Contabilidade e Ciebersegurança: uma Análise da Segurança da Informação Contábil

JULIANO CARLOS RADDATZ
Universidade Federal de Santa Maria – UFSM
RAMIRO RIBEIRO
Universidade Federal de Santa Maria – UFSM
CRISTIANE KRÜGER
Universidade Federal de Santa Maria – UFSM
CLÁUDIA DE FREITAS MICHELIN
Universidade Federal de Santa Maria – UFSM
VICTOR CEPILLO
Universidade Federal de Santa Maria - UFSM

Resumo

O avanço constante das tecnologias da informação trouxe à tona questões relevantes no que tange à segurança das informações. O Brasil é um dos países líderes no ranking mundial de ataques cibernéticos e essa exposição gera preocupação aos usuários, principalmente quanto aos aspectos contábil-financeiros. Diante disso, esta pesquisa objetivou analisar como o profissional contábil percebe na prática a segurança das informações contábeis no ciberespaço. Especificamente objetivou-se compreender a ocorrência dos processos de cibersegurança, verificar o conhecimento dos profissionais contábeis sobre o assunto, descrever a percepção deles quanto a segurança das informações e, identificar potencialidades e fragilidades relacionadas às rotinas de trabalho. Metodologicamente foi realizado um estudo de caso em um escritório de contabilidade, utilizando-se de uma pesquisa qualitativa e descritiva. A coleta dos dados foi realizada por meio de entrevistas semiestruturadas com indivíduos da entidade pesquisada. A análise de conteúdo categorial norteou a análise dos dados, por meio da qual emergiram categorias a posteriori de análise como Percepção, Gestão dos riscos cibernéticos, Fragilidades, Responsabilidade profissional e Potencialidades na segurança das informações. A partir da análise e discussão dos resultados percebeu-se que os profissionais estão cientes, porém não possuem conhecimento técnico, nem uma profunda percepção dos riscos sociais e materiais que estão expostos diariamente. Ainda, há dificuldade de os profissionais compreenderem que a segurança das informações contábeis não pode ser considerada um custo, mas sim um investimento. Desse modo, pode-se concluir que foi possível identificar as fragilidades e potencialidades existentes no local, além de projetar novos caminhos para pesquisas futuras referentes ao tema.

Palavras chave: Contabilidade, Sistema de Informação, Segurança, Usuários.

1. INTRODUÇÃO

Constantemente vivencia-se um avanço exponencial das tecnologias da informação, desse modo as atenções também se voltam para a segurança dessas informações (Laudon & Laudon, 2014). Nesse contexto, o Brasil é considerado um dos países líderes no ranking mundial de ataques cibernéticos (Norton Cyber Security Insigths Report Global Results, 2017). Diante disso, a cibersegurança tem-se tornado uma prática imprescindível nas organizações, pois assume um papel cada vez mais importante no que concerne à segurança dos sistemas de informação (Couto, 2018).

Adjacente aos avanços tecnológicos, a contabilidade deixou de ser um simples sistema de mensuração de dados e fornecimento de informações e tornou-se uma ferramenta de gestão que auxilia na tomada de decisões (Horngren, Sundem & Stratton, 2004). Essa nova era tecnológica tem proporcionado novos obstáculos à contabilidade, diretamente relacionados à crescente demanda de informações. Para Huerta e Jensen (2017), novas preocupações emergem para esses profissionais, e aqueles que utilizam recursos tecnológicos nos processos operacionais têm receio de como a informação é gerada e divulgada (Miller & Skinner, 2015).

Apesar dos benefícios proporcionados, conforme descreve Couto (2018), as tecnologias podem ser vulneráveis, criando riscos sociais e materiais. Estar conectado a uma rede global é estar exposto a ameaças constantes de roubo de dados e informações confidenciais, as informações contábeis estão em risco eminente, tornando-se alvo para ataques de hackers, espionagem e fraudes (Abu-Musa, 2003). Contudo, se houverem processos adequados para realizar um maior controle e proteção, como uma cultura de segurança e garantias de boas práticas, é possível evitar que a rede seja prejudicada com a tentativa de ataques cibernéticos (Pimenta & Quaresma, 2016).

Nesse sentido, cabe ao profissional contábil ter conhecimento quanto ao momento em que deve agir e as ferramentas que pode adotar para auxiliar na proteção, para isso, o primeiro passo é desenvolver um conjunto de políticas de segurança da informação (Knapp, Marshall, Byrd & Morris, 2009). Isso dependerá da criação e divulgação de um conjunto de boas práticas e comportamentos que sejam percebidos e adotados por todos na organização contábil (Kruger & Kearney, 2008). Diante disso questiona-se: na prática, como o profissional contábil percebe a segurança das informações contábeis no ciberespaço.

A fim de responder a problemática anteriormente estipulada, o objetivo geral consiste em analisar como o profissional contábil percebe na prática a segurança das informações contábeis no ciberespaço. Especificamente, almejou-se: i. compreender a ocorrência dos processos de cibersegurança em um escritório contábil; ii. verificar o conhecimento dos profissionais contábeis quanto a cibersegurança; iii. descrever a percepção desses profissionais contábeis quanto a segurança das informações na prática contábil; e, iv. identificar fragilidades e potencialidades da segurança das informações contábeis relacionadas às rotinas de trabalho.

Ademais, o presente estudo justifica-se pela busca de uma maior compreensão e constatação da utilização das tecnologias de segurança da informação no intuito de propiciar um ambiente seguro à atuação do profissional contábil, visto que a informação pode ser considerada um dos principais ativos de uma empresa, conforme ressalta a norma ABNT NBR ISO/IEC 17799 (2005). Inseridos em um ambiente extremamente competitivo, faz-se necessário que os gestores se baseiem em dados confiáveis para atender a rapidez do fluxo informacional (Faria, Maçada & Kumar, 2017).

Além disso, a ausência de estudos referentes a segurança da informação no âmbito contábil foi constada por Herath (2011), o que ressalta a importância de pesquisas nesta área, pois podem trazer resoluções aos problemas encontrados na prática. O profissional contábil ainda não possui uma percepção mais apurada quanto a segurança das informações, se tornando

mais vulnerável a ataques cibernéticos, visto que não são feitos investimentos consideráveis na estrutura de segurança informacional (Herath, 2011).

Torna-se relevante a realização dessa pesquisa, pois acredita-se ser significativo que o profissional se aproprie das tecnologias como um instrumento importante no desempenho de suas funções, segundo Oliveira (2003), as empresas que aderiram à contabilidade informatizada obtiveram resultados satisfatórios e assim buscaram cada vez mais melhorias nesse processo. Nesse contexto surge a necessidade de proteger essas informações, visto que para a Academia Latino-Americana da Segurança da Informação (2006), a segurança da informação tem como objetivo proteger o registro das informações independentemente de onde estas estejam situadas.

2. CONTABILIDADE

É uma ciência social cujo objetivo é mensurar a informação, registrar e interpretar os fatos ocorridos, e assim poder informar os aspectos do patrimônio de uma entidade e oferecer informações referentes a variação e a composição patrimonial (Greco & Arend, 2016). O objetivo da contabilidade, conforme discorrem Szuster et al. (2008), é fornecer informações úteis para o planejamento, controle e tomada de decisões de uma entidade, por meio de dados que demonstrem a situação econômica e financeira da entidade.

Diante disso, surge a responsabilidade do profissional contábil, tratada no Código Civil (Brasil, 2002), podendo responder pessoal e solidariamente, perante a empresa e terceiros, inclusive com o patrimônio pessoal. Além disso, o Código (Brasil, 2002) estabelece que esse profissional tem o dever de reparar aquele que, por ato ilícito, causar dano a outrem. Este dano pode advir de ação ou omissão voluntária, negligência ou imprudência (Brasil, 2002). Portanto, a partir do momento que a ação ou omissão do contador acarretar algum dano para o seu cliente ou terceiro, nasce a obrigação do mesmo em repará-lo integralmente.

O Código de Ética Profissional do Contador – CEPC vigente é previsto na NBC PG 01, e tem por objetivo fixar a conduta do contador no exercício de suas atividades e em assuntos relacionados à classe, podendo ser classificado o sigilo como um dos mais importantes deveres contador (CFC, 2019). Com o avanço das tecnologias, manter sigilo quanto a documentos e informações tem se tornado um problema, pois os profissionais da contabilidades guardam todas as informações contábeis, sejam fiscais ou financeiras de seus clientes, mantê-los seguros é necessário, tendo em vista o crescente número de empresas que comercializam dados de seus clientes sem autorização (Zanatta, 2015).

A partir das ocorrências de vazamentos de dados, em agosto de 2018 foi criada a Lei Geral de Proteção de Dados - LGPD, Lei nº 13.709 (Brasil, 2018), a qual visa ter maior transparência no uso e tratamento das informações pessoais, buscando assim prevenir invasões e roubos de dados (Cots & Oliveira, 2018). Desse modo, pode-se dizer que a referida lei vem também para orientar o papel do contador, pois apresenta como sua principal finalidade aumentar a proteção à privacidade dos indivíduos (Brasil, 2018). A partir da evolução da contabilidade juntamente com a tecnologia surgiu a necessidade de informatização das informações contábeis, tornando os sistemas de informação, os mais novos aliados e inimigos da contabilidade moderna.

3. SISTEMAS DE INFORMAÇÃO

O conceito de Sistema de Informação (SI) é dado a um conjunto de elementos, ou dados, que estão inter-relacionados, e neste meio há três procedimentos básicos (Stair & Reynolds, 2015). Desse modo, constata-se que os SI podem auxiliar os gerentes e colaboradores a analisar problemas, criar produtos que atendam às suas necessidades, e otimizem seus processos, ou

achar soluções (Oliveira, 2008). Esse autor define que SI como um conjunto de meios físicos e lógicos, financeiros, organizacionais, e humanos que interagem entre eles de forma racional, de forma a integrarem-se com o propósito de produzir, memorizar e distribuir informação, atendendo as necessidades dos gestores.

Nos SI são encontradas informações relativas a pessoas, fatos e locais com algum significado para a organização ou para o ambiente em que está inserida (Laudon & Laudon, 2014). Para esses autores dados são fatos sequenciais que ainda não foram analisados ou processados, os quais representam eventos ocorridos nas organizações ou em um ambiente físico, antes de serem tabulados e organizados de forma a serem compreensíveis pelos que o utilizam, e informação são dados que quando modelados passam a ser úteis e significativos para os usuários.

Os Sistemas de Informação Contábil (SIC) servem como instrumento de armazenamento das informações de acordo com os critérios contábeis aceitos, nesse sentido conceitua-se SIC como "o sistema de informação contábil pode ser definido como o conjunto de recursos humanos e de capital dentro da organização o qual é responsável pela preparação de informações financeiras e também das informações obtidas da coleta e processamento dos dados das transações" (Padoveze, 2000, p. 45).

Define-se um SIC, como uma estrutura unificada dentro de uma organização a qual engloba recursos físicos dentre outros componentes, a fim de transformar dados financeiros e econômicos em informação contábil, assim tendo o objetivo de atender as necessidades de seus usuários (Wilkinson et al., 2000). Para quaisquer níveis de atuação das empresas, sejam eles tático, operacional ou estratégico, é importante que a informação contábil seja modelada de acordo com o propósito, pois a forma tradicional, ou seja, a que atende ao fisco é diferente da que utilizamos com finalidade gerencial (Padoveze, 2016).

D'Andrea (2017) cita que o interesse das empresas em ter funções e processos críticos de seus negócios suportados pela tecnologia em nuvem, como a contabilidade, as operações e os recursos humanos, está crescendo. No entanto, o autor complementa que o campo cibernético ainda enfrenta muitas adversidades como o vazamento de informações.

A Associação Brasileira de Comunicação Empresarial – ABERJE em seu site destaca a pesquisa realizada pelo escritório de auditoria PricewaterhouseCoopers – PwC, no ano de 2017. Com o título de *Global Economic Crime and Fraud Survey*, a associação demonstra os principais crimes que as empresas sofreram nos últimos 24 meses, sendo:

a) fraude em compras (34% no Brasil e 22% no mundo);
b) corrupção ou suborno (26% no Brasil e 25% no mundo);
c) fraude cometida pelo consumidor (24% no Brasil e 29% no mundo);
d) crime cibernético (22% no Brasil e 31% no mundo);
e) fraude contábil (22% no Brasil e 20% no mundo);
f) má conduta empresarial (19% no Brasil e 28% no mundo).

A média percentual no Brasil é maior do que no mundo para os crimes de fraude em compras, corrupção ou suborno. Diante desse contexto não se pode ignorar o cuidado com a segurança dos dados, desse modo a seguir trata-se da cibersegurança.

3.1 CIBERSEGURANÇA

Pode-se definir cibersegurança como uma fração da segurança da informação, a qual refere-se a metodologia utilizada para proteger as informações no ciberespaço, a fim de evitar o furto de dados ou alterações (Nunes, 2012). Para isso se faz necessário a criação de estratégias de cibersegurança com o objetivo de gerenciar riscos, identidades e incidentes desse modo assegurando uma reação mais eficiente (Nunes, 2012).

As principais atividades da cibersegurança, segundo discorre Ralo (2013), são monitorar, prevenir e responder as ameaças que possam colocar em risco o espaço de liberdade coletiva ou individual, e a responsabilidade por esse serviço é de competência das forças de segurança e serviço de informações. Para Couto (2018), o principal objetivo da cibersegurança é assegurar a disponibilidade, integridade e confidencialidade dos ativos em relação às ameaças do ciberespaço.

Nesse sentido, a necessidade de criar ferramentas de proteção, com objetivos de assegurar a livre circulação na internet, está direcionando para a criação e cultivo de uma cultura de cibersegurança, auxiliando diretamente na no desenvolvimento das políticas de combate aos ataques cibernéticos afirma (IDN-CESEDEN, 2013).

O Centro Superior de Estudos da Defesa Nacional de Espanha do Instituto de Defesa Nacional (IDN-CESEDEN) (2013) apresentam o surgimento de normativos, os quais definem princípios e normas destinados a proporcionar sustentabilidade e um comportamento aceitável no ciberespaço. De acordo com a definição da *International Telecommunications Union* - ITU, a cibersegurança é definida como conjunto de guias, ferramentas, enfoques na gestão de risco, boas práticas e tecnologias de proteção de ativos organizacionais e usuários do ambiente virtual (ITU, 2009).

Os ativos são dispositivos conectados à rede, serviços e aplicações, bem como sistemas de telecomunicações e informação transmitida e armazenada no mundo virtual (ITU, 2009). A cibersegurança tem como finalidade assegurar a integridade e confidencialidade dos ativos em relação às ameaças existentes no ciberespaço (ITU, 2009). Na busca constante pela segurança no ciberespaço a ITIL (*Information Technology Infrastructure Library*), emitiu um processo de gestão de segurança das informações, o qual objetiva a garantia de que, conforme discorre BMC Software (2017), as informações estejam disponíveis para utilizar quando necessário.

Desse modo a ITIL não se trata apenas de uma metodologia de implantação de processos de cibersegurança, mas sim um agrupamento das melhores práticas que podem ser aderidas conforme as necessidades de cada organização (Magalhães & Pinheiro, 2007).

4. METODOLOGIA

O presente estudo teve como objetivo analisar como o profissional contábil percebe na prática a segurança das informações contábeis no ciberespaço, diante disso a pesquisa é classificada como qualitativa, descritiva e estudo de caso. Quanto a abordagem do problema, o estudo se apresenta como qualitativo, pois busca analisar a utilização da cibersegurança nos sistemas de informações pelo profissional contábil em sua prática. A definição da pesquisa qualitativa se dá pela relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números (Prodanov & Freitas, 2013).

No que tange aos objetivos o presente estudo discorre de forma descritiva, pois buscou observar, analisar, interpretar e identificar as ferramentas utilizadas sem a interferência do pesquisador diretamente no ambiente pesquisado. A pesquisa descritiva exige do investigador uma série de informações sobre o que deseja pesquisar, além disso exige um planejamento rigoroso no que tange à definição dos métodos e técnicas para a coleta e análise de dados Oliveira (1999).

Quanto aos procedimentos técnicos, utilizou-se de estudo de caso abordando um escritório de contabilidade, no intuito de aprofundar o conhecimento acerca dos processos e rotinas que envolvem a cibersegurança e segurança da informação contábil no contexto contábil, mediante os SI utilizados no escritório pesquisado. Esse aprofundamento, a busca por compreensões das razões e uma possível sugestão de resoluções de problemas relacionados ao

assunto estudado caracterizam o estudo de caso (Gil, 2017). Em outras palavras Yin (2010) elucida que o estudo de caso se trata de um estudo empírico que busca compreender o fenômeno atual dentro do seu contexto de realidade.

A unidade pesquisada para a coleta de dados refere-se a um escritório de contabilidade de um município da região central do Rio Grande do Sul. Para a coleta de dados utilizou-se de entrevista semiestruturada visando auxiliar no confronto dos objetivos com a realidade analisada. O roteiro de entrevistas foi desenvolvido a partir do referencial teórico apresentado. A escolha dos entrevistados se deu por conveniência do pesquisador. Para isso, definiu-se colaboradores com cargos de gestão e de gerência, bem como do responsável pela TI da empresa pesquisada. Nesse sentido, convidou-se para participar da entrevista o diretor geral, os gerentes contábil e fiscal, e o sócio da empresa pesquisada, e, o diretor da empresa a qual presta serviços de TI. O convite para participar da pesquisa ocorreu mediante contato prévio por e-mail e telefone, momento em que se apresentou o objetivo da pesquisa.

Após o aceite, agendou-se uma data para realizar a entrevista. As entrevistas foram realizadas no mês de outubro de 2019, individualmente, em local de preferência de cada entrevistado. A coleta de dados ocorreu por intermédio de gravação de áudio de cada entrevista, essa gravação posteriormente foi transcrita e analisada. Por meio da autorização institucional houve aceite da participação do escritório na pesquisa, contudo, exigiu-se anonimato, portanto, o nome da empresa e dos colaboradores foram preservados.

Os entrevistados, no momento de cada entrevista, receberam um Termo de Confidencialidade que assegura que as informações fornecidas serão utilizadas única e exclusivamente para execução do presente estudo. Além disso, o pesquisador obteve assinatura no Termo de Consentimento Livre e Esclarecido que dá ciência sobre o objetivo, procedimentos, benefícios, riscos e sigilo da pesquisa e autoriza a participação dos entrevistados no estudo.

A partir da gravação das entrevistas estes áudios foram transcritos em documentos de processamento de texto e posteriormente analisados. A fim de interpretar e compreender os dados coletados de maneira objetiva e sistemática foi utilizada a técnica de análise de conteúdo categorial a posteriori (Bardin, 2011), a qual serve para identificar os objetivos do presente estudo nos resultados alcançados, permitindo o enlace entre a teoria e a prática, no caso desta pesquisa refere-se ao embasamento teórico adotado. A seguir detalham-se os resultados.

5. ANÁLISE DOS RESULTADOS

A análise dos resultados é segregada em SIC, Caracterização dos Entrevistados e Categorias de Análise, apresentadas a seguir.

5.1 SIC

O sistema contábil que o escritório em estudo utiliza é o Athenas 3000, este sistema é subdividido em módulos: Administrativo, Fiscal, Contábil e Pessoal. Cada módulo opera de maneira independente, mas ao mesmo tempo estão interligados. São realizadas as integrações de operações no módulo fiscal, pessoal e administrativo integralmente na Contabilidade, bem como os lançamentos no Administrativo são informados no Fiscal.

No módulo administrativo são realizados lançamentos de liquidação e gestão de contas a pagar e a receber, gestão de estoque para as empresas que utilizam do Athenas como um Sistema Integrado de Gestão Empresarial (ERP), emissão de notas fiscais, boletos de cobrança, emissão de ordem de serviços, lançamentos bancários, cadastro de clientes e de fornecedores, relatórios de vendas. A Figura 1 apresenta os módulos do sistema e detalha o administrativo.

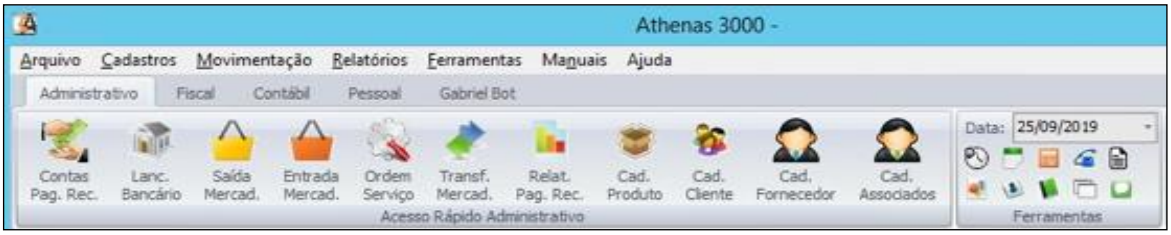

Figura 1. Módulo Administrativo
Fonte: Sistema Athenas 3000.

No módulo Contábil (Figura 1) são efetuados cadastros referentes à contabilidade: plano de contas, centros de custo, notas explicativas, bens do ativo imobilizado, relatórios contábeis e gerenciais, demonstrativos, rotinas contábeis de integrações. Nesse módulo também se efetuam apurações de depreciação e amortização, lançamentos contábeis, conciliações de contas contábeis, emissão de relatórios contábeis como balancetes, balanços, diários, razões, demonstrativos de resultado, relatórios de evolução de saldo das contas contábeis. Ainda, geram-se arquivos para importação em programas da Receita Federal: Escrituração Contábil Fiscal e Escrituração Contábil Digital.

Ainda, no módulo Fiscal são escrituradas as notas fiscais de compras vendas, serviços prestados e tomados, é possível escriturar por meio da importação dos arquivos XML ou importação da movimentação fiscal de sistemas ERP (Figura 1). Neste módulo constam livros para conferência de notas fiscais. Ainda, realiza-se o cadastro de fornecedores e pessoas, cadastro de parâmetros como Código Fiscal de Operações e Prestações (CFOP), produtos, Documento de Arrecadação de Receitas Federais (DARF), códigos de serviços de acordo com a legislação.

No Fiscal (Figura 1) são apurados os tributos federais, tais como PIS, COFINS, IRPJ, CSLL, Simples Nacional, e estaduais como o ICMS. Após a apuração destes tributos pode-se emitir os DARF e até o Documento de Arrecadação do Simples Nacional (DAS) de maneira automatizada, na qual o usuário executa somente a impressão do documento que já estará preenchido de acordo com o valor apurado.

Por fim, o módulo Pessoal é utilizado exclusivamente pelos usuários alocados no Departamento Pessoal, neste módulo é feito o cadastro de funcionários do escritório e dos clientes, no momento da admissão realiza-se todo o procedimento admissional de acordo com os documentos recebidos da empresa. Também cadastram autônomos, sócios e sindicatos (Figura 1). É possível cadastrar verbas, cargos, funções e benefícios, dados que serão utilizados posteriormente na apuração da folha de pagamento.

Por meio do módulo Pessoal efetua-se o lançamento de variáveis e o cálculo da folha. Após processada a folha encerra-se o período e apura-se a Guia da Previdência Social (GPS) de forma automatizada, necessitando-se apenas que o usuário realize a impressão. No módulo Pessoal existem relatórios relativos à folha de pagamento e movimentações trabalhistas, como agenda de férias, relatórios cadastrais com a movimentação de funcionários, admissões e demissões de um período e demais relatórios personalizáveis (Figura 1).

No momento da admissão de um funcionário, especificamente para trabalhar no escritório pesquisado, são realizadas entrevistas prévias, a partir da admissão o novo colaborador é alocado em um setor. Ao definir o setor, o coordenador responsável pelo setor e equipe deve solicitar ao coordenador de TI a criação do novo acesso aos servidores, e-mail e acesso ao sistema, bem como em qual nível hierárquico este funcionário se enquadra para que seja disponibilizado as permissões adequadas a ele.

Todos usuários possuem acesso ao módulo administrativo, portanto as restrições são diferenciadas com os funcionários do setor contábil e fiscal, que possuem acesso aos módulos

contábil e fiscal, e funcionários do setor pessoal acessam apenas o módulo pessoal. Há algumas restrições em rotinas, como as de cadastro que se restringem apenas aos coordenadores, e gerência, ficando aos demais permitido apenas as rotinas operacionais e de relatórios.

Os treinamentos aos novos usuários ocorrem de forma individual, sendo estes orientados pelos integrantes que já compõem a equipe, principalmente pelo seu coordenador. O treinamento é realizado durante o expediente e a demonstração das rotinas se dá de acordo com a demanda do momento. Se iniciar as atividades em um período na qual se está realizando operações no fiscal, o mesmo receberá as devidas orientações para operar no módulo fiscal, e na sequência, quando iniciar a contabilidade receberá o treinamento para o módulo respectivo.

Não há restrição de acessos aos usuários quanto à navegação *web*, apenas é restringido o acesso aos documentos no servidor local e na nuvem com *backups* diários. Também é utilizada uma plataforma *web*, na qual realizam-se a gestão de arquivos eletrônicos, que são permanentes, pois neste ambiente os documentos são criptografados e salvos em nuvem com a responsabilidade de proteção por parte de empresa terceirizada. Nesta plataforma, os documentos são arquivados de acordo com a empresa a que pertencem, a visualização destes documentos se dá mediante permissões definidas para os usuários de acordo com a equipe em que atuam.

5.2 CARACTERIZAÇÃO DOS ENTREVISTADOS

Ao longo da coleta de dados, que ocorreu em outubro de 2019, foram realizadas cinco entrevistas com colaboradores do escritório pesquisado e um terceirizado, que correspondem às unidades de análise. Essas unidades foram formadas por conveniência, esse tipo de seleção para Gil (2017) torna uma pesquisa mais rica em termos qualitativos. As entrevistas tiveram duração superior a 30 minutos cada, foram gravadas e transcritas na íntegra. A partir das entrevistas buscou-se obter informações quanto à percepção dos entrevistados sobre cibersegurança e segurança da informação contábil.

A análise dos dados foi estruturada pelos procedimentos de organização, tratamento e análise dos dados coletados, visando compreendê-los, atender à questão de pesquisa e gerar conhecimento (Sampieri et al., 2013). A análise se deu a partir dos resultados obtidos nas entrevistas em consonância ao referencial teórico levantado. A análise de conteúdo foi realizada com ênfase em categorias a posteriori. A análise categorial é estruturada a partir dos dados obtidos nas diferentes fontes, entrevistas e manual. As categorias de análise estabelecidas de forma a representar, a partir da frequência de aspectos similares entre os relatos da maioria dos entrevistados, similitudes entre suas características comportamentais e sua percepção sobre o fenômeno que está sendo estudado (Bardin, 2011). Diante disso, na Tabela 1 são apresentadas as características das unidades de análise.

Tabela 1. **Apresentação dos entrevistados**

ENT.	SEXO	IDADE	FORMAÇÃO	TEMPO DE ESCRITÓRIO
E1	F	38 anos	Graduação em Contabilidade	13 anos
E2	F	40 anos	Graduação em Contabilidade	12 anos
E3	M	56 anos	Graduação em Contabilidade	23 anos
E4	M	38 anos	Técnico em Contabilidade	22 anos
E5	M	45 anos	Superior Incompleto	3 anos

Fonte: Autores.

A partir da Tabela 1 complementa-se que o entrevistado “E1” é contador, possui um curso de especialização em andamento e trabalha no escritório há 13 anos. A entrevistada E1

atualmente ocupa o cargo de gerente fiscal e anteriormente já ocupou cargos como supervisora, assistente e analista. O entrevistado "E2" também é contador e possui um curso de especialização em andamento, o tempo de trabalho na empresa pesquisada é de 12 anos, o cargo atual é gerente contábil. E2 já ocupou os cargos de coordenação, assistente e auxiliar.

O entrevistado "E3" também é contador, com especialização em gestão de negócios, é o diretor da empresa e está neste cargo desde sua fundação, há 23 anos. Por conseguinte, o entrevistado "E4" é formado em técnico em contabilidade, empresário e ocupa o cargo de gerente administrativo. Trabalha na empresa há 22 anos. Por fim, o entrevistado "E5" é empresário e diretor da empresa terceirizada que presta serviços de TI no escritório estudado. Atua na área de TI desde 1999, e possui uma empresa há 10 anos, presta serviços há 3 anos e meio para o escritório pesquisado.

5.3 CATEGORIAS DE ANÁLISE

Os dados foram segmentados em categorias de análise a posteriori com base em Bardin (2011), sendo: Percepção sobre segurança da informação e cibersegurança, Gestão dos riscos cibernéticos, Fragilidades na segurança das informações, Responsabilidade profissional e Potencialidades na segurança das informações, esmiuçados adiante.

5.3.1 Percepção sobre segurança da informação e cibersegurança

Uma das percepções mais mencionadas pelos entrevistados refere-se à atualidade da segurança das informações, visto que é um dos principais temas em discussão, além de configurar uma temática preocupante. Diante da ciência dos frequentes ataques cibernéticos sofridos pelas empresas, cabe ao profissional contábil ter a percepção quanto ao momento em que deve agir e as ferramentas que pode utilizar para garantir a segurança da informação contábil, para isso, o primeiro passo é desenvolver um conjunto de políticas de segurança da informação (Knapp et al., 2009). As percepções dos entrevistados sobre segurança da informação e cibersegurança podem ser observadas a seguir, nos trechos das falas destacadas.

> [...] segurança da informação do meu ponto de vista seriam ferramentas que a empresa utiliza para que seus dados não venham a ser dispostos fora da empresa por concorrentes dos clientes, ou até mesmo questão de sequestro de informações [...] Eu acho que, principalmente no Brasil ainda estamos muito vulneráveis nessa questão da cibersegurança, uma prova disso são os ataques frequentes que as empresas sofrem assim, até sites do governo [...] E1

> [...] eu acredito assim, que a questão da cibersegurança, principalmente na área contábil hoje, é um ponto muito muito sensível e muito preocupante visto que a contabilidade depende dos sistemas de informação [...] E1

> [...] segurança da informação, eu entendo, que é aquela informação que foi coletada. Ela vai ter um uso por determinadas pessoas ou empresas e que se essa informação que foi coletada para um propósito, somente aquelas pessoas ou empresas deveriam ter acesso a ela. Portanto a partir do momento que alguém não autorizado acessa essas informações, já haveria uma quebra na segurança. E2

> [...] a cibersegurança, se não houver um investimento nessas ferramentas e nessas tecnologias, é muito difícil de proteger as informações, tanto as informações a nível empresarial, como de nível pessoal. Eu acho que a gente não tem nem metade do conhecimento do que está acontecendo quando navegamos na internet. Eu acredito que tem bastante a melhorar ainda. E2

> [...] segurança da informação é ter a certeza, a convicção de que a informação vai ficar aonde tem que estar e não vai ter outras pessoas que não sejam ligadas àquela informação tendo acesso. [...] eu acho que a cibersegurança, hoje em dia é essencial, mais do que nunca, porque na medida que nós estamos mudando os arquivos digitais e toda informação que antigamente era no papel, guardando ela através da tecnologia, então ela se torna cada vez mais imprescindível, mais necessária, sem dúvidas. E3

> [...] há uma preocupação de todos, inclusive nossos clientes, de repente eles perguntam como estão as nossas informações, já que eles deixam de ter livros e todas aquelas informações palpáveis que eles tinham antes e tão dependendo exclusivamente do escritório de contabilidade, então eles estão confiando que essas informações estejam bem seguras, então além de ser sigilosa ela tem que estar segura. Então cada vez mais há uma preocupação nesse sentido. E3

> Eu não entendo muito, mas eu acho que é importante essa parte de segurança da informação, eu acho que nós devemos ter a segurança de informações para preservar os dados dos clientes. E4

> Eu não tenho conhecimento ainda da cibersegurança, nunca ouvi falar. E4

> Então o que que eu vejo hoje, hoje pra mim segurança da informação é o principal tema, pra nós o norte principal é a questão da segurança, é primordial [...] tu começa a falar de segurança, todo mundo fala "ah, segurança da informação", todo mundo pensa no ataque hacker, primeira coisa que todo mundo pensa, só que tem muita coisa envolvida antes disso em segurança, é a segurança da informação de como é que os funcionários tem acesso as informações dentro do sistema, se as informações dentro do sistema elas estão segmentadas. E5

> Então existem vários graus de segurança, várias camadas de segurança envolvidas nessa questão, a primeira delas seria: como tu tá estabelecendo tua segurança interna, dentro da tua rede interna [...] E5

Ainda que estes profissionais não apresentem um amplo conhecimento técnico do tema, percebe-se o interesse por manter seguros os seus dados, pois estes são o maior ativo que possuem, corroborando à ISACA (2013), na qual a informação deve ser reconhecida como ativo que gera benefícios às empresas. Além disso é considerada uma ferramenta que agrega valor, cria uma vantagem competitiva no mercado e deve ser usada como auxílio na gestão (Marchand, 2000).

5.3.2 Gestão dos riscos cibernéticos

Foi constatado que a gestão de riscos quanto a ataques cibernéticos no escritório pesquisado está sendo realizada por uma empresa de TI terceirizada e um colaborador responsável pelas tecnologias no escritório. Não há um manual oficializado, nem mesmo escrito, a gestão ocorre de forma informal, por meio de reuniões internas com as equipes. A empresa de TI possui alguns recursos que auxiliam na gestão, como o bloqueio de acessos ao detectarem anomalias nas máquinas. Isso vai ao encontro dos autores Knapp, Marshall, Byrd e Morris (2009), na qual a primeira medida a ser tomada pela empresa para proteger-se de eventuais ataques, sejam estes de origem interna ou externa, é desenvolver um conjunto de políticas de segurança de informação.

A gestão dos riscos cibernéticos pode ser observada nos trechos das falas dos entrevistados E1, E3, E4 e E5:

> [...] a gestão dos riscos, são tomados pela nossa empresa de TI juntamente com o responsável dessa área, que fazem essa gestão e nos colocam os pontos que são

> necessários para decisão da direção, no caso, a gestão é feita por eles na prática, com a anuência da direção. E1
>
> [...] quanto a gestão dos dados de acesso externo, como navegação, nós não temos restrições, o que nós temos é um firewall que faz a gerência de sites e acessos de risco, bem como ferramentas como antivírus que fazem essa determinação, mas nós não temos restrição quanto a essa parte. E1
>
> [...] não existe um manual escrito e oficializado mas como nós temos uma pessoa que cuida dessa parte e a empresa de tecnologia de informação que nos assessora, e que estão constantemente orientando nossos colaboradores em como agir diante dessas situações e sempre que há a necessidade de informação de algum procedimento novo, essas informações são repassadas aos coordenadores das equipes que passam para os seus colaboradores. Então não vemos a necessidade de criar um manual escrito até porque engessa muito o processo, eu acho esse tratamento diário é mais dinâmico e mais eficiente. E1
>
> [...] não tem de maneira clara isso, acho que é uma coisa que precisa ser sistematizada para a gente ter convicção de que o que foi falado seja colocado na prática e a gente possa eventualmente enxergar isso. Então hoje nós terceirizamos os sistemas de informatização, que é nosso TI, e dependemos deles. E3
>
> [...] nós contratamos uma empresa de TI, juntamente com uma pessoa qualificada que atua no escritório, para atender as demandas e para nos colocar em segurança. E4
>
> A gente estabeleceu um tipo de política que se alguma máquina trabalhar em um tipo de situação anômala, que a gente acha que é uma situação que pode estar colocando em risco a empresa, nós bloqueamos o acesso dela. [...] mas inicialmente até conseguirmos trabalhar com governança em TI, tem que ter um planejamento muito grande, a direção tem que tá envolvida, se a direção não se envolver nisso aí, não vai pra frente. E5

Tratar a segurança da informação como elemento prioritário e estratégico, conforme Pedriali, Arima e Piacente (2020), é salutar para as empresas que buscam sustentabilidade em seus sistemas de gestão. Para isso, os usuários devem ser sensibilizados quanto às questões de segurança das informações, demonstrando-se que uma falha ou rompimento desta segurança pode provocar efeitos negativos (Kruger & Kearney, 2008). Desse modo, é importante que se promova dentro da empresa uma cultura de segurança, garantindo que as boas práticas devam ser algo natural do comportamento dos usuários (Pimenta & Quaresma, 2016).

Inevitavelmente as organizações precisam lidar com as várias ameaças e buscar identificar suas fragilidades. Diante da gestão dos riscos cibernéticos emergiu a categoria de análise fragilidades na segurança das informações, apresentada a seguir.

5.3.3 Fragilidades na segurança das informações

A partir da crescente dependência da tecnologia para obtenção de vantagem competitiva, os problemas de segurança têm sido um dos requisitos mais críticos e desafiadores para a realização de negócios bem-sucedidos (Pereira; Barreto & Amaral, 2017). Cada vez mais inseridos no mundo digital, enfrentam-se problemas que antes não eram tão visíveis, ou pelo menos não eram postos em assunto, o cuidado com os dados pessoais.

Há uma crescente preocupação de como esses dados estão sendo utilizados, e de que forma empresas os obtém, às vezes sem consentimento. O crime cibernético ascendeu nas últimas décadas, tornando-se reconhecido o ato de crime cibernético, definido como cibercrime, a partir do qual a conscientização com os gastos em segurança da informação sofreu um

aumento (ISACA, 2013). A seguir são apresentados os trechos das falas sobre as fragilidades da segurança das informações.

> A gente sabe que hoje as empresas de marketing também se utilizam de captura desses dados, a gente não sabe muito bem como esses dados pessoais nossos, enquanto pessoas físicas são capturados, e vendidos num mercado negro... Então não sabemos até que ponto isso não poderia evoluir para uma venda de informações confidenciais de empresas. E1

> [...] é muito difícil estar à frente e prever ataques, justamente pela velocidade do desenvolvimento dessas tecnologias, tanto para o bem quanto para o mal, então o que eu vejo que acontece na atualidade de uma forma global é que os ataques acontecem, e justamente quando eles acontecem é porque não houve uma previsão deles, e a partir daí, de um problema ocorrido é que se tomam as providências e essas providências se espalham de uma forma global. As dificuldades que eu percebo é que alguns investimentos são muito altos e acabam se tornando inviáveis para o porte da empresa e dentro do orçamento e fluxos de caixa, porque nem sempre conseguimos medir a eficácia desses investimentos, então acaba parecendo na maioria das vezes que eles foram investimentos que não deram retorno. E1

> A terceirização dessa mão de obra é uma dificuldade que enfrentamos, pois como não temos conhecimento específico dessa área, precisamos confiar no que nos dizem, por mais que sempre busquemos nos informar e aprofundar um pouco mais sobre o assunto, não possuímos o domínio pleno. E1

> Há dificuldades sim, e a maior é a gente ter a confiança em primeiro lugar em quem nos está prestando um serviço. Então nós precisamos buscar um embasamento seguro de quem nos presta serviço nessa área, tanto externa como interna, segundo que para garantir a segurança exige muito investimento tanto em dinheiro, valores monetários, como em tempo que também reflete valores, então há essas dificuldades nesse sentido que talvez muitos não invistam como deveria porque o custo ainda é elevado, mas não há como fugir dele... Eu acho melhor ver essa questão do custo como um benefício que ele só é percebido quando realmente há um ataque e tu consegue se proteger, pois não é um investimento palpável. E3

> [...] quanto maior a rotatividade de funcionários, maior é o risco de vazar as informações dos clientes, mas como eu digo isso é difícil de controlar, fazemos reuniões, e orientamos os colaboradores [...] Uma das dificuldades é a questão de custo, porque as ferramentas são caras, então buscamos no mercado as melhores ferramentas, mas sabemos que elas têm custos elevados. E4

> [...] aí tu me pergunta “nosso ambiente local tá totalmente seguro?” não, nosso ambiente local não está totalmente seguro, nós temos backups, mas backup dos dados, nós não temos ainda backup das máquinas, portanto, se acontece algum desastre com aquela máquina e nós precisarmos recuperar ela em 30 minutos a gente não tem, pra isso precisamos adquirir mais hardware pra conseguir contemplar. E5

> [...] a parte de segurança, a parte de tratamento de dados, ele entra como custo pra empresa, e a empresa que não tinha isso e agora ela tem que gastar com isso, se torna um custo alto, pois a empresa tem que gastar com backup, backup em nuvem, e ela vê isso somente como custo e não como um investimento. E5

> [...] cada vez mais tem novos tipos de riscos, se parar para analisar há cinco ou seis anos atrás não tinha sequestro de dados. E por que que ocorre isso muito no brasil, o sequestro de dados? Porque o brasil é um ambiente muito vulnerável, porque ele não tem uma política de antivírus, ele não tem uma política de backup, ele não tem uma política de licenciamento de software, a grande maioria das empresas não tem por que empresa não quer investir. E5

> Então, qual a melhor solução para segurança? Analisar o ambiente e tentar aumentar o número de variáveis, tentar atacar o maior número de variáveis, quanto mais variáveis tu atacar, mais investimento tu vais fazer, e menor será o teu risco, quanto menos variáveis tu atacar, menor será o teu investimento e maior o teu risco, é inevitável. Sabe, então o que eu vejo hoje nessa questão aí? é a direção compreender isso, quando a direção compreende e ela acha que é valido destinar um valor X pra segurança, ela vai começar a colher esses frutos. E5

Percebe-se que as falas dos entrevistados denotam a preocupação quanto à segurança e o alto custo necessários para manter as informações seguras, bem como a necessidade de confiança nas pessoas que trabalham com essas informações e as empresas que prestam serviços de proteção. Isso é reforçado por Sarder e Haschak (2019) que afirmam que a violação da segurança cibernética representa um desafio dinâmico para as empresas e ameaça suas operações e sua vantagem competitiva.

5.3.4 Responsabilidade profissional

A responsabilidade profissional sobre informações de outrem sempre existiu, mas atualmente a preocupação é maior devido ao meio em que os dados estão inseridos, ambientes virtuais, onde a informação flui de forma mais rápida (Gois, 2018). Com o avanço das tecnologias, manter sigilo quanto a documentos tem se tornado um problema, pois os profissionais guardam todas as informações contábeis, fiscais e financeiras de seus clientes.

Nesse contexto, manter esses dados seguros é necessário, ainda mais tendo em vista que é crescente o número de empresas que estão comercializando dados de seus clientes sem autorização (Zanatta, 2015). Diante disso surgiu a LGPD (Brasil, 2018) que visa proteger os dados, fiscalizando as empresas neste sentido, esta lei fará com que os profissionais tomem medidas a fim de atendê-la, conforme anteriormente referenciado neste estudo. A seguir constam os trechos das falas de todos os entrevistados sobre a responsabilidade profissional quanto a segurança das informações contábeis.

> É uma responsabilidade imensa, na verdade, essa responsabilidade sobre as informações dos usuários e clientes, e de dados financeiros ela sempre existiu, desde a existência da contabilidade, a questão é o meio e a rapidez com que o vazamento dessas informações podem fluir hoje em dia, mas essa responsabilidade sempre foi muito grande e ela sempre existiu, então também é uma confiança baseada em relações contratuais e eu entendo que isso seja um princípio ético da profissão do contador. E1

> Eu acho que a responsabilidade é total, porque assim como antigamente existiam os documentos físicos que a gente tomava todo cuidado para não extraviar, e até na hora de descartar, para que não fossem usados para outras coisas. Eu acho que a gente tem total responsabilidade, até porque hoje em dia existe o comércio desses bancos de dados. Acredito que se a gente recebe a informação, e estamos em posse daquela informação, penso que a responsabilidade seja sim do contador. E2

> A responsabilidade é total, porque na medida que as empresas, e os clientes confiam em nós, é nosso dever, e nossa obrigação ter essa responsabilidade, por isso é muito importante saber com quem você está compartilhando, buscando alternativas para essa segurança. Então responsabilidade de um escritório de contabilidade é toda, não tem dúvida. E3

> Eu acho que essa responsabilidade é muito importante, mesmo porque hoje também o profissional da contabilidade, se nós formos analisar esta nova geração, a geração "y" e "z" onde é muito fácil a troca de funcionários de um escritório para outro, então

> eu acho que o funcionário ele tem que estar com essa consciência de que as informações das empresas devem ficar seguras com ele. E4

> [...] responsabilidade que a empresa tem com os dados dos clientes dela, no caso do escritório de contabilidade se tem 100, 200, 500 empresas ele tem que ter uma responsabilidade sobre isso, com certeza tem que ter responsabilidade, e isso na empresa porque que a gente bate tanto na tecla que tem que ter um ambiente seguro, porque eu não estou preocupado somente com as informações administrativas do escritório de contabilidade, porque eu sei que tem informações de 300, 400, 500 empresas ali dentro, então é delicado, é bastante delicado. E5

Desse modo, percebe-se nas falas dos entrevistados a preocupação deles quanto a sua responsabilidade profissional, seja de manter os dados de clientes em sigilo, bem como a maneira que seus funcionários se utilizam destes dados. Carneiro (2009), propõe a segurança da informação no que diz respeito ao pessoal, ou seja, os funcionários que atuam em uma empresa, quando o principal foco é o risco associado a roubo, fraude, ou a utilização dos recursos de má fé.

Diante do exposto Carneiro (2009) menciona algumas questões fundamentais para se observar: a seleção e recrutamento dos recursos humanos, documentação para apoio à atuação, como manuais e normativos internos, formação dos recursos humanos, motivação e sensibilização dos colaboradores. Garantir que todos tenham conhecimento da política de segurança e que a empresa tenha uma gestão de acesso e uso da informação é imprescindível.

5.3.5 Potencialidades na segurança das informações

Apesar das dificuldades percebidas pelos entrevistados e as ameaças existentes na atualidade, pode-se identificar que existem maneiras de se proteger e os profissionais estão se utilizando delas na medida do possível, investindo recursos monetários e humanos para que cada vez mais possam se sentir seguros neste mundo conectado. Segundo descreve o ISACA (2010) um dos fatores na proteção da informação está em determinar e constituir boas bases para uma gestão eficaz da segurança da informação.

> Nós temos um serviço terceirizado de tecnologia da informação, bem como um responsável no setor que nos ajuda em relação a essas questões de sistemas, porque nós como gestores não temos como nos envolver no operacional dessas questões então nós precisamos nos cercar de pessoas que tenham o "*know how*", e confiar nelas para que elas cuidem dessa parte, então hoje isso melhorou muito, além desse serviço terceirizado e desse setor especifico dentro da empresa, nós temos backups em nuvem e outras ferramentas que é possível diante do nicho no nosso mercado e do porte da nossa empresa. Além disso, há cerca de um ano e meio atrás fizemos um investimento bem alto, então hoje trabalhamos apenas com a manutenção desse investimento, eu acredito que se tratando de região e porte da nossa empresa estamos dentro daquilo que é possível ter como ferramenta de segurança. E1

> O controle das informações das empresas clientes é feito através de bloqueios no sistema contábil que utilizamos, portanto, cada equipe só pode ter acesso às empresas as quais eles trabalham, e cada usuário tem a sua senha particular para acessar esses dados. E trabalhamos muito dentro do que é confiança, "em velocidade de confiança", digamos assim, e acreditamos também que nossos colaboradores estando consoantes com missão e valores da nossa empresa se utilizam do principal que é a ética de não compartilhar essas informações com as demais pessoas, quanto acesso e de outras informações que estejam fora do sistema também. Possuímos uma estrutura de usuários e senhas que é de uso pessoal e que não é compartilhada com demais usuários. E1

> Conforme os ataques e os vírus vão evoluindo, os antivírus evoluem também, e eles acabam exigindo mais recursos das máquinas. Então estamos sempre atentos para que essas ferramentas não atrapalhem o desempenho do trabalho de forma geral e para que elas possam funcionar corretamente, e não aconteça de o usuário ir lá e desconectar o seu antivírus, por exemplo. E1
>
> Essas informações dos clientes, acredito que estão mais protegidas por estarem ficando em um servidor mais seguro. E2
>
> Nós optamos em ter nosso sistema nuvem, onde a segurança se multiplicou e deixou bem mais tranquilo, então tiramos a informação de dentro do escritório e colocamos dentro de um servidor mais adequado, na nuvem, com toda a segurança que ela proporciona, ainda contamos com backups, então mesmo assim se der problema temos condições de recuperar informação rapidamente. E3
>
> Acredito que estamos no caminho certo, contratamos uma empresa de TI confiável que consegue fazer toda parte de backups e a segurança das informações de nossos clientes, temos uma pessoa qualificada na área que nos dá todo apoio que precisamos, e controla todas essas questões de TI. Então creio que estamos no caminho certo. E4
>
> Hoje trabalhamos com dois *backups*: do Athenas e dos arquivos. Os *backups* são feitos no servidor local e exportados para nuvem. assim como nós temos hoje os nossos arquivos todos lá [...], não é porque tá na nuvem que não tá suscetível a ter um ataque, a ter um desastre lá, então tu também tem que ter o *backup* fora daquele ambiente de onde tu tem, e esse backup ele é feito diariamente, com certeza. E5
>
> O *wifi* hoje é totalmente segmentado, o nosso *wifi* e o dos clientes, os clientes não têm acesso em nenhuma parte do ambiente corporativo nosso. Hoje todas as nossas máquinas estão estabelecidas no domínio, todo usuário tem seu usuário e senha, e quando o usuário sai do ambiente a conta dele é bloqueada então a gente tem esse tipo de artificio, a nossa rede na teoria é uma rede simples, ela tem um nível de segurança, mas sempre há espaço para evolução, sempre. A parte dos nossos servidores se formos analisar o nosso core *business* tá fora, ele tá em um ambiente fora, um ambiente em nuvem, mais seguro, em um sentido de tendências a desastres, etc e tal do que nosso ambiente local. E5

Conforme observa-se nas falas dos entrevistados percebe-se que na empresa em que o estudo foi realizado há investimentos em recursos que minimizam os riscos, bem como é feita uma gestão para proporcionar maior segurança. Para Nascimento et al. (2019) critérios de segurança mais rígidos nas organizações proporcionam maior credibilidade às informações geradas pelos sistemas que as mesmas utilizam.

5.3.6 Sumarização dos resultados

A sumarização dos resultados foi desenvolvida como forma de facilitar a compreensão e visualização dos resultados obtidos em cada uma das categorias de análise. Os resultados são apresentados na Tabela 2.

Tabela 2. **Sumarização das categorias de análise**

CATEGORIAS DE ANÁLISE	**Percepção**	Importância da segurança da informação e cibersegurança; Requer melhorias
	Gestão dos riscos cibernéticos	Informal; Terceirizada
	Fragilidades	Alto custo; Confiança; Falta de governança em TI
	Responsabilidade profissional	Total; Gigantesca
	Potencialidades	Nuvem; Restrição; Responsável pela TI

Fonte: Autores.

Na categoria Percepção (Tabela 2), observa-se que os entrevistados percebem a segurança das informações e a cibersegurança como algo importante em suas rotinas de trabalho, mas também apontam que precisam ser realizadas melhorias em seu ambiente, bem como de modo geral no país, conforme observado no referencial teórico. Quando se fala em gestão dos riscos cibernéticos nota-se que a gestão é terceirizada à uma empresa de TI, e existe uma pessoa responsável pelo TI dentro do escritório pesquisado. Esta gestão está ocorrendo com os funcionários de forma informal, com treinamentos personalizados e informativos no decorrer de atualizações do sistema ou da legislação, para que se possa atuar de acordo com as normas vigentes.

As fragilidades relatadas são questões difíceis de serem sanadas pela empresa pesquisada, principalmente devido ao alto "custo" das tecnologias de proteção, ao se buscar uma maior proteção recorre-se àquelas menos onerosas financeiramente. "Confiar" nas pessoas que manuseiam as informações das empresas, bem como garantir que não se tenha vazamentos de dados por funcionários é um risco que a empresa corre, pois não tem como garantir que terceiros sejam éticos, além disso, identificou-se a "falta de uma governança em TI". A partir do Tabela 2, na categoria Responsabilidade Profissional, os entrevistados percebem esta questão como algo "gigantesco", pois sempre existiu no exercício da profissão e atualmente com o novo modelo de trabalho ela é "total", aumentando a importância da profissão contábil, não só com a intenção de atender legislação, mas também pela ética profissional.

Quanto às potencialidades da segurança das informações menciona-se que o escritório fez investimentos em tecnologias há alguns anos, com a migração de servidores para a "nuvem", por exemplo, o que trouxe maior confiança para os gestores, pois estão mais seguros, com a realização de *backup* diariamente. Além disso, foi aprimorado a política de "restrições" entre os colaboradores, por meio da qual estruturou-se hierarquias de permissões e acessos, ou seja, somente gestores possuem acesso a tudo, os demais usuários manuseiam e visualizam apenas o que lhe é permitido. Menciona-se ainda que o escritório pesquisado possui um "responsável pela TI" que atua internamente analisando o cenário atual e buscando melhorias e tratamentos das deficiências observadas, realiza também a gestão de dados e permissões.

Na Figura 2 é apresentada uma nuvem de palavras com os termos que apareceram com mais frequência nas falas dos entrevistados.

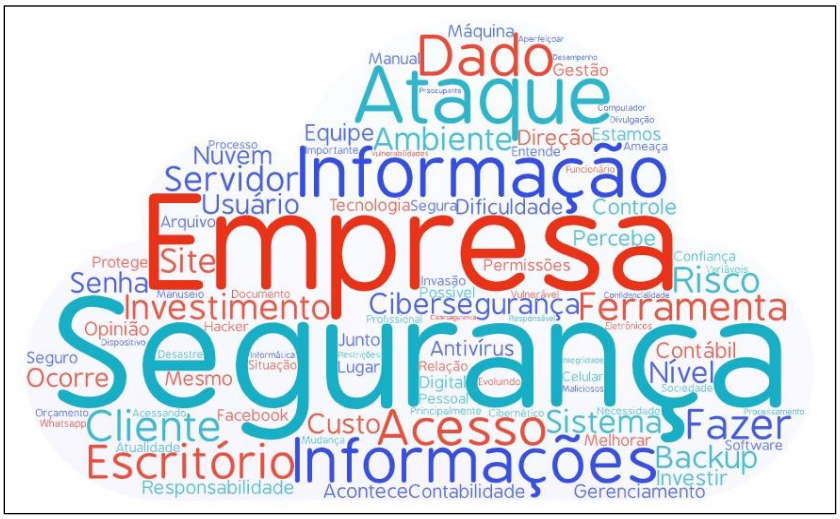

Figura 2. Nuvem de palavras
Fonte: Autores.

As palavras mais mencionadas pelos entrevistados (Figura 2), foram: Segurança, empresa, informação, ataque, acesso, dentre outras. A partir disso percebe-se que todas essas

palavras citadas estão de alguma forma interligadas e fazem parte do cotidiano do escritório em estudo. Os entrevistados denotam preocupar-se com a segurança das informações, mesmo que ainda alguns não possuam muito conhecimento a respeito do significa cibersegurança, a percepção sobre a importância da proteção do acesso aos dados da empresa e dos clientes se mostrou relevante mesmo diante das fragilidades identificadas.

6. CONCLUSÃO

O presente estudo teve como objetivo geral analisar como o profissional contábil percebe na prática a segurança das informações contábeis no ciberespaço. Este objetivo foi integralmente atendido a partir dos resultados obtidos por meio de entrevistas com os gerentes de cada setor, a direção do escritório pesquisado e a direção da empresa que presta serviços de TI. Com relação a percepção destes profissionais quanto a cibersegurança, percebeu-se que ainda há deficiências e um caminho a ser trilhado na busca por melhorias, pois alguns profissionais possuem conhecimento superficial sobre o tema, sequer compreendem os riscos que estão expostos.

Quanto ao primeiro objetivo específico – compreender a ocorrência dos processos de cibersegurança em um escritório contábil, tal objetivo foi alcançado na unidade de análise "Gestão dos Riscos cibernéticos". Para este objetivo identificou-se que a empresa pesquisada não possui um manual de uso e não há um controle rígido quanto aos acessos dos usuários em navegação *web*, ainda que participem de treinamentos e orientações constantes, não há nada formalizado. Também não existem tecnologias avançadas que possam minimizar os riscos, somente alguns procedimentos básicos são realizados como o antivírus nas máquinas.

Com relação ao segundo objetivo específico estabelecido – verificar o conhecimento dos profissionais contábeis quanto a cibersegurança – este objetivo foi atendido por meio das falas dos entrevistados. Verificou-se que os profissionais não possuem clareza do que é cibersegurança, ainda é uma temática que deixa dúvidas. No entanto, dentro do que conhecem do assunto, apesar de sempre buscarem alternativas e meios para promover uma maior segurança informacional, relatam que é uma temática preocupante e que não se sentem seguros.

No que se refere ao terceiro objetivo específico – descrever a percepção desses profissionais contábeis quanto a segurança das informações na prática contábil, concluiu-se que nas rotinas de trabalho há certas restrições quanto ao acesso de informações das empresas clientes, bem como restrições de uso das rotinas no sistema contábil. A empresa estruturou seus treinamentos e orientações a novos colaboradores de forma descentralizada, ou seja, cada coordenador de equipe é responsável por prestar as orientações ou delegar a um colega que já possui conhecimento. As rotinas de trabalho não são baseadas em nenhum manual, não existem regras específicas, contudo são realizados treinamentos personalizados, ministrados pela gerência aos coordenadores, de acordo com as demandas de rotinas ou legislações, os quais são replicados aos assistentes e auxiliares de cada equipe.

Por fim, o quarto objetivo específico – identificar fragilidades e potencialidades da segurança das informações contábeis relacionadas às rotinas de trabalho – foi alcançado nas categorias de análise de Fragilidades e Potencialidades na segurança das informações. Por meio da análise das falas dos entrevistados observou-se que o ambiente organizacional ainda possui diversas fragilidades, como a dificuldade de prever ataques, o alto custo de investimento que as ferramentas de proteção demandam, a confiança nos funcionários e a falta de uma governança em TI.

Já, quanto às potencialidades mencionadas, referem-se ao alto investimento que a empresa realizou para promover segurança e desempenho no uso das ferramentas no passado, portanto, hoje trabalha-se mais na manutenção das ferramentas existentes. Além disso, o SIC

utilizado na empresa permite restrições como os bloqueios de rotinas de acordo com o tipo de usuário e empresa que se atende, assim cada usuário tem acesso apenas ao que lhe é permitido. A empresa optou por ter uma pessoa responsável pelo setor de tecnologias, esta trabalha internamente analisando o cenário atual e buscando melhorias e tratamentos das deficiências observadas, realiza também a gestão de dados e permissões, o que também foi apontado como uma potencialidade.

A contribuição do presente estudo está em servir como base para um aprofundamento no assunto de segurança das informações e cibersegurança, pois a temática é atual e relevante no contexto organizacional. Ademais, a pesquisa apresenta uma constatação da percepção sobre a segurança da informação e a cibersegurança por parte de alguns profissionais em suas rotinas, o que contribui para propiciar um ambiente mais seguro à atuação do profissional contábil no escritório pesquisado. Outro ponto na qual este estudo pode contribuir é a acadêmica por possibilitar a replicação da pesquisa em outras empresas de contabilidade.

Esta pesquisa conta com alguns limitantes, o estudo contemplou apenas um escritório de contabilidade, portanto, não se espera generalizar os resultados aqui encontrados. Além disso, foram entrevistados somente cinco indivíduos que ocupam funções específicas na empresa pesquisada, dessa forma não sendo possível obter um levantamento mais amplo de percepções no que tange as temáticas pesquisadas.

A análise sobre segurança das informações contábeis, sistemas de informação e cibersegurança abre diversos caminhos para pesquisas futuras. Diante disso, seria interessante replicar essa pesquisa em empresas de tecnologias e empresas que utilizam sistemas de informação em suas rotinas de trabalho como as instituições financeiras, ou até mesmo órgãos públicos que se utilizam de sistemas para realizar cadastros e manutenção de solicitações. Ainda, para futuros estudos sugere-se realizar um levantamento de dados contemplando um número maior de sujeitos de pesquisa, bem como ampliar o número de empresas participantes.

REFERÊNCIAS

Associação Brasileira de Comunicação Empresarial. (2018). Metade das empresas brasileiras sofreu algum tipo de crime econômico. *Pesquisa da PWC*. Disponível em: https://www.pwc.com.br/pt/sala-de-imprensa/noticias/metade-das-empresas-brasileiras-foi-vitima-de-crimes-economicos-nos-ultimos-dois-anos.html

ABNT NBR ISO/IEC 17799. (2005). Tecnologia da informação: técnicas de segurança. *Código de práticas para a gestão da segurança da informação*. 2. ed. Rio de Janeiro.

Abu-Musa, A. A. (2003). The Perceived Theats to the Security Computerized of Computadorized Accounting Information Systems. *Journal of American Academy of Business.* Cambridge, v. 3.

Academia Latino Americana de Segurança da Informação. (2006). *Introdução à ABNT NBR ISO/IEC 17799:2005*. Microsoft Technet. Disponível em: http://download.microsoft.com/download/8/4/3/843dd576-aab2-462e-8a8d-88c0eee2db5e/ISO17799_Modulo1.pdf

Bardin, L. (2011). *Análise de conteúdo.* São Paulo: Edições 70.

BMC Software. (2017). *ITIL para pequenas empresas*. Disponível em: http://documents.bmc.com/products/documents/32/95/63295/63295.pdf

Brasil. (2002). *Código Civil*. Lei n. 10.406, de 10 de janeiro de 2002. Presidência da República, Brasília, DF. Disponível em: www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm

Brasil. (2018). *Lei n. 13.709 de 14 de agosto de 2018*. Lei de proteção de dados pessoais. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Carneiro, A. (2009). *Auditoria e Controle de Sistemas de Informação.* Rio de Janeiro: FCA - Editora Informática.

Conselho Federal de Contabilidade. (2019). *Resolução NBC PG 01*, de 07 de fevereiro de 2019. Aprova a NBC PG 01-Código de Ética Profissional do Contador. Disponível em: http://www2.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2019/NBCPG01&arquivo=NBCPG01.doc

Couto, J. C. P. (2018). *Auditoria de Cibersegurança: um caso de estudo.* 2018. 181 p. Dissertação (Mestrado em Auditoria) - Instituto Superior de Contabilidade e Administração do Porto, Instituto Politécnico do Porto, Portugal.

Cots, M., & Oliveira, R. (2018). *Lei geral de proteção de dados pessoais comentada*. 1. Ed. São Paulo: Thomson Reuters Revista dos tribunais.

D'Andrea, E. (2017). Cyber e Privacidade da informação. *Pesquisa global de segurança da informação.* Mar. Disponível em: https://www.pwc.com.br/pt/10minutes/assets/2017/10_min_Cyber_e_Privacidade_da_informação_17.pdf

Faria, F., Maçada, A. & Kumar, K. (2017). Modelo estrutural de governança da informação para bancos. *RAE-Revista de Administração de Empresas*, v. 57, n. 1, p. 79-95.

Gil, A. C. (2017). *Como elaborar projetos de pesquisa.* 6. ed. São Paulo: Atlas.

Greco, A. & Arend, L. (2016). *Contabilidade:* teoria e prática básicas. 5. ed. São Paulo: Editora Saraiva.

Gois, A. B. (2018). Segurança cibernética: o olhar da defesa nacional e da inteligência de estado frente às vulnerabilidades digitais. *O comunicante*, v. 8, n. 3.

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

Horngren, C. T., Sundem, G. L. & Stratton, W. O. (2004). *Contabilidade gerencial.* Tradução de Elias Pereira. 12. ed. São Paulo: Pearson Prentice Hall.

Huerta, E. & Jensen, S. (2017). An Accounting Information Systems Perspective on Data Analytics and Big Data. *Journal of Information Systems*, v. 31, n. 3, p. 101-114.

IDN-Ceseden. (2013). Estratégia da Informação e Segurança no Ciberespaço. Lisboa: Instituto da Defesa Nacional. *Caderno IDN*. Disponível em: https://docplayer.com.br/28249-Cadernos-estrategia-da-informacao-e-seguranca-no-ciberespaco-no-12-instituto-da-defesa-nacional.html

ISACA. (2010). *Information systems audit and control association IT Standards*, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals. USA: ISACA.

ISACA. (2013). Information systems audit and control association *COBIT 5*: Transforming Cybersecurity. Guide Using COBIT 5. ISACA.

International Telecommunication Union. (2009). *Understanding cybercrime:* a guide for developing countries. Technical report. Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

Knapp, K. J., Marshall, T. E., Byrd, T. A. & Morris, R. F. (2009). Information security policy: An organizational-level process model. *Computers & Security*, v. 28, n. 7.

Kruger, H. A. & Kearney, W. D. (2008). Consensus Rankink-An ICT security awareness case study. *Computers & Security*, v. 27, n. 1, p. 254-259.

Laudon, K. C. & Laudon, J. P. (2014). *Sistemas de informação gerenciais.* 11. ed. México: Pearson Educacion.

Magalhães, I. L. & Pinheiro, W. B. (2007). *Gerenciamento de TI na prática:* uma abordagem com base na ITIL: inclui ISO/IEC 20.000 e IT Flex. São Paulo: Novatec Editora.

Marchand, D. A. (2000). *Competing with Information:* A Manager's Guide to Creating Business Value with Information Content. New York: John Wiley & Sons.
Miller, G. & Skinner, D. (2015). The evolving disclosure landscape: how changes in technology, the media, and capital markets are affecting disclosure. *Journal of Accounting Research*, v.53, n. 2, p. 221-239.
Nascimento, D. J., Bento, M. L., Silva, V. P., Nascimento, L. G. & Pederneiras, M. M. M. (2019). Características do uso de sistemas ERPS na gestão de informações e controladoria no ramo da construção civil: um estudo de caso numa empresa paraibana. *Braz. J. of Develop.*, Curitiba, v. 5, n. 10, p. 22472-22493, out.
Norton Cybersecurity Insights Report Global Comparison. (2017). Disponível em: https://br.norton.com/norton-cybersecurity-insights-report-brazil
Nunes, P. V. (2012). A definição de uma estratégia nacional de cibersegurança: cibersegurança. *Caderno n. 133 IDN*. Lisboa.
Oliveira, A. M. S., Faria. A. O., Oliveira. L. M. & Alves. P. S. L. G. (2008). *Contabilidade internacional*: gestão de riscos, governança corporativa e contabilização de derivativos. São Paulo: Atlas.
Oliveira, E. (2003). *Contabilidade informatizada.* 3. ed. São Paulo: Atlas.
Oliveira, S. L. (1999). *Tratado de metodologia científica*: projetos de pesquisas, TGI, TCC, monografias, dissertações e teses. 2. ed. São Paulo: Pioneira.
Padoveze, C. L. *Contabilidade gerencial:* um enfoque em sistema de informação contábil. 3. ed. São Paulo: Atlas, 2000.
Padoveze, C. L. (2016). *Controladoria básica.* 3. ed. São Paulo: Cengage Learning.
Pedriali, D., Arima, C. H. & Piacente, F. J. (2020). Segurança da informação na Logística 4.0: um estudo bibliométrico. *Research, Society and Development*, v. 9, n. 2.
Pereira, T., Barreto, L. & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, v. 13, p. 1253–1260.
Pimenta, A. M. & Quaresma, R. F. (2016). A segurança dos sistemas de informação e o comportamento dos usuários. *Revista de Gestão da Tecnologia e Sistemas de Informação*, v. 13, n. 3, p. 533-552.
Prodanov, C. C. & Freitas, E. C. de. (2013). *Metodologia do trabalho científico:* métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale.
Ralo, T. J. (2013). *Artigo de opinião:* cibersegurança e ciberdefesa, direção geral de política de defesa nacional. Disponível em: http://dgpdn.blogspot.pt/2013/03/artigo-de-opiniao-ciberseguranca-e.html
Sampieri, R. H., Collado, C. F. & Lucio, M. P. B. (2013). *Metodologia de pesquisa.* 5. ed. Porto Alegre: Penso.
Sarder, M. D. & Haschak, M. (2019). Cyber security and its implication on material handling and logistics. *College-Industry Council on Material Handling Education, p*. 1–18.
Stair, R. M. & Reynolds, G. W. (2015). *Princípios de sistemas de informação.* Tradução Noveritis do Brasil. Revisão técnica Tânia Fátima Calvi Tait. São Paulo: Cengage Learning.
Szuster, N., Cardoso, R. P., Szuster, F. R., Szuster, F. R. & Szuster, F. R. (2008). *Contabilidade geral:* introdução à Contabilidade Societária. 2. ed. São Paulo: Atlas.
Wilkinson, J. W., Cerullo, M. J., Raval, V. & Wong-On. B. (2000). *Accounting information system essential concept and application,* 4. ed. John Willey & Sons Inc, New York-USA.
Yin, R. K. (2010). *Estudo de caso:* planejamento e métodos. 4. ed. Porto Alegre: Bookman.
Zanatta, R. (2015). *A Proteção de Dados entre Leis, Códigos e Programação*: os limites do Marco Civil da Internet. Em: De Lucca, N., Simão Filho, A., Lima, C. Direito e Internet III: Marco Civil da Internet. São Paulo: Quartier Latin, p. 447-470.