Temas gerais aplicáveis ao Secretariado
GT 8 - Temas correlatos ao Secretariado**.**

PRÁTICAS DE SEGURANÇA DAS INFORMAÇÕES DIGITAIS: UM OLHAR SOBRE OS DISCENTES DE SECRETARIADO EXECUTIVO

Franciele da Silva Peretti
Universidade Estadual do Centro-Oeste – UNICENTRO, francychz@gmail.com
Juliane Sachser Angnes
Universidade Estadual do Centro-Oeste – UNICENTRO**,** julianeangnes@gmail.com
Suélen Pontes Machado
Universidade Estadual do Centro-Oeste – UNICENTRO, suelenmachado@unicentro.br

Resumo: Os profissionais de Secretariado Executivo trabalham diariamente com informações e dados, os quais são sigilosos e necessitam de proteção. Para garantir a segurança dessas informações existem ferramentas que podem auxiliar no processo. Então, como questão de pesquisa indagou-se: como os profissionais de Secretariado Executivo mantém em sigilo e proteção as informações digitais pessoais e profissionais? O objetivo geral é verificar o grau de conhecimento dos discentes do curso de Secretariado Executivo relacionado ao sigilo e proteção das informações que estão sob guarda. Definem-se assim os objetivos específicos: a) quantificar o volume de informações digitais consideradas sigilosas pelos acadêmicos; b) mapear os dispositivos e práticas de segurança digital adotada pelos discentes de Secretariado Executivo; c) correlacionar o conhecimento de sigilo de dados e informações digitais às práticas de gestão do profissional de Secretariado Executivo. A pesquisa tem como público alvo os discentes do 1º ao 4º ano das universidades do estado do Paraná. Com natureza de dados quantitativa, de caráter descritivo e coleta de dados pelo *Google Forms* – por meio de um questionário. Para a análise dos dados utilizou-se a estatística descritiva e pode-se concluir que grande parte dos discentes mantém a proteção de suas informações digitais. No entanto, notou-se uma vulnerabilidade deles quanto ao uso do aplicativo *Whatsapp*.
Palavras-chave: Comunicação. Tecnologias. Formação secretarial.

1 INTRODUÇÃO

A segurança da informação é obtida através da implantação de controles, abrangendo processos, procedimentos, políticas, estrutura organizacional e funções de *software* e *hardware*. Esses controles devem ser estabelecidos, implantados, vigiados, examinados e aperfeiçoados quando houver necessidade, para garantir que os objetivos e a segurança das informações da organização e demais locais sejam mantidas em sigilo e segurança (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27002, 2013).

Os profissionais de secretariado executivo trabalham com a gestão da informação. O avanço tecnológico lhes trouxe benefícios para a realização das atividades, ocorrendo mudanças no perfil e na capacitação para poder atuar em diversas áreas. Assim, os profissionais que buscam as ferramentas tecnológicas disponíveis no mercado desfrutam de uma grande evolução pessoal e profissional (ADELINO; SILVA, 2012).

De acordo com Aguiar e Cabral (2017), devido aos prazos e demandas que os secretários executivos enfrentam dentro das organizações, exige-se que esses profissionais busquem uma constante atualização de conhecimentos, principalmente sobre as novas tecnologias. Isso é importante porque esse profissional utiliza dispositivos ligados à internet para executar atividades diárias, como: controlar a(s) agenda(s); planejar viagens do executivo; elaborar documentos, relatórios e planilhas; organizar os arquivos; executar os procedimentos relacionados a ligações telefônicas e recepção dos clientes; planejar e organizar eventos; preparar reuniões; entre outras atividades.

Segundo o Comitê Gestor da Internet no Brasil (CGI.BR, 2012), os dispositivos móveis como *tablets* e *smartphones*, celulares, entre outros, que trouxeram vantagens tanto pessoais como profissionais, popularizaram-se e são capazes de executar tarefas que antes eram realizadas somente em computadores. Há facilidade ao acesso à *web*, *internet banking*, *e-mails* e redes sociais. Assim como os computadores, os dispositivos móveis também podem ser usados para a prática de atividades maliciosas, como furto de dados, envio de *spam*, propagação de códigos maliciosos ou ser usado para disparar ataques na internet. Portanto, os usuários devem manter seus dados e informações sob proteção, utilizando ferramentas disponíveis para essa finalidade. Logo, para orientar a pesquisa, questiona-se: como os discentes do curso de Secretariado Executivo mantêm o sigilo e proteção das informações digitais pessoais e profissionais?

Possui como objetivo geral: verificar o grau de conhecimento dos discentes do curso de secretariado executivo relacionado ao sigilo e proteção das informações digitais pessoais e profissionais que estão sob sua guarda. Para a execução, apresentam-se os objetivos específicos: a) quantificar o volume de informações digitais consideradas sigilosas pelos acadêmicos; b) mapear os dispositivos e práticas de segurança digital adotada pelos discentes de Secretariado Executivo; c) correlacionar o conhecimento de sigilo de dados e informações digitais às práticas de gestão do profissional de Secretariado Executivo.

Dessa forma, os futuros profissionais de secretariado executivo, que têm acesso a inúmeras informações no seu dia a dia, dentro e fora das organizações, precisam proteger informações pessoais e profissionais, tanto em computadores, como em dispositivos móveis. Para Nonato (2009), nessa profissão, o sigilo das informações a eles confiadas é de extrema importância e exige total segurança.

Assim, este estudo pesquisa os acadêmicos do 1º ao 4º ano do curso de secretariado executivo das Universidades Estaduais do Paraná, sendo a Universidade Estadual de Londrina – UEL, Universidade Estadual de Maringá – UEM, Universidade Estadual do Centro-Oeste – UNICENTRO e Universidade Estadual do Oeste do Paraná – UNIOESTE.

2 REFERENCIAL TEÓRICO

2.1 O AVANÇO TECNOLÓGICO E O PROFISSIONAL DE SECRETARIADO EXECUTIVO

Quando se fala do avanço tecnológico, lembra-se das tecnologias, as quais estão presentes no dia a dia das pessoas, dos profissionais e das organizações. Elas trouxeram rapidez, soluções, produtividade, qualidade e eficiência nos produtos e serviços. Araújo e Silva (2018) consideram que a força do mercado tecnológico atual faz as organizações buscarem, de forma pertinente, ferramentas tecnológicas que possam manter a empresa no mercado, para diminuir

o tempo de processos, valorizar produtos, superar concorrentes, obter resultados por meio de processos sequenciais e, assim, aumentar o patrimônio rapidamente. Dessa forma, Kohn e Moraes (2007) destacam que as tecnologias também trouxeram benefícios para o uso pessoal. Por meio delas as pessoas podem se conectar com diversos lugares e pessoas, passam a ter mais acesso às informações, ampliando conhecimento, interagindo diariamente, entre outras atividades.

Compreende-se que as tecnologias digitais possibilitam uma dimensão de produtos, a transmissão de arquivo e o acesso às informações, mudando o cenário econômico, político e social. O desenvolvimento de novas tecnologias gerou um mercado mais competitivo, especializado e acelerado em processos, almejando altos padrões, fato resultante da globalização (KOHN; MORAES, 2007).

Segundo Nonato (2009, p 91), "o avanço tecnológico possibilitou que a profissão ganhasse novos rumos, [...], tendo recebido contribuição dos novos processos tecnológicos". Desse modo, destacam-se os profissionais de secretariado executivo, os quais sempre utilizam tecnologias disponíveis em cada fase da profissão. Esses profissionais estão presentes no avanço tecnológico, por ser intrínseco ao desempenho das suas funções secretariais técnicas e também de gestão.

2.2 A SEGURANÇA DAS INFORMAÇÕES DIGITAIS

Os sistemas de informações foram criados para melhorar o controle, o planejamento e a organização de uma empresa. Aliados a outras ferramentas de tecnologia de informação, são responsáveis pela entrada, processamento, armazenamento e recuperação da informação, para auxiliar na tomada de decisões dentro da organização (CUNHA; FENATO, 2012).

De acordo com a ABNT NBR ISO/IEC 27002 (2013), o valor das informações está além das palavras escritas, números, imagens, conhecimentos, conceitos, ideias e marcas. No mundo atual, tudo está interconectado. A informação e os processos relacionados com sistemas, redes e pessoas envolvidas nas suas operações são informações com valor para a organização, inclusive para as pessoas e, consequentemente, requer proteção contra os vários riscos.

A segurança da informação está relacionada com a proteção dos dados e informações de um indivíduo ou de uma determinada empresa. Há alta demanda na busca por integridade das informações e a confidencialidade de sistemas, como: arquivos, documentos, transações bancárias, senhas, entre outros. Assim, a maior parte das atividades necessita de conectividade e, por isso, as tecnologias voltadas à área de segurança estão sempre se revolucionando. Criaram-se ferramentas para ajudar na privacidade e na segurança das informações. Em computadores de mesa e dispositivos móveis há, por exemplo, o uso da digital do usuário para acesso aos dispositivos, extensores e módulos de segurança, bem como também existe a criptografia de dados. Destaca-se que a segurança das informações só é possível se as ferramentas certas forem aliadas a uma política de segurança bem elaborada. Com o avanço da tecnologia, as informações estão cada vez mais acessíveis e isso facilita que os usuários caiam em golpes na internet, como acesso a *sites* não confiáveis, através de páginas de sorteios, promoções, propagandas, entre outros. Os usuários não se atentam aos riscos e isso se torna caminhos para a efetivação de crimes. E, através desses erros, ocorre o acesso às informações pelos golpistas ou *hackers*, os quais querem acessar informações confidenciais, praticar desvios, efetuarem golpes, entre outras atividades ilegais (WEIGERT; CASTILHO, 2017).

Assim, o CGI.BR (2012) aponta que as informações podem ser acessadas por códigos maliciosos, os quais são programas especificamente desenvolvidos para executar danos em

computadores ou dispositivos móveis e destaca um dos códigos maliciosos chamado de vírus. Estes são programas que se propagam inserindo cópias de si mesmos dentro dos equipamentos, tornando-se parte dos programas e arquivos. Eles são encontrados em *links* não confiáveis, *sites* de propagandas, sorteios, promoções, dispositivos não seguros e arquivos corrompidos, podendo ser passados a outros dispositivos através da conectividade de ambos, ocasionando uma infestação. Desse maneira, não se pode deixar de destacar os *hackers*, os quais são programadores que se dedicam a acessar, obter e modificar informações pessoais e organizacionais através de dispositivos móveis, programas e redes de computadores.

Portanto, diante desses riscos e invasões, foram criadas as ferramentas antivírus e *Anti-malware*. Essas ferramentas procuram detectar, anular ou remover os códigos maliciosos de um computador ou dispositivo. O uso da ferramenta *Firewall* pode auxiliar e impedir que *hackers* ou códigos maliciosos consigam acesso ao computador ou dispositivo móvel conectado em uma rede ou à internet móvel. Isso impede que o computador envie um *software* mal-intencionado para outros computadores (WEIGERT; CASTILHO, 2017).

Torna-se necessário que os usuários utilizem essas ferramentas, as quais auxiliam na prevenção e no combate a códigos maliciosos e *hackers*, evitando assim possíveis ataques. Segundo Bine e Kuk (2016), existem ferramentas de defesa que podem ser utilizadas pelos usuários diretamente em seus sistemas de computadores e dispositivos móveis, diminuindo efetivamente golpes, fraudes, códigos maliciosos e *hackers*, sendo exemplos a criptografia, *Anti-malware*, *Firewall* e o uso de senhas fortes. Essas senhas não devem conter nomes de pessoas próximas, datas especiais ou números de documentos, o que as deixa frágeis para serem decifradas por *hackers*. Isso é uma forma de dificultar os acessos não autorizados pelos usuários. As senhas devem conter letras, números e/ou caracteres especiais para serem consideradas senhas fortes e difíceis de serem decifradas. O CGI.BR, 2012 disponibiliza algumas ferramentas que podem ser utilizadas pelos usuários para prevenção, defesa e proteção de seus dados e informações, as quais estão descritas no Quadro 1.

Quadro 1: Ferramentas de proteção e prevenção

Tipo	O que é/são	Para que serve
Antivirus, *Antimalware Antispyware, Antirootkit, Anti trojan*	São *softwares* que buscam detectar e depois anular ou remover os códigos maliciosos.	Para verificar toda e qualquer extensão de arquivo, analisar automaticamente arquivos anexados aos *e-mails* e obtidos pela internet e verificar automaticamente os discos rígidos e as unidades removíveis (como *pen-drives*, cd's, dvd's e discos externos),
Firewall	É um sistema de defesa, com barreiras de proteção para computadores e dispositivos móveis.	É uma ferramenta que serve para bloquear o acesso não autorizado aos computadores e dispositivos móveis
Atualização de *software*	O usuário deve sempre manter o sistema operacional e os *softwares* atualizados.	Para que os *softwares* estejam menos vulneráveis aos ataques cibernéticos, evitar falha do sistema, entre outros.
Criptografia	É uma ferramenta que serve para criar mensagens cifradas ou codificadas.	Para proteger dados contra os acessos indevidos, tanto os que trafegam pela internet como os já gravados no computador.
Backups (cd, dvd, *pen-drive*, disco de *Blu-ray*, disco removível	São cópias de segurança que devem ser feitas para poder recuperar dados e informações de possíveis	Proteção de dados: o usuário pode preservar seus dados para que sejam recuperados em situações como falhas de disco rígido, atualização mal sucedida do sistema operacional, exclusão ou substituição

interno e externo ou armazenamento remoto *online* – nuvem).	falhas ou perdas, por códigos maliciosos ou *hackers*.	acidental de arquivos, ação de códigos maliciosos ou atacantes e furto/perda de dispositivos; Recuperação de versões: o usuário pode recuperar uma versão antiga de um arquivo alterado, como uma parte excluída de um texto editado ou a imagem original de uma foto manipulada; Arquivamento: O usuário pode copiar ou mover dados que deseja ou que precisa guardar, mas que não são necessários no seu dia a dia e que raramente são alterados.

Fonte: Elaborado pela acadêmica com base no Comitê Gestor da Internet no Brasil, 2020.

Portanto, para a proteção de dados e informações em computadores e dispositivos móveis, contra códigos maliciosos e *hacker*, faz-se necessário o uso das ferramentas citadas no Quadro 1. Mas deve-se compreender que, para se protegerem de golpes, os usuários devem evitar passar informações sigilosas, principalmente pessoais, via telefone, *e-mails*, *chats*, *sites*, redes sociais, *Whatsapp*, entre outros, evitando assim passar por eventuais perdas e constrangimentos.

2.3 FRAGILIDADE DAS INFORMAÇÕES FRENTE AOS CÓDIGOS MALICIOSOS

De acordo com Bine e Kuk (2016), quando surge uma nova tecnologia, a forma de acessá-la torna-se mais fácil e rápida. Aparelhos como *smartphones*, *tablets* e demais dispositivos móveis armazenam inúmeras informações, tanto profissionais como pessoais. Essas informações são muito valiosas e, assim, esses aparelhos se tornam alvos constantes de ataques. Segundo o CGI.BR, (2012), quanto mais informações e dados forem disponibilizados, mais fácil para golpistas acessarem e roubarem dados. Assim, destacam-se alguns códigos maliciosos no Quadro 2.

Quadro 2: Códigos maliciosos

Tipo	O que é/são	Como agem
Códigos maliciosos (*Malware*)	São programas especialmente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.	Explorando vulnerabilidade nos programas, através de removíveis infectados (*pen-drives*), páginas da *web*, navegadores, invadindo um equipamento quando aberto anexo, *link*, *e-mails* infectados.
Vírus	É um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos.	Através de anexos em e-*mails*, páginas da *web*, entre outros. Infectam arquivos, são passados de celular para celular através de mensagem, *bluetooth*, envio de arquivos e dados corrompidos pelo vírus
Worm (Vermes)	É um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.	Propagam-se automaticamente pelas redes através de mensagens, *e-mails* e pastas compartilhadas via rede, buscando vulnerabilidades existentes.
Bot	É um programa que dispõe de mecanismos de comunicação com o invasor, o qual permite que o seu controle seja remoto.	Ao se comunicar, o invasor envia instruções para que ações maliciosas sejam executadas, como desferir ataques e furtar dados do computador infectado.

Botnet	É uma rede formada por centenas de computadores e que permite potencializar as ações danosas executadas pelo *bot*.	Ataques de negação de serviço, propagação de códigos maliciosos, coleta de informações de um grande número de computadores, envio de *spam* para ocultar a identidade do atacante.
Spyware	É um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.	*Keylogger*: capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador; *Screenlogger*: capaz de armazenar a posição do cursor do mouse e a tela apresentada no monitor, bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais principalmente em *sites* de "*internet banking"*; *Adware*: projetado para apresentar propagandas.
Backdoor	É um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modicados para isso.	Usado para assegurar o acesso futuro ao computador comprometido, sem que seja notado.
Cavalo de Troia (*Trojan*)	É um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.	*Trojan Downloader*: instala outros códigos maliciosos, obtidos de *sites* na internet; *Trojan Dropper*: instala outros códigos maliciosos, embutidos no próprio código do *Trojan*; *Trojan Backdoor*: inclui *backdoors*, possibilitando o acesso remoto do atacante ao computador; *Trojan DoS*: instala ferramentas de negação de serviço e as utiliza para desferir ataques; *Trojan Destrutivo*: altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação; *Trojan Clicker*: redireciona a navegação do usuário para *sites* específicos, com o objetivo de aumentar a quantidade de acessos a estes *sites*; *Trojan Proxy*: instala um servidor possibilitando que o computador seja utilizado para navegação anônima e para envio de *spam*; *Trojan Spy*: instala programas *spyware* e os utiliza para coletar informações sensíveis, como senhas, números de cartão de crédito e enviá-las ao atacante; *Trojan Banker*: coleta dados bancários do usuário, através da instalação de programas *spyware* que são ativados quando *sites* de "internet *banking"* são acessadas.
Rootkit	Conjunto de programas e técnicas que permitem esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.	Instalando outros códigos maliciosos para assegurar o acesso futuro ao computador infectado; escondendo atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede e mapeando vulnerabilidades em outros computadores, por meio de varreduras na rede. Capturando informações da rede onde o computador

		comprometido está localizado, pela interceptação de tráfego.
Spam	Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas.	Através de envio de mensagens via *e-mail*, assemelham-se a propagandas.
Cookie	São pequenos arquivos gravados no computador quando acessados em *sites* e reenviando os usuários a estes mesmos *sites* quando os acessa novamente.	São usados para manter informações sobre quem acessa, como carrinho de compras, preferências de navegação, senhas salvas ou autopreenchimento
Janelas de *pop-up*	São aquelas que aparecem automaticamente e sem permissão, sobrepondo à janela do navegador após acessar um *site*.	Apresentam mensagens indesejadas, contendo propagandas ou conteúdo impróprio; apresentam *links*, que podem redirecionar a navegação para uma página falsa ou induzi-lo a instalar códigos maliciosos.
Links	*Links* significa *hiper* ligação, ou seja, quando é clicado pelo usuário, é encaminhado para outra página na internet.	*Links* são bastante vistos por oportunistas com o intuito de criar redirecionamentos para páginas de *phishing* (técnica de fraude) ou contendo códigos maliciosos.
Através de programas de distribuição de arquivos	São aqueles que permitem que os usuários compartilhem arquivos entre si.	Caso possua vulnerabilidades, o programa de distribuição de arquivos pode permitir o acesso indevido a diretórios e arquivos. Esses arquivos podem conter códigos maliciosos e, assim, infectar o computador ou dispositivo móvel ou ainda permitir que o dispositivo seja invadido.
Através de compartilhamento de recursos	Sistemas operacionais permitem o compartilhamento, com outros usuários, dos recursos do seu computador ou dispositivo móvel, como diretórios, arquivos, impressoras, internet e dados.	O acesso não autorizado a recursos ou informações sigilosas é usado por oportunistas, caso estes não possua senhas para controle de acesso ou as senhas possam ser facilmente descobertas.

Fonte: Elaborado pela acadêmica com base no Comitê Gestor da Internet no Brasil, 2020.

Existem outras formas de se perderem informações pessoais. Segundo Bine e Kuk (2016), a engenharia social é um meio utilizado por golpistas para acessar e obter informações pessoais. Os golpistas tentam, por esse meio, obter alguns dados pessoais. Depois, quando ganham a confiança do usuário, fazem com que a vítima, induzida, forneça dados mais detalhados para que possam tirar algum proveito. Eles agem através de telefonemas, passando-se por uma pessoa do convívio social do usuário. Por exemplo, fazem uma ligação passando-se por um(a) filho(a) ou parente da vítima e pedem recompensa para soltá-lo(a) de um suposto sequestro. Atuam, também, analisando os usuários através das redes sociais, obtendo informações pessoais que são publicadas nessas redes, como *e-mails*, número de telefone, datas especiais. Analisam a rotina das pessoas e locais que costuma frequentar (através do *check-in*), instituição bancária e utilizam esse tipo de informações para identificar como possíveis senhas de acesso, possibilidade de sequestros, entre outros. Desta maneira, eles entram em contato com o usuário passando-se por instituições financeiras, afirmando conta irregular, limite de cartão estourado e uma possível renegociação de dívidas, requisitando dados para atualização de cadastro ou oferecendo produtos e serviços. Esses ataques acontecem devido à curiosidade, inocência e/ou ganância. As pessoas são atraídas por produtos interessantes, condições favoráveis em momentos oportunos ou com sentimentos envolvidos.

3 PROCEDIMENTOS METODOLÓGICOS

Trata-se de uma pesquisa de natureza de dados quantitativa, busca-se coletar e analisar dados sobre as variáveis e identificar a realidade do objeto, seus sistemas de relações e estrutura dinâmica (ESPERÓN, 2017). A pesquisa visa realizar um estudo direcionado à prática de proteção das informações no meio digital. Tende-se verificar o grau de conhecimento dos discentes do curso de secretariado executivo correspondente ao sigilo e proteção das informações que estão sob sua responsabilidade, estimando o volume de informações que acreditam ser sigilosas e quais as ferramentas utilizadas para a sua proteção.

Com caráter descritivo, pesquisas assim possuem como principal objetivo a descrição das características de uma determinada população ou fenômeno, utilizando-se uma técnica padronizada de coleta de dados (GIL, 2008). Sendo assim, pretendem-se apresentar as medidas tomadas pelos discentes em relação às informações digitais frente aos códigos maliciosos, para a proteção de seus computadores e dispositivos móveis.

Desse modo, o estudo utiliza o método *survey*, o qual, segundo Duarte (2010) é bastante utilizado em pesquisas de opinião, de mercado e pesquisas sociais que buscam descrever, explicar e explorar aspectos ou fatores de uma sociedade por meio de uma amostra. Portanto, o universo desta pesquisa consiste em identificar as práticas de segurança das informações digitais pessoais e profissionais dos discentes do 1º ao 4º ano do curso de secretariado executivo das Universidades Estaduais do Paraná, sendo a UEL, UEM, UNICENTRO e UNIOESTE.

Como instrumento de coleta de dados, utilizou-se a aplicação de questionário. Para Franco e Dantas (2017), é um método de pesquisa estruturado com perguntas claras e objetivas. O questionário foi estruturado na plataforma *Google Forms*, dividido em 4 constructos, possui 78 variáveis, as quais são relacionadas ao sigilo e informações digitais, vulnerabilidade ao compartilhar arquivos, internet e redes sociais, mapeando os tipos de dispositivos móveis usados pelos discentes e as práticas de segurança utilizadas. As variáveis estão dentro de uma escala *Likert* de cinco pontos. Segundo Silva e Costa (2014), um constructo é constituído por um conjunto de afirmações, nas quais os respondentes expõem o seu grau de concordância. Nesta pesquisa os cinco pontos são: 1 (concordo plenamente), 2 (concordo), 3 (não concordo e não discordo), 4 (discordo) e 5 (discordo plenamente).

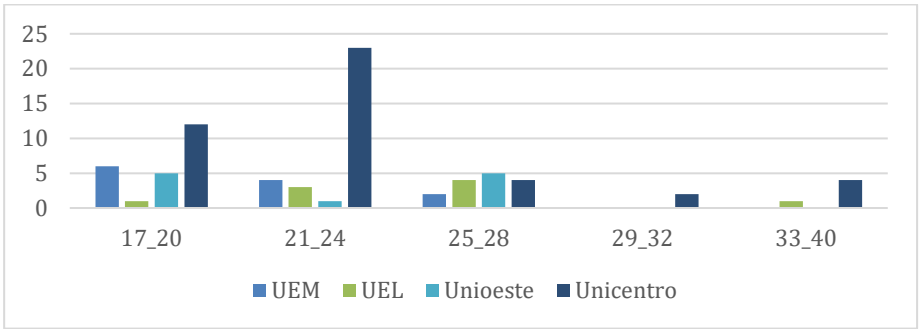
No que tange à temporalidade, caracteriza-se como transversal. Estudos transversais descrevem uma situação ou fenômeno em um momento não definido ou a um recorte de tempo, não em períodos longos (HOCHMAN *et al.* 2005). Dessa forma, Bastos e Duquia (2013, p. 231) destacam que esse tipo de estudo é utilizado "quando se deseja estimar a frequência com que um determinado evento se manifesta em uma população específica". Durante o período de setembro a novembro há a coleta dos dados e a análise ocorre em dezembro de 2020.

Por fim, utiliza-se o SPSS (*Statistical Package for the Social Sciences*) para analisar os dados coletados. Faz-se uma análise descritiva de cada universidade, sendo utilizada também a média geral de todas as variáveis, ou seja, a soma de todas as universidades para a análise geral. Isso é feito por meio de uma estatística descritiva, que, segundo Santos (2018), é um conjunto de procedimentos e técnicas que servem para recolher, organizar, sintetizar e descrever os dados, bem como efetuar inferências sobre uma população com base no estudo de amostras. Assim, os resultados desta pesquisa são recolhidos, organizados, sintetizados e descritos, retornando informações acerca do comportamento dos discentes frente ao sigilo e proteção dos dados.

4 RESULTADOS E DISCUSSÕES

Esta pesquisa apresenta respostas de 77 discentes, sendo 46 da UNICENTRO, 12 UEM, 11 da UNIOESTE e 09 da UEL, todos discentes do curso de Secretariado Executivo. Busca-se, com ela, conhecer o perfil dos acadêmicos, obtendo-se as idades descritas no Gráfico 1, em que a faixa etária mais expressiva está em 20 e 24 anos: 12 discentes possuem 20 anos e 23 discentes, 24. É notório que os discentes são a maioria jovens e, supostamente, devem acompanhar as novas tecnologias.

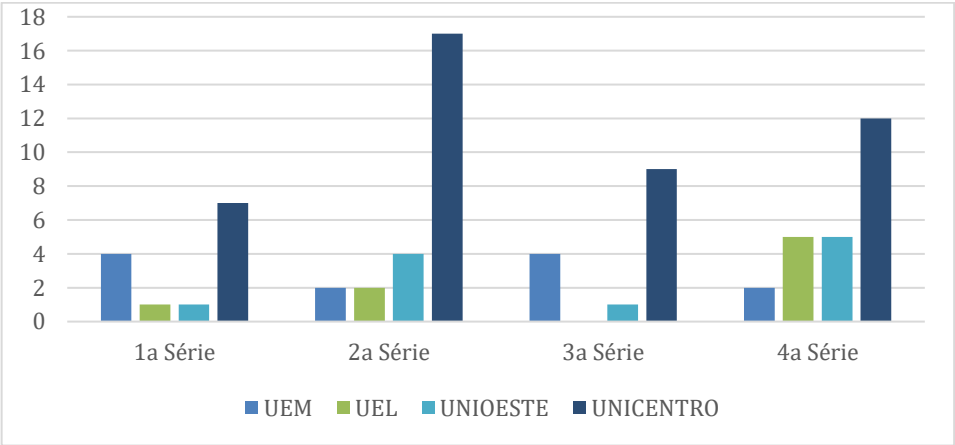
Gráfico 1: Faixa etária dos discentes.



Fonte: Elaborado pela acadêmica com base nos dados coletados, 2020.

Outro fator importante para a pesquisa é compreender qual o gênero do público entrevistado, visto que o curso de Secretariado Executivo possui predominância feminina. Segundo os dados coletados, a UEM conta com 10 respostas do gênero feminino, 1 do gênero masculino e 1 do gênero "Outro"; na UEL obtêm-se 7 respostas do gênero feminino e 2 do masculino; a UNIOESTE contou com 7 respostas do gênero feminino e 4 do gênero masculino; A UNICENTRO obtém o maior índice, representada por 39 respondentes do gênero feminino e 6 do gênero masculino. Conhecendo esse fator, compreende-se que o gênero feminino é predominante. Relacionado aos períodos que os discentes estão cursando, pode-se verificar o Gráfico 2:

Gráfico 2: Série dos discentes.



Fonte: Elaborado pela acadêmica com base nos dados coletados, 2020.

A segurança da informação visa à integridade e à confidencialidade de sistemas, como arquivos, documentos, transações bancárias, senhas, entre outros. A Tabela 1 é relacionada ao sigilo e proteção das informações. As respostas dos discentes das universidades UEL, UEM, UNICENTRO E UNIOESTE, do curso de Secretariado Executivo, são compostas pelo número da variável, descrição da variável e a média geral obtida. Utiliza-se uma escala *Likert* de 5 pontos: 1 (concordo plenamente); 2 (concordo), 3 (não concordo e não discordo), 4 (discordo) e 5 (discordo plenamente).

Tabela 1 – Sigilo e proteção das informações.

Número da Variável	Descrição da variável	Média Geral
1	Utilizo senhas com datas especiais e nomes de pessoas.	2,84
2	Utilizo senhas com números de documentos.	3,81
3	Utilizo senhas com letras e números.	1,55
4	Utilizo senhas em todos os meus locais de acesso.	1,98
5	Troco minha senha com frequência.	3,12
6	Utilizo senha em *smartphone*.	1,58
7	Utilizo senha em computadores.	1,83
8	Faço *download* de aplicativos somente em loja segura.	2,16
9	Baixo qualquer aplicativo do meu interesse.	2,93
10	Não instalo aplicativo.	4,28
11	Utilizo o aplicativo "*internet banking"* todos os dias.	3,16
12	Acesso o "*internet banking"* uma ou duas vezes por semana.	2,98
13	Acesso mais de quatro vezes por semana o "*internet banking"*.	3,53
14	Não utilizo o "*internet banking"*.	3,72
15	Envio somente mensagem pelo *whatsapp*.	3,36
16	Compartilho fotos, vídeos e áudios pelo *whatsapp*.	1,51
17	Compartilho informações, documentos e dados pelo *whatsapp*.	2,10
18	Não compartilho nada pelo *whatsapp*.	4,33

Fonte: Elaborado pela acadêmica com base nos dados coletados, 2020.

Nota-se uma similaridade entre as universidades no padrão de respostas obtidas sobre o uso de senhas para proteção (variável 4), as médias são UEM 1,58, UEL 1,11, UNIOESTE 2,18 e UNICENTRO 2,22; na variável 6, são UEM 1,41, UEL 1,11, UNIOESTE 1,72 e UNICENTRO 1,68; na variável 7, as médias são UEM 1,50, UEL 1,11, UNIOESTE 2,36 e UNICENTRO 1,93; e na variável 8, UEM 2,58, UEL 1,66, UNIOESTE 2,45 E UNICENTRO 2,08. Observa-se que, nas variáveis 4, 6 e 7, as médias das universidades estão próximas do "Concordo". Os discentes concordam que utilizam senhas em todos os locais de acesso, em *smartphones* e computadores, garantindo-lhes uma maior segurança. Na variável 8, percebe-se que os discentes da UEL, UNIOESTE e UNICENTRO fazem *download* de aplicativos em lojas seguras, já na UEM não são todos os discentes que o fazem, visto que a média está próxima do "Não concordo e não discordo". É notório que a maioria conhece e mantém a proteção de suas informações digitais, demonstrando que, independentemente do local de graduação, utilizam senhas com letras e números, indicando a sua preocupação em zelar pelos seus dados. Destaca-se a necessidade dos discentes usarem ferramentas de defesa que visem à segurança e que possam ser usadas por eles diretamente em seus sistemas de computadores e dispositivos móveis (BINE; KUK, 2016).

No entanto, observa-se uma vulnerabilidade deles: variável 16, UEM 1,25, UEL 1,11, UNIOESTE 1,81 e UNICENTRO 1,60; e na variável 17, UEM 1,58, UEL 1,88, UNIOESTE 2,36 e UNICENTRO 2,22, em que se obtêm as médias próximas do "Concordo plenamente" e "Concordo", ou seja, os discentes concordam que compartilham dados com fotos, áudios e vídeos, assim como informações e documentos através do aplicativo *Whatsapp*. Isso é propício para exposição a códigos maliciosos, como vírus e *Worm* (vermes), os quais infectam arquivos e são repassados de celular para celular através de mensagens, pastas compartilhadas, entre outros (CGI.BR, 2012). Diante desses riscos, os usuários devem utilizar as ferramentas de antivírus e *Anti-malware,* as quais detectam, anulam e removem códigos maliciosos, e utilizar também a ferramenta *Firewall*, a qual impede que *hackers* ou códigos maliciosos tenham acesso aos dispositivos (WEIGERT; CASTILHO, 2017). Ou, ainda, há ferramentas como criptografia, senhas fortes e "confirmação em duas etapas" no caso do *Whatsapp*, para dificultar ainda mais os acessos não autorizados (BINE; KUK, 2016).

Ao analisar a variável 14, observa-se que os discentes utilizam o *Internet Banking*, porque, ao serem questionados sobre "não usarem o aplicativo", a média da UNICENTRO (3,51) está próxima do "Discordo". E as médias da UEM (4,08) e UEL (4,77) estão próximas do "Discordo plenamente". Na UNIOESTE está próxima do "Não concordo e não discordo", ou seja, nem todos utilizam esse aplicativo. Destaca-se a importância de proteger esse aplicativo, porque, ao utilizá-lo, o usuário se torna vulnerável a vírus, como *Screenlogger*, muito utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados. Fixam-se principalmente em *sites* e aplicativos de *Internet Banking*. Ou, ainda, estão vulneráveis a vírus como *Trojan Banker*, o qual coleta dados bancários do usuário através de programas *Spyware*, sendo ativados quando acessados (CGI.BR, 2012). Há também as ferramentas que ajudam na privacidade e na segurança das informações, de computadores e dispositivos móveis, sendo uma possibilidade o uso da digital do usuário para acessar dispositivos, extensores e módulos de segurança, criptografia de dados, entre outros (WEIGERT; CASTILHO, 2017).

Desse modo, o constructo 2 possui variáveis sobre vulnerabilidade e sigilo. As respostas sobre as informações digitais estão representadas na Tabela 2.

Tabela 2 – Vulnerabilidade e sigilo.

Número da variável	Descrição da variável	Média Geral
19	Compartilho arquivo via *bluetooth*.	3,45
20	Compartilho arquivo via *torrent.*	3,90
21	Compartilho internet através do celular como roteador.	2,84
22	Compartilho arquivo através de dispositivos físicos.	2,42
23	Não compartilho arquivos ou internet.	4,01
24	Considero documentos pessoais sigilosos.	1,61
25	Considero documentos empresariais sigilosos.	1,32
26	Considero qualquer tipo de arquivo sigiloso.	2,66
27	Considero que senhas precisam ser mantidas em sigilo.	1,33
28	Considero dados pessoais sigilosos.	1,41
29	Considero informações bancárias sigilosas.	1,16

Fonte: Elaborado pela acadêmica com base nos dados coletados, 2020.

Sobre as informações digitais consideradas sigilosas (variáveis 24, 25, 26, 27, 28 e 30), quantifica-se que os discentes consideram documentos pessoais e empresariais sigilosos, podendo ser observado nas médias obtidas (variáveis 24 e 25, respectivamente), UEM 2,16 e 1,16, UEL 1,33 e 1,11, UNIOESTE 1,54 e 1,45 e a UNICENTRO 1,53 e 1,37. As respostas estão entre "Concordo plenamente" e "Concordo".

Uma questão feita aos discentes era sobre considerar qualquer tipo de arquivo sigiloso, (variável 26). Os discentes da UEM (2,83) ficam com a média próxima ao "Não concordam e não discordam", da UEL (3,88), a média mostra próximo ao "Discordo", a UNIOESTE (2,18) e a UNICENTRO (2,48) ficam com as médias próximas ao "Concordo". Diante disso, percebe-se que nem todos os discentes da UEM acham todos os arquivos sigilosos e os da UEL discordam de que todos os arquivos sejam sigilosos. Observa-se que a maioria dos discentes da UNIOESTE e UNICENTRO acha que todos os arquivos são sigilosos. Os arquivos sigilosos possuem informações e dados importantes, os quais podem causar sérios danos, constrangimentos, inconveniências – por menores que sejam –, ou causar impactos significativos, colocando a organização ou indivíduos em risco (ABNT NBR ISO/IEC 27002, 2013).

Sobre considerarem senhas e informações bancárias importantes (variáveis 27 e 28), os discentes concordam plenamente que senhas precisam ser mantidas em sigilo e informações bancárias são sigilosas, porque as médias da UEM (1, 41 e 1,16), UEL (1,0 e 1,0), UNIOESTE (1,27 e 1,27) e UNICENTRO (1,40 e 1,17) ficaram todas próximas ao "Concordo plenamente". Portanto, compreende-se que os discentes têm conhecimento da importância em se manter em sigilo e proteção informações e dados, evitando qualquer tipo de exposição desnecessária. A ABNT NBR ISO/IEC 27002 (2013) destaca que a segurança das informações só pode ser obtida com êxito quando elas forem mantidas em sigilo, segurança e proteção.

As tecnologias trouxeram benefícios para o uso pessoal, pois, através delas, as pessoas podem se conectar de diferentes locais com qualquer pessoa, interagindo sempre que tiverem vontade ou necessidade (KOHN; MORAES, 2007). Então, o constructo 3 questiona os discentes sobre o uso das redes sociais. As respostas estão descritas na Tabela 3.

Tabela 3– Sobre as redes sociais.

Número da variável	Descrição da variável	Média Geral
30	Utilizo o *facebook.*	1,72
31	Utilizo o *instagram*.	1,45
32	Utilizo o *snapchat.*	4,09
33	Utilizo o *twitter*.	2,96
34	Utilizo o *linkedin*.	3,05
35	Utilizo o *messenge*r.	2,53
36	Não utilizo nenhuma rede social.	4,64
37	Posto informações nas redes sociais.	2,85
38	Posto informações da minha rotina (*check-in*, entre outros)	3,54
39	Posto fotos com família.	2,70
40	Posto fotos com amigos.	2,23
41	Posto informações e fotos diariamente.	3,88
42	Posto informações e fotos semanalmente.	3,68
43	Posto informações e fotos de vez em quando.	2,24
44	Não posto informações e fotos nas redes sociais.	4,29

Fonte: Elaborado pela acadêmica com base nos dados coletados, 2020.

Quando questionados sobre não utilizarem nenhuma rede social (variável 36), as médias (UEM 4,83, UEL 4,66, UNIOESTE 4,81, UNICENTRO 4,55) estão próximas do "Discordo plenamente". Isso demonstra que os discentes utilizam alguma das redes sociais disponíveis. As mais utilizadas são *Facebook, Instagram e Messenger* (variável 30, 31 e 35). Observa-se, na variável 44, que os discentes postam fotos e informações em suas redes sociais, visto que as médias das respostas obtidas (UEL 4,41, UEL 4,55, UNIOESTE 4,45, UNICENTRO 4,17) ficam próximas ao "Discordo" e "Discordo plenamente". Percebe-se que não é dada a mesma atenção aos dados pessoais da mesma forma que eles consideram documentos sigilosos. Segundo os autores Weigert e Castilho (2017), devido ao avanço das tecnologias, as informações estão cada vez mais acessíveis e isso facilita que os usuários caiam em golpes na internet e redes sociais. Assim, há a necessidade de se ter cuidado quanto à exposição de dados e informações. Portanto, é essencial que os discentes mantenham suas informações pessoais e profissionais em segurança, evitando expô-las na internet e redes sociais (CGI.BR, 2012).

Segundo a ABNT NBR 27002 (2013), a segurança das informações é obtida através da implantação de controles, abrangendo procedimentos, funções *de software e hardware*, objetivando-se a segurança das informações da organização e demais locais. Desse modo, o constructo 4 contém perguntas sobre os dispositivos e práticas de segurança. As médias obtidas estão descritas na Tabela 4.

Tabela 4 – Dispositivos e práticas de segurança digital.

Número da variável	Descrição da variável	Média Geral
45	Tenho acesso à internet em qualquer local.	2,24
46	Tenho acesso à internet somente no trabalho.	4,18
47	Tenho acesso à internet somente em casa.	3,85
48	Tenho acesso somente na universidade.	4,10
49	Tenho computador.	3,51
50	Tenho *notebook*.	1,92
51	Tenho *tablet*.	4,14
52	Tenho *smartphone*.	1,28
53	Não tenho nenhum desses dispositivos.	4,61
54	Utilizo *firewall*.	3,44
55	Utilizo *anti-malware.*	3,40
56	Não utilizo *firewall* e *anti-malware*.	3,42
57	Faço *backup* em cd ou dvd.	4,40
58	Faço *backup* em *pendrive*.	4,01
59	Faço *backup* no google *drive* (nuvem)	2,06
60	Faço *backup* em HD externo.	3,77
61	Não faço *backup*.	3,68
62	Utilizo a criptografia.	3,46
63	Utilizo a criptografia só quando necessário.	3,23
64	Não utilizo a criptografia.	3,15
65	Já acessei *links* com propagandas e sorteios.	2,71
66	Já abri e-mails de remetente desconhecido.	2,62
67	Nunca acessei *links* e e-mail desconhecido.	3,25

68	Já perdi dados e informações por causa de códigos maliciosos (vírus).	4,03
69	Já tive dispositivos danificados por causa de códigos maliciosos (vírus).	3,74
70	Não tive perda ou acesso através dos códigos maliciosos.	2,44
71	Já tive dados e informações acessados pelos *hacker*s.	4,00
72	Já perdi dados e informações sigilosas e importantes.	4,07
73	Nunca perdi dados e informações.	2,49
74	Já cai no golpe do falso sequestro por telefone.	4,42
75	Já cai no golpe de falsa instituição financeira.	4,44
76	Já cai no golpe de cartão de crédito.	4,35
77	Já cai no golpe de empresa de cobrança.	4,44
78	Nunca cai em golpes	2,00

Fonte: Elaborado pela acadêmica com base nos dados coletados, 2020.

Os profissionais de Secretariado Executivo trabalham com muitas informações no decorrer do dia e o avanço tecnológico lhes trouxe benefícios para a realização de suas atividades. Então, esses profissionais devem utilizar e acompanhar a evolução das tecnologias (ADELINO; SILVA, 2012). Desse modo, ao analisar as variáveis e suas médias do constructo 4, na variável 49, a UNIOESTE (2,54), UNICENTRO (3,44), UEM (4,08) e UEL (4,33) estão com suas médias próximas ao "Não concordo e não discordo" e "Discordo". Nota-se que são poucos os discentes da UNIOESTE e UNICENTRO que utilizam computador, e os discentes da UEM e UEL não fazem uso constante do computador, visto que, conforme o resultado, "discordam". A variável 50 é sobre o uso de *Notebook*, nota-se que não são todos os discentes da UEL que possuem *Notebook*, porque a média (3,00) está próxima do "Não concordo e não discordo". Os demais discentes da UEM (2,50), UNIOESTE (1.36) e UNICENTRO (1,68) ficaram próximos do "Concordo plenamente" e "Concordo". Então, entende-se que esses discentes utilizam *Notebook*. E os discentes que fazem uso de *smartphones*, as médias (UEM 1,16, UEL 1,11, UNIOESTE 1,27 e UNICENTRO 1,35) estão todas próximas ao "Concordo plenamente". Nota-se que a maioria dos discentes já utiliza novas tecnologias, destacando que os profissionais de Secretariado devem buscar constante atualização sobre as novas tecnologias, devido ao fato de utilizá-las para executar atividades (AGUIAR; CABRAL, 2017).

Buscando mapear as práticas de segurança, a variável 54 mostra as médias (UEM 3,66, UEL 3,11, UNIOESTE 2,54 e UNICENTRO 3,66) próximas ao "Não concordo e não discordo" e "Discordo". Compreende-se que são poucos os discentes que utilizem *Firewall* para sua segurança. Não compreendem a importância de se utilizar o *Firewall*, visto que este é um sistema de defesa com barreiras de proteção para dispositivos móveis, que serve para bloquear o acesso não autorizado (CGI.BR, 2012). Logo, os discentes de Secretariado não conhecem todas as ferramentas que podem ser usadas para sua proteção. A ferramenta (*Firewall*) foi criada para impedir *hackers* ou códigos maliciosos de conseguir acesso a computadores e dispositivos móveis conectados a uma rede ou internet móvel e auxilia impedindo o envio de *softwares* mal intencionados para outros (WEIGERT; CASTILHO, 2017).

Quando questionados sobre o uso de *Anti-malware* (variável 55), a UEM ficou com a média 4,08, os discentes não utilizam antivírus, que é a média relacionada ao "Discordo". A UEL (3,22) e a UNICENTRO (3,53) ficaram com médias próximas ao "Não concordo e não discordo" e "Discordo", poucos deles utilizam o *Anti-malware*. E a UNIOESTE ficou com a média 2,27, ou seja, os discentes desta universidade fazem o uso de *Anti-malware*. Os discentes

não compreendem a importância de se ter um antivírus e *Anti-malware*, e este busca detectar, anular e remover os códigos maliciosos (Comitê Gestor da Internet no Brasil, 2012). Portanto, os discentes da UEM estão vulneráveis aos códigos maliciosos, pois não utilizam antivírus, os da UEL e UNICENTRO também correm o risco de ter acesso por códigos maliciosos, porque não são todos que utilizam o *Anti-malware*. Percebe-se que os únicos discentes mais protegidos são os da UNIOESTE, visto que fazem esse uso.

Uma ferramenta de proteção e prevenção é o *backup* – cópias de segurança que devem ser feitas para evitar possíveis perdas de dados, informações e falhas. Pode ser feito em *HD, Google drive,* entre outros (CGI.BR, 2012). Os *backups* dos discentes são feitos principalmente no *Google drive* (variável 59). Acredita-se que esse modelo de *Backup* é o mais utilizado devido ao fato de estar mais presente no cotidiano atual.

A criptografia é uma ferramenta que serve para criar mensagens cifradas ou codificadas. Serve para proteger dados contra acessos indevidos (CGI.BR, 2012). Sendo assim, verifica-se que a UEM (3,83) e UEL (4,0) não fazem o uso da criptografia e a UNICENTRO E UNIOESTE (3,0 e 3,37, respectivamente) não de maneira contundente. Compreende-se que os discentes não fazem o uso de todas as ferramentas disponíveis para sua proteção, estão vulneráveis por descuido. É necessário que os discentes utilizem ferramentas auxiliadoras na prevenção e combate a códigos maliciosos ou *hackers.* E a criptografia pode ser utilizada diretamente nos seus dispositivos móveis, diminuindo efetivamente fraudes, golpes ou acessos não autorizados (BINE; KUK, 2016).

Para finalizar a pesquisa, os discentes são questionados sobre como é a preparação dos secretários executivos em relação à proteção de dados digitais. Avalia-se a preparação dos futuros profissionais de Secretariado Executivo em relação à proteção dos dados digitais. O Quadro 3 apresenta as respostas dos discentes e suas respectivas universidades.

Tabela 3 – Preparação dos secretários executivos.

Universidade	Variáveis
UEL	Boa; pouca preparação na Universidade; conter na grade do curso aula específica sobre este assunto; importantíssimo e necessário; não tem como avaliar no momento; ruim; sem preparação.
UEM	Baixa; boa; deveria ser mais abordado esse tema na graduação; ótima; zero; 9; a graduação é o melhor lugar para preparar esses profissionais; incluir no curso uma disciplina relacionada a esse tema.
UNICENTRO	A grade está desatualizada; sigilo faz parte da profissão; Secretário Executivo deve buscar conhecimento nesta área; tem que saber como cuidar; boa preparação na graduação; fraca; tem total preparação; básica; completo despreparo; especialização em cursos de "TI"; importante disciplina em sigilo; falha; melhorar preparação dos profissionais de S.E; extremamente necessária; falta informações do que pode ser passado a terceiros; mediana; muitos não sabem se proteger; preparação excelente; razoável.
UNIOESTE	A empresa deve seguir seu protocolo de segurança de dados e informações; S.E deve sempre se atualizar; não existe matéria específica sobre isso no curso; a Universidade prepara como em qualquer outro lugar; boa; mediana; no 2º ano e até agora não foi discutido sobre isso; proteção dos dados digitais deve ser da empresa.

Fonte: Elaborado pela acadêmica com base nos dados coletados, 2020.

O curso de Secretariado Executivo busca preparar excelentes profissionais durante a graduação. Dessa forma, esta pesquisa questiona os discentes sobre a sua preparação para o mercado de trabalho. De acordo com os discentes da Universidade Estadual de Londrina – UEL,

que emitem sua opinião, a preparação é de um modo geral boa e apontam a importância de haver uma disciplina específica sobre esse assunto, visto que os profissionais de Secretariado Executivo acessam diariamente inúmeras informações e dados.

Os discentes da universidade Estadual de Maringá – UEM, que opinam sobre a preparação desses profissionais, avaliam de modo que as respostas variam entre zero, boa e ótima, "9". Também opinam sobre a importância de ser abordado mais esse tema. Esses discentes apontam que a graduação é o melhor lugar para preparar esses profissionais e há a importância de se incluir no curso uma disciplina relacionada a esse tema.

Segundo os discentes da Universidade Estadual do Oeste do Paraná – UNIOESTE, a preparação dos profissionais de Secretariado Executivo é considerada boa. Outra opinião é "Estou no 2º ano e até agora não foi discutido sobre isso". Outra perspectiva aponta que a proteção dos dados digitais deve ser da empresa, a qual deve seguir seu protocolo de segurança de dados e informações. A opinião do discente é relevante, porém cabe ao secretário executivo orientar as empresas quanto aos dados e informações que são sigilosos e encontrar ferramentas que auxiliem na proteção de dados digitais. Outra opinião relevante foi sobre a universidade não ter uma matéria especifica sobre o assunto.

A universidade Estadual do Centro-Oeste – UNICENTRO foi onde os discentes mais opinaram sobre a preparação dos profissionais em relação à proteção de dados digitais. Eles consideram a preparação desses profissionais fraca. Outra opinião aponta que os profissionais de Secretariado Executivo "Não sabem se proteger", sendo dever do secretário executivo se especializar nessa área ou que proteger dados e informações faz parte da profissão. Para finalizar, 12 discentes apontam que a grade do curso está desatualizada. Eles acreditam ser relevante uma atualização na grade do curso. Também opinam que, ainda, há muita coisa importante para ser melhorada na preparação. Existe a importância de se ter uma disciplina em sigilo e proteção, sendo interessante incluir na grade curricular uma disciplina de Tecnologia e Inovação (TI), a qual prepara esse profissional para a era digital. Os autores Adelino e Silva (2012) apontam que a tecnologia da informação pode ser utilizada para implementar estratégias competitivas e, tendo esse conhecimento, o profissional certamente se torna mais qualificado para as necessidades do mercado, agregando valor à empresa da qual esse profissional faz parte ou pretende fazer.

Desse modo, é possível verificar que, na opinião de alguns discentes, a preparação desses profissionais é considerada boa. Destaca-se que todas as universidades entrevistadas apontam a necessidade de uma atualização na grade curricular do curso e a indispensabilidade de inserir uma disciplina de "TI" na graduação, para poder sanar as dúvidas e preparar melhor os profissionais de Secretariado Executivo acerca do tema desta pesquisa – sobre dados digitais pessoais e profissionais.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa aborda o sigilo e a proteção das informações digitais pessoais e profissionais, devido ao fato de os profissionais de Secretariado Executivo trabalharem com muitas informações no seu dia a dia e utilizarem tecnologias e meios digitais para auxiliar seu trabalho.

A questão de pesquisa aborda como os discentes do curso de Secretariado Executivo mantêm o sigilo e proteção das informações digitais pessoais e profissionais, em que se observou que a maioria dos discentes conhece e mantém a proteção de suas informações digitais. Os resultados da pesquisa apontam que eles têm senhas em todos os seus locais de

acesso, em seus dispositivos móveis e computadores, assim como fazem *download* de aplicativos somente em lojas seguras. No entanto, observou-se a vulnerabilidade dos discentes quanto ao compartilhamento de dados e informações sigilosas, já que concordam que compartilham pelo aplicativo *Whatsapp* informações, dados, áudios, vídeos e documentos, ficando expostos a códigos maliciosos, *hackers* e oportunistas.

Quantifica-se que os discentes consideram documentos empresariais e pessoais sigilosos, sendo que os discentes da UNICENTRO e UNIOESTE consideram todos os tipos de arquivos sigilosos. Quantifica-se também que os discentes consideram senhas e informações bancárias sigilosas, assim como dados pessoais. Mapeiam-se os dispositivos utilizados pelos discentes e observa-se que alguns discentes fazem uso do *Notebook*, mas a grande parte possui *smartphones*.

No mapeamento das práticas de segurança adotadas pelos discentes, observa-se que são poucos os que utilizam a ferramenta de defesa *Firewall* para sua segurança. Nota-se que os discentes não compreendem a importância de se utilizar essa ferramenta, junto com as senhas que eles utilizam em seus locais de acesso e dispositivos, a qual iria dificultar ainda mais os acessos não autorizados. Percebe-se também que os discentes da UEM não utilizam nenhum antivírus, estando totalmente vulneráveis à perda de seus dados e informações para códigos maliciosos ou *hackers*. Já os discentes da UEL e UNICENTRO estão parcialmente seguros, visto que alguns utilizam antivírus. Nota-se que os únicos discentes que utilizam antivírus para sua proteção são os da UNIOESTE.

Quanto à proteção e segurança através de *backups*, nota-se que os discentes o fazem utilizando o *Google Drive*, relacionado ao uso da criptografia, a qual também é uma importante ferramenta de segurança. Observa-se que os discentes da UEM e UEL não fazem o uso da criptografia e os discentes da UNICENTRO e UNIOESTE utilizam somente quando há necessidade.

O sigilo é um valor intrínseco a qualquer prática executada pelo profissional de Secretariado Executivo, uma vez que essa profissão trabalha com informações significativas e de acesso restrito. Em muitas empresas, o Secretário Executivo é o único que tem acesso a todos os processos, documentos e arquivos da organização, por isso, cabe a esse profissional identificar e classificar as informações sigilosas (limitadas ao secretário e o superior), restritas (destinadas somente a um setor ou grupo) e abertas (domínio público). Esse profissional possui perfil de gestor, capacidade de analisar e interpretar qualquer informação pública ou privada, gerir e administrar processos e documentos, pois possui visão generalista da organização, funções gerenciais, habilidade de lidar com modelos inovadores de gestão, responsabilidade e respeito à ética profissional, gerenciamento de informações e maximização e otimização dos recursos tecnológicos. Assim, nota-se que o profissional de Secretariado Executivo possui como conduta ética manter em sigilo e proteção as informações e dados que a ele são confiadas, prezando pela discrição, independentemente do tipo de empresa.

Portanto, é de grande valia que as universidades abordadas nesta pesquisa analisem a possibilidade de incluírem na grade curricular do curso de Secretariado Executivo uma disciplina de TI, ou que incorporem este tema em alguma outra disciplina correlata. Isso auxilia os futuros profissionais de Secretariado Executivo quanto aos dados e informações sigilosas que requerem proteção no ambiente digital, sendo esta questão observada também pelos discentes das quatro universidades, os quais relatam a necessidade e importância deste tema ser abordado na graduação.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2013. **Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação**.

ADELINO, F. J. S.; SILVA, M. A. V. **A tecnologia da informação como agente de mudança no perfil do profissional de secretariado.** Revista de Gestão e Secretariado – GeSec. São Paulo: v. 3, n. 2, p. 05-23, jul./dez. 2012.

AGUIAR, M. E.; CABRAL, A. R. **Internet das coisas e o profissional de secretariado executivo.** Revista tecnologia em projeção. v. 8, n. 1, p. 112, 2017.

ARAÚJO, D. da S.; SILVA, V. L. **O profissional de secretariado e o uso das tecnologias da comunicação e informação nas organizações.** Revista Científica Semana Acadêmica.

BASTOS, J. L. D.; DUQUIA, R. P. **Um dos delineamentos mais empregados em epidemiologia: estudo transversal.** Revista Eletrônica. *Scientia* Medica, Porto Alegre, v. 17, n. 4, p. 229-232, out./dez. 2007.

BINE, J.; KUK, J. N. **Estudo da segurança em dispositivos móveis**. Departamento de ciência da computação. Semana acadêmica. Universidade do centro-oeste. UNICENTRO. Guarapuava, 2016.

CGI. BR. Comitê Gestor da Internet do Brasil. **Cartilha de segurança para internet**.

CUNHA, D.; FENATO, M. A. **A segurança da informação e a sua importância para a auditoria de sistemas.** Revista Científica Semana Acadêmica. Edição 29. V. 1. 2013.

DUARTE, A. W. B. D. **Survey**. Faculdade de Educação. UFMG. Belo Horizonte, 2010.

ESPERÓN, J. M. T. **Pesquisa quantitativa na ciência da enfermagem.** Universidade Federal do Rio de Janeiro. 2016-2017. Brasil.

FRANCO, M. V. A.; DANTAS, O. M. A. N. A. **Pesquisa exploratória: aplicando instrumentos de geração de dados – observação, questionário e entrevista.** XIII Congresso Nacional de Educação – EDUCERE. 2017.

GIL, A. C. **Métodos e técnicas ou pesquisa social**. Editora: Atlas. 6 ed. São Paulo, 2008.

HOCHMAN, B. et al. **Desenhos de pesquisa.** Acta Cirurgica Brasileira. vol.20. (supl. 2). São Paulo, 2005.

HOLANDA, M. T. de; FERNANDES, J. H. C. **Segurança no desenvolvimento de aplicações.** Curso de especialização em gestão de segurança da informação e comunicações. GSIC701. v. 1. 2009 – 2011.

KOHN, K.; MORAES, C. H. de. **O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital.** Universidade de Santa Maria. Intercom - Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. XXX Congresso Brasileiro de Ciências da Comunicação – Santos – 29 de agosto a 2 de setembro de 2007.

LIMA, M. A.; SOARES, A. de P. L. **O secretário executivo e a tecnologia da informação: Um estudo sobre a utilização de recursos tecnológicos pelos profissionais da cidade de Belém/PA.** Revista de gestão e Secretariado. GeSec.

NONATO JR. R. **Epistemologia e teoria do conhecimento em secretariado executivo: A fundação das ciências da assessoria.** Fortaleza: Expressão Gráfica, 2009.

SANTOS, C. M. L. da S. A. dos. **Estatística descritiva – Manual de auto-aprendizagem**. Ed. Sílabo, Lda. 3ª Edição – Lisboa, Setembro de 2018.

SILVA JÚNIOR, S. D. da; COSTA, F. J. da. **Mensuração e Escalas de Verificação: uma Análise Comparativa das Escalas de *Likert* e *Phrase Completion.*** PMKT – Revista brasileira de pesquisa de marketing, opinião e mídia. São Paulo, Brasil. V. 15, p. 1-16, outubro de 2014.

WEIGERT, A.; CASTILHO JUNIOR, G. O. de. **Utilização de firewall em aplicação de segurança e ferramentas gerenciais.** 2017. 62f. Trabalho de Conclusão de Curso.(Curso Superior de Tecnologia em Sistemas de Telecomunicações). Departamento Acadêmico de Eletrônica. Universidade Tecnológica Federal do Paraná. Curitiba, 2017.