A Percepção do Usuário Contábil Acerca da Segurança da Informação: Um Estudo de Caso nos Escritórios de Contabilidade de São João del-Rei/MG

Thiago Coelho Souza
thiago.souza.cont@outlook.com
UFSJ

Pablo Luiz Martins
pablo@ufsj.edu.br
UFSJ

Franciane de Oliveira Alvarenga
francianealvarenga@ufsj.edu.br
UFSJ

Resumo: Em uma época em que o uso da tecnologia no processamento das informações se tornou vital para as organizações, surgiu também a necessidade de atenção ao tema de segurança da informação afim garantir a proteção das informações em posse das organizações e, consequentemente, evitar os prejuízos e a perda de credibilidade no mercado a estas. Essa preocupação é multiplicada quando falamos dos escritórios de contabilidade, visto que estes detêm uma grande quantidade de informações de clientes e ex-clientes, e, consequentemente, precisam garantir a segurança dessas informações. O fator humano é considerado como uma vulnerabilidade a ser explorada para a execução de um ataque bem sucedido contra a segurança da informação, porém muitas vezes essa vulnerabilidade passa despercebida pelos gestores das organizações, o que pode deixa-las expostas a situações indesejadas e comprometer a continuidade do negócio. Olhando por este ângulo, o presente trabalho visa avaliar a percepção do usuário contábil acerca da segurança da informação na cidade de São João del-Rei/MG. Para alcançar esse objetivo foi realizado um levantamento bibliográfico com o objetivo de contribuir como fundamentação teórica sobre o tema. Além disso, foi elaborado e disponibilizado um questionário por meio da internet com o intuito de obtenção de respostas, o qual foi submetido a uma análise quantitativa, posteriormente. O resultado obtido evidenciou certa deficiência quanto ao conhecimento dos usuários contábeis acerca do assunto, desconhecendo certas medidas de segurança e agindo muitas vezes de forma

oposta ao recomendado, o que podemos associar a falta de políticas e treinamentos voltados para a segurança da informação por parte dos escritórios onde prestam serviços.

Palavras Chave: Contabilidade - Informações - Segurança - -

1. INTRODUÇÃO

Devido ao grande avanço tecnológico ocorrido nos últimos anos, se tornou vital para as organizações a adesão de sistemas de informações no dia-a-dia das empresas. Tal fato se tornou de extrema necessidade visto o aumento contínuo de transações comerciais, bancárias, obrigações, comunicação, entre outras atividades que tem como base o mundo digitalizado para a troca de informações a todo instante. Porém é importante ressaltar que esse "mundo digitalizado" está exposto a diversas ameaças diferentes que aumentam diariamente e podem comprometer a segurança de tais informações.

Nos escritórios de contabilidade o uso de informações tem grande relevância quando se trata de seu funcionamento, uma vez que a cada dia se tornam cada vez mais dependentes do uso de sistemas de informações para a realização de sua rotina diária, onde informações são recebidas e enviadas para seus clientes a todo instante, assim como também para o governo para o cumprimento de obrigações acessórias, por exemplo. Para que isso ocorra de maneira eficiente e segura, é de suma importância que tais informações sejam: confiáveis, disponíveis e íntegras.

De modo a evitar a perda da qualidade da informação, se viu necessário que as organizações voltassem sua atenção para a segurança dos sistemas de informações e um dos seus componentes merece destaque especial para que qualquer medida, política ou método possa funcionar: o fator humano. Para Mitnick, o fator humano tem grande importância quando tratamos da segurança de sistemas de informações, porém é também considerado como o componente mais vulnerável.

A Verizon (uma das principais empresas de telecomunicações do mundo) apresentou um relatório referente ao ano de 2018 onde em um terço dos casos de ataques sofridos pelas empresas, o autor utilizou da engenharia social para realizá-lo, ou seja, tais ataques ocorreram utilizando a falha humana como uma brecha para sua concretização. Dantas (2011) considera a falha humana como uma das maiores preocupações por parte das empresas para a implementação de políticas e treinamentos voltados para segurança da informação,

Neste contexto, o presente artigo apresenta o seguinte problema: Qual a percepção do usuário contábil acerca da segurança da informação nos escritórios de contabilidade da cidade de São João del-Rei do estado de Minas Gerais?

Corroborando com o problema apresentado anteriormente, o objetivo principal desse artigo é avaliar qual a percepção do usuário contábil dos escritórios de contabilidade da cidade de São João del-Rei do estado de Minas gerais acerca da Segurança da Informação. Como objetivos secundários, o presente artigo busca analisar o conhecimento dos usuários contábeis acerca da segurança da informação e verificar se existe alguma política de segurança da informação nos escritórios contábeis.

Em relação a metodologia utilizamos o modelo de pesquisa de levantamento, que tem como principal característica a interrogação direta das pessoas, onde foi elaborado um questionário que foi disponibilizado por meio da internet e remetido por e-mail tendo como alvo os escritórios contábeis e seus funcionários localizados na cidade de São João del-Rei no estado de Minas Gerais, e, posteriormente, foi realizada uma análise qualitativa dos dados coletados.

Atualmente, os sistemas de informações são considerados como essenciais dentro dos escritórios de contabilidade para a continuidade dos negócios e, devido a isso, a segurança da informação é indispensável. Considerando o disposto acima, a escolha do tema "A percepção do usuário contábil acerca da informação: Um estudo de caso nos escritórios de contabilidade de São João del-Rei/MG" se mostra relevante com o intuito de ampliar pesquisas e discussões acerca de um assunto tão importante e, muitas vezes, negligenciado pelos proprietários de escritórios contábeis denominado como segurança da informação, e buscando avaliar o nível

de conhecimento do funcionário que está em contato diário com informações sigilosas de diversas empresas.

2. REFERENCIAL TEÓRICO

2.1 Informação

A informação é definida por Lyra (2015) como um conjunto de dados tratados e organizados de maneira que traga significado ou sentido dentro do contexto, podendo assumir diferentes formas, como a informação falada, impressa, armazenada de maneira eletrônica, etc... Entretanto, independente da forma como a informação se encontra, sua segurança deve ser zelada.

A informação passa a ter valor para uma empresa ou usuário a partir do momento em que ela se torna, de alguma forma, útil para o mesmo. Segundo a NBR ISO/IEC 27002 (2005), a informação é considerada como um ativo essencial para a continuidade dos negócios de uma organização, sendo ela necessária para tomada de decisões, controle de estoque, controle de ativos, redução de custos, entre outras finalidades voltadas para a gestão.

Dantas (2011) acrescenta que a ausência da informação pode levar a extinção da organização, de onde surge a necessidade de sua proteção, o que é reforçado pelo TCU (Tribunal de Contas da União, 2012, p.10) que considera que “Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais.” Conforme os autores, a partir do momento em que a segurança da informação é comprometida de alguma forma, esta passa a colocar as operações e a existência das organizações em grande risco, onde podemos observar a necessidade, assim como também deve ser considerado como prioridade, a manutenção das informações de maneira segura.

Em 2018, afim de assegurar o valor da informação para as organizações, foi publicado o Ajuste Sinief nº 21/20, que altera o Ajuste Sinief 07/05, na qual restringe o acesso as informações contidas nas notas fiscais eletrônicas à somente os participantes da operação comercial descritos no documento eletrônico, tais como: emitente, destinatário, transportador e terceiros que forem informados na nota, como o contador, por exemplo. O ajuste já foi prorrogado algumas vezes, mas entrou em vigor a partir do dia 07/07/2020.

2.2 Sistemas de Informações

De modo a entender melhor o conceito relativo a segurança da informação, é necessário conceituar o que são sistemas de informações. Oliveira (2001, p. 277) define como “o processo de transformação de dados em informações”.

Stair & Reynolds (2002, p.20) tratam sistemas de informação como “um conjunto de elementos ou componentes inter-relacionados que coleta (entrada), manipula (processo), armazena e dissemina dados (saída) e informações, e fornece uma reação corretiva (mecanismo de realimentação) para alcançar um objetivo. “

O`Brien (2004, p.6) contribui definindo Sistemas de informações como “Um conjunto organizado de pessoas, hardware, software, redes de comunicações e recursos de dados que coleta, transforma e dissemina informações em uma organização”. Para se obter a segurança da informação de maneira efetiva, é preciso que cada um dos elementos, citados por O`Brien, que compõem o sistema de informações tenha a devida atenção. Daí surge a necessidade de adoção de procedimentos, políticas e boas práticas por parte das organizações visando alcançar esse objetivo.

No âmbito da contabilidade, um dos objetivos dos sistemas de informações é auxiliar os gestores na tomada de decisões fornecendo informações úteis para que isso ocorra, deixando de ser apenas um instrumento fiscal utilizado pelo governo para o envio das obrigações diariamente.

Conforme o que define Padoveze (2009):

> O Sistema de Informação Contábil ou Sistema de Informação de Controladoria são os meios que o contador geral, gerencial ou controller utilizará para efetivar a contabilidade e a informação contábil dentro da organização, para que a contabilidade seja utilizada em toda sua plenitude. (Padoveze, 2009, p.123)

Para que tal plenitude seja alcançada, é de extrema necessidade que a qualidade das informações seja mantida para que as organizações consigam utilizar os sistemas de informações contábeis para a tomada da melhor decisão possível em relação a situação atual da mesma de maneira confiável. Sendo assim, surge a necessidade da implantação da Segurança da informação nas organizações.

2.3 Segurança da Informação

A NBR ISO/IEC 27001 define Segurança da Informação como a proteção da informação de vários tipos de ameaças de modo a garantir a continuidade dos negócios e complementa que para que isso ocorra deve ser mantido a "Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas." (NBR ISO/IEC 27001, 2006, p.2)

Hintzbengen et al. (2018) trata a confidencialidade, integridade e disponibilidade como princípios críticos da segurança da informação, e devem ser respeitados como tal afim de preservar o valor de uma informação.

Considerados como os três pilares mais importantes para a segurança da informação, a confidencialidade, integridade e disponibilidade são utilizados como base para criação e implantação de políticas de segurança da informação nas organizações.

Confidencialidade: busca prevenir que a informação não seja divulgada de maneira intencional ou acidental restringindo seu acesso aos usuários delimitados. Dessa forma, apenas usuários autorizados terão acesso as informações armazenadas ou transmitidas. (Hintzbergen et al., 2018)

Integridade: princípio que busca prevenir a alteração da informação, sendo ela mantida na mesma condição na qual foi disponibilizada inicialmente, sem que possa ocorrer qualquer alteração indevida, de modo intencional ou não. (Sêmola, 2003). A informação perde a integridade quando houver qualquer alteração na mesma, seja a inserção ou exclusão de dados.

Apenas definir quem pode ter acesso às informações garante a confidencialidade, porém não a integridade das mesmas. É necessário que as organizações definam também quem tem o poder de alterá-las ou deletá-las, restringindo assim o poder apenas de consulta para algumas pessoas. Isso limita a possibilidade de quebra da integridade, assim como também facilita a identificação do responsável de qualquer alteração que possa ocorrer. Os backups (cópias de segurança) também é uma medida importante afim de assegurar a integridade tornando reversíveis certas alterações.

Disponibilidade: tal princípio garante que a informação ou ativos associados esteja disponível para uso quando necessário para aqueles que tem autorização para seu uso. (Beal, 2008). Caso a informação não esteja disponível por qualquer que seja o motivo, o princípio da disponibilidade é quebrado

Lyra (2008) destaca ainda outros aspectos que servem como complemento para os princípios da segurança da informação:

Legalidade: que visa garantir que o sistema esteja dentro dos conformes das leis vigentes no local;

Autenticidade: que tem como finalidade garantir a legítima identificação do usuário que está enviando ou modificando a informação, e;

Não repúdio: princípio que garante que nem o emissor nem o receptor da informação possam negá-la.

É importante ressaltar ainda que o custo da segurança da informação deve ser proporcional aos benefícios que isto trará para a organização. Apesar de algumas exceções existirem, na grande maioria das vezes a organização deverá avaliar o custo que será dispendido e o valor da informação a ser protegida. (Caruso e Steffen, 1999)

No ano de 2019, a Cert.Br (grupo responsável por registrar os incidentes relacionados à segurança de sistemas de computação ou redes de computadores) registrou 875.327 incidentes relacionados a segurança da informação, sendo o maior número registrado (com exceção do ano de 2014 que alcançou a incrível marca de mais de 1 milhão de incidentes registrados).

Em 2018, houve um marco importante relativo a segurança da informação no brasil, quando foi sancionada a Lei Nº13.709/2018, denominada como Lei Geral de Proteção de Dados (LGPD), que regulamenta o tratamento de dados pessoais de clientes e usuários pelas empresas, sejam públicas ou privadas, sendo que o não cumprimento das exigências que constam na lei pode acarretar em multas que podem chegar a até 50 milhões de reais por infração, conforme art. 52, inciso II, da referida Lei. A LGPD gera grande impacto no tratamento de dados das empresas, tornando necessárias as adoções de medidas de segurança da informação de forma imediata (caso ainda inexistentes). Um ponto a ser destacado é que caso ocorra algum “incidente de segurança que possa acarretar risco ou dano relevante aos titulares”, a lei pode obrigar que as organizações façam a divulgação do incidente em meios de comunicação, o que pode causar perda de confiança perante clientes e fornecedores.

2.4 Vulnerabilidades e ameaças

Conforme Semôla (2003):

> A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada. (Semôla, 2003, p.18)

Dantas (2011) define vulnerabilidades como fragilidades que podem provocar danos decorrentes da utilização dos dados em qualquer fase do ciclo de informações, sendo que Sêmola (2003) complementa que tais fragilidades ao serem exploradas passam a permitir os incidentes na segurança da informação.

Segundo Dantas (2011):

> As vulnerabilidades podem advir de vários aspectos: instalações físicas desprotegidas contra incêndio, inundações e desastres naturais; material inadequado empregado nas construções; ausência de políticas de segurança para RH; funcionários sem treinamento e insatisfeitos nos locais de trabalho; ausência de procedimentos de controle de acesso e de utilização de equipamentos por pessoal contratado; equipamentos obsoletos, sem manutenção e sem restrições para sua utilização; software sem patch de atualização e sem licença de funcionamento, etc. (Dantas. p.25, 2011)

A prioridade de uma organização que tenha como objetivo manter a segurança de suas informações é justamente identificar e reduzir essas vulnerabilidades, e, consequentemente, o risco de sofrer um incidente. A simples existência de uma vulnerabilidade não provoca incidentes contra a informação, porém isso pode ocorrer quando tal vulnerabilidade entra em contato com algum tipo de ameaça.

Diferente das vulnerabilidades, as organizações não têm controle das ameaças que as rodeiam, sendo que basta que uma vulnerabilidade exista para existir a chance de que uma ameaça possa entrar em contato com a mesma para causar danos a um sistema ou organização.

Segundo Campos (2007), "a ameaça é um agente externo ao ativo de informação, que se aproveitando de suas vulnerabilidades poderá quebrar a confidencialidade, integridade ou disponibilidade da informação suportada ou utilizada por esse ativo" (Campos, p.25, 2007). Sêmola complementa tratando ameaças como agentes ou condições que causam incidentes comprometendo as informações e seus ativos ao explorarem as vulnerabilidades.

Dantas (2011) classifica as vulnerabilidades em oito categorias diferentes que são descritas por ele como:

Naturais: este tipo de vulnerabilidade tem relação com as condições da natureza ou meio ambiente. Como exemplo podemos citar as empresas que estão localizadas em um lugar suscetível a enchentes, o que pode ser considerado como uma vulnerabilidade.

Organizacional: as vulnerabilidades organizacionais englobam a falta de constituição de políticas e procedimentos de segurança da informação pelas empresas. Para exemplificar temos a falta de treinamento e conscientização dos funcionários; ausência de políticas de segurança e planos de contingência.

Física: as vulnerabilidades físicas estão relacionadas com o ambiente na qual as informações são processadas. Podemos citar como exemplo: instalações elétricas inadequadas o que pode ocasionar um incêndio; ausência de geradores de energia; a ausência de câmeras de segurança para inibir furtos e roubos, entre outros.

Meios de armazenamento: são todos os equipamentos físicos utilizados para o armazenamento de dados, tais como: pen drives, HD`s internos e externos; etc. Como vulnerabilidades podemos citar a depreciação desses equipamentos; defeitos de fabricação; roubo; entre outros. As vulnerabilidades desse grupo tornam como obrigatório o armazenamento das informações em, no mínimo, dois locais diferentes.

Comunicação: nessa categoria os meios de comunicação podem ser considerados como vulnerabilidades. Isso pode ocorrer devida a má escolha dos sistemas de comunicações; a falta de criptografia do sistema escolhido e a conexão a redes múltiplas são alguns dos exemplos.

Humanas: como já citamos anteriormente, o fator humano é uma das vulnerabilidades que mais preocupam os especialistas da área. Tais vulnerabilidades se dão por meio da falta de treinamento ou conhecimento acerca da segurança da informação, assim como as atividades desempenhadas afim de evitar erros. O treinamento dos funcionários torna-se essencial para aumentar a conhecimento dos mesmos acerca do tema da segurança da informação, fazendo com que estes tenham consciência das vulnerabilidades e ameaças a qual estão sujeitos, assim como entenderem a importância da instalação de atualizações do sistema, gerenciamento das senhas que estão em seu poder, medidas gerais de segurança, entre outras ações com o objetivo de mitigar os riscos.

As vulnerabilidades descritas acima merecem atenção por parte dos gestores dos escritórios de contabilidade, buscando meios de evitá-las ou, pelo menos, mitigar os danos causados pelas mesmas, garantindo assim a segurança das informações.

2.5 Segurança da informação nos escritórios de contabilidade

Os escritórios de contabilidade trabalham com grande volume de documentos e informações de diferentes empresas, informações estas de grande valor, tais como: extratos bancários, dados pessoais de funcionários, fornecedores e clientes, entre outras diversas informações sigilosas, sendo que, recentemente a contabilidade digital se tornou uma realidade ao redor do mundo. As informações registradas antes em grandes quantidades de papéis, hoje são enviadas e recebidas quase que totalmente pela internet, o que exige que os gestores dos escritórios de contabilidade façam investimentos na área de segurança da informação visando a proteção desses ativos afim de garantir a continuidade do negócio.

Atualmente, diversas atividades necessárias para as atividades dentro dos escritórios de contabilidade e funcionamento das empresas em geral ocorrem eletronicamente, como por exemplo: a emissão de notas fiscais, recebimento e envio de documentos em geral, alterações contratuais, admissão de novos funcionários, entre outras operações, sendo que muitas delas só se tornaram possíveis devido a utilização de certificados digitais.

O Relatório de Investigações de Violações de Dados 2020 divulgado pela Verizon (Data Breach Investigations Report – DBIR), que considerou 32 mil ataques e 4 mil invasões executadas, reunindo dados de 81 países, apontou que 22% dos vazamentos ocorreram por falha humana. Além disso, o relatório aponta que 30% dos vazamentos envolveram atores internos, fato que vem tendo um aumento nos últimos anos. Apesar disso, o relatório entende que seja mais provável que isso tenha relação com erros e não que tenha sido de forma intencional. Tal fato reforça a falta de instrução dos funcionários presentes nas empresas onde lidam diariamente com diversas informações, demonstrando a necessidade de treinamento e conscientização dos mesmos.

Considerado por Mitnick e Simon (2003) como “o elo mais fraco da segurança”, o fator humano necessita grande destaque no processo de adoção e manutenção de medidas de segurança da informação. Os autores reforçam ainda que as organizações em geral se preocupam na maior parte das vezes com soluções para a redução de riscos das ameaças relacionadas a área da informática, deixando o fator humano em segundo plano, sendo que talvez este seja o que necessite de maior atenção.

Em escritórios contábeis, por exemplo, o fator humano é aquele que estará em contato constante com as informações dos clientes e basta a existência de um funcionário mal treinado (ou mal-intencionado) para que este possa causar danos, muitas vezes irreparáveis, a partir das informações na qual tenha acesso. De modo a evitar isso, as organizações devem adotar diversas políticas de segurança minimizando o risco de um incidente.

O TCU (2012) define as políticas de segurança como:

> ...conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial, e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações. (TCU, 2012, p.10)

A definição é complementada por Soares (1997), definindo políticas de segurança como um conjunto de leis e regras que têm como objetivo regular o comportamento de uma organização em função do gerenciamento, proteção e distribuição de suas informações e recursos.

A partir da implantação de Políticas de Segurança as organizações conseguem definir procedimentos, normas e ferramentas a serem adotados afim de reduzir os riscos e prevenir incidentes de maneira estratégica. Tais políticas irão definir quais ações são aceitáveis ou não pela empresa, limitando o acesso das informações à somente aqueles que precisam desta e adotando procedimentos que deverão ser tomados por todos que tiverem acesso às informações, sejam estes colaboradores, clientes ou fornecedores.

É recomendado que os programas de treinamento e conscientização sobre segurança da informação sejam elaborados visando a participação de todos os funcionários inclusive os novos. (Mitnick e Simon,2003). Ao implantar as políticas de segurança, as diretrizes a serem tomadas devem ter uma linguagem de fácil compreensão para seus usuários, onde a companhia deve pressupor que seus colaboradores não possuem conhecimento algum sobre o assunto. Além disso, devem deixar bem claro a necessidade de adoção das normas de segurança pela empresa, sendo exigido que elas sejam respeitadas por todos os funcionários, inclusive nos cargos mais altos.

De acordo com o TCU (2012), a adoção de senhas por parte das organizações também é considerada como uma importante política de segurança, porém é válido mencionar que a falta de proteção dos arquivos as mantém organizadas pode deixar a organização vulnerável a ataques. Uma pessoa não autorizada em posse do identificador do usuário (ID) e senha do mesmo, pode livre acesso ao sistema ao se passar por um usuário autorizado podendo vir a causar danos à organização. Também em relação a senha é recomendado: evitar seu registro em papel, assim como seu compartilhamento; alterar as senhas de forma regular; não incluir senhas em processos automáticos; manter sua confidencialidade; entre outras medidas de segurança.

3. METODOLOGIA

De modo a alcançar os objetivos propostos no presente artigo foi utilizado o modelo de pesquisa de levantamento que consiste em obter dados e informações sobre opiniões de um grupo de pessoas selecionado como representante da população para análise posterior mediante procedimentos estatísticos, denominado também como método Survey. Segundo Gil (2002):

> As pesquisas deste tipo caracterizam-se pela interrogação direta das pessoas cujo comportamento se deseja conhecer. Basicamente, procede-se à solicitação de informações a um grupo significativo de pessoas acerca do problema estudado para, em seguida, mediante análise quantitativa, obterem-se as conclusões correspondentes aos dados coletados. (Gil, 2002, p.50)

A partir daí foi elaborado um questionário com a finalidade de avaliar a percepção dos respondentes acerca da segurança da informação. Segundo Uwe Flick (2013), os estudos por meio de questionários têm como propósito obter respostas comparáveis de todos os participantes, sendo que para isso as questões são elaboradas e apresentadas de forma idêntica a todos eles. As opções de respostas do questionário foram elaboradas com base na escala de Likert sendo enumeradas em “1 - Discordo totalmente” à “5 – Concordo totalmente”, e “1 – Nunca” à “5 – Sempre”. A escala de Likert foi criada com o objetivo de mensurar o sentido e intensidade de uma atitude. (Likert, 1932)

Tal questionário foi disponibilizado por meio da internet e remetido por e-mail aos possíveis respondentes tendo como alvo os escritórios contábeis e seus funcionários localizados na cidade de São João del-Rei no estado de Minas Gerais. O questionário foi elaborado com 27 questões tendo como opções de resposta: “1-Discordo totalmente” à “5-Concordo totalmente” na primeira parte do questionário das questões relacionadas a avaliação da percepção dos respondentes, e “1-Nunca” à “5-Sempre” na segunda parte nas questões relacionadas ao escritório de contabilidade em que os respondentes se encontravam empregados no momento. Foram obtidas 28 respostas sendo que 27 foram consideradas como válidas.

A partir dos dados coletados por meio do questionário, estes foram submetidos a análise quantitativa para obtenção de resultados. Richardson (1999) caracteriza a análise quantitativa pelo emprego da quantificação das maneiras mais simples, como percentual e médias, às mais complexas, como coeficiente de correlação e análise de regressão, o que varia de acordo com o objetivo a ser atingido.

4. ANÁLISE DE RESULTADOS

O questionário para coleta de dados foi disponibilizado na internet através de um link podendo ser respondido entre a data 24 de setembro à 23 de novembro do ano de 2020. Os escritórios de contabilidade localizados na cidade de São João del-Rei/MG, na qual são os alvos da pesquisa, foram convidados a participar por meio de um convite enviado via e-mail. Ao final do prazo da coleta de dados, foram obtidas 28 respostas, das quais 27 foram consideradas válidas neste artigo como amostra final.

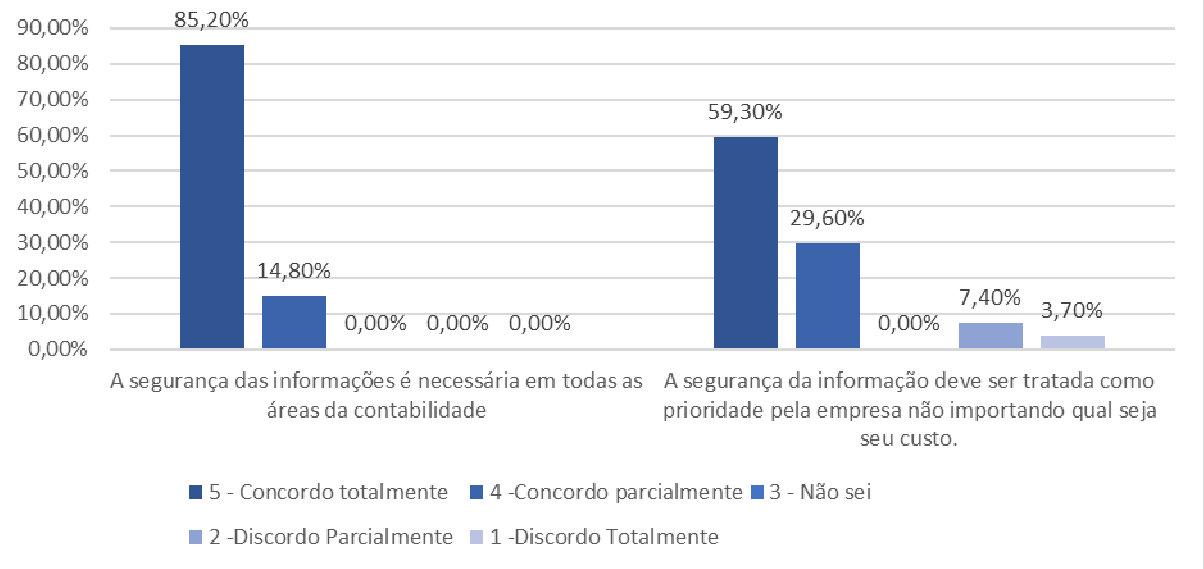
De modo a caracterizar o perfil dos elementos que compõem o estudo, os respondentes foram avaliados primeiramente pelo nível de formação, onde sua maioria possui superior incompleto com 35,7%, seguida por 32,1% com superior completo, 17,9% possuem pós-graduação e 14,3% optaram por "Outros". A maior parcela dos respondentes está cursando ou possui graduação em Ciências Contábeis, constituindo 53,6% da amostra.

Ao questionar o período em que trabalham na área da contabilidade, 57,1% responderam de 1 a 5 anos, 14,3% estão de 6 a 10 anos na área e 21,4% dos respondentes trabalham na área no período entre 11 a 20 anos.

Visando estimar o tamanho dos escritórios em que os respondentes atuam, também foi questionado a quantidade de funcionários empregados em cada deles, onde, de acordo com as respostas obtidas, 57,1% dos escritórios possuem de 6 a 10 funcionários, e 35,7% empregam de 1 a 5 funcionários, e apenas 3,7% estão empregados em escritórios com 11 a 15 funcionários, ou seja, a grande maioria atua em escritórios considerados pequenos com até 10 funcionários empregados.

Dentre os respondentes, a idade predominante é de 24 a 29 anos, representando 39,3% da amostra, 22,2% têm idade entre 30 a 35 anos, 18,5% com idade de 18 a 23 anos, e 20% dos respondentes que constituem da amostra possuem idade igual ou superior a 36 anos. É importante mencionar ainda que, do total da amostra analisada, 60,7% dos respondentes pertencem ao sexo feminino.

Gráfico 1 – Percepção quanto a necessidade e custo da segurança de informação



Fonte: Elaborado pelos autores (2021)

Conforme demonstra o gráfico 1, ao indagar a respeito da necessidade da segurança das informações, 85,2% e 14,8%, concordam totalmente ou parcialmente, respectivamente,

que a mesma é necessária em todas as áreas da contabilidade. Questionando o custo necessário para manutenção da segurança das informações, a grande maioria dos respondentes concordaram, totalmente (59,3%) ou parcialmente (29,6%), que a segurança deve ser tratada como prioridade pela empresa seja qual for o seu custo, entretanto o custo investido em segurança da informação deve ser menor do que o valor da informação a ser protegida para que faça valer o investimento da organização. Conforme Caruso e Steffen (1999), a partir de determinado valor, os custos investidos em segurança passam a serem considerados como inaceitáveis.

Quadro 1 – Conhecimento acerca dos procedimentos tomados

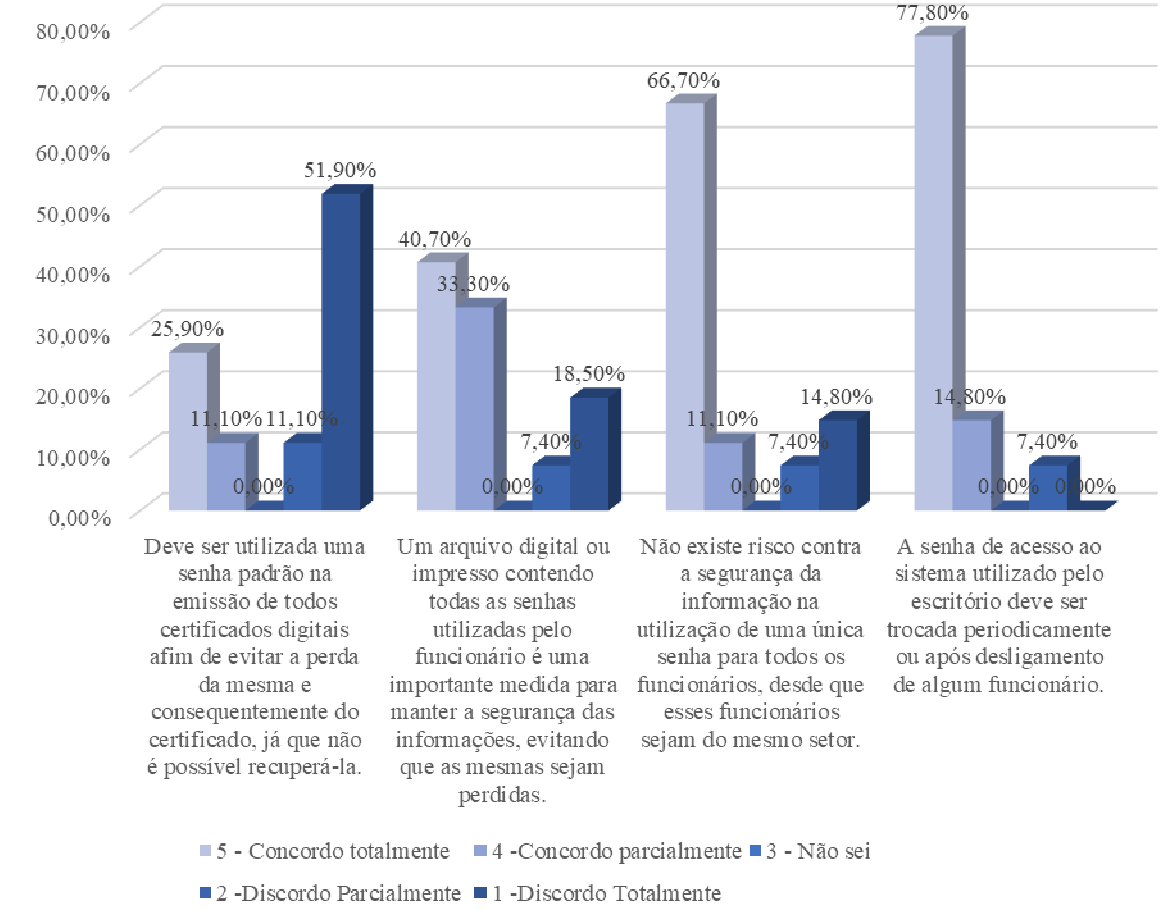
	5 - Concordo totalmente	4 -Concordo parcialmente	3 - Não sei	2 -Discordo Parcialmente	1 -Discordo Totalmente
Os computadores devem ser desligados todos os dias como uma medida de segurança de informação ou pelo menos retirar seu acesso a internet.	66,70%	14,80%	7,40%	11,10%	0,00%
O acesso aos e-mails não oferece riscos a organização.	22,20%	22,20%	7,40%	3,70%	44,40%
O acesso remoto (team viewer, any desk) não oferece risco ao cliente, desde que este esteja monitorando todo o acesso em seu próprio computador.	40,70%	18,50%	0,00%	14,80%	25,90%
Ao conectar o celular no computador utilizado no escritório o funcionário coloca a organização em grande risco.	7,40%	22,20%	3,70%	18,50%	48,10%

Fonte: Elaborada pelos autores (2021)

No quadro 1, 66,7% dos respondentes concordam que os computadores devem ser desligados diariamente como medida de proteção, o que pode ser considerado totalmente válido evitando qualquer tipo de acesso externo não autorizado durante o período noturno em que estiver ocioso, o qual podemos considerar também como período mais vulnerável devido à falta de presença de uma pessoa que possa identificar qualquer acesso externo não autorizado. Porém, 22,20% afirmam que o acesso aos e-mails não oferece nenhum tipo de risco a organização, mas de acordo com o relatório da Verizon no ano de 2020, o e-mail é considerado como principal vetor utilizado para infecções via malware. Dentre os respondentes, 40,70% afirmam que o acesso remoto não oferece risco ao cliente, desde que o mesmo esteja monitorando, entretanto, um funcionário mal-intencionado pode "facilmente" instalar softwares ou copiar arquivos para o computador da vítima sem que esta tenha ciência do que está ocorrendo no momento.

O estudo apontou que 48,10% dos respondentes discordam totalmente que conectar celulares aos computadores utilizados no escritório colocam a organização em risco, e ainda, 51,9% discordaram sobre a existência de riscos de segurança da informação em serviços em nuvem utilizados pelas organizações. Entretanto, de acordo com o relatório elaborado pela Sophos (empresa voltada para o desenvolvimento e fornecimento de softwares e hardwares de segurança) sete em cada dez empresas já sofreram algum ataque em serviços de nuvem pública.

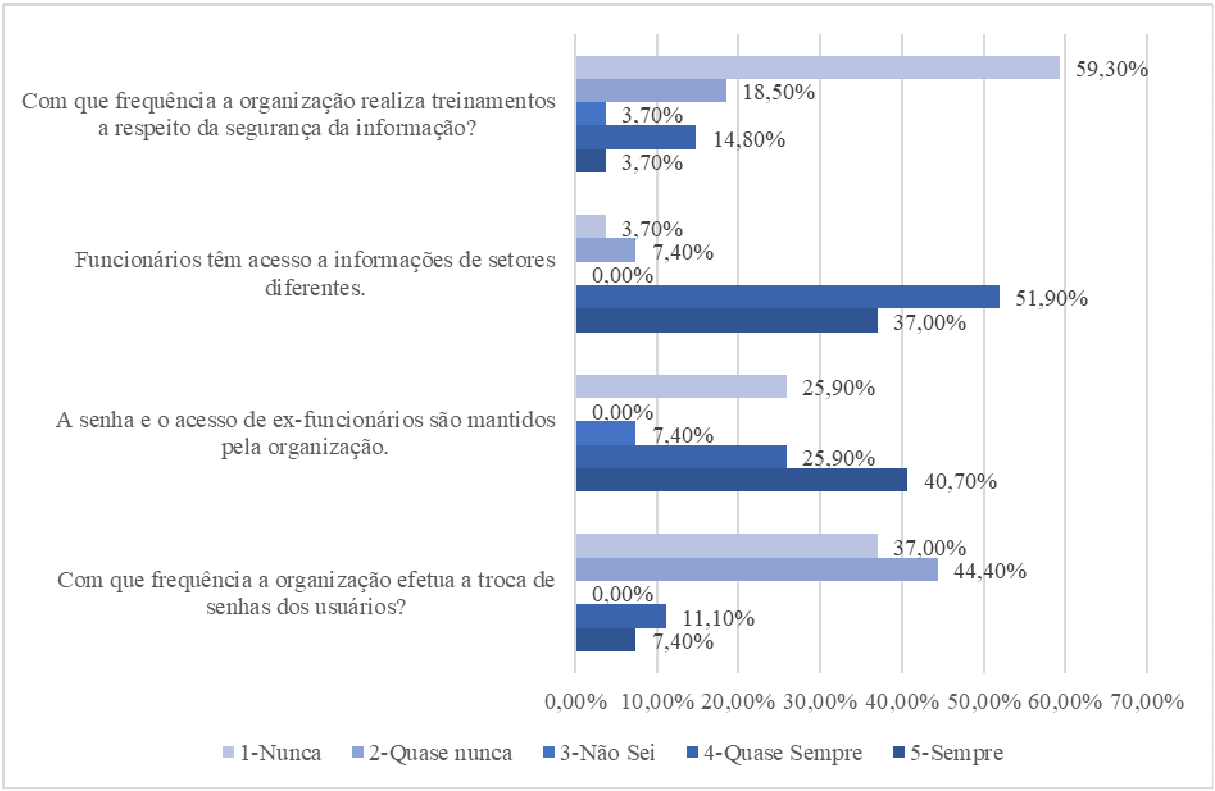
Gráfico 2 – Percepção quanto ao grau de importância das senhas



Fonte: Elaborado pelos autores (2021)

De acordo com o gráfico 2, em relação as senhas e acessos, 51,9% discordaram da utilização de uma senha padrão para todos os certificados digitais em posse da empresa, no qual podemos considerar como um ponto positivo, pois é necessário e altamente recomendado que cada certificado tenha uma senha única. O resultado apontou também que 40,7% dos respondentes concordam que deve ser mantido um arquivo digital ou impresso contendo todas as senhas utilizadas pelo funcionário, 66,7% dos respondentes concordam que não existe risco contra a segurança da informação na utilização de uma única senha para todos os funcionários, desde que estes pertençam ao mesmo setor, e, segundo consta no gráfico 2, 88,9% afirmam que os funcionários dos escritórios na qual trabalham têm acesso a informações de setores diferentes, sempre ou quase sempre. Entretanto, o TCU (2012), o compartilhamento de senhas, além do acesso de informações de setores diferentes daquele em que o funcionário pertence sem a devida necessidade não é recomendado, visto que fere o princípio da confidencialidade da informação, conforme já tratamos anteriormente. O TCU (2012) também ressalta que a falta de proteção adequada dos arquivos contendo senhas de acesso ao sistema pode comprometê-lo totalmente caso pessoas não autorizadas tenham acesso a estes arquivos.

Gráfico 3 – Políticas de segurança tomadas pelos escritórios de contabilidade



Fonte: Elaborado pelos autores (2021)

Conforme exposto no gráfico 2, a senha de acesso ao sistema utilizado pelo escritório deve ser trocada periodicamente ou após desligamento de algum funcionário, de acordo com 77,8% dos respondentes, o que é altamente recomendado afim de preservar a segurança das informações. Porém, no gráfico 3 podemos verificar que 76,6% dos respondentes responderam que a senha e o acesso de ex-funcionários são mantidos sempre ou quase sempre pela organização e 81,4% responderam que as senhas dos usuários nunca, ou quase nunca, são trocadas. o que indica que apesar dos respondentes terem ciência das medidas de segurança, como a necessidade de troca de senhas, por exemplo, estas são praticadas apenas eventualmente. O manual de Boas Práticas de Segurança da Informação – TCU (2012) recomenda o bloqueio das senhas de ex-funcionários e a troca regular de senhas, e condena o compartilhamento de senhas assim como seu registro em arquivo físico.

Dentre os respondentes do questionário, 18,5% e 59,3% afirmaram que nunca ou quase nunca, respectivamente, são realizados treinamentos a respeito da segurança da informação. Dados que se mostram preocupantes, visto que é altamente recomendado que as organizações realizem treinamentos de forma periódica afim de garantir que seus funcionários tenham um nível adequado de conhecimento acerca da segurança da informação para que possam identificar qualquer comportamento suspeito, assim como evitar que se exponham a riscos desnecessários. Ao compreenderem os riscos enfrentados diariamente, estes serão reduzidos proporcionalmente.

Quadro 2 – Políticas básicas de segurança

	5 - Concordo totalmente	4 -Concordo parcialmente	3 - Não sei	2 -Discordo Parcialmente	1 - Discordo Totalmente
Os backups são necessários apenas quando for necessária a atualização do sistema ou correção de erros do mesmo.	7,40%	22,20%	0,00%	25,90%	44,40%

Os backups realizados devem ser armazenados tanto em mídia digital quanto física.	40,70%	7,40%	0,00%	40,70%	11,10%
Para a efetiva manutenção de um nível alto de segurança das informações alguns itens são recomendados, tais como: Alarmes, Geradores de energia e Câmeras de segurança.	51,90%	7,40%	3,70%	11,10%	25,90%

Fonte: Elaborada pelos autores (2021)

No quadro 2, pode-se observar que 100% dos respondentes afirmaram que sempre, ou quase sempre, é realizado backup nos escritórios na qual trabalham. Entretanto, 40,7% deles discordam parcialmente a respeito da necessidade de armazenamento simultâneo dos backups em mídia física e digital, e 29,6% concordam, totalmente ou parcialmente, que tais backups são necessários apenas quando houver atualização do sistema e/ou correção de erros do mesmo, o que pode ser considerado como preocupante, segundo Rhee, Cheongtag, & Ryu (2009), os usuários da informação devem ser conscientes acerca da necessidade da realização de backups de maneira regular.

Com relação a itens físicos, que poderiam muitas vezes serem negligenciados pelos respondentes, 51,9% concordam totalmente alguns itens, tais como: alarmes, geradores de energia e câmeras de segurança são importantes para a manutenção da segurança da informação. Porém faltou questionar se nos escritórios em que os respondentes trabalham existem tais itens.

5. CONSIDERAÇÕES FINAIS

A segurança da informação se torna a cada dia que passa mais essencial nas organizações em geral. Sendo a contabilidade a principal responsável pelas informações, que são consideradas como principal ativo das organizações, passa a ser relevante avaliar a percepção do usuário contábil acerca da segurança da informação o qual foi demonstrado no presente artigo.

Com o principal objetivo de avaliar a percepção do usuário contábil acerca da segurança da informação, notamos que, apesar dos usuários terem ciência da importância da segurança da informação, estes demonstraram certas deficiências, desconhecendo os riscos o qual estão expostos ou mesmo o valor das informações que lidam no dia-a-dia. Além disso, os resultados obtidos demonstraram que mesmo quando os respondentes possuem consciência de qual medida deve ser adotada com o objetivo de manter o nível de segurança das informações, estas nem sempre são colocadas em prática.

Em relação ao primeiro objetivo específico, que visava avaliar os conhecimentos dos usuários acerca da segurança da informação, percebe-se que os respondentes possuem um nível de conhecimento superficial sobre o assunto, sendo ainda que os usuários da informação agem, muitas vezes, de forma oposta ao considerado como recomendado. A falta da realização de treinamentos a respeito do tema pode ser considerada como fator crucial para o resultado apresentado.

Como segundo objetivo específico, foi verificado se existe alguma política de segurança da informação nos escritórios contábeis. O resultado aponta que políticas simples, como a troca de senhas, por exemplo, não são atendidas, inclusive as senhas de ex-funcionários são mantidas pelos escritórios em questão, fator considerado como preocupante. Além disso, como citado anteriormente, não são realizados treinamentos dos funcionários a respeito do tema na grande maioria dos escritórios, o que demonstra certa despreocupação por parte dos gestores quanto a qualificação de seus funcionários para prever e evitar situações que possam comprometer as informações em posse da empresa, e expô-la ao risco.

O presente estudo evidencia a importância e necessidade de investimento na área, onde podemos sugerir que as organizações direcionem seus esforços para conscientizar seus funcionários e, principalmente, seus gestores, pois estes serão os principais responsáveis por liderarem a implantação políticas de segurança e a realização periódica de treinamentos com o objetivo de instituir uma cultura organizacional a respeito do tema de segurança da informação buscando construir um ambiente de trabalho mais seguro aos escritórios de contabilidade e, sobretudo, seus clientes.

Como limitação de pesquisa, podemos apontar ao número de respondentes obtidos. Uma amostra maior poderia ser considerada como recomendada afim de obter um resultado mais fidedigno sobre o tema. Além disso, não é possível identificar qual função é realizada por cada respondente nas organizações a partir do questionário elaborado, sendo difícil analisar a percepção da segurança da informação de acordo com o cargo desempenhado.

Para trabalhos futuros recomenda-se a inclusão de outros parâmetros afim de avaliar o valor do investimento desembolsado pelos escritórios na área de segurança da informação. Uma análise relacionando a função desempenhada pelo funcionário e seu nível de conhecimento também é recomendada.

REFERÊNCIAS

ABNT, NBR ISSO/IEC 27001: **Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação — Requisitos**. Rio de Janeiro: ABNT, 2006.

ABNT, NBR ISSO/IEC 27002: **Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005.

BEAL, Adriana. **Segurança da Informação:** Princípios e melhores práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo: Editora Atlas –2008.

BRASIL. Conselho Nacional de Política Fazendária – CONFAZ. **Ajuste Sinief 21/20.** 2020. Disponível em: < https://www.confaz.fazenda.gov.br/legislacao/ajustes/2020/ajuste-sinief-21-20>. Acesso em: 15/03/2021

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República; 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> . Acesso em: 07/03/2021

BRASIL. Medida provisória nº 2.200-2, de 24 de Agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em: 07/03/2021.

BRASIL. Tribunal de Contas da união. **Boas Práticas em Segurança da Informação.** 4º Edição Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0B226095120B> . Acesso em: 07/03/2021.

CAMPOS, A. **Sistemas de Segurança da Informação**. 2º Edição. Florianópolis: Visual Books, 2007

CARUSO, C.A.A.; STEFFEN, F.D. **Segurança em Informática e de Informações**. São Paulo: Ed. Senac. 1999.

DANTAS, Marcus Leal. **Segurança da Informação:** uma abordagem focada em gestão de riscos**.** Recife: Livro Rápido-Elógica, 2011.

CERT.BR. **Estatísticas dos Incidentes Reportados ao CERT.BR..** Cert.br. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 07/03/2021.

CERTISIGN. **Certificado Digital:** O que é?. Certisign. Disponível em: <https://blog.certisign.com.br/o-que-e-certificado-digital/>

FONSECA, J. J. S. **Metodologia da Pesquisa Científica**. Fortaleza: UEC, 2002. Apostila.

GIL, Antonio Carlos. **Como Elaborar um Projeto de Pesquisa**. 4º Edição, São Paulo: Editora Atlas S.A, 2002.

HINTZBERGEN, J. et al. **Fundamentos da segurança da informação.** 3ª edição revisada. São Paulo. Brasport Livros e Multimídia Ltda, 2018
LIKERT, R. (1932). A technique for the measurement of attitudes. Archives of Psychology, 22(140), 1-55.

LYRA, Mauricio Rocha. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008.

LYRA, Mauricio Rocha. **Governança da Segurança da Informação**. 1º edição. Brasília: 2015.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

O'BRIEN, J. A. **Sistemas de Informação e as Decisões Gerenciais na Era da Internet.** 2ª. Ed. São Paulo: Saraiva, 2004.

OLIVEIRA, Jayr Figueiredo. **Uma Reflexão dos Impactos da Tecnologia da Informação no Brasil**. São Paulo: Érica, 2001.

PADOVEZE, Clóvis Luís. **Sistemas de Informações Contábeis:** fundamentos e análises. São Paulo: Atlas, 2009.

RHEE, H.-S., CHEONGTAG, K., & RYU, Y. U. **Self-Efficacy in Information Security:** Its Influence on End Users' Information Security Practice Behavior. Computers & Security. 2009

RICHARDSON, R.J. **Pesquisa Social:** métodos e técnicas. 3.ed. São Paulo Atlas: 1999.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** Uma visão executiva**.** 1º edição – Rio de Janeiro: Campus, 2003.

SILVA T.P; CARVALHO H; TORRES B.C. **Segurança dos Sistemas de Informação – Gestão Estratégica da Segurança Empresarial**. Portugal. Atlântico, 2003.

SOARES, Luiz Fernando Gomes**. Redes de Computadores**. São Paulo: Editora Campus, 1995

SOPHOS. **THE STATE OF CLOUD SECURITY 2020**. Disponível em: <https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx>. Acesso em: 07/04/2021.

STAIR, R. M.; REYNOLDS, G. W. **Princípios dos Sistemas de Informação.** Rio de Janeiro: LTC, 2002.

UWE, Flick. **Introdução à Metodologia de Pesquisa.** São Paulo: Penso Editora Ltda, 2013;

VERIZON. **2019 Data Breach Investigations Report**. Disponível em: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf Acesso em: 07/03/2021

VERIZON. **2020 Data Breach Investigations Report**. Disponível em: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf Acesso em: 07/03/2021.