técnica de desmagnetização; e destruição lógica (sanitização). (HASSAN, 2019)

[5] Disponível em: <https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/esteganografia/>

Segundo o autor, a destruição física refere-se a perda total de disco rígido, cartões de memória, fitas magnéticas e usa-se o equipamento “triturador de unidade de disco rígido”. A técnica de desmagnetização visa expor dispositivos que tenham armazenamento magnético, como HDD (Hard Disk Drive) ao campo de um desmagnetizador, desta forma conseguindo eliminar os dados do dispositivo.

E a destruição lógica (sanitização), é a técnica mais utilizada, visto que é uma ferramenta de limpeza, assim elimina os dados sem danificar o *hardware* que os contém. Não é totalmente garantida, uma vez que não elimina dados de armazenamentos magnéticos e há softwares que conseguem recuperar dados já removidos. (HASSAN, 2019)

A técnica de criptografia pode ser utilizada para ocultação e proteção dos dados, visto que ela converge dados legíveis em ilegíveis utilizando chaves para codificar e decodificar as informações.

Há dois tipos de chaves, sendo as simétricas, no qual utiliza apenas uma chave secreta para codificar e decodificar as informações, assim buscando a confiabilidade dos dados, contudo caso a chave caia em mãos erradas, o sistema inteiro estará comprometido. (CERT.br, 2012)

Já as assimétricas, se utilizam de duas chaves sendo uma pública que pode ser divulgada a quem deseja manter contato e uma chave privada, nesse método a chave que codifica não pode ser usada para decodificar, assim as chaves estão matematicamente associadas e proporcionam maior segurança às informações. (CERT.br, 2012)

As técnicas criptográficas de anonimato utilizam “algoritmos de criptografia e *software* de anonimato criptográfico para ocultar a identidade durante a transmissão”. Assim os usuários fazem o uso de redes anônimas como a TOR para ocultar o seu verdadeiro endereço de IP, um endereçamento único que cada dispositivo conectado à rede possui, assim quando ocultado o verdadeiro IP, não tem como saber a origem daquele usuário, desta forma facilitando a prática de crimes e dificultando o rastreamento dos infratores. (HASSAN, 2019, p. 277)

E os ataques diretos contra ferramentas de computação forense, no qual os cibercriminosos utilizam “empacotadores de programas (program packers), técnicas

antiengenharia reversa e ataque à integridade da evidência digital obtida durante a investigação. Se bem-sucedidos, eles podem prejudicar a credibilidade da evidência durante o processo judicial". (HASSAN; 2019, p. 278)

2.3 SOFTWARES MALICIOSOS: MÉTODOS DE ATAQUES

O desenvolvimento da tecnologia proporcionou ao mundo diversos benefícios no ambiente digital, assim ampliando o acesso à informação e auxiliando nas atividades do cotidiano de empresas e usuários em geral. Segundo Carvalho (2022), atualmente é difícil encontrar alguém ou algo que não dependa de algum dispositivo de computação para armazenar dados, se comunicar ou se informar. Nos Estados Unidos, 64% das moradias utilizam o serviço e a tendência é de alta, mesmo após a pandemia.

Proporcionalmente ao crescimento do uso de sistemas computadorizados, tem-se o aumento da insegurança cibernética, visto que nos últimos anos os métodos de ataques se aperfeiçoaram, utilizando dispositivos de computação e/ou redes de computadores como a Internet para a prática de delitos.

Os escritores Wendt e Jorge (2013, p.18-20) utilizam a expressão "condutas indevidas praticadas por computador" para se referirem aos crimes por intermédio de computadores, no qual divide as condutas em dois tipos, sendo: ações prejudiciais atípicas e crimes cibernéticos, no qual o último é subdividido em crimes cibernéticos abertos e crimes exclusivamente cibernéticos.

Segundo os autores, as "ações prejudiciais atípicas" são condutas que utilizam a internet, causam transtornos, prejuízos para as vítimas, mas que não tem previsão penal para o infrator, quanto aos "crimes cibernéticos abertos" são atos que podem ser praticados de forma tradicional ou com o uso de computadores. Já os "crimes exclusivamente cibernéticos" são práticas somente desenvolvidas por intermédio de computadores ou demais dispositivos que possibilitem o acesso à internet. No Quadro 01 tem alguns exemplos de atividades desempenhadas.

Quadro 01: Condutas indevidas praticadas por computadores

CONDUTAS INDEVIDAS PRATICADAS POR COMPUTADOR		
AÇÕES PREJUDICIAIS ATÍPICAS	**CRIMES CIBERNÉTICOS ABERTOS**	**CRIMES EXCLUSIVAMENTE CIBERNÉTICOS**

✓Invasão de computador sem o fim de obter, adulterar ou excluir dados e informações. ✓Difusão de *phishing scam*	✓Crimes contra honra ✓Ameaça ✓Pornografia infantil ✓Estelionato ✓Furto mediante fraude ✓Racismo ✓Apologia ao crime ✓Falsa identidade ✓Concorrência desleal ✓Tráfico de drogas	✓Invasão de computador mediante violação de mecanismo de segurança com o fim de obter, adulterar ou excluir informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. ✓Interceptação telemática ilegal ✓Pornografia infantil por meio de sistema de informática ✓Corrupção de menores em sala de bate papo ✓Crimes contra a urna eletrônica

Fonte: Wendt e Jorge (2013, p. 20)

O cibercrime, segundo definição do Departamento de Justiça dos Estados Unidos (DOJ, Department of Justice) é “qualquer ofensa criminal contra ou com o uso de um computador ou rede de computadores”, e que tem como principal objetivo o ganho financeiro, como o roubo de senhas e códigos de acesso a contas bancárias.

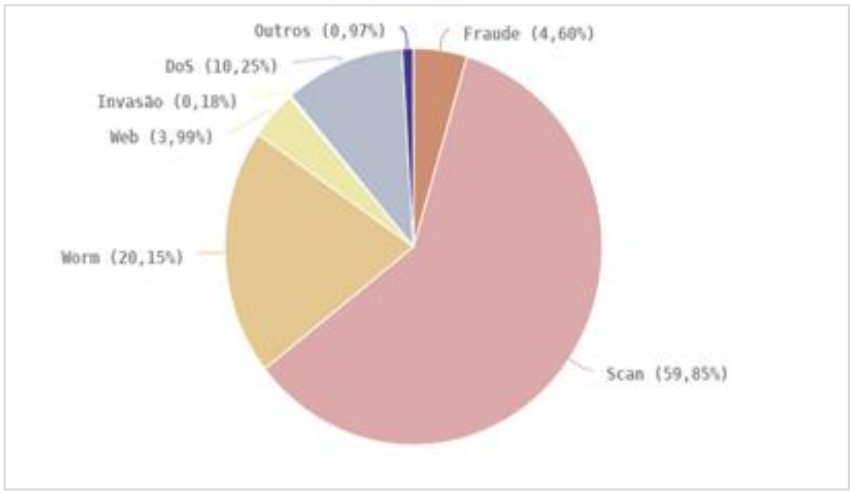
Segundo Hassan (2019), o cibercrime origina-se de duas fontes, sendo os ataques internos e externos. Os ataques internos são os mais perigosos e podem demorar a serem descobertos, visto que ocorrem com a quebra de confiança por pessoas, que tinham acesso ao sistema, como: ex-funcionários, sócios, profissionais terceirizados.

Já os ataques externos são executados fora da empresa-alvo, geralmente desempenhado por hackers experientes, que com o auxilio de algum funcionário da empresa ou por métodos próprios consegue invadir o sistema e ter o acesso ilegal.

Os criminosos, quando em uso de dispositivos de computação, geralmente o utilizam para três fins, sendo: o dispositivo como ferramenta para o crime, por exemplo: enviar um ransomware, ataques de negação do serviço (DoS); o dispositivo é o alvo do crime, assim o intuito é invadir o computador e o utilizar da forma que convier; e o dispositivo como facilitador do crime, quando utilizado para armazenar provas incriminatórias ou como meio de comunicação entre os infratores. (HASSAN, 2019)

Entre os softwares maliciosos (malwares) com maior incidência reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) no ano de 2020, destaca-se a Gráfico 01 abaixo.

Gráfico 01: Incidentes reportados ao CERT.br – Janeiro a Dezembro de 2020



Fonte: CERT.br[6]

O ataque por *Scan* ou por *Port Scanning Attack*, como é conhecido no meio digital, é um *malware* que é programado para fazer varreduras em redes de computadores, com a finalidade de identificar possíveis vulnerabilidades a serem exploradas. Já o *Worm*, é um software que se propaga automaticamente nas redes, enviando cópias de si mesmo, explorando a vulnerabilidade e/ou falhas na configuração de softwares já instalados no computador e tem a finalidade de consumir muitos recursos, assim diminuindo o desempenho dos sistemas. (VECCHIA, 2019, p. 38)

Os ataques por DoS (*Denial of Service*), segundo Vecchia (2019) são ataques que objetivam interromper atividades legítimas, como páginas *web*, sistemas *online*, visando à inutilidade ou lentidão do serviço por um determinado tempo. Os atacantes exploram alguma vulnerabilidade do dispositivo, software da vítima ou começam a enviar muitas requisições (mensagens), assim esgotando os recursos do dispositivo, como: processador, banda de rede e memória.

O uso de outros softwares para ataques cibernéticos também é muito frequentes, como: os vírus, que são uma categoria de *malwares* e que tem como principais características “a necessidade de execução para entrar em atividade e a realização de cópia de si próprio para novos arquivos ou agregando-se a outros (arquivos hospedeiros)” (VECCHIA, 2019). Esse *malware* geralmente infecta suas

[6] Acesso em 17/09/2022, disponível em: <https://cert.br/stats/incidentes/2020-jan-dec/tipos-ataque.html>

vítimas por abertura de anexos enviados por e-mail, instalação de softwares de origem duvidosa e conexão de um dispositivo infectado no computador, como *pen drive*.

O Cavalo de Troia é um tipo de *malware* que a princípio executa as funções previstas, contudo ao ser executado, instala um sistema espião oculto, assim conseguindo ter acesso a informações sensíveis, como senhas e a possibilidade de fazer cópias e manipular informações. (VECCHIA, 2019) Conforme o CERT.br a diversos tipos de *trojans* e eles são classificados de acordo com as ações criminosas descritas no Quadro 02.

Quadro 02: Tipos de Trojan

TIPOS DE TROJAN	
TIPO	**ATUAÇÃO**
Downloader	Instala outros *sofwares* maliciosos utilizando a Internet
Dropper	Instala outros códigos *malware*, embutidos do próprio código *trojan*
Backdoor	Adiciona *backdoors*, assim liberando o acesso remoto do atacante
DoS	Instala ferramentas de negação do serviço e as usa para ataques
Destrutivo	Modifica, excluir arquivos e pode deixar o computador inoperante
Clicker	Redireciona o usuário para sites específicos, como nas propagandas online
Proxy	Instala um servidor *proxy*, possibilitando o acesso do computador por navegação anônima e envio de spam
Spy	Instala o programa *spyware* e o uso para coleta de senhas e números de cartão de crédito
Banker ou Bancos	Semelhante ao *Spy*, porém visa a coleta de informações bancárias do usuário

Fonte: Adaptado do CERT.br (2012, p. 28-29)

O *Spyware* e *Adware* são *softwares* do tipo espiões e podem ser de uso legítimo ou não, o *spyware* monitora os acessos e informações de computadores, desta forma podendo atuar como método de segurança da informação pela empresa, mas também pode ser interpretado como sistema de invasão de privacidade, quando utilizado sem a autorização ou aviso aos usuários. Já o *adware*, atua de outra forma, visto que é um programa que exibe anúncios conforme os acessos no computador, assim rastreando a movimentação dos internautas nos dispositivos conectados a Internet.

O Backdoor, conforme CERT.br (2012, p. 28) “é um programa que permite o retorno de um invasor a um computador comprometido, por meio de inclusão de serviços criados ou modificados para este fim.” Assim, quando instalado possibilita o acesso futuro do criminoso, não necessitando investir novamente em métodos de invasão e infecção do dispositivo, além do fato de raramente ser notado.

Um dos *malwares* mais utilizados na atualidade para ataques as empresas é o *Ransomware*, no qual tem por objetivo negar o acesso do usuário aos arquivos da rede e do computador, assim usando técnicas como a criptografia para embaralhar os dados e impossibilitar a descodificação sem as chaves pública e privada do usuário. Normalmente, os criminosos solicitam que a vítima pague o resgate para liberar o acesso às informações.

Conforme o relatório *Fast Facts* da empresa *Trend Micro*, o Brasil é o quarto país com mais ataques de *ransomware* no mundo, ficando atrás somente de Taiwan, Japão e Estados Unidos. Só nos primeiros seis meses de 2022 foram mais de 08 milhões de casos no Brasil, no qual 3,8 milhões foram desferidos ao setor governamental, em que visam principalmente às áreas da educação, indústria, seguros e saúde. (ISTO É DINHEIRO, 26/08/2022)

Além dos métodos que utilizam o computador como meio para a prática de crimes, outro tipo de ataque também pode ser realizado utilizando truques psicológicos e emocionais das vítimas, esse tipo de ataque caracteriza-se como Engenharia Social, no qual os criminosos visam ludibriar as vítimas, de forma a convencê-las a disponibilizar as informações requeridas, visto que eles utilizam instituições confiáveis, órgãos do governo para garantir a veracidade. Não há um método definido de ataque, os cibercriminosos utilizam a criatividade e possíveis vulnerabilidades das vítimas para aplicarem golpes. (WENDT; JORGE, 2013)

2.4 PREVENÇÃO DE AMEAÇAS: CONHECIMENTOS BÁSICOS

Um dos fatores que contribuem para as vulnerabilidades do ciberespaço das empresas é a falta de conhecimento das pessoas que lidam, desenvolvem suas atividades em computadores, redes, e-mails e demais dispositivos e meios de contato à Internet. Essas pessoas, por vezes, não são treinadas, preparadas para o ambiente e equipamento de uso, assim podendo colocar a empresa em risco.

Além de conhecer os softwares maliciosos e como eles atuam, demais conhecimentos também são importantes para a prevenção de ameaças tecnológicas e a segurança da informação.

Segundo a “ABNT NBR ISO/IEC 27002: 2005 – Código de prática para gestão da segurança da informação”, a Segurança da Informação (SI) pode ser compreendida como um conjunto de medidas a garantir a proteção das informações de diversos tipos de ameaças, assim incluindo “políticas, processos, procedimentos, estruturas organizacionais, e funções de *software* e *hardware*”, desta forma buscando a continuidade da entidade e minimização de riscos.

O autor Vecchia (2019) descreve 03 (três) elementos básicos do SI, sendo: os mecanismos, políticas e cultura. Os mecanismos de proteção se apresentam de duas formas, podendo ser físicos com a implementação de barreiras, cadeados, cofres e meios de comunicação biométrica, e os mecanismos lógicos, no qual protegem de acessos ao meio digital indevidamente.

Entre as políticas do SI tem-se a Política de Segurança da Informação (PSI), documento que visa prover “uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”. (ABNT NBR ISO/IEC 27001, 2006)

Como Oliveira (2007, p.166-167) descreve, a PSI deve ser desenvolvida por um grupo contendo pessoas de diversas áreas do negócio, sendo o RH, o jurídico, o TI, a fim de construir uma política corporativa, assim o grupo deve criar um comitê e “zelar pelo cumprimento, divulgação, atualização e conscientização”, do documento.

O PSI é um contrato que visa definir direitos e responsabilidades, esclarecendo o que as pessoas vão fazer, conforme sua função e como devem usar o sistema, desta forma orientando quanto ao acesso de sítios inadequados e práticas indevidas com os equipamentos da empresa, ademais é um instrumento que dá suporte legal a empresa e ao funcionário. (VECCHIA, 2019)

Já a cultura, relaciona-se ao uso dos sistemas, *softwares*, pelos colaboradores e os impactos que a falta de conhecimento de como utilizar os equipamentos de forma segura pode colocar a entidade em risco, assim a organização deve procurar investir em treinamentos, palestras aos funcionários e

orientá-los amplamente dos riscos que o vazamento de informações da empresa pode proporcionar, por exemplo: o descarte indevido de papéis, no qual contém dados cadastrais de clientes. (VECCHIA, 2019)

As propriedades que mais representam os objetivos do SI são a confidencialidade, integridade e disponibilidade, que juntas formam a sigla CID, conforme definidas pela ISO/IEC 13335-1:2004:

> **"Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados";
>
> **"Integridade**: propriedade de salvaguarda da exatidão e completeza de ativos[7]";
>
> **"Disponibilidade**: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada".

Além dos conhecimentos expostos, há ferramentas e medidas defensivas que auxiliam na segurança dos dispositivos e informações, para O'Brien (2010, p.382-390) destaca-se: criptografia; firewalls; defesas contra a negação de serviços (DoS); monitoramento de e-mail; defesas de vírus (antivírus); códigos de segurança; cópias de segurança (*backup*); monitores de segurança de sistemas; controles biométricos; controles de falhas no computador; sistemas tolerantes a falhas; e recuperação de desastres.

Firewall, ou parede de fogo, é um recurso que pode se apresentar como software ou hardware, dependendo da necessidade e fluxo de informações da empresa, é responsável por filtrar as informações que chegarem à rede, assim caso o *firewall* detecte que o dado é malicioso, seu acesso não será permitido e será imediatamente bloqueado. (COSTA, 2020)

Cópias de Segurança (Backups) são medidas defensivas extremamente importantes para a salvaguarda das informações, visto que o procedimento permite a proteção de dados, recuperação de versões e arquivamento, contudo precisa-se de atenção quanto a gravar os backups, utilizando *pen drive*, CD, DVD, armazenamento nas nuvens; quais dados copiar, assim precisando verificar a confiabilidade dos arquivos, se não contém vírus e demais softwares maliciosos; e a

[7] A compreensão de ativo, segundo o ISO/IEC 13335-1:2004 é "qualquer coisa que tenha valor para a empresa".

periodicidade das cópias, no qual depende da frequência de uso e modificação dos documentos. (CERT.br, 2012)

E um método importante para segurança do perímetro é o uso de uma Rede Privada Virtual (Virtual Private Networking – VPN), no qual utilizam a criptografia combinada ao *firewall* para “permitir apenas tráfego filtrado e anônimo entre a rede privada e a Internet pública”, assim garantindo a comunicação direta com a rede local da empresa. (TURBAN, 2010)

Turban (2010, p.656) também apresenta alguns objetivos das estratégias de defesa para a prática de gestão de segurança de TI, conforme o Quadro 03, que auxilia a empresa a estabelecer métodos de defesa e prevenção às ameaças.

Quadro 03: Estratégias de Defesa

Estratégias de Defesa	
Tipo de Defesa	**Atuação**
Prevenção e Desencorajamento	Uso de sistemas que possam deter a ação de criminosos e negar acesso a pessoas não autorizadas
Detecção	Uso de software com diagnóstico especial, ao ser detectado alguma falha ou ataque
Limitação do dano	Estabelecer um sistema tolerante a falhas, que permita a utilização das operações de modo degradado até que a recuperação completa seja feita
Recuperação	Definir um plano de recuperação que possa corrigir o sistema danificado o mais rápido possível
Correção	Identificar as causas dos problemas anteriores e corrigi-las
Conscientização e fiscalização de normas/regulamentos	Consciência dos perigos e fiscalização quanto ao cumprimento de regras e regulamentos

Fonte: Adaptado de Turban (2010, p. 630)

2.5 A ATUAÇÃO CONTÁBIL FRENTE AO CIBERCRIME

A contabilidade, segundo Coliath (2014) na percepção como ciência social tem como objetivo ser um instrumento de medição e mediação, no qual interage com os aspectos quantitativos e qualitativos que as relações humanas e sociais recebem em decorrência das prestações de contas disponibilizadas. Desta forma, a Ciência Contábil busca fornecer informações que possam interligar a exatidão dos números aos elementos sociais, políticos e culturais da sociedade.

Assim, com o desenvolvimento tecnológico e maior dependência a dispositivos, softwares conectados a Internet, os profissionais contábeis precisam

buscar a especialização de suas funções para além das atividades tipicamente contábeis e financeiras, ampliando a percepção para as necessidades do mercado e aspectos que podem impactar na confiabilidade das informações divulgadas.

Enquanto presidente do CFC, o Sr. Zulmir Ivânio Breda (2019, p. 01) descreve que o contador na preparação das demonstrações contábeis, como também o auditor ao revisar os demonstrativos “têm o compromisso público de levar toda a verdade aos usuários das informações produzidas. Esta é a postura que a sociedade espera do profissional da contabilidade e é, também, a única razão pela qual a profissão é regulamentada em lei”.

Entre as áreas de atuação da contabilidade que podem cooperar com o combate aos crimes cibernéticos, tem-se: a auditoria, perícia e a contabilidade forense.

A auditoria, conforme objetivos do auditor, busca identificar riscos de distorções que se apresentam nos demonstrativos financeiros decorrentes de fraudes, assim procurando obter evidências para conseguir responder corretamente em caso de fraude ou suspeita de fraude. (NBC TA 240, 2016)

A concepção de fraude pela NBC TA 240 (2016, p. 04) é de um “ato intencional de um ou mais indivíduos da administração, dos responsáveis pela governança, empregados ou terceiros, que envolva dolo para obtenção de vantagem injusta ou ilegal”. Desta forma a auditoria tem a responsabilidade de garantir a segurança razoável dos demonstrativos financeiros, ilustrando que não há distorções relevantes por fraude e erros. (NBC TA 240, 2016)

A Public Company Accounting Oversight Board (PCAOB), ou seja, o Conselho de Auditores de Companhias Abertas que estabelece as normas de auditoria para empresas sujeitas à Lei Sarbanes Oxley (SOX), conforme palestra de Hamm (2019) descreve que a princípio a atuação dos auditores a incidentes relacionados à segurança cibernética é limitada, visto que caso a empresa divulgue os impactos de ataques cibernéticos o auditor verificará se a escrituração das contas e menção ao fato está de acordo com os princípios contábeis e caso não haja divulgação da informação e o auditor venha a ter acesso, ele só precisará saber se o fato apresenta distorção relevante ou inconsistente para as demonstrações financeiras.

Contudo, segundo a Hamm (2019) essa metodologia não consegue avaliar o risco de auditoria, desta forma o auditor deve procurar compreender o ambiente interno e externo da empresa, assim avaliando sistemas de TI que sejam relevantes para relatórios financeiros, como subsistemas relacionados, independentemente se há incidência ou não, o objetivo é planejar e caso necessite executar procedimentos para lidar com os riscos cibernéticos que possam ter efeito material nos demonstrativos.

> Como parte da avaliação de risco, acredito que o auditor também deve entender os métodos usados pela empresa para prevenir e detectar incidentes cibernéticos que possam ter um efeito material nas demonstrações financeiras: os processos da empresa que bloqueiam e identificam tentativas de transações ou acesso não autorizados aos ativos, bem como a familiaridade dos funcionários com esses processos. Outras áreas de foco devem incluir os processos da empresa para avaliar e tratar de incidentes cibernéticos relevantes, uma vez identificados. Isso inclui entender, por exemplo, como a empresa garante a avaliação oportuna e a geração de relatórios de incidentes cibernéticos materiais. Também inclui como a empresa garante o encaminhamento adequado ao conselho e a consideração oportuna das obrigações de divulgação para investidores e outros. (HAMM, 2019)[8]

Desta forma, o serviço de auditoria procurando desenvolver um plano de ação em caso de identificação de incidentes cibernéticos, alinhando conhecimentos financeiros, contábeis e de cyber segurança, poderá ser uma aliada ao departamento de segurança da informação da empresa, reportando à administração ou responsáveis da governança a identificação e “respostas aos riscos de fraude na entidade”. (NBC TA 240, 2016)

Enquanto a auditoria visa à análise dos demonstrativos financeiros por amostragem de um período específico, a fim de verificar se a entidade está em conformidade com os padrões, regras e leis vigentes, para a elaboração do parecer. A perícia contábil se apresenta como um “conjunto de procedimentos técnicos e científicos destinados a levar à instância decisória elementos de prova necessários a subsidiar à justa solução do litígio, mediante laudo pericial contábil e/ou parecer pericial contábil, (...)”. (NBC TP 01, 2020)

Desta forma a perícia busca investigar, analisar a matéria periciada respondendo aos quesitos formulados pelas partes contratantes, sendo nas esferas judicial, extrajudicial ou arbitral.

[8] Disponível em: <https://pcaobus.org/news-events/speeches/speech-detail/cybersecurity-where-we-are-what-more-can-be-done-a-call-for-auditors-to-lean-in_700> sob tradução do Google.

Segundo Turban (2010) a perícia forense aplicada à informática pode ser utilizada para descoberta de “ataques de hackers, invasões, fraudes, roubos de propriedade intelectual, violação de normas da empresa (...) e outras atividades criminosas”.

Além disso, existem fraudes de computador ou eletrônicas, que são crimes informacionais que envolvem dinheiro, assim para a investigação desses crimes é essencial que o perito além de possuir conhecimentos de informática e *cyber security* tenha também noções de contabilidade.

A contabilidade forense, segundo Moreira (2009) é uma área do conhecimento que agrega diversos saberes, como “informática, psicologia, criminologia e investigação criminal”, com o objetivo de combater as fraudes.

Assim, é uma área da contabilidade que busca apurar atos intencionais que estão prejudicando a empresa ou pessoas específicas, desta forma utilizando diversos métodos e conhecimentos para conseguir comprovar as práticas criminosas. (SENA *et al*, 2020)

A contabilidade forense é uma área de atuação da Ciência Contábil voltada à investigação e apuração dos dados necessários à resolução de crimes contra o patrimônio e demais aspectos que podem vir a impactar na continuidade do negócio, assim é a área contábil mais relacionada ao combate da criminalidade.

A auditoria, perícia e a contabilidade forense são áreas da contabilidade que pelo desempenho das atividades e busca de especialização pelos profissionais podem vir a auxiliar no combate aos crimes cibernéticos e fazer parte da gestão de segurança de informação da entidade.

Contudo, cabe a todos os profissionais contábeis a preservação da qualidade da informação, assim ao verificar uma ameaça, risco que possa vir a influenciar, interferir no objetivo da contabilidade que é fornecer informações úteis à tomada de decisões, o profissional deve segundo os Deveres do Contador, item (i) “comunicar, desde logo, ao cliente ou ao empregador, em documento reservado, eventual circunstância adversa que possa gerar riscos e ameaças ou influir na decisão daqueles que são usuários dos relatórios e serviços contábeis como um todo”. (NBC PG 01, 2019)

2.6 A ABORDAGEM DO TEMA NA GRADUAÇÃO DE CIÊNCIAS CONTÁBEIS

A Resolução CNE/CES nº 10, de 16 de dezembro de 2004, instituiu as “diretrizes curriculares nacionais para o Curso de Graduação em Ciências Contábeis”. Desta forma, estabelecendo uma organização curricular que deve ser observada pelas Instituições de Ensino Superior (IES) por meio da aprovação do Projeto Pedagógico do curso.

A Resolução descreve capacidade, competências e habilidades que o curso de graduação em Ciências Contábeis deve possibilitar a formação do profissional, quanto à temática de tecnologia da informação, o dispositivo nos artigos 3º e 4º descreve:

> Art. 3º, item III – revelar capacidade crítico-analítica de avaliação, quanto às implicações organizacionais com o advento da tecnologia da informação. (...) Art. 4º, item VII – desenvolver, analisar e implantar sistemas de informação contábil e de controle gerencial, revelando capacidade crítico analítica para avaliar as implicações organizacionais com a tecnologia da informação. (RESOLUÇÃO CNE/CES nº 10, 2004)

Além disso, o artigo 5º ilustra que o currículo dos cursos de graduação devem ter conteúdos do “cenário econômico e financeiro, nacional e internacional”, de modo a proporcionar a harmonia entre as normas nacionais e estrangeiras e a formação exigida pela Organização Mundial do Comércio e peculiaridades de organizações governamentais, assim quanto a conteúdos de formação teórico-prática tem-se a orientação para a prática em softwares de contabilidade nos laboratórios de informática.

A ONU (Organização das Nações Unidas) por meio do ISAR *(Intergovernmental Working Group of Experts on International Standards of Accounting and Reporting)* da *UNCTAD (United Nations Conference on Trade and Development)* divulga em 2011 um modelo de currículo de contabilidade, em que no módulo 02 (dois) apresenta a tecnologia da informação.

O intuito da organização é descrever a importância do tema para “atender aos objetivos e necessidades do negócio e entender procedimentos para o

desenvolvimento, introdução e uso de sistemas baseados em computador"[9]. (ISAR/UNCTAD/ONU, 2011)

O ISAR/UNCTAD/ONU (2011), ainda descreve que o assunto não deve ser um fim em si mesmo e que deve ser ensinado com aplicação nas situações do negócio. Além disso, o documento também ilustra diversos fatores relacionados à tecnologia da informação, como: conceitos de TI, de acordo às funções contábeis; controles internos; gestão de adoção e implementação de TI; gerenciamento da segurança da informação; e comércio eletrônico.

Quanto ao gerenciamento da segurança da informação, orienta para o controle da integridade, privacidade e segurança dos dados; princípios da segurança da informação; melhores formas e abordagens para a implementação do tema; e o trade-off entre custo e valor da segurança.

Outro documento também analisado para a percepção da temática segurança da informação e tecnologia na formação dos profissionais contábeis foi a minuta colocada pelo CFC em audiência pública em 02 de maio de 2022 que propõe a atualização do currículo de Ciências Contábeis, assim alterando a então vigente Resolução CNE/CES nº 10/2004 que instituiu as diretrizes curriculares do curso.

Segundo o presidente do CFC, Sr. Aécio Dantas:

> Considerando o impacto dos profissionais da contabilidade na economia e no desenvolvimento sustentável do país, precisamos manter o currículo de Ciências Contábeis atualizado e alinhado com o mercado. Dessa forma, formaremos profissionais aptos a atuarem com excelência. (APEX, 2022)[10]

Desta forma, o CFC visa atualizar a base curricular dos cursos de graduação inserindo assuntos voltados à tecnologia, sustentabilidade, ciência de dados e outros. O Quadro 04 descreve competências e habilidades técnicas que os profissionais de contabilidade deverão aperfeiçoar, de acordo com a minuta divulgada.

Quadro 04: Competência e Habilidades Técnicas

[9] Tradução Nossa, original: "The objective of this module is to ensure that candidates appreciate the contribution of information systems to meet the goals and needs of business and to understand procedures for the development, introduction and use of computer-based systems."

[10] Disponível em: <https://cfc.org.br/noticias/profissional-da-contabilidade-fortalece-empresas-transforma-vidas-e-faz-o-pais-crescer/>

Competência Técnica	Habilidades
Compreender como a tecnologia da informação contribui para a análise de dados e geração de informação	**a)** saber usar o sistema de informação com uso da tecnologia para apoiar o processo de geração e interpretação da informação contábil; **b)** explicar como a tecnologia da informação contribui para análise de dados e tomada de decisão; **c)** conhecer tecnologias de captura, armazenamento, mineração e análise de dados.

Fonte: Adaptação Proposta de Resolução Oriunda do Conselho Federal de Contabilidade, Apêndice I, Quadro I (2022, p. 01)

3. PROCEDIMENTOS METODOLÓGICOS

O método utilizado na realização da pesquisa caracteriza-se como exploratório e descritivo, buscando descrever os principais riscos tecnológicos que afetam o objetivo da contabilidade, como também identificar e entender fenômenos com intuito de compreender seus aspectos, segundo Martins Junior (2008 apud ALVES, 2020).

Uma pesquisa exploratória tem por objetivo “proporcionar maior familiaridade com o problema com vistas a torná-lo mais explícito”, além disso, visa o “aprimoramento de ideias ou a descoberta de intuições”, por isso o método é visto como flexível e que possibilita a apresentação de diversos aspectos, desta forma sendo usado mais para pesquisas bibliográficos e estudos de caso. (GIL; 199, p. 41)

Já a pesquisa descritiva, segundo Malhota (2001) é um tipo de pesquisa conclusiva, que tem por “objetivo a descrição de algo”, como evento, fatos, características. Conforme Gil (2001, p. 45), esse tipo de pesquisa costuma utilizar “técnicas padronizadas de coleta de dados, tais como questionário e a observação sistemática”.

Além disso, a pesquisa utiliza como abordagem instrumentos qualitativos e quantitativos para a coleta de dados e comprovação das hipóteses levantadas. Segundo Oliveira, Ponte e Barbosa (2006), a pesquisa qualitativa busca “moldar a compreensão da pesquisa”, assim “respondendo a questões do tipo “o quê?,” “por quê?” e “como?””. E pelo aspecto quantitativo, utiliza de técnicas de estatística, como percentual, média, desvio-padrão, (...)”, para quantificar as informações coletadas. (RICHARDSON, 2012, p. 70)

Com isso, utilizou-se a pesquisa bibliográfica para a análise dos planos de ensino das Universidades Federais do Nordeste, levantando quais disciplinas atendem ao requisito de tecnologia da informação conforme o modelo de currículo de contabilidade revisado em 2011 pela ONU (Organização das Nações Unidas) através do *ISAR (Intergovernmental Working Group of Experts on International Standards of Accounting and Reporting)* da *UNCTAD (United Nations Conference on Trade and Development)*, e minuta proposta pelo CFC para alteração da Resolução CNE/CES nº 10, de 16 de dezembro de 2004 e medindo o percentual representativo

das disciplinas de tecnologia da informação quanto ao total de disciplinas ofertadas na estrutura curricular.

Além disso, realizou-se um questionário online contendo 18 (dezoito) questões fechadas e de múltipla escolha, de acordo com o apêndice A, através do *Google Forms* e tendo como população os alunos do curso de Ciências Contábeis da Universidade Federal de Pernambuco, matriculados nos 08 semestres disponíveis, nos turnos vespertino e noturno e nos formatos presencial e EAD. Ao todo foram respondidos 28 (vinte e oito) formulários que serão analisados para a apuração dos resultados, no qual se apresentará através de gráficos.

A pesquisa com os alunos buscou medir a importância do tema e a necessidade de mais conhecimento sobre os riscos tecnológicos e sua percepção sobre a abordagem na Universidade Federal de Pernambuco. Já a pesquisa bibliográfica teve a pretensão de analisar os planos de ensino e verificar como as universidades estão implementando temas relacionados à tecnologia da informação e os riscos tecnológicos na formação dos bacharéis em Contabilidade.

3.1 DESCRIÇÃO DAS GRADES CURRICULARES

3.1.1 Universidade Federal da Bahia (UFBA) – Campus Salvador

O curso de bacharelado em Ciências Contábeis foi criado em 22 de setembro de 1945 pelo Decreto-Lei nº 7.988, a princípio com o nome de Ciências Contábeis e Atuariais. O desmembramento dos cursos só aconteceu em 1951 e desde então apenas o curso de Ciências Contábeis é ofertado pela Universidade.

Segundo o Projeto Pedagógico do Curso de Ciências Contábeis (noturno) ano 2008, disponibilizado no sítio[11] do departamento de Contábeis, atualmente o curso é normatizado pela Resolução CNE/CES nº. 10/2004 e pelo Parecer CNE/CES nº. 329/2004, assim definindo a carga horária em 3.026 horas, com duração mínima de quatro anos e meio ou nove semestres, e com máxima de oito anos ou dezesseis semestres.

Conforme o artigo 5º da Resolução CNE/CES nº 10/2004, o curso contempla três tipos de formação, sendo a formação básica, profissional e teórico-prático, além

[11] Disponível em: https://contabeis.ufba.br/projeto-pedagogico-do-curso-de-ciencias-contabeis-noturno/

das disciplinas optativas. Das 69 (sessenta e nove) disciplinas disponíveis ao aprimoramento dos alunos, verificou-se que apenas 03 (três) compõem o item 02 – Tecnologia da Informação do ISAR/UNCTAD/ONU ou a competência em tecnologia da informação e análise de dados da minuta do CFC, sendo elas: Informática Aplicada à Contabilidade; Sistemas de Informação Gerencial; e Introdução ao Processamento de Dados.

As disciplinas têm carga horária de 68 horas/aula cada e formação obrigatória para as matérias Informática Aplicada à Contabilidade e Sistemas de Informação Gerencial, disponíveis nos semestres 4º e 7º, respectivamente. Sendo unicamente a cadeira de Introdução ao Processamento de Dados opcional, sendo ofertada para discentes que desejam se aprofundar na linguagem de programação e processamento de dados.

3.1.2 Universidade Federal de Sergipe (UFS) – Campus São Cristóvão

Segundo o sítio[12] do departamento de Ciências Contábeis a estrutura curricular vigente é do ano 2013, o curso contempla a carga horária mínima de 3.000 horas, no qual 2.820 horas são para disciplinas obrigatórias, 120 horas para atividade acadêmica especial e 180 horas para matérias optativas.

A duração média do curso é de 05 anos ou 10 semestres, sendo o máximo 07 anos e meio ou 15 semestres. Entre as 67 (sessenta e sete) disciplinas ofertadas, apenas uma refere-se à tecnologia da informação, sendo a cadeira de microcomputadores, disponível no segundo período, com carga horária de 60 horas/aula e formação obrigatória.

Verificou-se que a disciplina Práticas e Rotinas Contábeis, disponível no décimo período e obrigatória a formação descreve em sua ementa a utilização de sistemas informatizados para a rotina das atividades contábeis, contudo o foco da matéria não é a tecnologia, por isso não está sendo considerada no estudo.

3.1.3 Universidade Federal de Alagoas (UFAL) – Campus A. C. Simões

[12] Disponível em: https://www.sigaa.ufs.br/sigaa/public/curso/curriculo.jsf

O curso de Ciências Contábeis na UFAL tem como base as Diretrizes Curriculares Nacionais do Curso de Graduação da Resolução CNE/CES nº 10/2004 e orientações estabelecidas pela universidade.

Com carga horária de 3.005 horas e duração mínima de 4,5 anos e máxima de 6,5 anos, ou seja, 09 e 13 semestres respectivamente, o curso dispõe de 64 disciplinas, sendo 43 de caráter obrigatórias e 21 a escolha do discente, contudo apresenta apenas uma matéria destinada ao estudo de tecnologia da informação, sendo a cadeira de Tecnologia e Sistemas de Informação Gerencial, com carga horária de 72 hora/aula e formação obrigatória.

A ementa da disciplina descreve o estudo aos sistemas de informação, sistemas integrados de gestão e estruturas de internet, extranet e comércio eletrônico, conforme o Projeto Pedagógico de 2019[13].

3.1.4 Universidade Federal de Pernambuco (UFPE) – Campus Recife

O curso de Ciências Contábeis foi criado na UFPE em 1951, conforme autorizado pelo Conselho Universitário da instituição em 3º sessão no dia 01 de fevereiro, depois do reconhecimento do curso através da Lei nº 1.254 de 04 de dezembro de 1950.

Conforme Projeto Pedagógico de 2008[14], a criação do curso de Contábeis foi “um verdadeiro marco para a História da Contabilidade em Pernambuco”, visto que foi o início do ensino superior em contabilidade no Estado.

O curso tem como base o Regimento Geral da Universidade, a Resolução nº 04/94 e conforme perfil curricular implantado em 2009 possui carga horária de 3.000 horas, distribuídas em 08 períodos. Das 50 disciplinas ofertadas pelo curso, 02 compreendem a necessidade de tecnologia de informação nos currículos, sendo as matérias Computação Aplicada à Contabilidade e Sistemas de Informações Contábeis e Gerenciais, ambas obrigatórias e com carga horária de 60 horas/aula.

3.1.5 Universidade Federal da Paraíba (UFPB) – Campus Mamanguape

[13] Disponível em: https://ufal.br/estudante/graduacao/projetos-pedagogicos/campus-maceio/ppc-contabeis-versao-12_08_2021-prograd-1.pdf/view

[14] Disponível em: https://www.ufpe.br/ciencias-contabeis-bacharelado-ccsa

O curso de Ciências Contábeis apresentado na universidade tem como base a Resolução nº 66/2010 do CONSEPE, que altera a Resolução nº 31/2006 e aprova o novo Projeto Pedagógico[15] do bacharelado em vigor no primeiro semestre de 2011.

Atualmente o curso tem carga horária mínima de 3.000 horas, sendo 2.460 horas para as disciplinas obrigatórias, 420 horas para atividade acadêmica especial e mínima de 240 horas para disciplinas optativas. Além disso, dispõe de 76 disciplinas, sendo 40 obrigatórias e 36 optativas, e complementar flexiva.

Verificando a proposta do CFC e ISAR/UNCTAD/ONU quanto a disciplinas que compreendam a tecnologia da informação, identificou-se que a instituição apresenta 03 matérias, sendo Informática Aplicada à Contabilidade, Sistemas de Informações Gerenciais e Introdução ao Processamento de Dados. As duas primeiras são de formações obrigatórias e ministradas nos períodos 3º e 7º respectivamente, já a última é opcional, todas tem carga horária de 60 horas/aula.

3.1.6 Universidade Federal do Rio Grande do Norte (UFRN) – Campus Natal

O curso de Ciências Contábeis teve início pela promulgação do Decreto nº 813, de 10 de março de 1962, e posteriormente alterado pelo Decreto nº 1.201, de 19 de junho de 1962, no qual autorizou o funcionamento da Faculdade de Ciências Econômicas, Contábeis e Atuariais de Natal.

Desde então, o curso passou por diversas mudanças, principalmente em seu plano curricular. No site[16] da instituição consta o Projeto Pedagógico aprovado em julho de 2013, no qual detalha que o curso tem como base a Resolução CNE/CES nº 10/2004 e Resolução CNE/CES nº 02/2007, possui carga horária de 3.000 horas, com duração média de 10 semestres.

No PPC consta a descrição de 62 disciplinas, sendo 41 obrigatórias e 21 eletivas, dentre elas apenas a matéria de Sistemas de Informações Gerenciais, compreende a proposta de Tecnologia da Informação no currículo, no qual tem carga horária de 60 horas/aula e é opcional ao aluno.

[15] Disponível em: https://sigaa.ufpb.br/sigaa/public/curso/ppp.jsf?lc=pt_BR&id=1626789
[16] Disponível em: https://sigaa.ufrn.br/sigaa/public/curso/ppp.jsf?lc=pt_BR&id=2000011

Contudo o curso apresenta disciplinas que contemplam o uso de sistemas informatizados e softwares, como as matérias de prática empresarial I, II e III e prática contábil, todavia o objetivo das disciplinas não é o ensino dos sistemas ou apresentação da tecnologia da informação, mas sim o uso dos sistemas para as atividades contábeis.

3.1.7 Universidade Federal do Ceará (UFC) – Campus Fortaleza

O bacharel em Ciências Contábeis da FEAAC/UFC foi criado através do Decreto nº 26.142 de 1949 e reconhecido pelo provimento nº 13 do Conselho Federal de Educação. Tem a Resolução CNE/CES nº 10/2004 como base e procura desenvolver no aspecto ensino-aprendizagem as áreas cognitiva, humanística, psicomotora e ética nos alunos.

O curso tem carga horária mínima de 3.000 horas, com duração média de 4,5 anos ou 09 semestres. Conforme o Projeto Pedagógico[17], que entrou em vigor a partir de 2007.1 e site do departamento de Contábeis, aba Estrutura Curricular, o curso dispõe de 41 disciplinas obrigatórias e 37 optativas, porém só disponibiliza uma disciplina para a área de tecnologia da informação a matéria Gestão de Sistema de Informação, de caráter obrigatório e carga horária de 64 horas/aula.

3.1.8 Universidade Federal do Piauí (UFPI) – Campus Ministro Reis Velloso – Parnaíba

O curso de Ciências Contábeis foi criado em 04 de fevereiro de 1976 por Ato da Reitoria nº 33 e reconhecido pelo MEC, através da Portaria nº 085 de 1981, desde então o curso já passou por diversas mudanças, visando adaptar sua estrutura curricular as exigências legais e de mercado.

Atualmente o curso tem como base a Resolução CNE/CES nº 10/2004 e aspectos revistos pelo Núcleo Docente Estruturante – NDE. Tem a carga horária definida em 3.045 horas, com duração mínima de 04 anos e máxima de 06 anos, dispõem de 41 disciplinas obrigatórias e 09 eletivas, tendo apenas a cadeira de Sistema de Informação Gerencial – SIG, de formação obrigatória e carga horária de

[17] Disponível em: https://prograd.ufc.br/pt/cursos-de-graduacao/ciencias-contabeis-noturno-fortaleza/

30 horas/aula, como disponibilidade para proposta de Tecnologia da Informação, conforme Projeto Pedagógico[18] em vigor desde 2014.2.

3.1.9 Universidade Federal do Maranhão (UFMA) – Campus São Luis

Os estudos em contabilidade no Estado do Maranhão remontam há um século, contudo o curso só foi criado em 1974, quando da Resolução CONSUN nº 30, de 24 de setembro de 1974 e Resolução nº 287/74, obtendo reconhecimento 05 anos após, com o Decreto nº 83.307/79 e Parecer nº 174/79 pelo Conselho Federal de Educação. (UFMA, 2015).

O curso tem a carga horária mínima de 3.000 horas, com duração padrão de 04 anos e máxima de 06 anos, e dispõe de 63 disciplinas, sendo 46 obrigatórias e 17 eletivas, entre as disponibilidades tem-se somente uma disciplina com fundamentação em tecnologia da informação, sendo a matéria Análise de Sistemas Contábeis, carga horária de 60 horas/aula e formação obrigatória. Além disso, o Projeto Pedagógico[19] proposto em 2012 tem como base a Resolução nº 10/2004 e Resolução nº 02/2007.

[18] Disponível em: https://sigaa.ufpi.br/sigaa/public/curso/curriculo.jsf?lc=pt_BR&id=74227

[19] Disponível em: https://sigaa.ufma.br/sigaa/public/curso/ppp_curso.jsf?lc=pt_BR&lc=pt_BR&id=85772

4. ANÁLISE E INTERPRETAÇÃO DOS RESULTADOS

A descrição das grades curriculares das 09 (nove) Universidades Federais do Nordeste procurou descrever características em comum entre elas e verificar se disponibilizam de disciplinas que contemplem a temática da tecnologia da informação e ensinam sobre os riscos tecnológicos a que as empresas e os profissionais estão sujeitos. A Tabela 01 ilustra as semelhanças entre as IFES (Instituto Federal de Ensino Superior).

Tabela 01: Semelhanças entre as Universidades Federais do Nordeste

Universidade (UF)	Carga Horária Total	PPC Atual (ano)	Disciplinas Obrigatórias	Disciplinas Optativas	Disc. Tecnologia da Informação
UFBA	3.026	2008	35	35	03
UFS	3.000	2013	45	22	01
UFAL	3.005	2019	43	21	01
UFPE	3.000	2008	33	17	02
UFPB	3.000	2011	40	36	03
UFRN	3.000	2013	41	21	01
UFC	3.000	2007	41	37	01
UFPI	3.045	2014	41	09	01
UFMA	3.420	2015	46	17	01

Fonte: Elaborada pelo autor

Verificou-se pela pesquisa bibliográfica que todas as Universidades Federais em estudo contemplam pelo menos uma disciplina direcionada a tecnologia da informação, conforme ISAR/UNCTAD/ONU (2011)

> O assunto deve ser ensinado do ponto de vista de sua utilidade e aplicação a situações de negócios; a tecnologia não deve ser vista como um fim em si mesma. (...) O estudo de tecnologia da informação deve ser integrada na medida do possível, ao estudo de disciplinas em outros módulos, não como um curso de habilidades técnicas separadas e independente. (Tradução Nossa)[20]

Compreende-se ainda, que o estudo da tecnologia da informação não precisa ser ministrado em disciplina específica para o assunto, dessa forma podendo ser abordado em matérias que utilizam os sistemas informacionais como ferramentas para elaboração de suas atividades, como as disciplinas de práticas contábeis, práticas empresariais, análise das demonstrações contábeis e outras.

[20] No original "The subject matter should be taught from the perspective of their usefulness and application to business situations; the technology should not be seen as an end in itself. (...)The study of information technology should be integrated as far as possible in the study of subjects in the other modules, and not as a separate stand-alone, self-contained technical skills course."

Outra questão analisada refere-se ao percentual representativo das disciplinas de tecnologia da informação na estrutura curricular nos cursos de Ciências Contábeis em relação ao ano de criação e/ou que entrou em vigor o Projeto Pedagógico do curso e o total de disciplinas ofertadas, como mostra a Tabela 02 abaixo.

Tabela 02: Percentual de aproveitamento de disciplinas relacionadas à Tecnologia da Informação

Universidade	PCC Atual (ano)	Total Disc. Ofertadas	Disc. Tecnologia da Informação	Percentual Aproveitamento (%)
UFBA	2008	70	03	4,29
UFS	2013	67	01	1,49
UFAL	2019	64	01	1,56
UFPE	2008	50	02	4,00
UFPB	2011	76	03	3,95
UFRN	2013	62	01	1,61
UFC	2007	78	01	1,28
UFPI	2014	50	01	2,00
UFMA	2015	63	01	1,59

Fonte: Elaborada pelo autor

O estudo evidenciou que as Universidades UFBA e UFPE apresentam os melhores percentuais de desempenho quanto à inclusão de disciplinas relacionadas à tecnologia da informação em suas grades curriculares, ressaltando ainda que possuem projetos pedagógicos com mais de 10 anos em vigor, assim rompendo o paradigma que quanto mais atual for o projeto mais compacto ao mercado ele estará.

O percentual apresentado ainda é mutável quando questionado sobre a obrigatoriedade da formação das disciplinas, assim evidenciando apenas as matérias obrigatórias que obedecem ao tema, destaca-se a Tabela 03:

Tabela 03: Percentual de aproveitamento das disciplinas obrigatórias

Universidade	PCC Atual (ano)	Total Disc. Ofertadas	Disc. Obrigatórias	Percentual Apoveitamento (%)
UFBA	2008	70	02	2,86
UFS	2013	67	01	1,49
UFAL	2019	64	01	1,56
UFPE	2008	50	02	4,00
UFPB	2011	76	02	2,63
UFRN	2013	62	0	0,00

UFC	2007	78	01	1,28
UFPI	2014	50	01	2,00
UFMA	2015	63	01	1,59

Fonte: Elaborada pelo autor.

Observa-se que o percentual de aproveitamento da Universidade Federal de Pernambuco se mantém mesmo após adesão de nova condição à análise.

Analisou-se também a ementa de cada disciplina que contempla a temática de Tecnologia da Informação, buscando identificar os assuntos discutidos e se eles dão destaque aos riscos tecnológicos e a segurança no meio digital, o conteúdo não é evidenciado na ementa das 09 (nove) Universidades Federais analisadas.

Quanto ao estudo quantitativo, obtendo como base o percentual de aproveitamento, a minuta do CFC que propõe a mudança do currículo de Ciências Contábeis e o modelo de currículo apresentado pelo ISAR/UNCTAD/ONU (2011) não apresentam ou obrigam a adesão de algum percentual específico, os documentos são orientações para uma melhor formação do profissional contábil. Assim, o estudo utilizando percentuais buscou simplesmente quantificar a importância e relevância que o tema apresenta nas IFES da região Nordeste do Brasil.

Além disso, salienta-se que não foram considerados na análise o caráter qualitativo das disciplinas e/ou questões econômicas, políticas e sociais. Além disso, buscou-se embasar a pesquisa utilizando estruturas curriculares mais recentes de cada instituição de ensino, assim procurando em cada polo disponível que continha o curso de Ciências Contábeis a base curricular e/ou projeto pedagógico mais atualizado.

4.1 RESULTADOS DO QUESTIONÁRIO

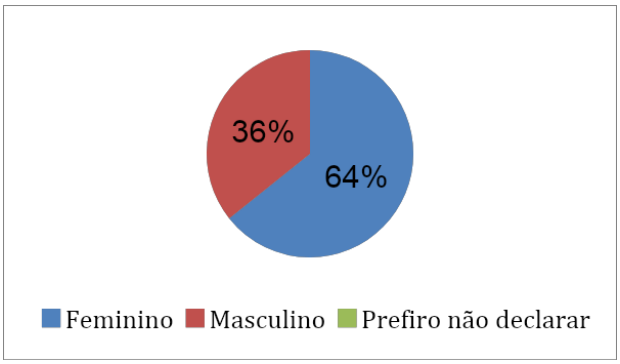
Com o objetivo de medir a importância do tema riscos tecnológicos à contabilidade e verificar quais conhecimentos básicos em segurança da informação os alunos da Universidade Federal de Pernambuco possuem foi aplicado um questionário através da plataforma *Google Forms*, no qual requer o uso do e-mail institucional para poder responder, assim não admitindo o preenchimento de pessoas diferentes a população descrita. Ademais, o formulário continha 18 perguntas, no qual 17 eram de respostas obrigatórias e apenas a quinta questão

opcional, visto que somente os entrevistados que não estudaram o assunto na Universidade deveriam responder.

4.1.1 Sexo / Gênero

A primeira pergunta refere-se ao sexo e/ou gênero que os participantes se identificam, conforme o Gráfico 02.

Gráfico 02: Sexo/Gênero dos alunos entrevistados



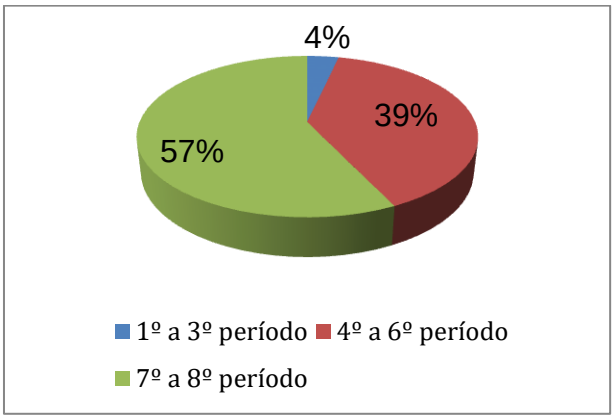
Fonte: O autor

Dos resultados obtidos, 64% identificaram-se como feminino e 36% como masculino, respectivamente 18 e 10 entrevistados. Não houve respostas para a opção “Prefiro não declarar”.

4.1.2 Grau de Escolaridade

A segunda pergunta procura saber o grau de escolaridade dos entrevistados, possibilitando o preenchimento de apenas uma resposta para as opções 1º a 3º período, 4º a 6º período e 7º a 8º período, como apresenta o Gráfico 03.

Gráfico 03: Grau de escolaridade dos entrevistados



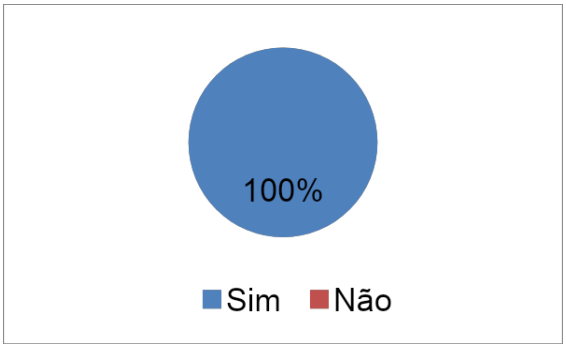
Fonte: O autor

Conforme respostas, 57% dos alunos estão nos últimos semestres da graduação, 39% estão entre o 4º a 6º período e apenas 4% ainda está no 1º a 3º período. Com o resultado observou-se que 96% dos entrevistados estão cursando ou já cursaram pelo menos uma das disciplinas relacionadas à Tecnologia da Informação, visto que segundo a Estrutura Curricular de Ciências Contábeis da UFPE em vigor desde o semestre 2009.1, no quarto período cursa-se a matéria Computação Aplicada à Contabilidade e no sétimo período cursa-se Sistemas de Informações Contábeis e Gerenciais ambas de forma obrigatória.

4.1.3 Conhecimento na Área de Tecnologia

Quanto à terceira pergunta, procurou-se saber se é importante que o profissional de contabilidade tenha conhecimentos na área de tecnologia e de acordo com o Gráfico 04, a resposta foi unânime.

Gráfico 04: A importância do profissional de contábeis ter conhecimento na área de tecnologia

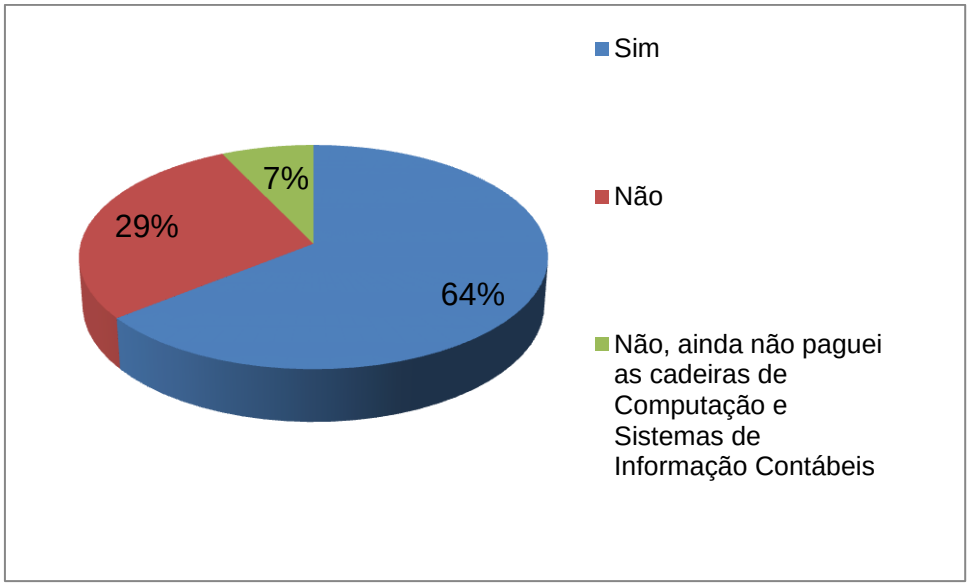


Fonte: O autor

4.1.4 O Estudo de Sistemas Contábeis na UFPE

A questão perguntou ao entrevistado se ele já estudou sistemas contábeis, redes de computadores, armazenamento nas nuvens e/ou pacote *office* na Universidade, o resultado é apresentado no Gráfico 05.

Gráfico 05: O estudo de sistemas contábeis e outros elementos tecnológicos na Universidade



Fonte: O autor

O resultado foi favorável, sendo 64% sim, 29% não e 7% de alunos que ainda não cursaram as disciplinas relacionadas à Tecnologia da Informação, e verificando a ementa das disciplinas, de fato cumprem com os requisitos propostos, como: utilizar aplicativos, programas da "área contábil e financeira, prática com software em laboratório de informática", (...) "conhecimento sobre sistemas integrados de gestão, gerenciais e de apoio à decisão com aplicações práticas em ciências contábeis". (UFPE, 2008)

4.1.5 Por qual meio adquiriu conhecimento

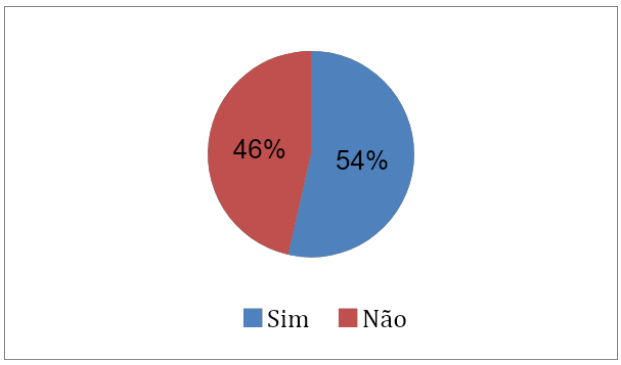
A quinta pergunta procurava conhecer por qual meio o estudante que "não" estudou sobre sistemas contábeis, rede de computadores e outros aspectos perguntados na questão anterior tinha adquirido conhecimento, assim apresentando 04 (quatro) respostas possíveis, sendo: estágio, trabalho, por conta própria e não tive contato.

Observou-se que muitas pessoas que responderam "sim" na pergunta anterior, também preencheram uma das alternativas da questão presente, visto que era opcional. Desta forma, a pergunta não cumpriu com o objetivo proposto e para não obter um resultado enviesado preferiu-se anular a questão, vale ressaltar que o cancelamento da pergunta não interfere no resultado das demais indagações.

4.1.6 Sistema de Segurança da Informação

A sexta questão pergunta se o entrevistado sabe o que é um Sistema de Segurança da Informação (SI), o resultado é apresentado no Gráfico 06.

Gráfico 06: Conhecimento sobre Sistema de Segurança da Informação (SI)



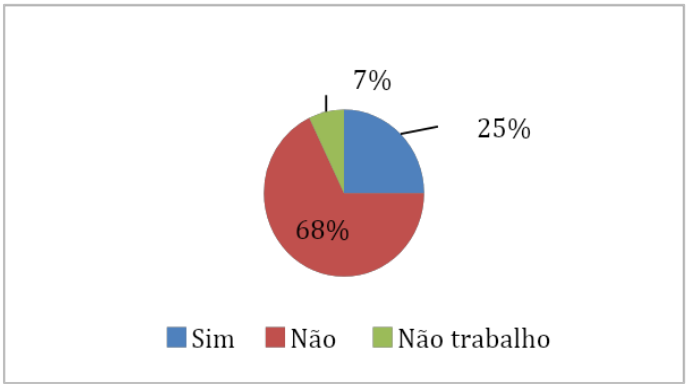
Fonte: O autor

O resultado mostrou que a maioria dos alunos conhece o sistema, contudo a variação entre os saberes dos entrevistados é pouca, assim não sendo tão relevante como critério determinante da área de segurança, visto que das 28 respostas, 15 foram a favor e 13 contra.

4.1.7 Treinamento em Riscos Cibernéticos

Essa pergunta procurou conhecer se os entrevistados já tinham vivenciado algum tipo de treinamento, curso, instrução sobre riscos cibernéticos no ambiente de trabalho, visto que com o aumento dos cibercrimes muitas empresas de médio e grande porte estão instruindo seus colaboradores sobre o tema, o resultado é apresentado no Gráfico 07.

Gráfico 07: Treinamento contra riscos cibernéticos



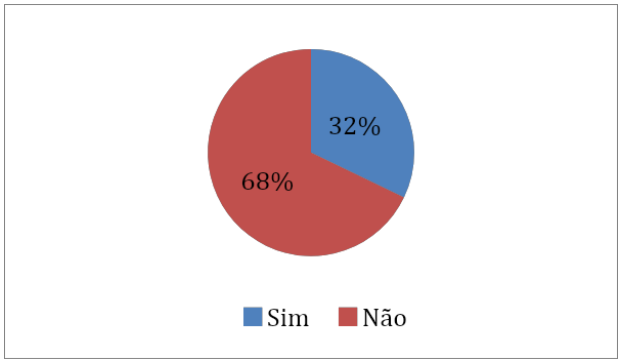
Fonte: O autor

O resultado mostrou que das 26 pessoas que trabalham, ou seja, 93% dos entrevistados, apenas 25% ou 07 (sete) receberam algum tipo de instrução, curso sobre o tema.

4.1.8 Contrato de Política de Segurança da Informação (PSI)

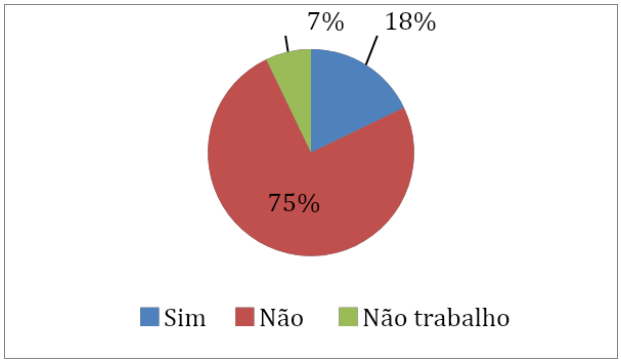
As perguntas oito e nove referem-se ao contrato de Política de Segurança da Informação (PSI), no qual na oitava busca saber se o entrevistado conhece esse tipo de medida recentemente adotada pelas empresas e na pergunta nove se ele já teve a oportunidade de assinar esse documento, conforme resultado nos Gráficos 08 e 09.

Gráfico 08: Você sabe o que é um PSI?



Fonte: O autor

Gráfico 09: Você já assinou um PSI?



Fonte: O autor

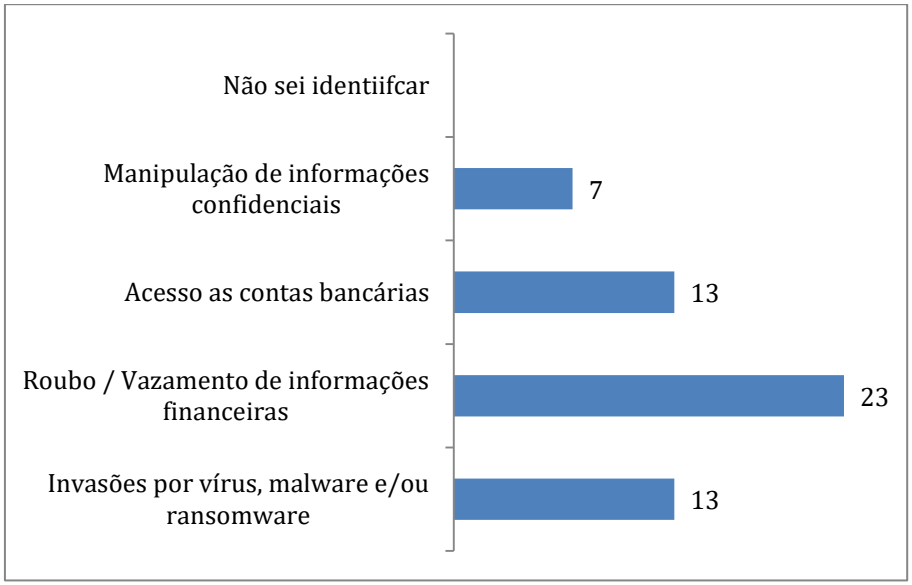
Analisando os resultados das perguntas 07, 08 e 09 do formulário, percebe-se uma relação entre elas, visto que o mesmo percentual de pessoas que não receberam ainda um treinamento quanto aos riscos tecnológicos é o mesmo de entrevistados que também não conhecem o PSI. Quanto à pergunta se já assinaram o contrato PSI o percentual cresce 7% referente à alternativa “não”, os 7% de “não

trabalho” manteve-se e o percentual de pessoas que receberam algum treinamento e sabem o que é o PSI saem de 25% para 18%, assim evidenciando uma contrariedade no mercado de trabalho, visto que a assinatura do contrato juntamente ao aprimoramento do conhecimento do profissional assegura a entidade quanto a segurança de dados, transparência e adequação à LGPD.

4.1.9 Impacto dos Riscos Cibernéticos na atividade contábil

A questão dez possibilita ao entrevistado a escolha de até 02 (duas) alternativas para identificação dos principais riscos cibernéticos que afetam o objetivo e a atividade contábil, como apresenta o Gráfico 10.

Gráfico 10: Impacto dos riscos cibernéticos na contabilidade



Fonte: O autor

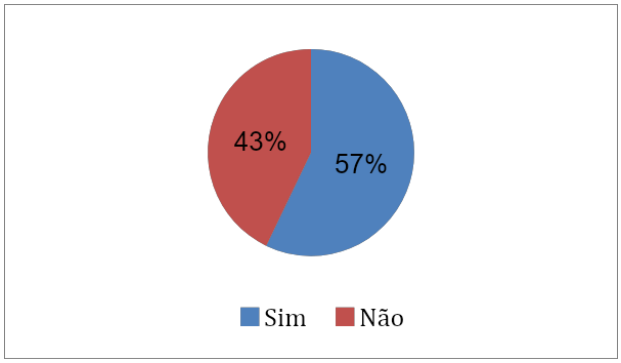
A pergunta admitia a possibilidade de até 56 respostas, no qual foi amplamente atendida, tendo à alternativa “Roubo / Vazamento de informações financeiras” como o maior impacto que pode prejudicar as atividades contábeis, as opções “Acesso às contas bancárias” e “Invasões por vírus, *malware* e/ou *ransomware*” ficaram empatadas em 13 ou 23,21% e a “Manipulação de informações confidenciais” ficaram com 7 ou 12,5%.

4.1.10 *Software Malware*

As perguntas 11 (onze) e 12 (doze) do formulário referem-se aos *softwares malwares* (maliciosos), no qual a primeira questão pergunta se o aluno sabe qual é

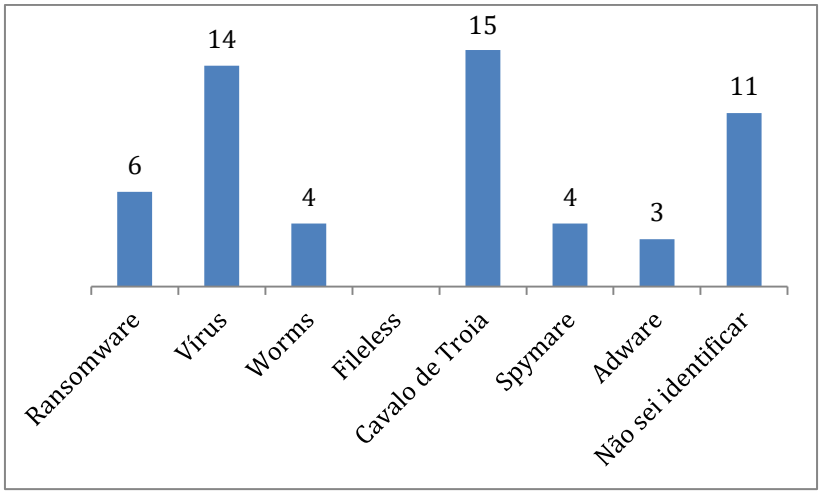
esse tipo de software e posteriormente pede que escolha até 03 (três) opções das alternativas descritas, conforme os Gráficos 11 e 12 abaixo.

Gráfico 11: Conhecimento de *Software Malware*



Fonte: O autor

Gráfico 12: Tipos de *Softwares Malwares*



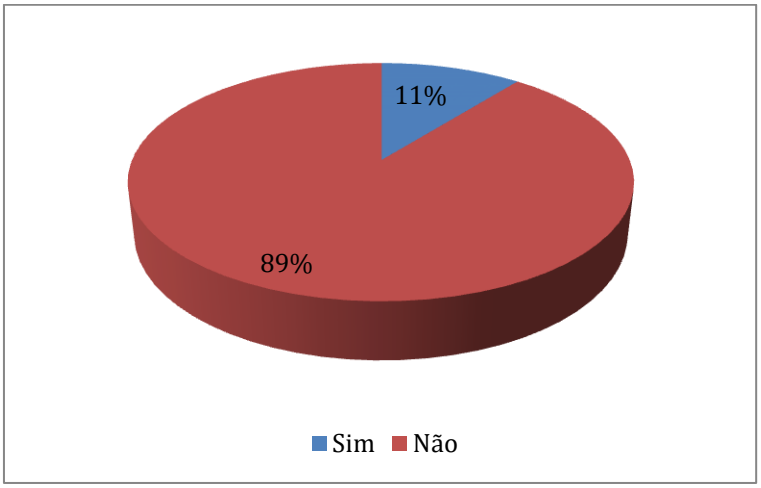
Fonte: O autor

Conforme o resultado, observou-se que a maioria dos entrevistados conhecem ou tem uma noção do que são softwares maliciosos, contudo sabem identificar apenas os mais conhecidos socialmente, como: vírus e cavalo de troia. Outro aspecto analisado é o percentual de pessoas que não souberam identificar algum sistema descrito, representando 11 ou 19,30% das respostas e a opção “Fileless” que não foi escolhida por nenhum participante, ressaltando que a questão possibilitava até 84 respostas e obteve-se ao todo 57.

4.1.11 Técnicas Antiforenses

A pergunta buscou saber se os entrevistados conheciam as técnicas antiforenses, visto que são práticas, por vezes, desenvolvidas sem a intenção e conhecimento das vítimas e/ou criminosos do cibercrime, conforme resultado apresentado no Gráfico 13.

Gráfico 13: Técnicas Antiforenses



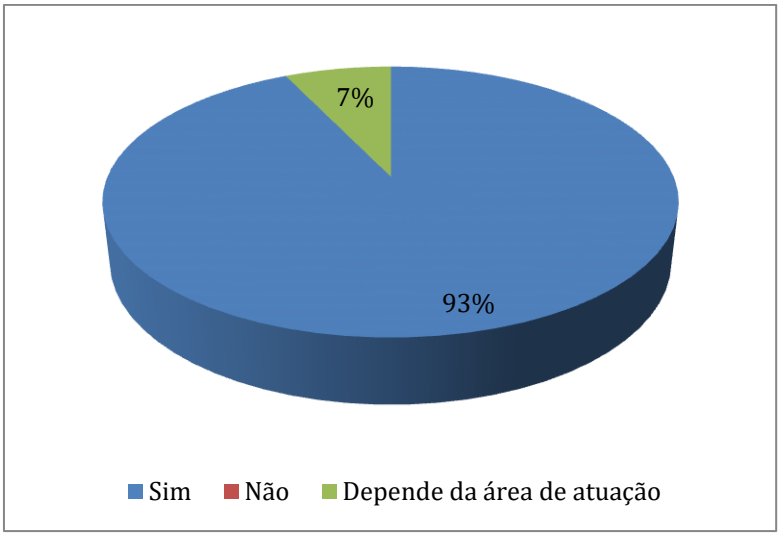
Fonte: O autor

O resultado dessa pergunta evidencia a falta de um conhecimento importantíssimo para o combate aos riscos e crimes tecnológicos, visto que conforme apresentado no referencial teórico, são práticas que buscam atrapalhar a investigação da perícia forense e podem ser realizadas com o intuito de encobrir crimes ou por falta de conhecimento da vítima, assim apagando provas e evidências significativas a coleta e análise dos dados.

4.1.12 O Profissional Contábil e a Tecnologia

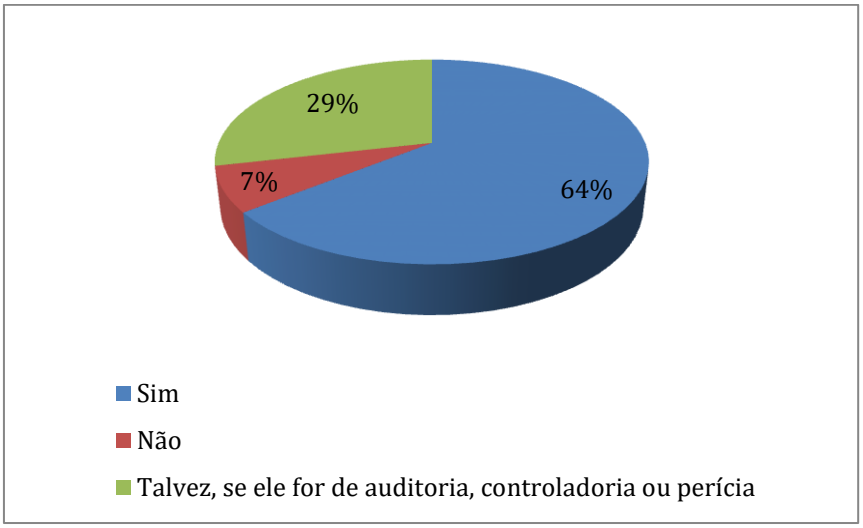
As perguntas 14 (catorze) e 15 (quinze) do questionário buscaram conhecer a opinião dos alunos quanto ao estudo e conhecimento dos profissionais contábeis à área de tecnologia, assim perguntando se eles teriam mais chances de atuação no mercado e se poderiam ser aliados no combate aos crimes digitais, os Gráficos 14 e 15 ilustram os resultados.

Gráfico 14: O estudo de tecnologia e as chances no mercado de trabalho



Fonte: O autor

Gráfico 15: Aliados no combate aos crimes cibernéticos



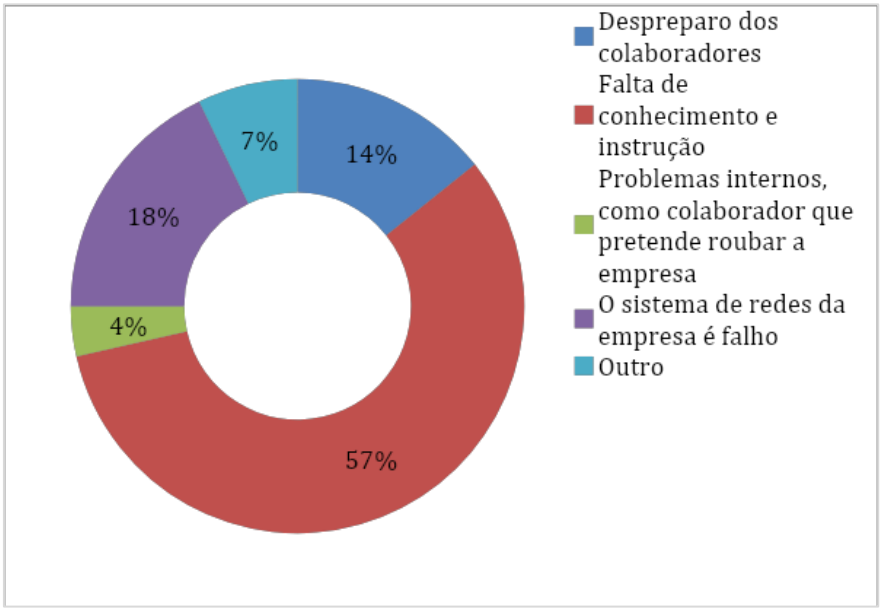
Fonte: O autor

Os resultados mostraram que mais de 60% dos alunos nas duas perguntas acreditam que o conhecimento em tecnologia pode aumentar as chances de atuação no mercado de trabalho, como também ser um aliado no combate aos crimes cibernéticos, visto que com a informatização da contabilidade os profissionais precisam, cada vez mais, se adequarem ao ambiente digital e como são profissionais que lidam com a saúde financeira da entidade é de suma importância que sua atividade possa ser mais estratégica e consultiva, visando a qualidade e segurança das informações.

4.1.13 Motivo dos Crimes Cibernéticos

A pergunta procurou saber entre os entrevistados quais motivos deixam as empresas vulneráveis aos crimes cibernéticos, o Gráfico 16 descreve o resultado.

Gráfico 16: Motivo dos crimes cibernéticos



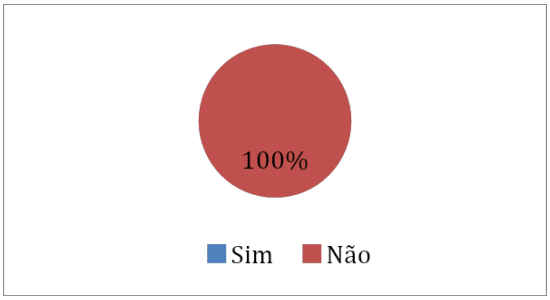
Fonte: O autor

Para os entrevistados a “Falta de conhecimento e instrução” é o motivo predominante para colocar a empresa em situação propícia aos crimes cibernéticos, visto que geralmente a área de segurança da informação é restrita a um grupo de pessoas, assim não ocorrendo à interligação tecnologia, pessoas e processos, tão necessária para conhecer e implantar um sistema de segurança personalidade e com foco no combater a possíveis vulnerabilidades da empresa.

4.1.14 Atuação da UFPE e Órgão de Classe

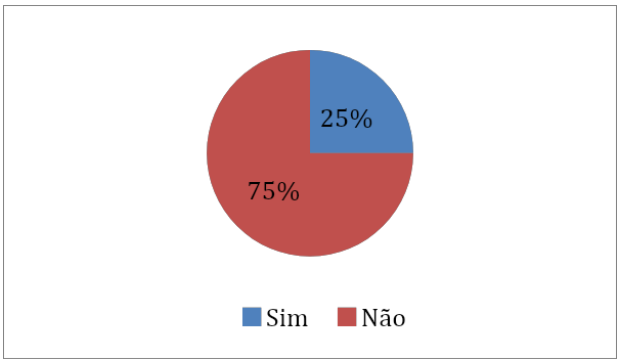
A questão procurou saber a opinião dos alunos quanto à compatibilidade do plano de ensino da UFPE com a demanda tecnológica e também verificar entre a amostra a percepção da atuação do CFC e/ou CRC quanto ao tema, conforme respostas dos Gráficos 17 e 18.

Gráfico 17: Demanda tecnológica na UFPE



Fonte: O autor

Gráfico 18: Atuação do CFC / CRC



Fonte: O autor

Dos 28 entrevistados, todos consideram que o plano de ensino da UFPE é incompatível com a demanda tecnológica do mercado, contudo vale lembrar que pela análise das grades curriculares nas Universidades Federais do Nordeste a UFPE apresentou o melhor resultado, quanto a abordagem da tecnologia no plano de ensino, contudo não se analisou a qualidade do ensino e esse aspecto pode ter influenciado nas respostas.

Além disso, verificou-se também que grande parte dos entrevistados não percebe a atuação do Conselho de Classe da Profissão quanto ao tema, visto que o órgão tem por objetivo fiscalizar o exercício da profissão e verificar a qualidade dos serviços prestados.

CONSIDERAÇÕES FINAIS

O trabalho teve como objetivo geral identificar os principais riscos tecnológicos que podem impactar na realização das atividades contábeis, como também analisar quais áreas de atuação contábil podem auxiliar no combate as práticas criminosas.

Tendo o meio digital e as operações que ali ocorrem como ambiente a ser estudado, procurou-se de início conhecer como a contabilidade, que a princípio começou de forma manual, foi se desenvolvendo com os avanços tecnológicos até a informatização. Posteriormente, são apresentados os riscos tecnológicos que impactam a contabilidade e as empresas, assim descrevendo desde aspectos subjetivos ao uso de métodos intencionais para a realização dos cibercrimes.

Ao longo da monografia foram detalhados os objetivos específicos propostos, assim foram evidenciados os conhecimentos básicos que são importantes para a detecção e prevenção aos crimes cibernéticos, além de apresentar meios de proteção à segurança da informação para as empresas e seus colaboradores.

Ademais, verificou-se que as áreas de auditoria, perícia e contabilidade forense, através das metodologias aplicadas a execução das funções, podem ser grandes aliadas do combate aos crimes nos ambientes digitais, aliás todos os profissionais contábeis possuem essas qualificações e habilidades, visto que ao detectar algo que apresente fraude e/ou erros é dever do contador comunicar a administração, direção para que se realize os devidos ajustes.

O trabalho também pôde verificar, analisando os planos de ensino das Universidades Federais do Nordeste e as respostas ao questionário online, que a temática da pesquisa é relevante, contudo não se identificou nos projetos pedagógicos e grades curriculares o tema sendo discutido nas disciplinas ofertadas, principalmente aquelas relacionadas à tecnologia da informação, todavia compreende-se que o assunto pode ser abordado a critério do professor e solicitações dos alunos.

E com as respostas dos alunos ao questionário, conseguiu-se alcançar o objetivo de averiguar a opinião dos futuros profissionais contábeis quanto à relevância do tema, no qual grande parte dos respondentes confirmaram a necessidade de se conhecer ainda mais o assunto, os métodos utilizados, as formas de atuação e validaram a possibilidade do profissional contábil ser um aliado na prevenção e combate aos crimes cibernéticos.

REFERÊNCIAS

ALBERTIN**,** Alberto Luiz**. Administração de Informática: funções e fatores críticos de sucesso**. 5. ed. São Paulo: Atlas, 2004. 208 p.

ALVES, Mateus do Canto. **Indústria 4.0 e a Contabilidade**: um estudo pela ótica de uma empresa desenvolvedora de software contábil e de empresas portadoras de serviços contábeis do sul de santa catarina. 2020. 31 f. TCC (Graduação) - Curso de Ciências Contábeis, Universidade do Extremo Sul Catarinense, Criciúma, 2020. Disponível em: http://repositorio.unesc.net/bitstream/1/8048/1/MATEUS%20DO%20CANTO%20ALVES.pdf. Acesso em: 03 out. 2022.

APEX, Agência (org.). **Profissional da Contabilidade fortaleze empresas, transforma vidas e faz o país crescer**. 2022. Disponível em: https://cfc.org.br/noticias/profissional-da-contabilidade-fortalece-empresas-transforma-vidas-e-faz-o-pais-crescer/. Acesso em: 02 out. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **27001**: Tecnologia da Informação - Técnicas de Segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro: Abnt, 2006. Disponível em: https://jkolb.com.br/wp-content/uploads/2016/09/ABNT-NBRISOIEC27001-20060331Ed1.pdf. Acesso em: 02 out. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **27002**: Tecnologia da Informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: Abnt, 2005. Disponível em: https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf. Acesso em: 02 out. 2022.

BRANCO, Dário Castelo. **5 sinais de que sua identidade digital foi roubada**. 2022. Disponível em: https://canaltech.com.br/seguranca/5-sinais-de-que-sua-identidade-digital-foi-roubada-207961/. Acesso em: 13 out. 2022.

BRASIL. Constituição (1940). **Decreto-Lei nº 2848, de 07 de dezembro de 1940.** . Rio de Janeiro, Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato. Acesso em: 02 out. 2022.

BRASIL. **Resolução nº 10**, de 16 de dezembro de 2004. Institui as Diretrizes Curriculares Nacionais para o Curso de Graduação em Ciências Contábeis, bacharelado, e dá outras providências.. . Brasília, Disponível em: http://portal.mec.gov.br/cne/arquivos/pdf/rces10_04.pdf. Acesso em: 30 set. 2022.

BREDA, Zulmir Ivânio. **Uma reflexão sobre os impactos da tecnologia na Contabilidade**. 2019. Disponível em: https://cfc.org.br/destaque/uma-reflexao-sobre-os-impactos-da-tecnologia-na-contabilidade/. Acesso em: 02 out. 2022.

CARROLL, Gwendolyn; DRAKE, Matthew; LIVERGOOD, Rob (org.). **Cybercrime**. 2021. Disponível em: https://www.justice.gov/usao-edmo/cybercrime. Acesso em: 03 out. 2022.

CARVALHO, Carlos. **A onipresença de dispositivos conectados à internet: presente e futuro.** 2022. Disponível em: https://mercadoeconsumo.com.br/20/04/2022/artigos/a-onipresenca-de-dispositivos-conectados-a-internet-presente-e-futuro/amp/. Acesso em: 14 out. 2022.

Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012

CERT.BR. **Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2020**. 2020. Disponível em: https://cert.br/stats/incidentes/2020-jan-dec/tipos-ataque.html. Acesso em: 02 out. 2022

COLIATH, Gleubert Carlos. A contabilidade como ciência social e sua contribuição para o capitalismo. **Eniac Pesquisa**, Guarulhos, v. 3, n. 2, p. 152-161, dez. 2014. Disponível em: file:///C:/Users/Usuario/Downloads/Dialnet-AContabilidadeComoCienciaSocialESuaContribuicaoPar-5261048.pdf. Acesso em: 30 set. 2022.

CONSELHO FEDERAL DE CONTABILIDADE. **Proposta de Resolução nº 1,** de 2022. Institui as Diretrizes Curriculares Nacionais para o curso de Graduação em Ciências Contábeis, bacharelado. . Brasília, 02 maio 2022. Disponível em: https://www.gov.br/participamaisbrasil/proposta-de-resolucao-oriunda-do-conselho-federal-de-contabilidade. Acesso em: 30 set. 2022

CONSENZA, José Paulo; ROCCHI, Carlos Antonio de. **A automação da escrituração contábil no Brasil:** desenvolvimento e utilização do sistema ficha tríplice. Revista de Contabilidade: do Mestrado de Ciências Contábeis da UERJ, Rio de Janeiro, v. 19, n. 1, p. 2-23, abr. 2014. Disponível em: https://www.e-publicacoes.uerj.br/index.php/rcmccuerj/article/view/7504/pdf. Acesso em: 29 set. 2022.

COSTA, Matheus Bigogno. **O que é Firewall**. 2020. Disponível em: https://canaltech.com.br/internet/o-que-e-firewall/. Acesso em: 29 set. 2022.

CREPALDI, Silvio Aparecido. **Auditoria Contábil**: teoria e prática. 6. ed. São Paulo: Atlas, 2010. Disponível em: https://wiac.info/docview. Acesso em: 30 set. 2022.

Gil, Antônio Carlos, 1946- **Como elaborar projetos de pesquisa** / Antônio Carlos Gil. — 3. ed. — São Paulo : Atlas, 1991.

HAMM, Kathleen M.. **Cibersegurança**: onde estamos; o que mais pode ser feito? um chamado para os auditores se apoem. Onde Estamos; O que mais pode ser feito? Um chamado para os auditores se apoem. 2019. 18º Conferência Anual de Relatórios Financeiros do Baruch College. Disponível em: https://pcaobus.org/news-events/speeches/speech-detail/cybersecurity-where-we-are-what-more-can-be-done-a-call-for-auditors-to-lean-in_700. Acesso em: 29 set. 2022.

HASSAN, Nihad A.. **Perícia Forense Digital**: guia prático com uso do sistema operacional windows. São Paulo: Novatec, 2019. 295 p. Tradução de: Aldir Coelho Corrêa da Silva.

HERNANDES, Anderson. **Como a tecnologia está mudando as empresas contábeis**. São Paulo: Tactus Editora Ltda, 2018.

IMPÉRIO DO BRASIL. Constituição (1850). Lei nº 556, de 25 de junho de 1850. **Código Commercial do Império do Brasil**. Rio de Janeiro, Disponível em: https://www2.camara.leg.br/legin/fed/leimp/1824-1899/lei-556-25-junho-1850-501245-publicacaooriginal-1-pl.html. Acesso em: 29 set. 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **13335-1**: Information technology - Security techniques - Management of information and communications technology secutity. Genova: Iso/Iec, 2004. Disponível em: https://webstore.iec.ch/preview/info_isoiec13335-1%7Bed1.0%7Den.pdf. Acesso em: 02 out. 2022.

KEMP, Simon. **Digital 2022:**: april global statshot report. April Global Statshot Report. 2022. Disponível em: https://datareportal.com/reports/digital-2022-april-global-statshot. Acesso em: 02 out. 2022.

Malhota (2001): MALHOTRA, Naresh K. **Pesquisa de marketing:** uma orientação aplicada. 3 .ed. Porto Alegre: Bookman, 2001.

MARCELINO, Gileno Fernandes. **A indústria nacional de computadores**. Revista de Administração, São Paulo, v. 18, n. 2, p. 90-95, jun. 1983. Disponível em: file:///C:/Users/Usuario/Downloads/166948-Texto%20do%20artigo-393477-1-10-20200220%20(1).pdf. Acesso em: 30 set. 2022.

MELO, Sandro Pereira de. **Taxonomia de Técnicas Furtivas e Antiforenses utilizadas em Ataques Cibernéticos**. 2018. 126 f. Tese (Doutorado) - Curso de Tecnologias da Inteligência e Design Digital, Pontifícia Universidade Católica Puc-Sp, São Paulo, 2018. Disponível em: https://tede2.pucsp.br/bitstream/handle/21181/2/Sandro%20Pereira%20de%20Melo.pdf. Acesso em: 30 set. 2022

MOREIRA, Nuno Ricardo de Oliveira. **A Forensic Accounting em Portugal**: evidências empíricas. 2009. 205 f. Dissertação (Mestrado) - Curso de Contabilidade, Escola de Economia e Gestão, Universidade do Minho, Braga, 2009. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/10948/1/tese.pdf. Acesso em: 29 set. 2022.

MOUTINHO, Célia. **O tempo da máquina de escrever**: sobre a coleção de máquinas de escrever da caixa geral de depósitos. Sobre a coleção de máquinas de escrever da Caixa Geral de Depósitos. 2011. CGD. Disponível em: https://www.cgd.pt/Institucional/Patrimonio-Historico-CGD/Estudos/Documents/Maquinas-de-escrever.pdf. Acesso em: 03 out. 2022.

NORMAS BRASILEIRAS DE CONTABILIDADE. **01**: Código de Ética Profissional do Contador. Brasília: Nbc, 2019. Disponível em: https://www1.cfc.org.br/sisweb/SRE/docs/NBCPG01.pdf. Acesso em: 03 out. 2022

NORMAS BRASILEIRAS DE CONTABILIDADE. **01**: Perícia Contábil. 1 ed. Brasília: Nbc, 2020. Disponível em: https://www1.cfc.org.br/sisweb/SRE/docs/NBCTP01.pdf. Acesso em: 03 out. 2022.

NORMAS BRASILEIRAS DE CONTABILIDADE. **240**: Responsabilidade do auditor em relação a fraude, no contexto da auditoria de demonstrações contábeis. 1 ed. Brasília: Nbc, 2016. Disponível em: https://www1.cfc.org.br/sisweb/SRE/docs/NBCTA240(R1).pdf. Acesso em: 03 out. 2022.

NOZOMI NETWORKS (Rio de Janeiro) (org.). **O que precisa de saber para combater o ransomware e as vulnerabilidades da IoT**: inclui recomendações sobre como melhorar a ciber-resiliência. Botafogo: Nozomi Networks, 2021. 9 p. Disponível em: https://www.nozominetworks.com/downloads/PT/NN-OT-IoT-Security-Report-2021-1H-ES-PT.pdf. Acesso em: 30 jul. 2022

O'BRIENS, James A.. **Sistemas de informação e as decisões gerenciais na era da Internet**. 3. ed. São Paulo: Saraiva, 2010. Tradução: Célio Knipel Moreira; Cid Knipel Moreira.

OLIVEIRA, E. **Contabilidade Informatizada**. São Paulo: Atlas, 1997.

OLIVEIRA, Fátima Bayama de (org.). **Tecnologia da informação e da comunicação**: a busca de uma visão ampla e estruturaada. São Paulo: Pearson Prentice Hall: Fundação Getúlio Vargas, 2007. 269 p.

OLIVEIRA, Marcelle Colares; PONTE, Vera Maria Soares; BARBOSA, João Victor Bezerra. **Metodologias de pesquisa adotadas nos estudos sobre Balanced Scorecard**. In: CONGRESSO BRASILEIRO DE CUSTOS, XIII, 2006**.** Belo Horizonte: Congresso, 2006. p. 1-16. Disponível em: file:///C:/Users/Usuario/Downloads/cbc,+XIIICongresso_artigo_0098.pdf. Acesso em: 30 set. 2022.

PRADO, Filipe. **Brasil foi o 5º país com mais ataques cibernéticos no ano**: relembre os principais. 2021. Disponível em: https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/. Acesso em: 30 jul. 2022.

REDAÇÃO. **Ransomware**: Brasil é o 4º país com mais crimes de extorsões de dados. Brasil é o 4º país com mais crimes de extorsões de dados. 2022. Disponível em: https://www.istoedinheiro.com.br/ransomware-brasil-e-o-quarto-pais-com-mais-crimes-de-extorsoes-de-dados/. Acesso em: 03 out. 2022.

REPORTING, Conceptual Framework For Financial. **Pronunciamento Técnico CPC 00 (R2)**: estrutura conceitual para relatório financeiro. 2. ed. Brasília: Comitê de Pronunciamentos Contábeis, 2019. 62 p. Disponível em: http://static.cpc.aatb.com.br/Documentos/573_CPC00(R2).pdf. Acesso em: 30 jul. 2022.

RICHARDSON, Roberto Jarry. **Pesquisa social**: métodos e técnicas. 3. ed. São Paulo: Atlas, 2012.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução Daniel Moreira Miranda. 1º ed. São Paulo: Edipro, 2016.

SÊMOLA, Marcos. **Gestão da segurança da informação:** visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003 – 12º reimpressão.

SENA, Janaína Duarte de *et al*. Contabilidade Forense: um estudo sobre a percepção de docentes e discentes em uma instituição de ensino superior de brasília. In: A CONTABILIDADE COMO MECANISMO DE GOVERNANÇA, Não use números Romanos ou letras, use somente números Arábicos., 2020, São Paulo. **Congresso USP de Iniciação Científica em Contabilidade.** São Paulo: Usp, 2020. p. 1-15. Disponível em: https://congressousp.fipecafi.org/anais/20UspInternational/ArtigosDownload/2722.pdf . Acesso em: 29 set. 2022.

TECH, Forbes. **Ataques de Ransomwares podem provocar fechamentos de mais de 30% dos negócios em alguns países**. 2021. Disponível em: https://forbes.com.br/forbes-tech/2021/07/ataques-de-ransomwares-podem-provocar-fechamento-de-mais-de-30-dos-negocios-em-alguns-paises/. Acesso em: 30 jul. 2022.

TROMBETTA, Daniel dos Passos; TROMBETTA, Luis Carlos. **A filosofia e a sociologia aplicadas às Ciências Contábeis**. 2016. 27 f. TCC (Graduação) - Curso de Ciências Contábeis, Faculdades Integradas de Taquara, Taquara, 2016. Disponível em: file:///C:/Users/Usuario/Downloads/297-Texto%20do%20Artigo-631-1-10-20160628.pdf. Acesso em: 13 out. 2022.

TURBAN, Efraim *et al.* **Tecnologia da informação para gestão**; tradução: Edson Furmankiewicz. – 6 ed. – Porto Alegre: Bookman, 2010.

UNIT NATIONS. **Model Accounting Curriculum (Revised**). Genova: Onu, 2011. Disponível em: https://unctad.org/system/files/official-document/diaemisc2011d1_en.pdf. Acesso em: 30 set. 2022.

UNIVERISIDADE FEDERAL DE PERNAMBUCO. **Projeto Pedagógico** do **Curso** de Ciências Contábeis. Recife, 2008.

UNIVERISIDADE FEDERAL DO CEARÁ. **Projeto Pedagógico** do **Curso** de Ciências Contábeis. Fortaleza, 2006.

UNIVERISIDADE FEDERAL DO MARANHÃO. **Projeto Pedagógico** do **Curso** de Ciências Contábeis. São Luis, 2012.

UNIVERISIDADE FEDERAL DO PIAUI. **Projeto Pedagógico** do **Curso** de Ciências Contábeis. Parnaíba, 2014.

UNIVERSIDADE FEDERAL DA BAHIA. **Projeto Pedagógico** do **Curso** de Ciências Contábeis. Salvador, 2008

UNIVERSIDADE FEDERAL DA PARAÍBA (Estado). **Resolução nº 66**, de 2010. . Paraíba, Conselho Superior de Ensino, Pesquisa e Extensão. Disponível em: https://sig-arq.ufpb.br/arquivos/2020020187ea322156207915eb5c4e533/Reseluo_N66_2010C._Contbeis_CCAE.pdf. Acesso em: 03 out. 2022.

UNIVERSIDADE FEDERAL DE ALAGOAS. **Projeto Pedagógico** do **Curso** de Ciências Contábeis. Maceió, 2019

UNIVERSIDADE FEDERAL DE SERGIPE. **Estrutura Curricular**. 2013. Disponível em: https://www.sigaa.ufs.br/sigaa/public/curso/curriculo.jsf. Acesso em: 03 out. 2022.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE. **Estrutura Curricular**. 2018. Disponível em: https://sigaa.ufrn.br/sigaa/public/curso/curriculo.jsf. Acesso em: 03 out. 2022.

VECCHIA, Evandro Dalla. **Perícia digital:** da investigação à análise forense. 2 ed. Campinas, SP: Millennium Editora, 2019.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=iGY-AgAAQBAJ&oi=fnd&pg=PA1&dq=crimes+cibern%C3%A9ticos+no+brasil&ots=OsGUQEc7Tl&sig=KQkpI_eyeeszOuurVbMzyx0r1Qo#v=onepage&q&f=true. Acesso em: 26 set. 2022.

APÊNDICE A – QUESTIONÁRIO RISCOS TECNOLÓGICOS À CONTABILIDADE

1- Qual é o seu sexo?*

( ) Feminino

( ) Masculino

( ) Prefiro não declarar

2- Qual o seu grau de escolaridade?*

( ) 1º a 3º período

( ) 4º a 6º período

( ) 7º a 8º período

3- Você acha importante que o profissional contábil tenha conhecimentos na área de tecnologia?*

( ) Sim

( ) Não

4- Você já estudou sobre sistemas contábeis, rede de computadores, armazenamento nas nuvens e/ou pacote office na universidade?*

( ) Sim

( ) Não

( ) Não, ainda não paguei as cadeiras de computação e sistemas de informações contábeis

5- Se você não estudou esses assuntos, teve contato com eles por qual meio?

( ) Estágio

( ) Trabalho

( ) Por conta própria

( ) Não tive contato

6- Você sabe o que é um sistema de segurança da informação (SI)?*

( ) Sim

( ) Não

7- Você já recebeu algum treinamento, curso ou instrução de riscos cibernéticos na empresa que trabalha?*

( ) Sim

( ) Não

( ) Não trabalho

8- Você sabe o que é um contrato de Política de Segurança da Informação (PSI)?*

( ) Sim

( ) Não

9- Você já assinou um contrato de Política de Segurança da Informação (PSI), onde trabalha?*

( ) Sim

( ) Não

( ) Não trabalho

10- Escolha até 02 riscos cibernéticos que você acredita que pode impactar nas atividades contábeis:*

□ Invasões por vírus, malware e/ou ransomware
□ Roubo / Vazamento de informações financeiras
□ Acesso as contas bancárias
□ Manipulação das informações confidenciais
□ Não sei identificar

11- Você sabe o que é um software malware?*

( ) Sim

( ) Não

12- Escolha até 03 tipos de software malware, que você conheça:*

□ Ransomware
□ Vírus
□ Worms
□ Fileless
□ Cavalo de Troia
□ Spymare
□ Adware
□ Não sei identificar

13- Você sabe o que são técnicas antiforenses?*

( ) Sim

( ) Não

14- Você acredita que um profissional que tenha conhecimentos em tecnologia terá mais chances de atuação no mercado?*

( ) Sim

( ) Não

( ) Depende da área de atuação

15- Você acha que o profissional contábil poderá ser um aliado no combate aos crimes cibernéticos?*

( ) Sim

( ) Não

( ) Talvez, se ele for de auditoria, controladoria ou perícia

16- Você acredita que os crimes cibernéticos nas empresas acontecem por qual motivo?*

□ Despreparo dos colaboradores
□ Falta de conhecimento e instrução

- □ Problemas internos, como colaborador que pretende roubar a empresa
- □ O sistema de redes da empresa é falho
- □ Outro

17- Você acha que o plano de ensino da UFPE está compatível com a demanda tecnológica do mercado?*

( ) Sim

( ) Não

18- Você percebe a atuação do CFC ou CRC quanto a assuntos tecnológicos na contabilidade?*

( ) Sim

( ) Não

As perguntas com o asterisco * (sinal gráfico em forma de estrela) são de resposta obrigatória.