UNIVERSIDADE DE BRASÍLIA
FACULDADE DE CIÊNCIA DA INFORMAÇÃO
GRADUAÇÃO EM BIBLIOTECONOMIA
TRABALHO DE CONCLUSÃO DE CURSO

Igor Lukas Kleftakis de Carvalho

CIBERSEGURANÇA:
UM ESTUDO COMPORTAMENTAL DE USUÁRIOS DA INFORMAÇÃO

Brasília
2023

Igor Lukas Kleftakis de Carvalho

CIBERSEGURANÇA:
UM ESTUDO COMPORTAMENTAL DE USUÁRIOS DA INFORMAÇÃO

Monografia apresentada como parte das exigências para obtenção do título de Bacharel em Biblioteconomia pela Faculdade de Ciência da Informação da Universidade de Brasília

Orientadora: Professora Doutora Fernanda Farinelli

Brasília

2023

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

KC331c

Kleftakis de Carvalho, Igor Lukas
Cibersegurança: Um estudo comportamental de usuários da informação / Igor Lukas Kleftakis de Carvalho; orientador Fernanda Farinelli. -- Brasília, 2023.
96 p.

Monografia (Graduação - Biblioteconomia) -- Universidade de Brasília, 2023.

1. Cibersegurança. 2. Segurança da Informação. 3. Estudo de Comportamento. 4. Estudo de Usuário. 5. Biblioteconomia. I. Farinelli, Fernanda, orient. II. Título.

Universidade de Brasília

FOLHA DE APROVAÇÃO

Título: Cibersegurança: Um Estudo Comportamental de Usuários da Informação

Autor(a): Igor Lukas Kleftakis de Carvalho

Monografia apresentada em **20 de julho de 2023** à Faculdade de Ciência da Informação da Universidade de Brasília, como parte dos requisitos para obtenção do grau de Bacharel em Biblioteconomia.

Orientador(a) (FCI/UnB): Dra. Fernanda Farinelli

Membro Interno (FCI/UnB): Dr. Márcio Bezerra da Silva

Membro Interno (FCI/UnB): Dr. Márcio de Carvalho Victorino

Em 20/10/2022.

Documento assinado eletronicamente por **Fernanda Farinelli**, **Professor(a) de Magistério Superior da Faculdade de Ciência da Informação**, em 25/07/2023, às 12:18, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Marcio Bezerra da Silva**, **Professor(a) de Magistério Superior da Faculdade de Ciência da Informação**, em 25/07/2023, às 12:23, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Marcio de Carvalho Victorino**, **Professor(a) de Magistério Superior da Faculdade de Ciência da Informação**, em 25/07/2023, às 12:32, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **10055030** e o código CRC **2B66E288**.

Esse trabalho é dedicado a todas as pessoas que fizeram do mundo um lugar melhor,
cujos nomes a história não se importou em lembrar.

AGRADECIMENTOS

Ao finalizar minha jornada na graduação e completar este trabalho de conclusão de curso, gostaria de agradecer a todo o curso de Biblioteconomia da Universidade de Brasília, minha orientadora, o corpo docente e discente, do qual me orgulho de fazer parte. Agradeço a minha família, meus colegas, meus amigos e meu amor pela paciência e suporte de todos.

RESUMO

Este estudo investiga o problema da segurança da informação no meio digital, e como as pessoas se comportam neste ambiente. Dados pessoais são disponibilizados *online* todos os dias, muitas vezes esses são sensíveis e vulneráveis. A pesquisa busca determinar o conhecimento e atitudes de usuários da informação em relação à cibersegurança. Uma fundamentação teórica foi realizada a fim de desenvolver um embasamento para a pesquisa, posteriormente, um questionário foi aplicado a uma amostra de 40 alunos cursando Biblioteconomia na Universidade de Brasília. Os resultados da pesquisa demonstram que, em média, os participantes possuem um conhecimento sólido sobre alguns aspectos básicos da segurança da informação, porém outros participantes apresentam hábitos arriscados em relação à segurança informacional. A partir da comparação entre pesquisa e resultados, foi possível concluir que, apesar de ser determinado um grau razoável de conhecimento sobre cibersegurança, os alunos podem se beneficiar bastante de exposição mais aprofundada nesta área; que estudos mais detalhados devem ser realizados, se possível com maiores amostras; e ainda, foram recomendados mais esforços por parte das instituições para trazer conscientização e educação aos estudantes em relação a este tópico.

Palavras-chave: Cibersegurança; Segurança da Informação; Estudo de Comportamento; Estudo de Usuário; Biblioteconomia.

ABSTRACT

This study investigates the information security issue on a digital environment and how people behave in this environment. Personal data is made available online every day, these are often sensitive and vulnerable. The research aims to determine the knowledge and behaviors of information users in relation to cybersecurity. A theoretical foundation was conducted as a means to develop a basis for the research, afterwards, a questionnaire was applied to a sample of 40 students undergoing Library Science on University of Brasília. The research results show that, on average, the participants have a solid knowledge over some basic aspects of information security, however other participants show risky habits related to information security. From comparison between research and results, it was possible to conclude that, although it was determined a reasonable degree of knowledge over cybersecurity, the students could greatly benefit from further exposition to this area; that more detailed studies must be carried on, with larger samples if possible; and yet, more efforts were recommended on the institutions part, in order to bring awareness and education to students on this topic.

Keywords: Cybersecurity; Information Security; Behavior Study; User Study; Library Science.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

CI	-	Ciência Da Informação
DoS	-	*Denial of Service* (Negação de Serviço)
DDoS	-	*Distributed Denial of Service* (Negação de Serviço Distribuída)
FCI	-	Faculdade de Ciência da Informação
FOMO	-	*Fear of Missing Out* (Medo de Ficar de Fora)
GDPR	-	*General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados)
LGPD	-	Lei Geral de Proteção de Dados Pessoais
NASA	-	*National Aeronautics and Space Administration* (Administração Nacional da Aeronáutica e Espaço)
OT	-	*Operational Technology* (Tecnologia Operacional)
PPC	-	Projeto Pedagógico do Curso
RDP	-	*Remote Desktop Protocol* (Protocolo de Desktop Remoto)
SIGAA	-	Sistema Integrado de Gestão de Atividades Acadêmicas
TDAH	-	Transtorno do Déficit de Atenção com Hiperatividade
UFSM	-	Universidade Federal de Santa Maria
UnB	-	Universidade de Brasília

SUMÁRIO

1 INTRODUÇÃO

A segurança da informação (SI) pode ser entendida como a barreira que impede o uso ou acesso não autorizado à informação, que também garante a preservação da integridade e confidencialidade dessas informações (SILVA; STEIN, 2007). Métodos como a criptografia vem sendo usados desde 600 A.C. pelos hebreus, já nas décadas de 1950 e 1960, a ameaça de espiões na Guerra Fria levou oficiais a utilizar práticas de proteção da informação. Portanto, é evidente, que a preocupação do ser humano em cuidar adequadamente da informação não é recente, registros históricos demonstram que essa questão é mais antiga do que se imagina (PERALLIS).

Desde a ascensão dos computadores, a segurança da informação chegou no ambiente digital, se tornando cada vez mais relevante. O surgimento da *Internet*, a consolidação da informação como um bem de valor tanto social quanto financeiro e a difusão da comunicação em um mundo globalizado são todos fatos que se apresentam no cenário moderno. As informações sobre a vida dos cidadãos comumente se encontram *online*. Diante desta realidade, é necessário perceber como a segurança destes dados e informações se tornou mais complexa, importante e desafiadora (PERALLIS).

A Segurança da Informação é vital na era digital, e o comportamento humano está no centro desse novo mundo. Na era moderna, as pessoas têm grande influência sobre o fluxo de suas informações, assim como das outras, gerando a possibilidade de vários riscos, como a infecção por vírus de computador. De acordo com Norton (c2021), “um vírus é um tipo de programa ou código malicioso criado para alterar a forma como um computador funciona e desenvolvido para se propagar de um computador para outro”. Algumas das outras principais ameaças virtuais conhecidas são: *spyware*, ou *software* espião, ataca dispositivos para coletar informações; *ransomware*, criptografa dados no dispositivo, impedindo acesso aos arquivos; *trojan*, ou cavalo de troia, *software* que se disfarça por programa legítimo, simulando uma funcionalidade útil; *phishing*, prática que rouba dados de cadastro de clientes por meio de mensagens iscas, comumente por *e-mail*; e ataques ao serviço *RDP* (*Remote Desktop Protocol* - Protocolo de Desktop Remoto), permite o acesso remoto à dispositivos na área de trabalho (ASER, c2022).

Mas uma forma de ameaça se destaca para este estudo, a “engenharia social”, é uma forma de manipulação do comportamento humano, por indivíduos mal-intencionados, que busca violar a confidencialidade, disponibilidade e/ou integridade de dados dos cidadãos

(GLOBALSIGN, 2020). A tecnologia evolui, as plataformas de armazenamento se renovam, mas o fator humano permanece o mesmo. É vital que as pessoas entendam os riscos e saibam se proteger.

1.1 Problema

Como foi sugerido, o comportamento humano é uma peça central para a Segurança da Informação, sendo imprevisível e falível em termos de confiabilidade. Frequentemente o elemento humano é considerado o elo mais fraco na corrente da defesa cibernética, pois "Não há *Patch* contra a Burrice Humana." (MARCELO; PEREIRA, 2005, p. 3). De fato, o descuido pessoal abre as portas para inúmeros riscos com consequências graves, dessa forma, muitos criminosos modernos se aproveitam das aberturas criadas por esses riscos. Com roubo de dados e informações das pessoas, pode haver chantagens pela ameaça de expor fotos ou informações íntimas; venda de dados; se uma pessoa expõe sua vida em redes sociais, pode revelar sua rotina e facilitar um sequestro; e a desconformidade com a Lei Geral de Proteção de Dados (LGPD) também é recorrente entre empresas (ASER, c2022). Percebe-se que diversos novos tipos de crimes ocorrem hoje, nem sempre havendo justiça, e vários cidadãos continuam cegos a estes perigos na contemporaneidade. Talvez existam poucas ações sendo tomadas para remediar e prevenir esses problemas, e uma propagação insuficiente de discussões acerca da importância deste tópico. Muito pode ser feito neste setor, a relevância de conscientizar e educar os usuários a proteger seus dados e informações é enorme; mais educação, trabalhos, discussão e atenção para esta problemática é necessária. Dessa forma, mais pesquisa e investimento podem ajudar a identificar fatores que levam a comportamentos inseguros, e como resolver esses problemas.

1.2 Questão de pesquisa

Dentro deste contexto, são estabelecidos alguns pressupostos os quais direcionam este trabalho.

- Em pleno 2023, os usuários da informação deveriam ser responsáveis com seus dados.
- Devem ter conhecimento sobre a 'engenharia social' e outras ameaças à segurança da informação, e quais métodos são usados cotidianamente para manipulá-los.
- Poderiam estar familiarizados com a LGPD e seus direitos.

- As pessoas precisam se importar com quem tem acesso aos seus dados e o que é feito com eles, assim como perceber a gravidade da situação.

Dessa forma, a pergunta é: **Como se apresenta o comportamento dos alunos do Curso de Biblioteconomia da UnB sobre segurança da informação e aspectos que a fomentam?**

Os alunos da Biblioteconomia trabalham intimamente com a gerência de informação, dados e sistemas de organização e preservação do conhecimento. No Projeto Pedagógico do Curso (PPC) de Biblioteconomia (2018) da UnB é determinado que, parte do objetivo geral requer formar profissionais capazes de atender às necessidades de demanda, geração, processamento, disseminação e utilização de dados, informações e conhecimentos registrados nos mais diferentes suportes.

Portanto, uma pesquisa realizada com essa população, pode revelar o quanto eles estão cientes sobre a importância em cuidar de forma adequada da disponibilidade, integridade e confidencialidade das próprias informações, assim como as de outras pessoas.

1.3 Objetivo geral

Este estudo tem como objetivo geral identificar o comportamento dos alunos do curso de Biblioteconomia da UnB em relação à segurança da informação.

1.4 Objetivos específicos

Os objetivos específicos deste estudo são:

- Identificar as características sociodemográficas dos alunos do curso de Biblioteconomia da UnB;
- Identificar o comportamento dos alunos do curso de Biblioteconomia da UnB em relação às ações que garantam a segurança da informação;
- Identificar se os alunos do curso de Biblioteconomia da UnB têm conhecimentos gerais sobre conceitos relacionados à segurança da informação;

1.5 Justificativa

Este estudo é relevante em um contexto social, vez que a pesquisa e discussão levantadas são necessárias tanto para uma maior conscientização, quanto para adquirir mais informações que ajudem a compreender o comportamento dos cidadãos. Ainda há pouca atenção para os

problemas do fator humano neste ambiente, e ainda menos sobre formas efetivas de resolvê-los. Portanto, a importância consiste em prevenir incidentes criminais reais do cotidiano social.

Já pela perspectiva dos profissionais da Biblioteconomia, assim como da Ciência da Informação (CI) em geral, esta questão pode ser de interesse. Uma das principais funções dos profissionais na área é o armazenamento e preservação de materiais e as informações contidas neles, tanto em formato físico quanto na mídia digital. Brechas de segurança e comportamentos irresponsáveis dos funcionários responsáveis pelos materiais podem ser altamente prejudiciais para os materiais e suas informações, especialmente quando se fala de obras raras.

Considerando também o ângulo da sociedade acadêmica, estudos como esse podem prover uma oportunidade para refletir sobre a importância desse tópico. Estabelecendo-se aqui a relação íntima entre a segurança da informação e a Ciência da Informação, pode ser considerada relevante a necessidade dos estudantes e professores estarem cientes dessa temática. Talvez possa ser aconselhável até integrar disciplinas que tratem desta compreensão durante a formação.

1.6 Estrutura do trabalho

A seção 2 apresentará o referencial teórico do trabalho, introduzindo e explicando diversos conceitos e ideias importantes para a melhor compreensão do tema que serve como base da pesquisa; além disso, serão expostos os pensamentos e informações de vários autores, artigos, notícias e até documentários, e como o conhecimento de cada um desses conversam entre si, complementando uns aos outros.

Na seção 3, será explicada e detalhada a metodologia do estudo, dissertando acerca dos instrumentos e procedimentos metodológicos que foram utilizados para realizar a pesquisa, a população que foi escolhida como objeto de estudo, assim como a caracterização da amostra com a qual de fato foi realizada a pesquisa.

Durante a seção 4, será explicitada a análise que decorreu a respeito dos resultados de pesquisa. Neste tópico, o trabalho buscou relacionar os resultados estatísticos provenientes das respostas do questionário, com o embasamento teórico que foi consolidado durante a seção da fundamentação teórica. A partir desta relação entre as pesquisas e ferramentas, a seção almeja compreender e explicar o que foi observado nas respostas do questionário, e se necessário, explicar quaisquer disparidades entre o referencial teórico e os resultados práticos da pesquisa.

Finalmente, na seção 5, são apresentadas as considerações finais e recomendações acerca do tema. Serão consideradas a análise dos dados e interpretação dos resultados em ordem

de evidenciar o que o estudo foi capaz de alcançar; indicando os limites e reconsiderações da pesquisa. Em suma, apresentar a condensação dos conceitos, pesquisas, resultados, interpretações e como eles se complementam.

2 FUNDAMENTAÇÃO TEÓRICA

No decorrer desta seção, a monografia procura realizar um embasamento a respeito de alguns conceitos relevantes relacionados à segurança da informação, daquilo que for pertinente à literatura existente. Por meio de pesquisa, conceituações de diversos pensadores e compreensão de suas ideias, a seção busca apresentar citações e criar subsídios para o presente estudo, com base nessas informações. Serão discutidos os assuntos centrais, desde a explicação de conceitos mais primordiais como informação e ameaça, até elementos mais específicos e aprofundados como a engenharia social e a legislação existente sobre proteção de dados, tanto brasileira quanto internacional.

2.1 Segurança da Informação e Cibersegurança

Começando pela conceituação da cibersegurança, também conhecida como segurança da tecnologia da informação, é uma área que envolve técnicas e ações que juntas almejam defender sistemas, programas, equipamentos, redes e indivíduos de ataques cibernéticos, crimes virtuais e terrorismo cibernético (ALURA, 2022).

Mencionando alguns dos princípios básicos da cibersegurança, podem ser citados e explicados brevemente os cinco pilares da segurança da informação. Os quais consolidam a fundação e estabelecem o propósito para a racionalização e desenvolvimento deste trabalho, definidos segundo Barcelos (2019), GATInfoSec (c2020) e Senhasegura (2021) e ilustrados a seguir na Figura 1:

Figura 1: Os cinco pilares da segurança da informação

Fonte: Atlântico, 2019

CONFIDENCIALIDADE: o primeiro princípio é aquele que garante o acesso aos dados e à informação exclusivamente para as pessoas ou entidades devidamente autorizadas.

Estabelecendo privacidade e evitando ataques cibernéticos ou espionagem, se aplica especialmente a dados pessoais, sensíveis, financeiros, psicográficos e outras informações sigilosas. Esta proteção pode ser feita por autenticação de senha, verificação biométrica e criptografia, por exemplo. Deve também se atentar ao fato de que a confidencialidade de dados pessoais de usuários é um dos requisitos centrais para estar em conformidade com a LGPD e com o Regulamento Geral sobre a Proteção de Dados (*GDPR*).

INTEGRIDADE: este é o princípio responsável por manter a veracidade, originalidade, preservação, precisão, consistência e confiabilidade dos dados, não permitindo a alteração destes sem autorização. Havendo modificações inadequadas nos dados, a informação contida neles pode se tornar incorreta, comprometendo a sua integridade; são necessários mecanismos de controle para mediar uma interação adequada. Assim se garante a integridade dos dados, que frequentemente é afetada por erros humanos, políticas de segurança inadequadas, processos falhos e ciberataques.

DISPONIBILIDADE: é o princípio que garante que os dados estejam disponíveis para serem acessados pelos indivíduos, entidades ou processos sempre que o acesso à informação for necessário. Para isso, é necessária a estabilidade e acesso aos dados nos sistemas, por intermédio de atualizações, manutenções, solução de vulnerabilidades e protocolos para gerenciamento de crises. É importante ressaltar que os sistemas são vulneráveis a diversas ameaças que prejudicam este pilar, tais como blecautes, ataques de negação de serviços, incêndios e ainda desastres naturais, entre outros.

AUTENTICIDADE: pilar responsável pela validação do usuário para acessar, transmitir e receber determinadas informações. Seus mecanismos básicos são *logins* e senhas, mas também podem ser utilizados recursos como a autenticação biométrica, por exemplo. Esse pilar confirma a identidade dos usuários antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por terceiros.

IRRETRATABILIDADE: ou o "não repúdio", esse pilar garante que uma pessoa ou entidade não possa negar a autoria da informação fornecida, como no caso do uso de certificados digitais para transações *online* e assinatura de documentos eletrônicos. Na gestão da segurança da informação, isso significa ser capaz de provar o que foi feito, quem fez e quando fez em um sistema, impossibilitando a negação das ações dos usuários.

2.2 Vulnerabilidades e ameaças

Prosseguindo para outros conceitos importantes, é necessário compreender a natureza dos perigos que põem em risco a plena atividade desses cinco pilares. Por exemplo, no mundo da cibersegurança, existe o conceito de vulnerabilidade. A ISO 27000 apresenta uma visão geral e de vocabulário para Sistemas de Gestão de Segurança da Informação. A norma define uma **vulnerabilidade** como "uma fraqueza de um ativo que poderia ser potencialmente explorada por uma ou mais ameaças". Correlacionada a esta definição, a norma ISO também descreve o termo **ameaça** como qualquer "causa potencial de um incidente não desejado que possa resultar em dano ao sistema ou organização" (ADVISERA, 2015). Compreendendo esses dois últimos conceitos, podemos entender que o **ataque** seria a relação que ocorre de fato entres a vulnerabilidade e a ameaça; dessa forma, o ataque cibernético seria uma tentativa de desabilitar computadores, roubar dados ou usar um sistema de computador violado para lançar ataques adicionais (UNISYS, c2023).

Pelo nascimento dos computadores, a segurança da informação chegou no ambiente digital. Nos anos 1980, vírus, antivírus e outros recursos surgiram, de modo que, agora, a informação e os dados são mais importantes do que nunca, e hoje, são alvos do cibercrime. Alguns autores definem o cibercrime como atividades, realizadas mediante o uso de computadores, que sejam consideradas ilegais, também podendo ser efetuadas por meio de redes globais (PALMIERI; SHORTLAND; MCGARRY, 2021). A ameaça destes tipos de ataques é substancial, podendo causar danos tanto financeiros quanto físicos, criminosos podem impedir acesso aos dados e pedir resgate em dinheiro como recuperação dos dados, isso chama-se ataque de *ransomware*. Em pesquisa, Fortifirewall (2022) afirma que esses ataques aumentaram 10 vezes entre 2020 e 2021, com 51% das empresas afetadas sofrendo ataques de tecnologia operacional (*OT*) que prejudicaram a produtividade, enquanto que 45% foram alvo de ataques de *OT* que expuseram à risco a integridade física de funcionários.

Ainda nesta frente, existem os *malwares*, ou *softwares* maliciosos que prejudicam e exploram qualquer dispositivo, e Li (2020) afirma que vários aplicativos de fontes desconhecidas, contendo *malware*, se disfarçam de aplicativos normais. Um exemplo recente seria o aplicativo *NU Trade*, que tenta se associar ao *NUbank* através da semelhança entre os nomes. Segundo os autores Borkovich e Skovira (2019), a presença de *malwares* em dispositivos móveis aumentou consideravelmente nos últimos anos, havendo diversos casos de

golpes *online*. Evidentemente, os cibercriminosos dispõem de diversos métodos para roubar dados e informações das mais diversas naturezas.

Existem vários tipos de invasores que podem ameaçar a segurança de um sistema ou dispositivo, conhecidos como *hackers*. Quanto ao termo *hacker*, o BugHunt (2022) o define como pessoas com extenso conhecimento em computação e informática, que operam com desenvolvimento e modificação de *hardwares* e *softwares*. Portanto, não são necessariamente criminosos, aqueles que usam dessas habilidades para fins ilegais são aqueles referidos como cibercriminosos. O termo já via uso desde os anos 1960, quando pessoas tentavam usar o sistema de telefonia para realizar ligações gratuitas, esses indivíduos posteriormente ficaram conhecidos como *phreakers*. Hoje em dia, ainda conforme BugHunt (2022), existem vários tipos de *hackers*, sendo os principais:

- *White Hat*: também conhecidos como "hackers éticos", profissionais especialistas em cibersegurança que procuram auxiliar empresas e instituições a se protegerem de ataques cibernéticos com ajuda de seus conhecimentos e habilidades;
- *Black Hat*: também chamado de "cibercriminoso", desrespeita códigos de ética comuns e leis na sociedade, utilizando seus conhecimentos para cometer ataques e invasões a redes e sistemas. Geralmente motivados por ganhos financeiros ou espionagem criminosa;
- *Grey Hat*: um tipo de intermediário entre os anteriores. Cometem invasões de forma despretensiosa, às vezes por entretenimento, mas com objetivo de divulgar as vulnerabilidades do alvo, por um lado ajudando a empresa, mas ao mesmo tempo os cibercriminosos;
- *Crackers*: também podem ser considerados cibercriminosos, pois usam de suas habilidades para quebrar vários sistemas e *softwares* de segurança, contribuindo no aumento da pirataria e recebendo recompensas em troca de suas ações. Muitas vezes são motivados por reconhecimento de suas técnicas e popularidade;
- *Script Kiddies: black hats* iniciantes, usam programas e *scripts* já existentes e baixados da *Internet*, a fim de atacar redes e *sites*, ganhando popularidade, sendo considerados "amadores". Operam dessa maneira pois não possuem as habilidades e conhecimento necessários para escreverem seus próprios códigos, mas querem se tornar *black hats*.

Conhecendo agora os tipos de *hackers*, é necessário entender como são os ataques mais comuns, existem diversas ferramentas e estratégias. Conforme 33Giga (2022), Jorge e Wendt (2006), Linkedin (2022), e VaultOne (2021), os descritos a seguir são alguns dos principais:

- *Backdoor* (Porta dos Fundos): um programa malicioso que fica escondido em segundo plano. Pode servir como entrada para espiar e gerenciar o sistema operacional através de acesso remoto não-autorizado. É instalado manualmente por outro *software;*
- *Ransomware*: ou "sequestrador digital", o invasor usa de criptografia para bloquear os arquivos do terminal invadido e exige vantagem financeira, muitas vezes em criptomoedas, para devolver o acesso aos arquivos criptografados;
- *Trojan Horse* (Cavalo de Troia): é enviada ao usuário como um convite ou em anexo a outro programa que o usuário queira realmente instalar. Esta aplicação é bem mais complexa e permite o acesso remoto do terminal invadido pelo terminal invasor. Em muitos casos após realizar as atividades a que foi destinado o programa causa algum dano no terminal. Pode também realizar suas atividades impróprias fazendo uso do terminal infectado para dificultar sua localização;
- *Spyware*: é responsável por recolher informações sobre o usuário, sobre seus hábitos na *Internet* e envia essas informações a um outro terminal na *Internet*, sem que o usuário sequer desconfie do que está acontecendo, pois sua ação é silenciosa;
- *Keylogger*: registra todas as teclas digitadas pelo usuário. Geralmente é utilizado pelos desenvolvedores para obter *logins* e senhas. Muitas vezes está escondido no plano de fundo de um terminal. É um dos mais simples tipos de *spyware*, tanto para implementar quanto para resgatar as informações capturadas. É um dos mais utilizados em empresas, pais e cônjuges para obter informações sigilosas;
- Vírus: é uma aplicação maliciosa desenvolvida por programadores que, tal como um vírus biológico, contamina o sistema, faz réplicas de si mesmo e tenta se espalhar para outros terminais, utilizando-se de diversos meios. Em via de regra as contaminações ocorrem pela ação do usuário executando o anexo de um *e-mail* ou acessando *sites* que automaticamente carregam os arquivos da aplicação. Em outros casos a causa de contaminação se dá por sistema operacional desatualizado, sem a aplicação de corretivos que bloqueiam chamadas maliciosas nas portas do terminal;

- Ataques *DoS* (*Denial of Service*): o ataque de negação de serviço almeja sobrecarregar um servidor ou computador para que o sistema fique indisponível para o usuário. São feitos para impedir o servidor de atender os clientes, assim são usadas técnicas que enviam vários pedidos de pacotes para que o mesmo fique sobrecarregado e não consiga realizar atendimentos, porém feito por um único atacante;
- Ataque *DDoS* (*Distributed Denial of Service*): o ataque de negação de serviço distribuído é realizado através de vários computadores executando o ataque em conjunto contra um único alvo. Para realizar esse ataque, os *hackers* ou *crackers* enviam *trojans* juntamente com o programa utilizado para fazer o ataque *DDoS*;
- *Port Scanning*: programa que aproveita uma vulnerabilidade no sistema para realizar buscas no servidor, procurando uma brecha de segurança. Ao encontrar, rouba informações e dados com o objetivo de danificar o sistema ou sequestrar dados;
- Quebra de força bruta: se equivale ao invasor testar todas as chaves de um chaveiro ao abrir uma porta. O computador do *hacker* tenta diferentes combinações de nomes de usuários e senhas em uma alta velocidade até encontrar uma que funcione. Uma vez dentro, o *hacker* pode enviar mensagens com remetente conhecido para outros usuários com conteúdo de *phishing* e *spam*, pedindo depósitos, transferências, senhas e outros dados;
- *Phishing*: ataques através do qual o *hacker* leva o usuário a entregar informações sigilosas, como senhas, dados bancários e CPF. Geralmente, este ataque redireciona o usuário a um *site* idêntico ao verdadeiro de uma agência bancária, por exemplo. Funciona como “isca” para “pescar” os dados dos usuários, está entre os ataques mais populares;
- *Cryptojacking*: este ataque consiste em usar o computador do usuário para minerar criptomoedas. Instalando um *malware* na máquina da vítima, os criminosos exploram a capacidade e recursos do dispositivo para gerar moedas. Normalmente, o usuário nem percebe a ação dos *hackers*, exceto quando a lentidão do sistema se torna perceptível;
- *Zero Day*: ou Dia Zero, ciberataque que busca falhas em programas recém-lançados, buscando brechas e *bugs* antes da correção. Ataque menos comum, mas desenvolvedores costumam se deparar com esta ameaça; e

- Ataque de *RDP* (*Remote Desktop Protocol*): permite acesso remoto ao computador por outro computador. Através de portas abertas o *hacker* invade máquinas, injetando *malwares* no sistema acessado remotamente. Por exemplo, um funcionário trabalha remotamente e acessa sua estação de trabalho remotamente em sua empresa, isto pode servir como porta aberta para um ataque, quando não configurado corretamente.

Na perspectiva da CI, "a informação é um fenômeno e a comunicação é o processo de transferência ou compartilhamento deste fenômeno" (SARACEVIC, 1999), no processo da comunicação é quando existem vários riscos. Por intermédio de telefones celulares, redes sociais, contas bancárias e tantas outras formas de comunicação, um grande fluxo de dados e informações é transmitido a todo instante, esses dados são vulneráveis.

A vulnerabilidade de dispositivos, dados, informações e pessoas é uma questão central no cenário moderno, os cibercriminosos nunca param de explorar e abusar de vulnerabilidades nos sistemas, nas práticas de segurança das organizações e no comportamento das pessoas. De acordo com Mitnick e Simon (2003):

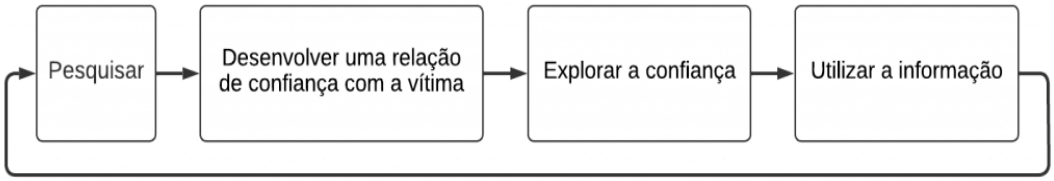
> *Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis (MITNICK; SIMON, 2003, p. 3).*

Complementando esta linha de raciocínio a respeito da vulnerabilidade, ao decorrer de seu trabalho, os autores LéVESQUE et al. (2018) afirmam que mesmo quando se lida com usuários que têm conhecimento acerca da segurança da informação no ambiente digital, eles podem estar vulneráveis. Também comentam que mesmo os melhores sistemas de segurança podem ser comprometidos por ações descuidadas dos usuários.

Schultz (2005) comenta que em uma pesquisa realizada com determinada amostra, um total de 80% das pessoas que foram analisadas tinham conhecimento da existência de vírus, e devido à experiência sabiam que devem evitar abrir anexos desconhecidos; entretanto, os 20% restantes não sabiam que deveriam ignorar anexos desconfiáveis, potencialmente maliciosos. Ou seja, ao menos duas em cada 10 pessoas ainda estão suscetíveis a ataques simples como esse, que podem oferecer grande perigo.

Os especialistas Parsons et al. (2017) relatam que estas situações de descuido dos usuários e vulnerabilidade dos indivíduos não são casos atípicos. Na realidade, eles chegaram a um consenso em termos de qual seria o elo mais fraco na defesa dos sistemas de segurança informacional em qualquer organização, as próprias pessoas. Um dos principais perigos para a segurança da informação explora e abusa exatamente deste elo frágil na corrente da cibersegurança, “A engenharia social, propriamente dita, está inserida como um dos desafios (se não o maior deles) mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação.” (PEIXOTO, 2006, p. 36). A engenharia social ataca a vulnerabilidade humana, manipula seu psicológico e usa as pessoas para se infiltrar em qualquer fonte de informação. Há várias etapas do processo utilizado pela engenharia social para enganar, convencer e se aproveitar destas brechas, há uma versatilidade quase infinita para as técnicas e métodos que podem ser empregados neste processo. Na Figura 2 podemos conferir uma ordenação genérica desta atividade:

Figura 2: O Ciclo da Engenharia Social



Fonte: Universidade Federal de Santa Maria (UFSM), 2023

Como a engenharia social trabalha especialmente com a manipulação e persuasão de pessoas, tanto para roubar dados confidenciais pessoais ou de empresas e instituições, Rahman et al. (2021) afirmam que as técnicas e metodologias empregadas para realizar várias atividades ilegais observadas podem ser esclarecidas por meio de teorias das áreas das ciências sociais, cognitivas e psicológicas.

2.3 A psique humana, abusos e direitos

A respeito de que tipos de teorias podem ser levadas em consideração nessa questão, segundo os autores Gratian et al. (2018), traços de personalidade podem gerar sérios riscos na área da segurança da informação. Quando esta depende de pessoas, a maneira como tomam decisões, preferências de riscos e fatores demográficos também são considerados importantes quando se lida com ameaças. São mencionadas cinco principais categorias da personalidade,

conceito proveniente da psicologia, conhecido como "*Big Five*" (CATÓLICA DE PELOTAS, 2022), definidos a seguir:

- Abertura à experiência: determina o interesse por novas vivências, são pessoas aventureiras, curiosas e imaginativas, com ideias incomuns;
- Conscienciosidade: define o grau de autocontrole sobre emoções e impulsos, são pessoas com comportamento mais planejado, possuem forte autodisciplina e foco nos objetivos;
- Extroversão: indica a tendência de se envolver com outras pessoas e o mundo exterior, são pessoas sociáveis, animadas e dispostas a criar novas relações;
- Agradabilidade: aponta o nível de simpatia e cooperação com os outros, costumam ter boas relações e serem respeitosos, amigáveis e prestativos; e
- Neuroticismo: este fator mede a tendência de sentir emoções negativas como raiva, ansiedade e depressão constantemente. Pessoas neuróticas são pessoas reativas e instáveis emocionalmente.

Nobles (2022) expande a conceituação acerca da teoria do *"Big Five"*, oferecendo uma categorização sobre as diferentes manifestações do estado de fadiga, seguem:

- Fadiga de Autenticação: estado de exaustão proveniente da recomendação de que se deve gerar senhas complexas, renova-las periodicamente e tomar múltiplas medidas de verificação no acesso;
- Fadiga de Decisão: estado de cansaço devido a um desgaste extensivo da capacidade cognitiva ao efetuar várias tarefas repetitivas sequencialmente;
- Fadiga de Alerta: estado de exaustão devido à análise de demasiadas ocorrências para verificar sua importância em relação à segurança;
- Fadiga de Treinamento: estado de exaustão que ocorre quando a educação dos usuários é excessiva e ineficiente; e
- Fadiga Regulatória: estado de exaustão que acontece quando as leis e normas estabelecidas pela organização são excessivas e sobrecarregam as capacidades cognitivas das pessoas.

Esses conceitos e teorias devem possuir extensa literatura na área da psicologia, porém estudo deste tipo talvez não sejam tão abundantes nas áreas da Ciência da Informação e da segurança. No caso de suscetibilidade ao *phishing*, técnica da engenharia social que envolve

persuadir o usuário a entregar suas informações pessoais por intermédio de *e-mails*, mensagens de texto e contato pelas redes sociais; foi determinado que pessoas com um traço forte de neuroticismo possuem mais brechas e tem configurações de privacidade vulneráveis, se tornando alvos fáceis, segundo os autores (HALEVI; LEWIS; MEMON, 2013).

No período contemporâneo, apesar da gravidade de todas estas formas de decaimentos, o cansaço cognitivo e os transtornos psicológicos não são as únicas fontes de influência de comportamento nos usuários da informação, existem outras, talvez até ainda mais preocupantes. Durante o documentário *O Dilema das Redes* (2020), da *Netflix*, vários especialistas em tecnologia do Vale do Silício (famosa região na Califórnia, Estados Unidos da América, conhecida por abrigar grandes empresas de tecnologia) falam a respeito do perigoso impacto das redes sociais na democracia e na humanidade em geral. O longa-metragem retrata cenas do cotidiano na era digital, e levanta discussões que demonstram como as pessoas são condicionadas por intermédio de algoritmos a desenvolverem vícios na tecnologia e nas redes, a fim de gerar lucro para grandes empresas.

O roubo de dados e informação dos usuários representado é assustadoramente grande, permitindo ainda o monitoramento, rastreamento e medição das atividades, preferências pessoais e traços de personalidade. O nível de especificidade e profundidade com a qual essas metodologias são capazes de induzir o comportamento e a forma de pensar dos indivíduos é mais relevante para o mundo real do que se imagina. Através de *fake news* e outras técnicas de influência, os algoritmos e os detentores dessas informações são verdadeiramente capazes de manipular as ações das pessoas no mundo real.

Seguindo uma linha semelhante, o documentário *Privacidade Hackeada* (2019) também está disponível na *Netflix*. Este segundo tem foco na condição do usuário como o produto, como seus dados, suas atividades *online* e suas formas de pensar são utilizadas meramente como moeda de troca entre companhias e governos de diversos países. Neste caso, acompanha-se principalmente o caso do vazamento massivo de dados da rede social *Facebook*, que aparentemente foram coletados e vendidos para a empresa britânica *Cambridge Analytica*. A qual foi acusada de atuar como uma "máquina de propaganda" imoral durante as campanhas eleitorais americanas de 2016.

A *Cambridge Analytica* buscava influenciar a decisão de voto de eleitores considerados "persuasíveis", ou seja, eleitores que ainda não estavam totalmente decididos sobre sua opção de voto. Então, a companhia usava psicografia, ou "táticas de comunicação", para bombardear estes perfis de usuários com *vlogs*, notícias geradas automaticamente e vídeos com fluxo de

conteúdo personalizado, a fim de moldar sua visão de forma favorável ao candidato preferido. Essa mesma estratégia também foi utilizada durante a campanha de separação entre o Reino Unido e a União Europeia, sendo que o próprio governo britânico categoriza este tipo de estratégia como tática militar. Um dos principais facilitadores para esta espécie de empreitada seria que as pessoas não reconhecem o valor que seus dados têm, não se importando muito em facilmente prover suas informações. O documentário conclui assinalando o fato de que hoje praticamente não existem muitas leis no mundo que estabelecem direitos concretos sobre nossos dados, e que direto sobre seus próprios dados devem ser considerados direitos humanos.

Uma das principais ferramentas hoje para essa coleta de dados em larga escala são os *cookies*, segundo Barros (2021), ao notarmos uma propaganda nas redes sociais a respeito de um produto que temos interesse, não se trata de uma mera coincidência. Com a atividade no ambiente digital tendo um tráfego cada vez maior, a coleta de dados aumenta ao mesmo tempo, especialmente na indústria do *marketing*. É fácil perceber que quando você mostra interesse na *Internet* por certos produtos, através de cliques em matérias, assistindo vídeos, dentre outras formas, rapidamente começará a ver diversas propagandas a respeito dos assuntos e itens de interesse. Esta coleta de dados é realizada em grande escala mediante o uso de *cookies*, com cada vez que navegamos nas redes, diversos arquivos são baixados com o intuito de coletar dados sobre o que fazemos *online* e então essas informações são enviadas aos donos das páginas. Informações como o tempo que passamos em determinados *sites*, suas áreas de interesse, os tipos de páginas que você costuma acessar, entre outras informações. Desta forma, fornecemos vários detalhes de nossa atividade nas redes e até dados pessoais em troca de informações, nos tornando um produto para a indústria do *marketing*.

Entretanto, apesar destas estratégias de coleta de dados, é claro que existe um certo nível de legislação hoje a respeito do processamento de dados e informações, apesar de insuficientes, são um bom começo. Por exemplo, a LGPD, conforme o portal oficial do Governo Federal brasileiro, é a legislação brasileira vigente que regula as atividades de tratamento de dados pessoais, feito por pessoa física ou jurídica de direito público ou privado. Este tratamento diz respeito a qualquer atividade que faz uso de dados pessoais na execução de sua operação, a lei determina também que o órgão que coleta deve informar de forma transparente qual dado será compartilhado e com quem; enquanto que o órgão que solicita o compartilhamento deve justificar o acesso, descrevendo o motivo da solicitação de acesso e o uso que será feito com os dados. Porém em pesquisa, ASER (c2022) afirma que apenas 38% das empresas brasileiras demonstraram, em março de 2020, estar alinhadas com as exigências feitas pela lei oficial. Já

na perspectiva europeia, existe também uma legislação mais abrangente o *GDPR*, é um regulamento europeu sobre privacidade e proteção de dados pessoais, aplica-se a todos na UE e Espaço Econômico Europeu, criado em 2018, regula também a exportação de dados pessoais para fora. O *GDPR* é aplicável também para cidadãos europeus que vivem mesmo fora do território europeu, por isso seu alcance mais extenso. Segundo Bertolli (2019), no primeiro ano efetivo da *GDPR* houve 144 mil reclamações e 89 mil violações de dados registradas.

2.4 Ações contra incidentes de segurança da informação

Dias (2021) aponta alguns hábitos arriscados do usuário ou funcionário comum que permitem brechas a prática de *phishing* e comprometem a segurança da informação. Seguem alguns exemplos:

- A mistura entre atividades de *e-mails* pessoais e profissionais;
- O acesso a páginas *online* não autênticas;
- Abrir *e-mails* com anexos e *links* de fontes desconhecidas ou suspeitas; e
- Compartilhar senhas e informações pessoais.

O autor ainda indica alguns hábitos saudáveis para se manter seguro:

- Criar senhas únicas para cada aplicação, assim como fazer uso de composições de caracteres complexas;
- Fazer uso de autenticação de múltiplos fatores;
- Efetuar a atualização do sistema sempre que disponível; e
- Instalar aplicativos de antivírus e sistemas de segurança legítimos e próprios para cada dispositivo.

O professor Hadlington (2017), da *Nottingham Trent University*, relaciona estas duas últimas temáticas discutidas: tanto a questão psicológica do usuário quanto os riscos provenientes da prática do *phishing*. Ele afirma que a tendência em não identificar *e-mails* de *phishing* é comum entre indivíduos com Transtorno do Déficit de Atenção com Hiperatividade (TDAH), visto que o grau de atenção reduzido entre aqueles que possuem tal transtorno pode induzi-los a tomar decisões erradas e ocasionar um maior número de cibercrimes efetivos.

Cada usuário da informação possui um perfil diferente, nos mais diversos aspectos, logo percebe-se que a interação de cada um e as formas como podem tomar decisões em relação a segurança e integridade dos dados e/ou material armazenado pode sempre ser diferente e

imprevisível. Reconhecendo esta realidade, Lahcen et al. (2020) comentam sobre a importância de realizar uma avaliação a respeito das características dos usuários, através de um questionário, seria possível determinar tanto seus traços pessoais, quanto aqueles relacionados ao seu ambiente e sensitivos ao seu contexto e vivência atuais. Mediante este método é possível ainda identificar relações imprevisíveis entre as características individuais, que podem tanto causar problemas quanto resolvê-los, variáveis físicas somadas a atitudes humanas, assim como aspectos psicológicos interagem com elementos físicos. Para exemplificar esse argumento, o autor cita o estado de fadiga ou exaustão laboral e a distração como fatores determinantes para erros acidentais, e como as consequentes perdas de percepção e controle atreladas podem induzir a erros ainda mais graves.

Todas essas questões em torno da segurança informacional se mostram deveras problemáticas para a sociedade, entretanto, as pessoas devem exercer seu controle sobre a tecnologia, antes que elas fiquem à sua mercê, pois isso já está acontecendo. Com a existência hoje de uma diversidade imensa de formas e meios de tecnologia, provavelmente será necessário um número substancial de pessoas especializadas na segurança da informação preparados para tratar do componente humano nesta questão.

Mesmo assim, existem múltiplas formas do usuário proteger seus dados e a si mesmo, tanto de cibercriminosos comuns quanto de companhias e governos que almejam manipular seu comportamento por meio de seus dados. Por exemplo, Modic e Anderson (2014) determinaram um erro comum entre usuários, frequentemente avisos de *software* de segurança aparecem na tela, advertindo sobre riscos de segurança, apenas para serem ignorados pelos usuários, alguns até optam por desligar as notificações completamente. Os autores ressaltam que situações como essa são bastante comuns, dito isso, também comentam que essas mesmas notificações deveriam ser mais simples, em ordem de facilitar a sua compreensão.

A fim de aprofundar ideias sobre que tipo de postura é recomendável para evitar estar vulnerável *online* e praticar bons hábitos de segurança, Sikder et al. (2020) oferecem alguns conselhos:

- Os usuários precisam compreender os recursos, permissões e classificações de aplicativos antes de instalá-los;
- Manter desativadas as funções como *NFC*, *Bluetooth*, *Wi-Fi*, *GPS* e outros quando não estão sendo usadas, para economizar bateria e evitar deixar portas abertas para cibercrimes;

- Checar se aplicativos estão atualizados e otimizados, assim como manter aplicativos de manutenção padrão em funcionamento;
- Permitir em seus celulares apenas os aplicativos realmente relevantes para o cotidiano; e
- Desinstalar aqueles que forem desnecessários, a fim de evitar coleta de dados particulares e uso de bateria.

Em complemento às recomendações anteriores, Weichbroth e Lysik (2020) referem mais algumas dicas e revigoram outros pontos:

- Bloquear seus dispositivos por meio de alguma autenticação;
- Fazer *backup* de dados importantes com certa frequência;
- Dispor de criptografia de dados;
- Evitar realização de conexão a *Wi-Fi* de rede pública sem utilizar alguma opção de transmissão com segurança, como um canal virtual privado de *VPN*;
- Se atentar aos métodos de cibercrime da engenharia social;
- Conceder apenas as permissões necessárias aos aplicativos;
- Não remover restrições dos aplicativos; e
- Garantir que seu telefone tenha algum *software* de segurança, que funcione corretamente.

Seria interessante que as pessoas adotassem essas práticas e recomendações no seu cotidiano e em maior escala, pois, certamente, isso ajudaria a reduzir a quantidade de incidentes e indivíduos prejudicados. Entretanto, nem sempre isto é o suficiente, principalmente quando falamos de organizações e instituições, dentro das quais é preciso ter processos, tecnologias e pessoas em sincronia para garantir a segurança dos dados, com uma base sustentada pelos pilares da segurança da informação, conforme comentam Mitnick e Simon (2003).

Razaque et al. (2021) comentam que cibercriminosos se interessam por invadir qualquer tipo de instituição, seja para se apossarem de contas bancárias, ou mesmo furtar documentos importantes com informações pessoais ou institucionais, havendo precedente de ataques a bibliotecas públicas, escolares e em ministérios. Esses fatos ressaltam a relevância de considerar esta temática com um pouco mais de atenção na óptica da CI. Imagina-se que haja uma quantidade substancial de estudos dirigidos aos elementos de viés tanto técnico quanto tecnológico na segurança da informação, porém seria interessante observar se existem estudos

o bastante que examinam a questão com olhar direcionado ao comportamento do usuário, esse poderia ser o foco da CI nesta temática.

Pensando nessa preocupação não somente em relação aos usuários mais comuns do dia-a-dia, mas também em qualquer um conectado ao ambiente da sociedade acadêmica, ou mesmo funcionários de qualquer instituição. Borkovich e Skovira (2019) apresentam algumas possíveis práticas que podem expressar a importância do assunto para as pessoas, assim como educá-los a respeito de bons hábitos, seguem alguns:

- Determinar metas de segurança informacional ao Código de Conduta e Ética do Funcionário;
- Elaborar e estabelecer treinamentos para conscientização;
- Elaborar políticas que classifiquem informações e dados;
- Elaborar treinamento para os funcionários saberem identificar e evitar abertura a engenharia social, com simulação de tentativas;
- Encorajar funcionários a terem bons hábitos de segurança por auxílio de premiações;
- Efetuar a divulgação de práticas de segurança com uso de pôsteres, anúncios digitais, vídeos e boletins;
- Fazer convites a especialistas na área que tenham interesse de apresentarem palestras a respeito de segurança da informação e comportamento do usuário; e
- Construir uma cultura de segurança de forma geral, que favoreça uma conscientização de profissionais e usuários.

Práticas organizacionais a fim de defender a segurança da informação como as citadas acima são bem comuns há décadas; uma vez que, desde os anos 1960, a Administração Nacional da Aeronáutica e Espaço (*NASA*) distribuía pôsteres com alertas sobre atitudes simples que põem em risco essa mesma segurança. Outra recomendação seria manter uma comunicação ampla, clara e saudável entre a equipe de trabalho, visto que a falta dessa poderia ocasionar diversas ações e decisões descuidadas.

Construir essa cultura de segurança pode ser bem impactante, quando falamos de segurança da informação, o assunto deve ser tratado com seriedade, mas ainda sim várias organizações não tratam o assunto com a devida atenção. Gonçalves (2019) discorre sobre como várias organizações menosprezam essa problemática, e como se assemelha à desvalorização de questões de saúde humana, não se tomam providências até que incidentes de fato ocorram. Essa tendência de investir na segurança cibernética apenas quando danos reais acontecem, pode vir

de uma ideia de que não seja viável financeiramente aplicar na segurança e conscientização, porém as perdas de dados, documentos e informações podem ser muito superiores aos gastos em defesa.

Ao mesmo tempo, é claro que treinar e educar adequadamente usuários e funcionários não é uma tarefa simples, é um processo lento e rigoroso, não basta apenas realizar uma ou outra palestra e estabelecer algumas normas para verdadeiramente construir uma cultura de segurança. Gonçalves (2019) ainda comenta que, para proteger efetivamente uma organização, é necessário conhecer, compreender, aceitar e ser competente em termos tecnológicos e de seguridade.

De frente a esta realidade, é preciso que atitudes sejam tomadas o quanto antes, pois esses riscos serão cada vez mais relevantes. Creese et al. (2020) divulgaram um alerta, dizendo que “A menos que medidas sejam tomadas agora, até 2025, a tecnologia da próxima geração, na qual o mundo confiará cada vez mais, terá o potencial de sobrecarregar as defesas da comunidade de segurança global”. Como foi sugerido anteriormente, mais estudos e artigos publicados focados no comportamento humano nessa temática são sempre bem-vindos, talvez seria uma forma interessante de encorajar estas mudanças.

3 METODOLOGIA

Nesta seção serão descritos os elementos essenciais para o entendimento da metodologia escolhida, com o intuito de atingir os objetivos pré-definidos.

De acordo com Moresi, a metodologia de pesquisa é

> *o estudo que se refere a elaboração de instrumentos de captação ou de manipulação da realidade. Está, portanto, associada a caminhos, formas, maneiras, procedimentos para atingir determinado fim. Construir um instrumento para avaliar o grau de descentralização decisória de uma organização é exemplo de pesquisa metodológica. (MORESI, 2003, p. 9)*

3.1 Classificação da pesquisa

A presente pesquisa é descritiva, com delineamento de levantamento, buscando descrever uma determinada população, além de ter um aspecto quantitativo, procurando descrever de modo geral uma situação específica. Uma pesquisa quantitativa "se caracteriza pelo emprego de instrumentos estatísticos, tanto na coleta como no tratamento dos dados, e que tem como finalidade medir relações entre as variáveis." (ZANELLA, 2011, p. 35).

3.2 Procedimentos metodológicos da pesquisa

Realizou-se uma pesquisa bibliográfica, que originou a seção 2 deste trabalho, a fim de explorar o conhecimento existente do assunto segurança da informação, vulnerabilidades e ameaças de segurança, e estabelecer um referencial teórico que embasou a construção do instrumento de coleta de dados.

O objetivo da pesquisa bibliográfica é situar o pesquisador no contexto teórico existente sobre o tema, identificar lacunas de conhecimento, analisar abordagens e resultados anteriores e embasar teoricamente a pesquisa em questão. Dessa forma, a pesquisa bibliográfica contribui para a fundamentação teórica do estudo (GIL, 2008; MARCONI E LAKATOS, 2003).

Durante o processo de pesquisa bibliográfica, é importante estabelecer critérios de seleção das fontes, como a relevância do autor, a atualidade das publicações, a qualidade das revistas científicas e a pertinência dos conteúdos abordados. A utilização de bases de dados especializadas e sistemas de indexação acadêmica pode facilitar a busca por artigos e publicações relevantes (GIL, 2008; MARCONI E LAKATOS, 2003). Sendo assim, nesta pesquisa, as fontes de informação usadas foram as seguintes: Decanato de Planejamento, Orçamento e Avaliação Institucional; Google Acadêmico; Repositório Comum; *Science Direct;*

ACM Digital Library; SpringerOpen; Hindawi; Academia.edu; *Research Gate*; ATF Cursos Jurídicos; o *site* Arquivos.unb.br e o canal de *streaming Netflix*; assim como diversos *blogs* e *sites* de notícias. A escolha pelo uso de *blogs* e outros *sites* neste estilo foi feita por causa da facilidade da linguagem empregada para compreensão dos leitores, assim como a atualidade dos materiais disponíveis, visto que essa é uma área em constante desenvolvimento. Nestas fontes, os tipos de documentos utilizados foram: artigos científicos, artigos de *blogs*, notícias, anuários, teses de doutorado e documentários.

Nesta pesquisa, foi adotado o questionário como instrumento de coleta de dados. O questionário é uma técnica amplamente utilizada na pesquisa científica, permitindo obter informações de forma padronizada e objetiva dos participantes.

Para Silva e Menezes (2005), o questionário é

> *uma série ordenada de perguntas que devem ser respondidas [...] pelo informante. O questionário deve ser objetivo, limitado em extensão e estar acompanhado de instruções. As instruções devem esclarecer o propósito de sua aplicação, ressaltar a importância da colaboração do informante e facilitar o preenchimento. (SILVA E MENEZES, 2005, p. 33)*

O questionário é um instrumento amplamente utilizado na pesquisa científica para coletar dados de forma padronizada e sistemática. Consiste em uma série de perguntas estruturadas e padronizadas que são administradas aos participantes de um estudo, com o objetivo de obter informações específicas e relevantes para a pesquisa em questão (MARCONI E LAKATOS, 2003).

Através de uma série de perguntas estruturadas, aplicadas aos participantes do estudo, busca-se obter informações específicas e relevantes para o propósito da pesquisa.

3.2.1 Instrumento de coleta de dados

Os questionários são uma ferramenta flexível de coleta de dados que podem ser projetados de diferentes formas, adaptando-se aos objetivos específicos de cada pesquisa. Eles oferecem uma ampla gama de opções de resposta, como perguntas de múltipla escolha com resposta única ou múltipla, perguntas abertas e escalas *Likert* (MARCONI E LAKATOS, 2003).

O questionário foi elaborado pelo pesquisador responsável e está apresentado na íntegra no Apêndice 1. O questionário contou com um total de 35 questões. Dessas, 9 questões visavam obter informações para a caracterização demográfica dos participantes, 6 questões buscaram coletar dados sobre o conhecimento dos alunos sobre segurança da informação, enquanto as

demais 20 perguntas foram direcionadas para entender a experiência pessoal e os hábitos dos estudantes em relação à cibersegurança.

O questionário elaborado possui questões de múltipla escolha e perguntas que seguem o modelo de escala *Likert*. As perguntas de múltipla escolha com resposta única são úteis para obter respostas precisas e padronizadas, permitindo uma análise quantitativa dos dados. Por outro lado, as perguntas de múltipla escolha com respostas múltiplas fornecem aos participantes a oportunidade de selecionar mais de uma opção, permitindo uma visão mais abrangente das suas opiniões e comportamentos. As questões de escala *Likert* são um tipo de pergunta que solicita aos participantes que indiquem seu nível de concordância ou discordância com determinadas afirmações. Ela oferece uma abordagem quantitativa para medir atitudes, opiniões e crenças dos participantes, permitindo uma análise estatística dos dados.

A coleta de dados da amostra foi realizada por intermédio desses questionários respondidos no período de 5 a 16 de junho de 2023. Durante o período em que o questionário esteve disponível para acesso no *Google Forms*, foram registradas 40 respostas.

3.3 População e Amostra

Em termos da população selecionada, essa pode ser entendida como “um conjunto de elementos (empresas, produtos, pessoas, por exemplo) que possuem as características que serão objeto de estudo” (VERGARA, 2004, p. 50).

Neste contexto, a população selecionada para esta pesquisa consiste nos estudantes da Universidade de Brasília (UnB), mais especificamente, os 336 alunos ativos que estão atualmente cursando a graduação em Biblioteconomia. O número total de alunos foi obtido por meio de questionamento à coordenação do curso, que consultou o Sistema de Gestão Acadêmica SIGAA em 20/07/2023, verificado às 15h30.

A presente pesquisa adotou uma amostra composta por 40 alunos que prontamente responderam ao questionário.

A amostra foi selecionada de forma aleatória, e o questionário foi divulgado entre os membros da população pelo auxílio de canais de comunicação, como *e-mail* e redes sociais. Essa estratégia de divulgação buscou alcançar uma maior abrangência e garantir que os alunos tivessem a oportunidade de participar voluntariamente da pesquisa, contribuindo para uma representação diversificada dos participantes na amostra. O uso de uma amostragem aleatória e a divulgação aberta do questionário são práticas fundamentais para minimizar possíveis vieses e assegurar a validade dos resultados obtidos na pesquisa.

A divulgação do questionário entre os membros da população teve um limite de tempo preestabelecido para que os participantes tivessem a oportunidade de responder dentro de um prazo específico. O período que o questionário ficou disponível para coletar repostas foi entre 5 de junho a 16 de junho de 2023. Esse limite de tempo é uma prática comum em pesquisas para garantir que a coleta de dados seja realizada de maneira eficiente e que os resultados possam ser analisados em tempo hábil.

Para avaliar a representatividade de uma amostra em relação à população, é necessário considerar a técnica de amostragem utilizada, o tamanho da amostra e a heterogeneidade da população. Uma amostra de 40 alunos para uma população de 336 pode ser considerada representativa se a amostra for selecionada de forma aleatória e se os 40 alunos escolhidos representarem de forma adequada a diversidade e características da população maior.

Quanto maior for o tamanho da amostra em relação ao tamanho da população, maior será a probabilidade de que as características da população estejam refletidas na amostra.

No caso específico de uma amostra de 40 alunos para uma população de 336, a representatividade dependerá de quão bem os 40 alunos selecionados representam a diversidade da população maior de estudantes de Biblioteconomia na Universidade de Brasília. Se a amostra foi selecionada de forma aleatória e abrange uma variedade adequada de características presentes na população, então a amostra pode ser considerada razoavelmente representativa. No entanto, é importante reconhecer que, quanto maior o tamanho da amostra em relação à população, maior será a confiabilidade dos resultados obtidos a partir dela. Portanto, ao analisar os resultados da pesquisa, é fundamental considerar a margem de erro e a validade das conclusões em função do tamanho da amostra e das técnicas de amostragem utilizadas.

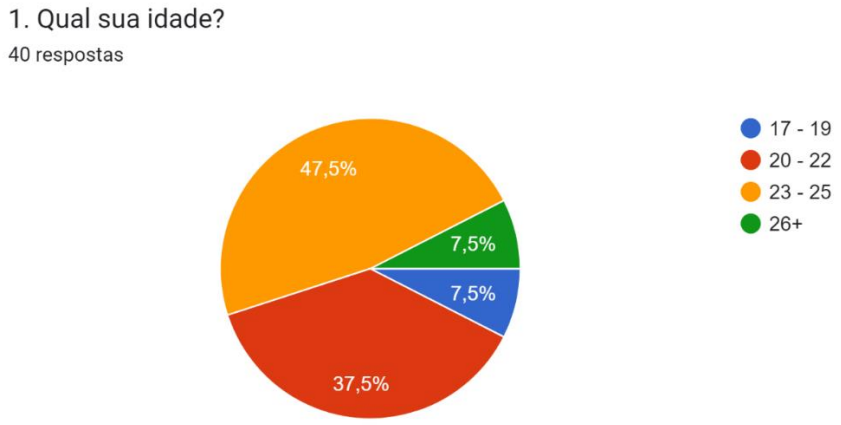
4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Finalizada a coleta de respostas, a análise se iniciará pela primeira seção do questionário, relativa às características sociodemográficas da amostra. Em seguida, serão analisadas as questões a respeito dos conhecimentos gerais dos participantes em termos de segurança da informação. Posteriormente, serão avaliadas as perguntas relativas às experiencias e hábitos dos alunos em relação a comportamentos que garantem ou arriscam a cibersegurança. Por fim, uma breve síntese dos resultados apresentará e discutirá alguns dos principais pontos da seção atual.

4.1 Caracterização da amostra

A amostra selecionada para este estudo consiste em alunos atualmente matriculados no curso de graduação em Biblioteconomia na Universidade de Brasília. A faixa etária da maioria dos participantes situa-se entre 20 e 25 anos. A amostra apresenta uma predominância do gênero feminino, embora também inclua alguns participantes identificados como masculinos ou não-binários. Quanto à experiência acadêmica, a maioria dos participantes são veteranos, com uma proporção menor de calouros.

Figura 3: Faixa etária



Fonte: Do autor, 2023.

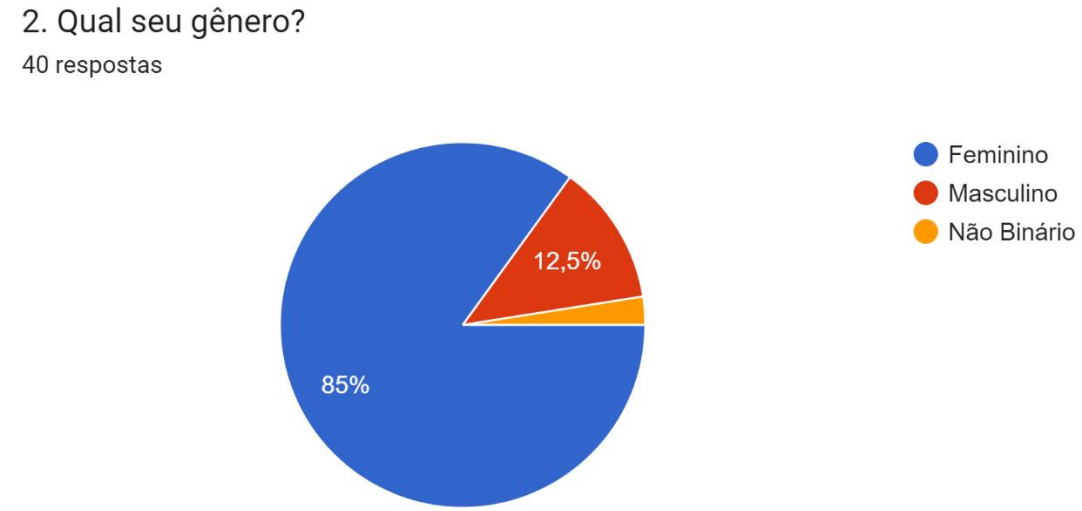
A Figura 3 ilustra os resultados obtidos na pergunta 1 do questionário. Observou-se que 19 participantes se encontram na faixa etária entre 23 a 25 anos, enquanto outros 15 participantes estão na faixa de 20 a 22 anos. Os demais participantes foram igualmente distribuídos, com 3 respondendo pertencer à faixa etária de 17 a 19 anos e outros 3 na faixa de

26 anos ou mais. A partir desses dados, foi possível calcular as proporções aproximadas em números decimais. A faixa etária de 23 a 25 anos representa aproximadamente 74,3% dos participantes, a faixa de 20 a 22 anos corresponde a cerca de 25,3% dos participantes, e as faixas de 17 a 19 anos e 26 anos ou mais representam cada uma aproximadamente 7,5% dos participantes.

A maioria significativa da amostra encontra-se na faixa etária compreendida entre os 20 e 25 anos, um período de tempo comumente associado a estudantes universitários que concluíram o ensino médio e prosseguem com seus estudos até a conclusão da graduação. Em contraste, uma parcela menor da amostra refere-se aos indivíduos que ingressaram no curso antes dos 20 anos, bem como àqueles que, com mais de 26 anos, ainda buscam obter sua formação acadêmica ou que iniciaram a graduação em Biblioteconomia em uma fase posterior de suas vidas.

Conforme ilustrado na Figura 4, que representa os resultados da pergunta 2 do questionário, a respeito da identificação de gênero, nota-se que 34 participantes, ou seja 85%, se identificaram como do gênero feminino. Enquanto apenas 5 se identificaram como pertencentes ao gênero masculino, compondo 12,5% do total, e finalmente os restantes 2,5% foram ocupados por um único participante, que se identificou como não binário.

Figura 4: Informação sobre gênero



Fonte: Do autor, 2023.

Em números gerais, significa afirmar que a presença feminina na Biblioteconomia é maior que a masculina nesta amostra. Entretanto, como a amostra é proporcionalmente pequena

em relação à população, não é possível afirmar que as pessoas de gênero feminino são a maioria no curso de Biblioteconomia oferecido pela Universidade de Brasília.

Ao analisar a pergunta 3 do questionário (Figura 5), que solicitava aos participantes que indicassem o semestre atual em que estavam cursando Biblioteconomia, observou-se o seguinte padrão na distribuição dos dados:

- Um total de 17 alunos e alunas, o que corresponde a aproximadamente 42,5% da amostra, são classificados como veteranos, estando no 9º semestre ou além. Essa categoria representa quase metade dos participantes.
- Apenas 8 alunos (20%) são considerados calouros, ou seja, estão cursando entre o 1º e o 2º semestre.
- Um total de 4 alunos (10%) estão no 3º e 4º semestres.
- Há 7 alunos (17,5%) que atualmente estão cursando entre o 5º e o 6º semestres.
- Por fim, apenas 4 alunos (10%) se encontram entre o 7º e o 8º semestre.

Esses resultados evidenciam que a maioria dos alunos que participaram da pesquisa já possui uma experiência de pelo menos dois anos cursando Biblioteconomia na graduação. Portanto espera-se que demonstrem uma melhor percepção sobre a importância do tratamento adequado de dados e informações.

Figura 5: Semestre de ingresso

Fonte: Do autor, 2023.

Ao avaliar os dados adquiridos na pergunta 4 (Figura 6), que indaga os participantes a respeito do ano em que ingressaram no curso de Biblioteconomia, é possível perceber que as

informações apresentadas neste gráfico são condizentes com os dados da questão anterior. As respostas para esta questão apresentaram uma distribuição bastante variada. No entanto, foi possível identificar que a maioria dos participantes ingressou no curso de Biblioteconomia entre os anos de 2017 e 2020. A seguir, apresentam-se os números percentuais correspondentes a cada ano de ingresso:

- 3 alunos (7,5%) ingressaram em 2017.
- 8 alunos (20%) ingressaram em 2018.
- Outros 8 alunos (20%) ingressaram em 2019.
- 6 alunos (15%) ingressaram em 2020.

Os valores acima correspondem aos alunos mais antigos na amostra. Por outro lado, os alunos mais recentes compõem uma minoria, conforme demonstrado a seguir:

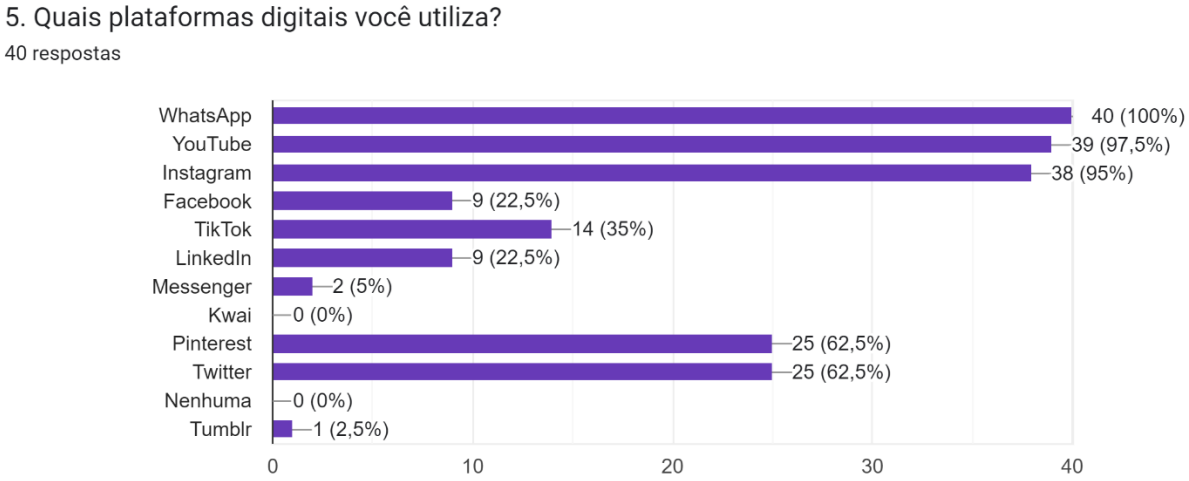
- 6 alunos (15%) ingressaram em 2021.
- 7 alunos (17,5%) ingressaram em 2022.
- Os últimos 2 alunos (5%) ingressaram em 2023.
- Esses números indicam uma menor representação dos alunos mais recentes na amostra.

Figura 6: Data de ingresso

Fonte: Do autor, 2023.

Na pergunta 5 (Figura 7), a pesquisa buscou descobrir quais as plataformas digitais mais populares entre os participantes. Com a oportunidade de selecionar várias opções dentre as plataformas apresentadas ou até mesmo indicar que não utilizam nenhuma delas.

Figura 7: Plataformas digitais populares



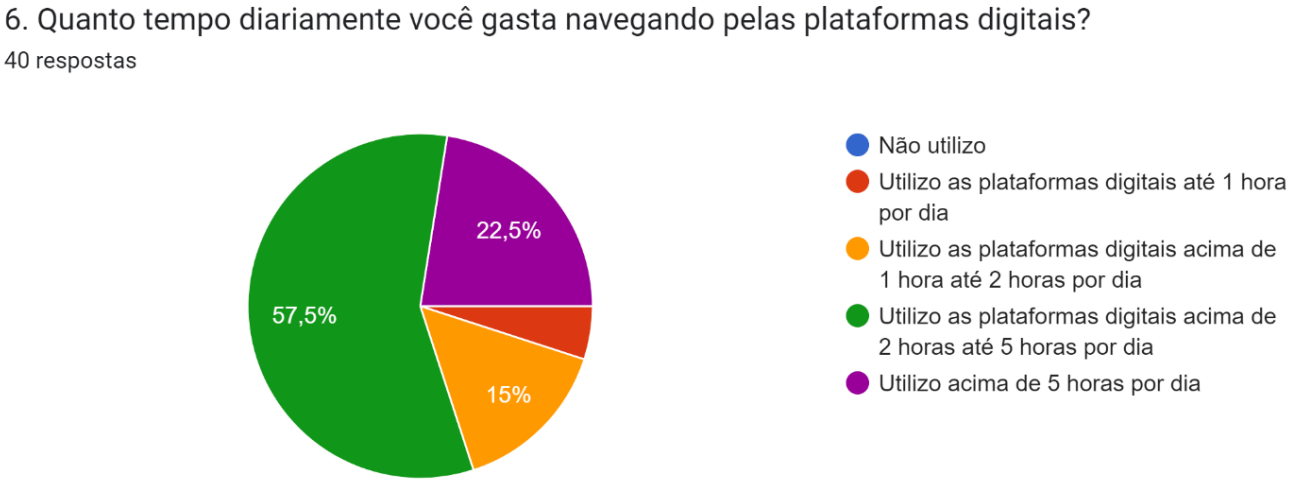
Fonte: Do autor, 2023.

As plataformas mais populares entre os alunos se mostraram o *WhatsApp* em primeiro lugar, com 40 votos, ou seja, 100% dos alunos na amostra utilizam a plataforma. O que pode ser explicado pela popularidade altíssima do aplicativo no Brasil, tornando-o quase uma

necessidade para os estudantes, especialmente considerando a prevalência de grupos na plataforma sobre disciplinas ou grupos de trabalho. Em segundo lugar, ficou o *YouTube*, 39 alunos admitiram utilizar a plataforma, englobando 97,5% da amostra. Em terceiro lugar encontra-se o *Instagram*, também bastante popular, especialmente entre a população mais jovem, 38 alunos utilizam a plataforma, totalizando 95% da amostra. Menos prevalentes, mas ainda populares, seguem as plataformas *Pinterest* e *Twitter*, empatadas com contagem de 25 cada, ambas sendo utilizadas por 62,5% da amostra. Em seguida aparece o *TikTok*, com 14 usuários (35%), o *Facebook* e *LinkedIn* empatados com 9 usuários (22,5%) cada, então o *Messenger* com apenas 2 usuários (5%), finamente o *Tumblr* com apenas 1 usuário (2,5%), e por último fica o *Kwai*, que nenhum participante alega utilizar. Interessante destacar também que nenhum dos participantes declarou não utilizar nenhuma plataforma digital, o que demonstra a forte aderência e presença dos universitários dessa amostra no ambiente digital.

Estando ciente da aderência dos participantes as plataformas digitais e quais são algumas das principais preferidas, podemos avaliar na questão 6 o período de tempo em média que os alunos costumam investir diariamente em suas navegações virtuais (Figura 8).

Figura 8 Tempo diário em plataformas digitais



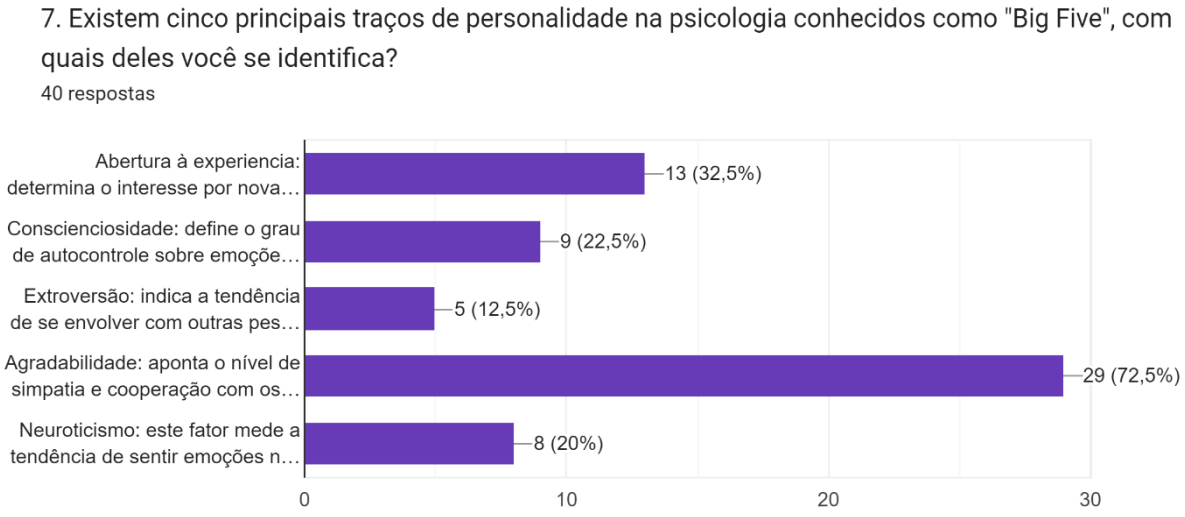
Fonte: Do autor, 2023.

Fica claro que os participantes gastam múltiplas horas diariamente navegando pelas plataformas digitais. Apenas 2 alunos (5%) dizem utilizá-las por no máximo 1 hora por dia; mais 6 alunos (15%) utilizam mais de 1 hora até 2 horas por dia; enquanto um total de 23 alunos

(57,5%) da amostra utilizam acima de 2 horas até 5 horas por dia; e ainda 9 participantes (22,5%) afirmaram utilizar as plataformas digitais por um período acima de 5 horas diárias. Dessa forma, podemos ter uma noção das plataformas preferidas pelos participantes e quanto tempo costumam gastar nestas plataformas. Será interessante manter esta perspectiva em mente durante a análise de futuras questões, levando em consideração o tempo que estão suscetíveis às ameaças identificadas.

Na questão seguinte de número 7 (Figura 9), os participantes foram questionados em relação ao "*Big Five*", os cinco principais traços de personalidade e com quais deles se identificavam mais.

Figura 9: "*Big Five"*



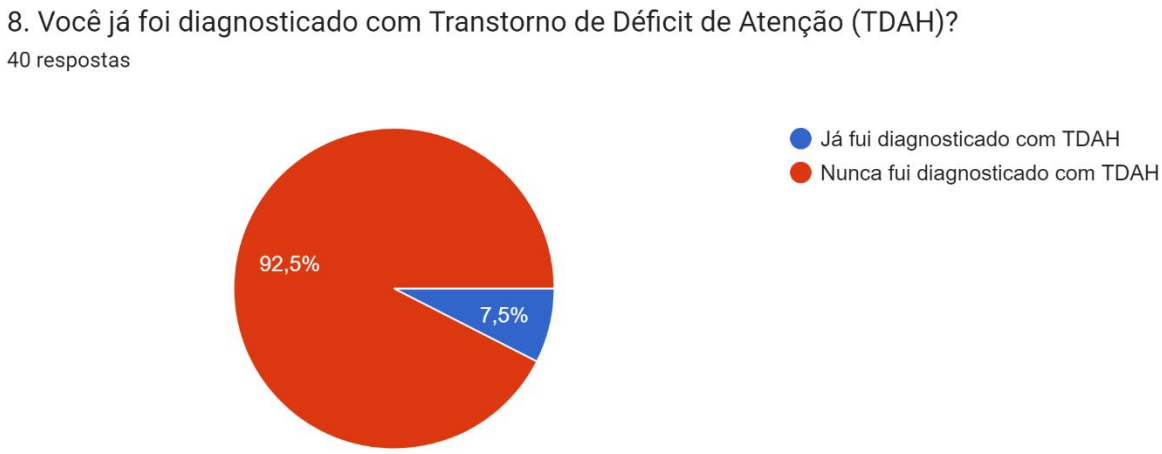
Fonte: Do autor, 2023.

Os cinco fatores são: abertura à experiência, conscienciosidade, extroversão, agradabilidade e neuroticismo. As respostas para esta questão foram variadas, e cada fator representa tendências comportamentais e emocionais a respeito de cada indivíduo, porém o traço mais relevante para evidenciar-se no contexto desta pesquisa é o neuroticismo. Este traço de personalidade mede a tendência de sentir emoções negativas como raiva, ansiedade e depressão constantemente, determina que essas pessoas são reativas e instáveis emocionalmente. Os autores Halevi, Lewis e Memon mencionados na fundamentação teórica, citam que o traço do neuroticismo pode indicar uma maior suscetibilidade a técnicas de engenharia social como o *phishing*, sendo possível observar nos dados da pesquisa que 20% dos participantes se identificam com este traço de personalidade. Logo, pode-se dizer que 1 a

cada cinco 5 alunos da amostra possuem uma tendência de estarem mais vulneráveis a essas ameaças, o que pode ser um fator relevante a se levar em consideração na área.

Ainda na perspectiva de características psicológicas dos participantes, a pergunta 8 questionou os alunos sobre a possibilidade de terem sido diagnosticados com o TDAH em algum momento da vida (Figura 10).

Figura 10: Diagnóstico de TDAH

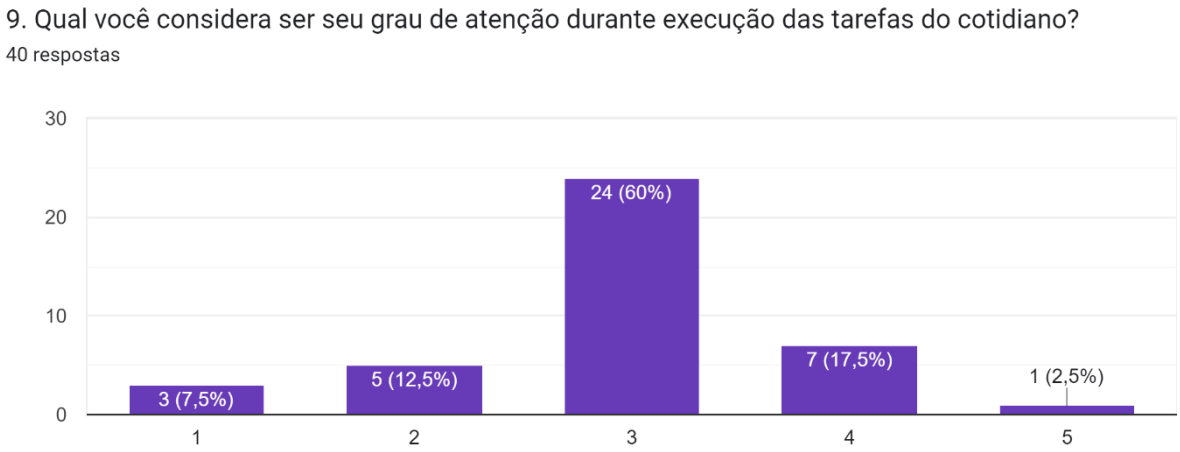


Fonte: Do autor, 2023.

A relevância desta questão para a temática vem da tese do professor Hadlington (2017), que afirma que é bastante comum entre pessoas com TDAH a tendência de não identificar *e-mails* de *phishing*, considerando seu grau de atenção reduzido, que pode induzi-los a tomar decisões descuidadas em relação a segurança da informação. Como pode ser observado pelos dados, uma quantidade pequena de participantes declarou ter recebido um diagnóstico de TDAH, apenas 3 (7,5%), enquanto os outros 37 (92,5%) nunca receberam esse diagnóstico. Mesmo assim, não desmerece a necessidade de ressaltar a importância de bons hábitos de segurança informacional, tanto para a maioria, quanto principalmente para esta minoria.

Seguindo nesta mesma vertente do grau de atenção dos participantes, a pergunta 9 indaga os alunos desta vez a respeitos da sua própria percepção sobre sua concentração ao realizar as tarefas do dia-a-dia (Figura 11).

Figura 11: Grau de atenção



Fonte: Do autor, 2023.

Para melhor compreensão das questões realizadas na escala *Likert*, como a questão 9, é necessário esclarecer que o eixo Y sempre representa o número de participantes que escolheram determinada resposta, enquanto o eixo X sempre representa o nível de concordância dos alunos com a afirmação. Vale esclarecer também que no eixo X, o número 1 representa o menor grau de conhecimento, ou menor grau de concordância, enquanto o número 5 representa o maior grau de conhecimento, ou maior grau de concordância. Enquanto os restantes número seguem de forma crescente entre 1 e 5.

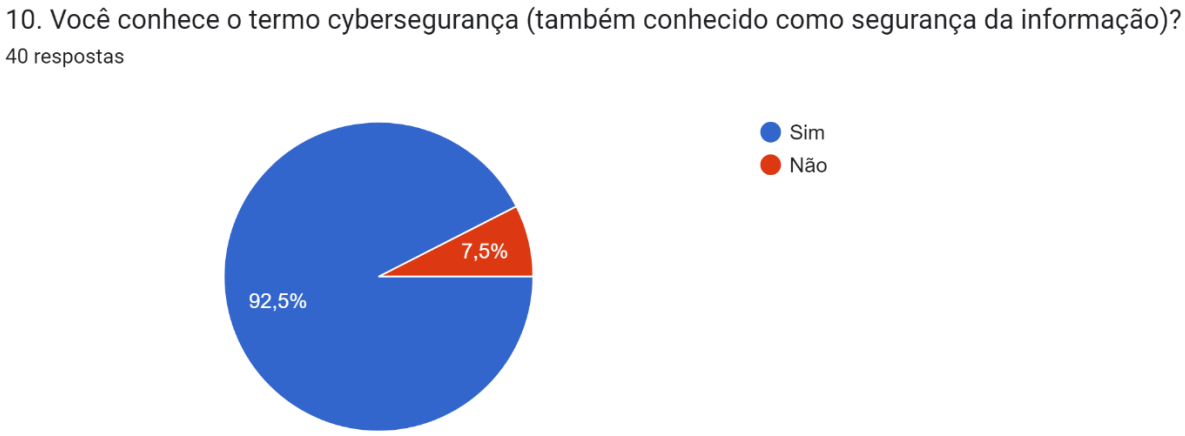
A maioria dos estudantes – 24 (60%), para ser exato – parece considerar o seu grau de atenção razoável, enquanto alguns consideram-no baixo; 3 alunos (7,5%) marcaram o menor nível de atenção, 5 alunos (12,5%) marcaram o segundo menor nível, totalizando 20% da amostra que considera seu grau de atenção baixo. Outrora, 7 alunos (17,5%) afirmaram considerar seu nível de atenção mais alto que a média, e apenas 1 (2,5%) marcou o grau máximo de atenção durante as tarefas do cotidiano. Esta noção é relevante visto os erros humanos que podem ocorrer em momentos ordinários do dia-a-dia quando riscos podem passar despercebidos, como por exemplo, digitando senhas sigilosas de aplicativos bancários. De toda forma, uma estatística que vale a pena manter em mente ao refletir sobre as outras questões, vez que pode se dizer que um grau de atenção baixo ou mediano pode ter sido causa de alguns incidentes vivenciados pelos participantes.

4.2 Conhecimentos gerais sobre cibersegurança

Encerrada a análise das questões relacionadas aos aspectos demográficos da amostra, prossegue-se para as perguntas referentes aos conhecimentos gerais sobre cibersegurança. Nesta segunda seção, os participantes tiveram seus conhecimentos avaliados com base em conceitos relacionados à segurança da informação.

A questão 10, ilustrada na Figura 12, marca o início desta seção, abordando a familiaridade dos estudantes com o conceito central desta discussão, que é a segurança da informação.

Figura 12: Conhecimento sobre o termo *cybersegurança*

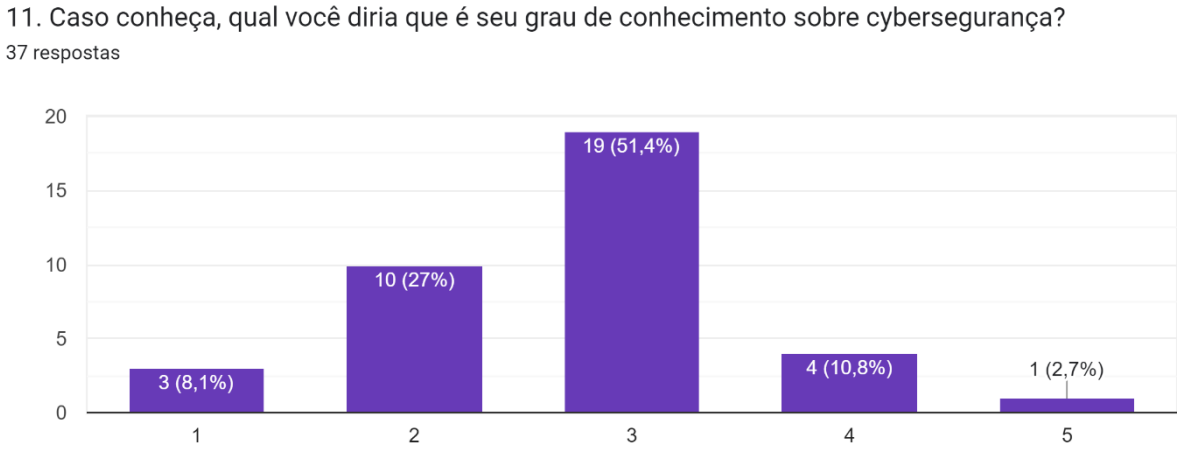


Fonte: Do autor, 2023.

Partindo dos dados obtidos, percebe-se que a grande maioria dos alunos, ou seja, 37 (92,5%) relatam conhecer o termo *cybersegurança*, e/ou segurança da informação, enquanto apenas 3 (7,5%) afirmam desconhecer estas nomenclaturas. Entretanto, apenas o fato de alguns estudantes não conhecerem os termos, não significa que tenham um comportamento inadequado em relação às práticas de segurança informacional, assim como aqueles que conhecem não necessariamente seguem uma boa conduta em relação à segurança de seus dados e informações sigilosas.

A questão 11 é a primeira questão opcional do questionário, destinada somente aos participantes que afirmaram ter conhecimento de algum dos termos mencionados na questão 10. Assim, 37 pessoas responderam esta questão.

Figura 13: Grau de conhecimento sobre *cybersegurança*

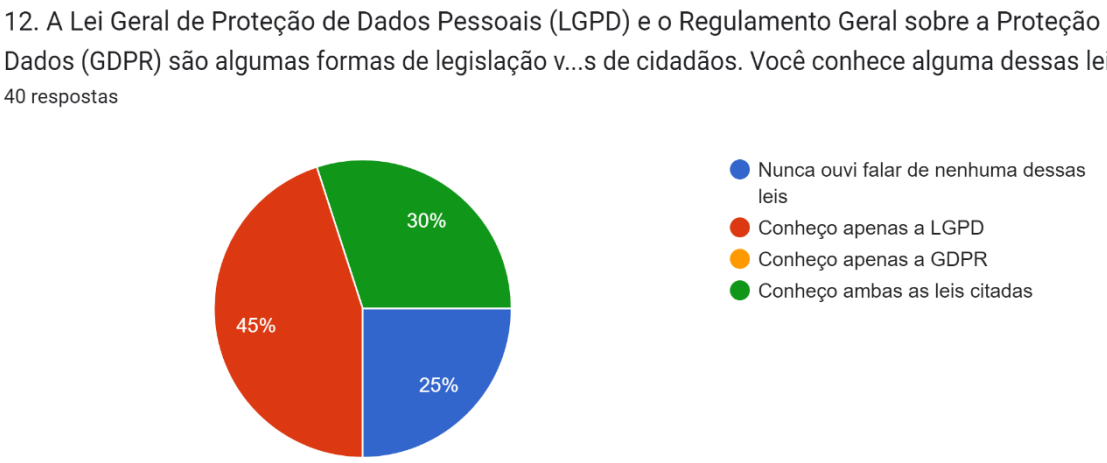


Fonte: Do autor, 2023.

Ao serem questionadas a respeito do seu nível de conhecimento no assunto, 3 alunos (8,1%) afirmaram ter um nível de conhecimento mínimo a respeito, 10 participantes (27%) selecionaram um nível ainda baixo, 19 participantes (51,4%) acreditam ter um nível razoável de conhecimento, mais 4 (10,8%) afirmaram terem um nível um pouco mais alto, enquanto um único estudante (2,7%) afirmou ter um nível alto de conhecimento a respeito da segurança da informação. Em média, a maioria dos alunos afirmou ter um nível de conhecimento de mediano a alto nesta questão, será verificado se esses dados se mostraram condizentes em relação às perguntas mais aprofundadas do questionário.

Na questão 12, adentra-se na área da legislação vigente relativa aos direitos e proteção dos dados dos cidadãos. Os participantes são questionados sobre duas leis específicas relacionadas a esse tema: a lei nacional LGPD e a *GDPR*, que é europeia, mas atua de forma internacional.

Figura 14: Conhecimento sobre a LGPD e *GDPR*



Fonte: Do autor, 2023.

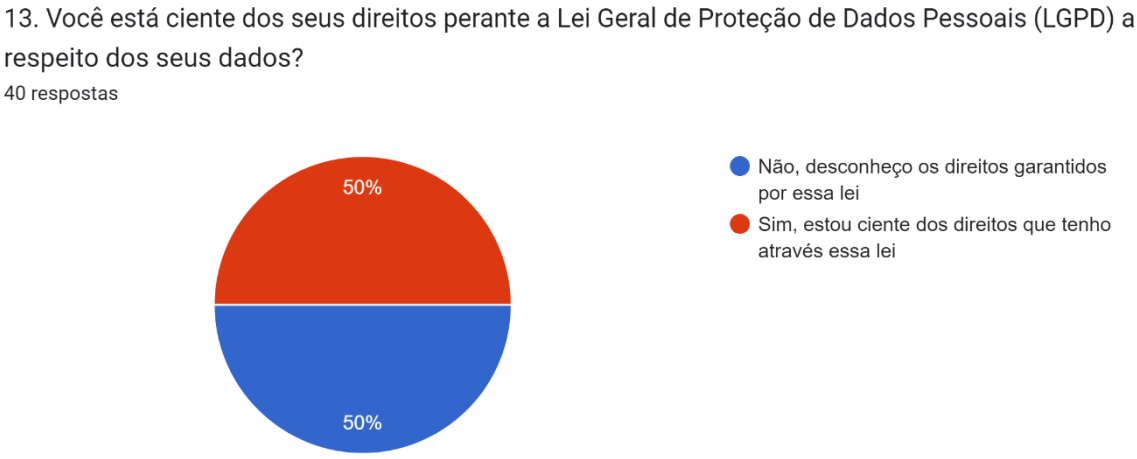
Ao serem questionadas se conheciam ou a LGPD ou o *GDPR*, ou ambos; 10 alunos (25%) afirmaram jamais ter ouvido falar de qualquer uma dessas leis, 18 alunos (45%) dizem conhecer apenas a LGPD, enquanto 12 alunos (30%) afirmam conhecer tanto a LGPD quanto a *GDPR*. Algumas possíveis explicações para estes dados podem ser o fato de que a LGPD é uma legislação brasileira e é referenciada com certa frequência no curso de Biblioteconomia, enquanto a *GDPR* é uma legislação europeia, não tão comentada no curso de Biblioteconomia da UnB quanto a LGPD, apesar de ter uma influência global. O fato que ao menos 30% dos participantes estão cientes de ambas as leis é um bom sinal, porém o curso poderia reforçar o ensino da *GDPR*; os outros 25% que desconhecem qualquer uma destas leis, possivelmente podem ser atribuídos aos calouros identificados anteriormente nos dados, que ainda estão começando a conhecer a área da Ciência da Informação.

A pergunta 13, conforme mostrado na Figura 15, persiste a temática legislativa, questionando agora os participantes se eles estão cientes de seus direitos perante a Lei Geral de Proteção de Dados Pessoais.

As respostas foram divididas simetricamente, com 50% dos 40 alunos respondendo estarem cientes dos direitos que são oferecidos por essa lei, enquanto os outros 50% afirmam não conhecer os direitos que lhe são garantidos por essa lei. Considerando que desses 40 participantes ao menos 25%, 10 alunos, da questão anterior que disseram não conhecer a lei, provavelmente podem ser assimilados à metade dos alunos nesta questão que afirmam não conhecer seus direitos. Então isso quer dizer que dos outros 75%, 30 alunos, que afirmaram

conhecer a lei na questão anterior, 20 desses 30 alunos não só conhecem a lei, como estão cientes dos seus direitos, correlacionando os dados entre as questões 12 e 13.

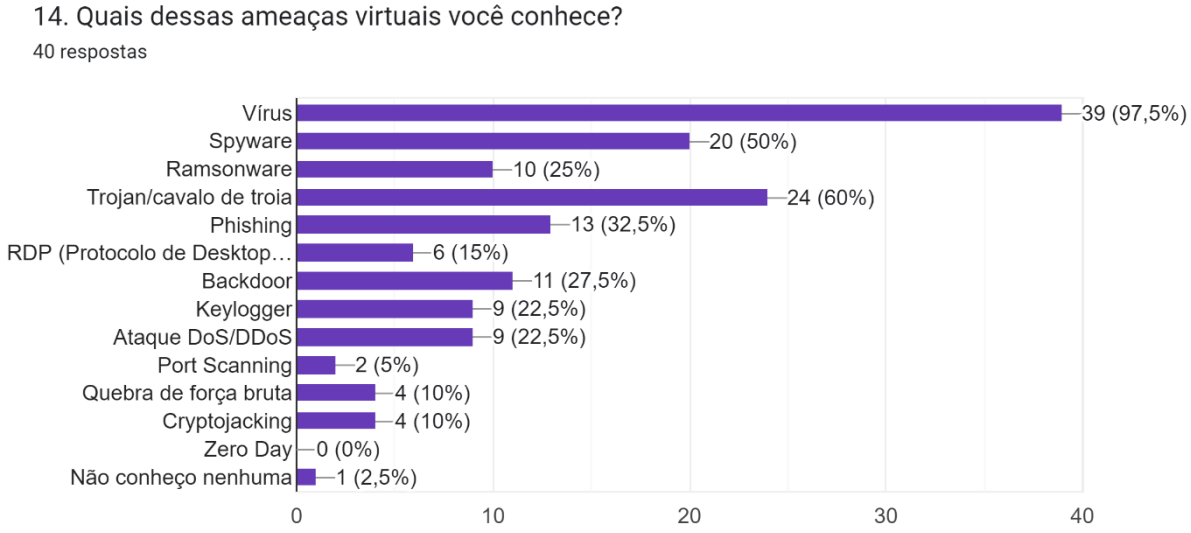
Figura 15: Conhecimento sobre direitos da LGPD



Fonte: Do autor, 2023.

Prosseguindo agora para a questão 14 (Figura 16), os alunos são indagados a respeito de seus conhecimentos gerais em termos de ameaças virtuais que conheçam.

Figura 16: Conhecimento sobre ameaças virtuais



Fonte: Do autor, 2023.

Ao analisar as ameaças virtuais mais conhecidas, é observado que o vírus é amplamente reconhecido por 39 dos participantes (97,5%). Esse resultado não surpreende, uma vez que o

vírus é a ameaça virtual mais divulgada e conhecida pela população em geral. Em seguida, o *trojan* ou cavalo de Troia é conhecido por 24 alunos (60%), o que indica que é uma ameaça comum e amplamente conhecida por uma porção significativa da amostra. O *spyware* é reconhecido por 20 alunos (50%), sendo uma ameaça amplamente comentada devido ao perigo que representa na captura não apenas de dados internos do computador, mas também de imagens por via de dispositivos com câmeras.

Após essas ameaças mais conhecidas, surgem algumas que são menos reconhecidas pela amostra em geral. A técnica de *phishing*, que envolve engenharia social, é conhecida por 13 alunos (32,5%). O *backdoor* é conhecido por 11 alunos (27,5%), enquanto o *ransomware* é conhecido por 10 alunos (25%), ainda que de forma relativamente menor. As ameaças restantes são menos reconhecidas pela amostra, o que é compreensível, uma vez que são menos divulgadas ao grande público em comparação com aquelas que alcançaram um reconhecimento de 25% ou mais.

Em relação às ameaças menos conhecidas, o *keylogger* e os ataques de negação de serviço (DoS/DDoS) são conhecidos por 9 alunos cada (22,5%). O Protocolo de Desktop Remoto é conhecido por 6 estudantes (15%), enquanto a quebra de força bruta e o *cryptojacking* são conhecidos por 4 participantes cada (10%). O *port scanning* é conhecido por apenas 2 alunos (5%), e nenhum participante afirmou conhecer a ameaça *zero day*. Um aluno (2,5%) indicou que não conhece nenhuma das ameaças virtuais mencionadas, o que pode representar um perigo potencial considerável, uma vez que a falta de conhecimento sobre as ameaças pode levar à falta de proteção contra elas.

Esses resultados destacam a necessidade de uma educação formal sobre esse assunto para toda a população, especialmente para aqueles que trabalham frequentemente com dados, como profissionais da CI.

Para finalizar as questões relativas a conhecimentos gerais e ao mesmo tempo fazer uma ponte para a próxima seção, a pergunta 15 opera de forma subsequente à pergunta 14, questionando os participantes se tomam medidas para se proteger dessas ameaças (Figura 17).

Figura 17: Medidas contra ameaças

Fonte: Do autor, 2023.

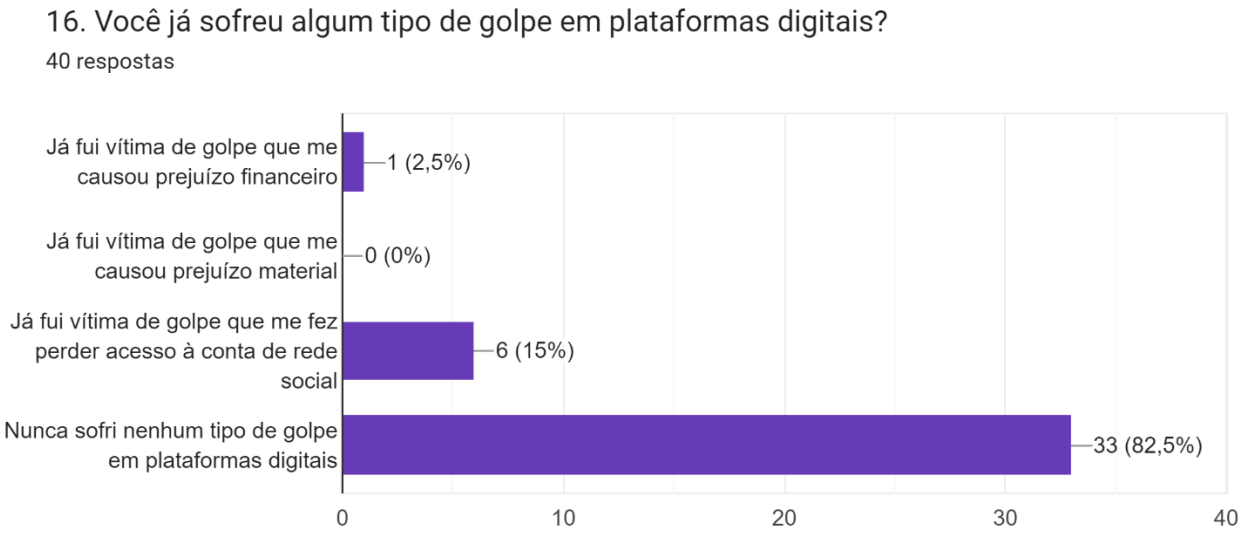
Quando indagados se adotam quaisquer medidas de segurança para se defender contra as ameaças citadas, apenas 29 estudantes (72,5%) afirmaram positivamente, indicando que adotam medidas de proteção. Por outro lado, um total de 11 estudantes (27,5%) negaram adotar medidas protetivas contra ameaças virtuais. Praticamente mais de ¼ da amostra aparentemente não tem a atitude de tomar qualquer ação preventiva contra os perigos presentes no ambiente digital. Este é um número desfavorável à segurança da informação e reforça a necessidade de maior conscientização e educação em cibersegurança.

4.3 Experiência pessoal dos indivíduos

Na seção 3 do questionário de pesquisa, voltada para a experiência pessoal dos participantes, foram feitos questionamentos em relação a eventos vividos e atitudes rotineiras relacionadas à segurança da informação.

A primeira pergunta desta seção, de número 16 (Figura 18), buscou identificar se os participantes já foram vítimas de algum golpe em plataformas digitais e qual tipo de prejuízo eles sofreram como resultado desses eventos.

Figura 18: Golpe em plataformas digitais

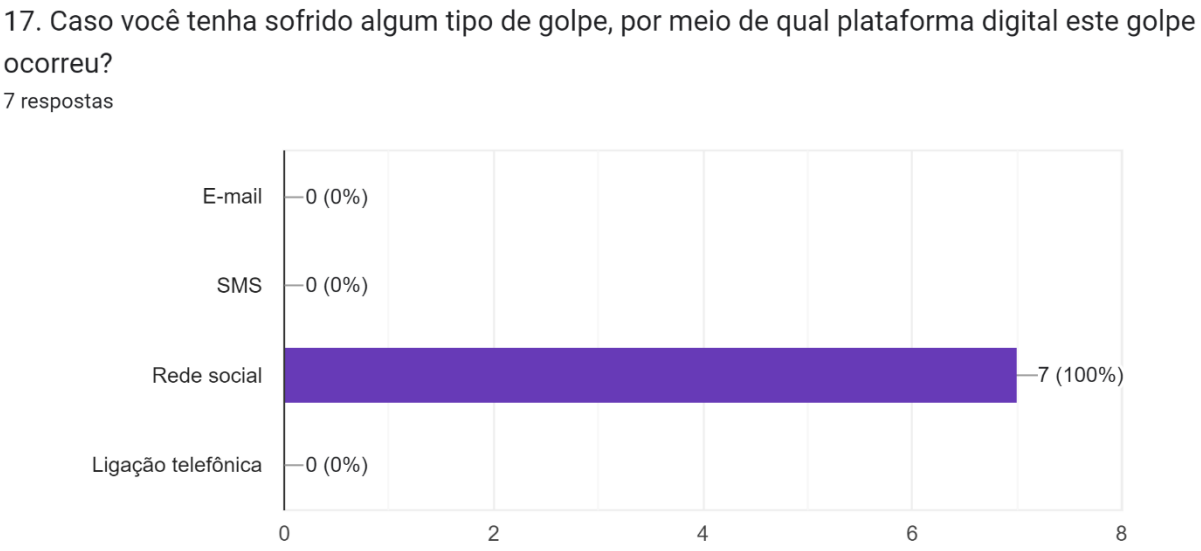


Fonte: Do autor, 2023.

Apenas um participante (2,5%) afirmou ter sido vítima de um golpe que lhe causou prejuízo financeiro. Outros 6 (15%) afirmaram ter perdido acesso a contas de redes sociais, os restantes 33 alunos (82,5%) negam terem sofrido qualquer tipo de golpe em plataformas digitais. Embora o número de vítimas seja relativamente baixo, talvez esses incidentes poderiam ser evitados se as vítimas tivessem melhor conhecimento sobre medidas de segurança e adotassem boas práticas de segurança.

Na questão 17, direcionada apenas aos participantes que relataram terem sido vítimas de golpes na pergunta anterior, buscou-se identificar por meio de quais tipos de plataformas digitais esses golpes ocorreram. Observando-se os dados adquiridos, apresentados na Figura 19, todas as 7 vítimas sofreram golpes em plataformas de redes sociais, totalizando 100% desta parcela da amostra. Tendo em vista a popularidade do uso das redes sociais entre os jovens principalmente, e a facilidade com que se conectam e interagem com outras pessoas pelo uso delas. É plausível que esta população mais jovem esteja mais propensa a serem vítimas de golpes por redes sociais, mais do que qualquer outro tipo de plataforma digital, menos utilizadas e com menos facilidade de proximidade, tornando as redes sociais um ambiente mais propenso para técnicas de engenharia social, quando mirada a esta população demográfica especificamente. Porém esta é apenas uma reflexão, vez que não é possível verificar o cruzamento entre os dados.

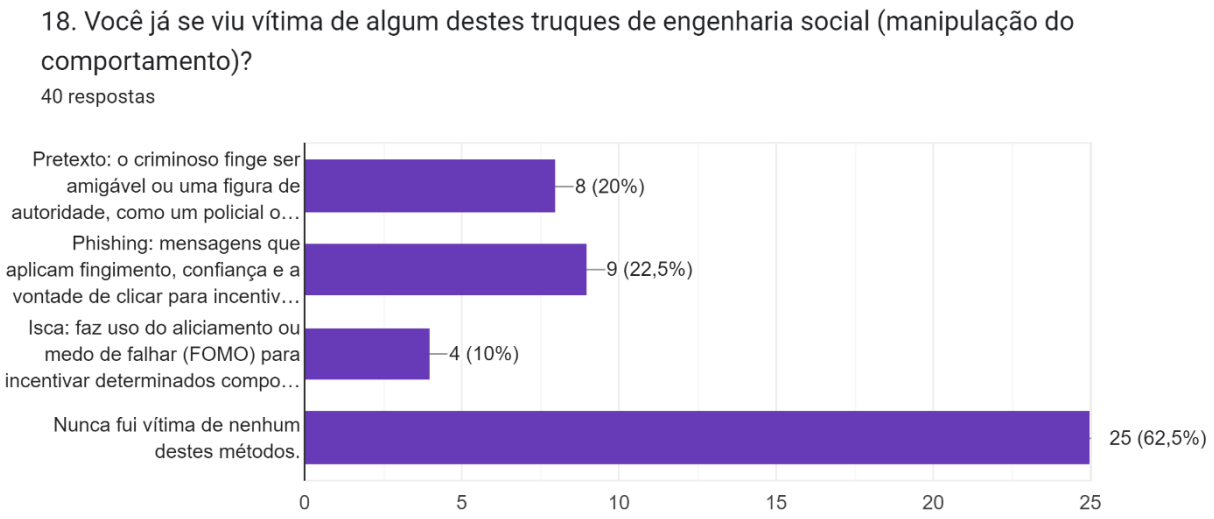
Figura 19: Tipo de plataforma digital do golpe



Fonte: Do autor, 2023.

Já na questão 18, a pesquisa indaga os estudantes de uma forma mais direta sobre as técnicas de engenharia social, não se limitando a nenhuma plataforma específica ou mesmo ao ambiente digital (Figura 20). Várias técnicas comuns são citadas e os alunos responderam se já foram vítimas de algum desses métodos de manipulação do comportamento.

Figura 20: Truques de engenharia social



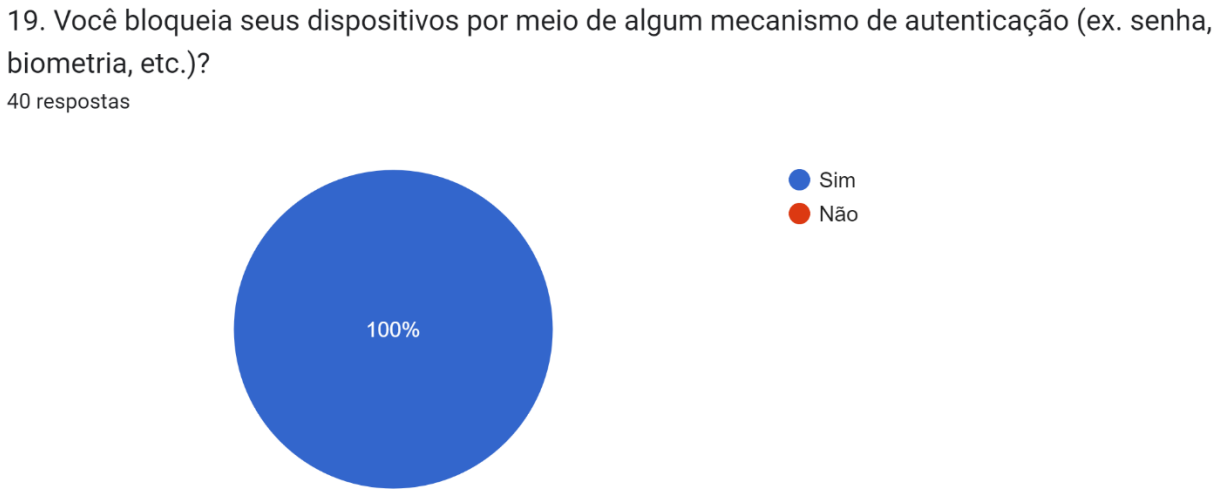
Fonte: Do autor, 2023.

A primeira técnica mencionada foi o pretexto, onde o criminoso se passa por uma figura amigável ou de autoridade, como um policial ou funcionário empresarial, usa então da confiança ganha para extrair dados e informações financeiras das vítimas. Neste caso, 8 alunos (20%) afirmam terem sido enganados desta maneira. A segunda técnica citada foi o *phishing*, que na questão 14, 32,5% da amostra afirmou conhecer, esse método consiste em mensagens que aplicam fingimento, confiança e despertam a vontade de clicar dos usuários, os convencendo a compartilhar informações pessoais particulares. Assim, 9 alunos (22,5%) afirmaram terem sido manipulados por essa técnica. A terceira citada foi a "isca", que utiliza o *Fear of Missing Out* (*FOMO)*, ou "medo de ficar de fora", para incentivar certos comportamentos, podem ser oferecidos presentes gratuitos ao usuário caso forneça informações pessoais ou acesse *links*/botões suspeitos. Neste caso, 4 alunos (10%) afirmaram serem fisgados por esse truque. Por fim, observa-se que 25 dos alunos (62,5%) negam terem sido vítimas de qualquer um desses métodos. É importante lembrar que as técnicas da engenharia social são muito diversas, e nem sempre a vítima percebe que foi manipulada.

Na questão 19, os participantes foram questionados se usam algum mecanismo de autenticação para bloquear seus dispositivos, como senhas ou biometria. O resultado foi interessante e otimista. Todos os 40 participantes da pesquisa afirmaram que fazem uso de algum mecanismo de autenticação, seja senha, biometria ou outros métodos para bloquear e assegurar seus dispositivos. Este dado é favorável à cibersegurança, pois mesmo aqueles que

não tomam outras medidas de proteção mencionadas na questão 15, ao menos utilizam mecanismos de autenticação, o que evita ficarem totalmente desprotegidos.

Figura 21: Bloqueio de dispositivos



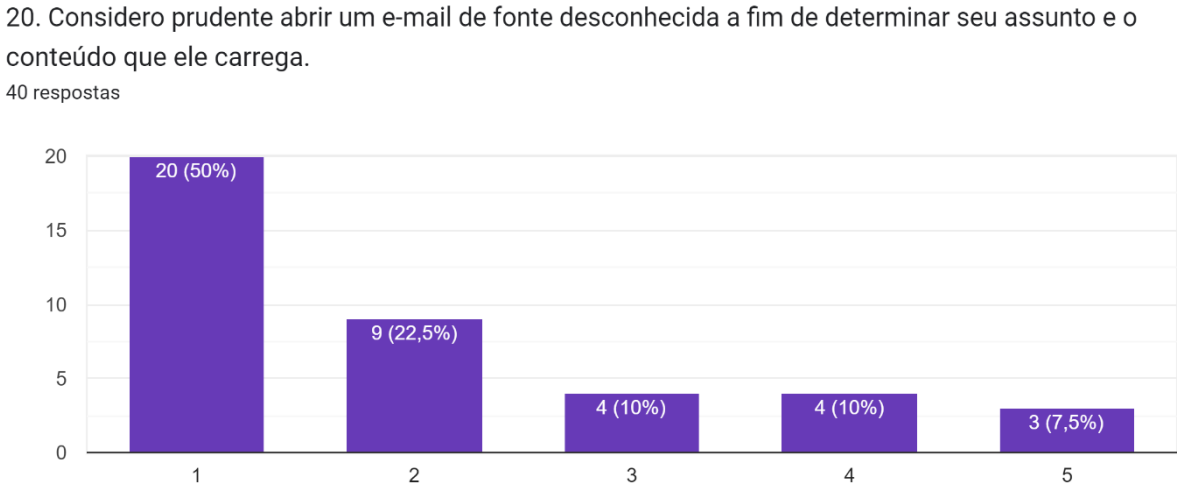
Fonte: Do autor, 2023.

Nas questões 20 a 28, os participantes foram solicitados a indicar seu nível de concordância com as afirmações apresentadas. Essas perguntas foram formuladas para avaliar as atitudes, percepções ou crenças dos participantes em relação a determinados tópicos relacionados à segurança da informação.

Essa escala de concordância geralmente varia de "discordo totalmente" (equivalente ao número 1) a "concordo totalmente" (equivalente ao número 5), permitindo que os participantes expressem seu grau de concordância em relação a cada afirmação específica.

Na primeira questão de grau de concordância, a questão 20 da seção de conhecimento gerais, os alunos se posicionam em relação à seguinte afirmação (Figura 22).

Figura 22: *E-mail* de fonte desconhecida

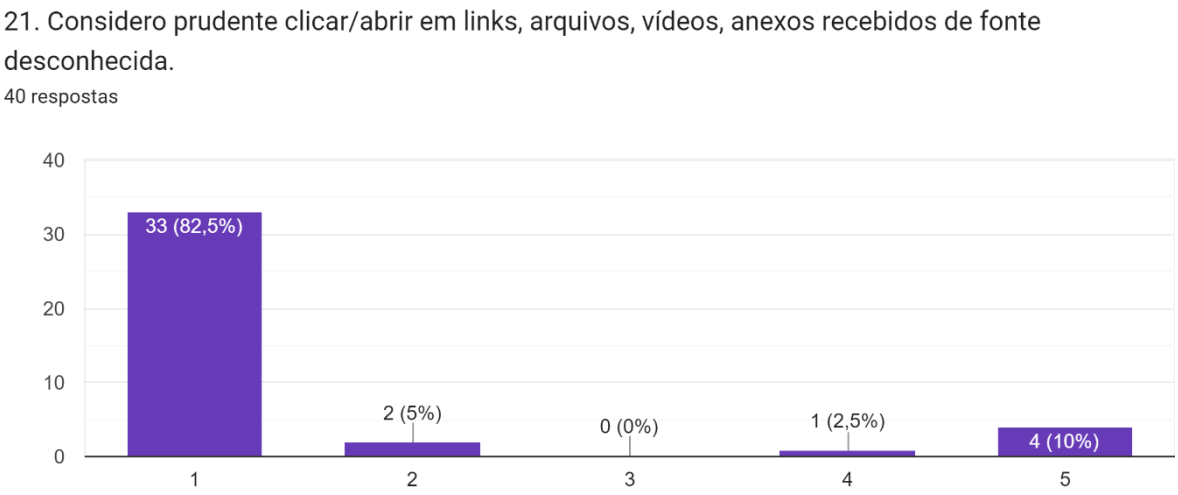


Fonte: Do autor, 2023.

Dentre os 40 participantes, 20 deles (50%) discordaram fortemente da afirmação, 9 (22,5%) discordaram levemente, um total de 4 (10%) tem uma opinião neutra sobre a afirmação, e outros 4 (10%) concordaram levemente, enquanto os outros 3 (7,5%) concordaram fortemente com a afirmação. De acordo com Schultz (2005), 20% de sua amostra não estava ciente que deveriam ignorar anexos desconfiáveis e potencialmente maliciosos, ataques simples que podem oferecer grande perigo, o mesmo parece se repetir nesta pesquisa. Os dados mostram que ao menos 17,5% da amostra não percebe o risco a que estão se expondo ao abrir *e-mails* de fontes desconhecidas, enquanto outros 10% parecem ter ficado incertos quanto a que atitude tomar. Uma estatística desfavorável para cibersegurança, que poderia ser facilmente resolvida com educação e divulgação adequada do assunto.

A afirmação seguinte foi semelhante, porém levou a situação anterior um pouco além. Conforme apresentado na Figura 23, o nível de concordância médio foi menor, 33 participantes (82,5%) discordaram completamente da afirmação, 2 deles discordaram levemente, nenhum ficou em posição neutra, enquanto apenas 1 (2,5%) concordou levemente, porém ainda 4 concordaram completamente. O nível de dúvida e de concordância nesta questão parece ter diminuído, provavelmente pela maioria dos alunos reconhecer o perigo mais direto e iminente em acessar páginas e baixar arquivos desconhecidos. Entretanto, vale lembrar que Dias (2021) ainda apontou que abrir *e-mails* de fonte desconhecida é um hábito arriscado dos usuários que permite brechas à prática de *phishing*, comprometendo a segurança da informação e ainda sendo perigoso.

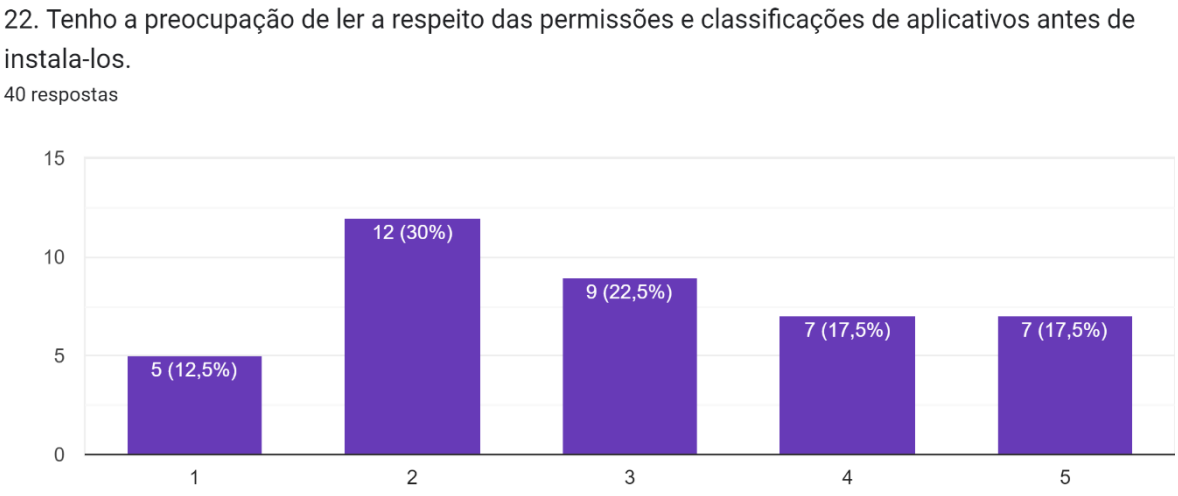
Figura 23: Arquivos de fonte desconhecida



Fonte: Do autor, 2023.

A afirmação da questão 22 indagou os participantes a respeito da instalação de aplicativos e se eles se preocupam em ler e entender as permissões que estão concedendo e as classificações antes.

Figura 24: Permissões e classificações de aplicativos



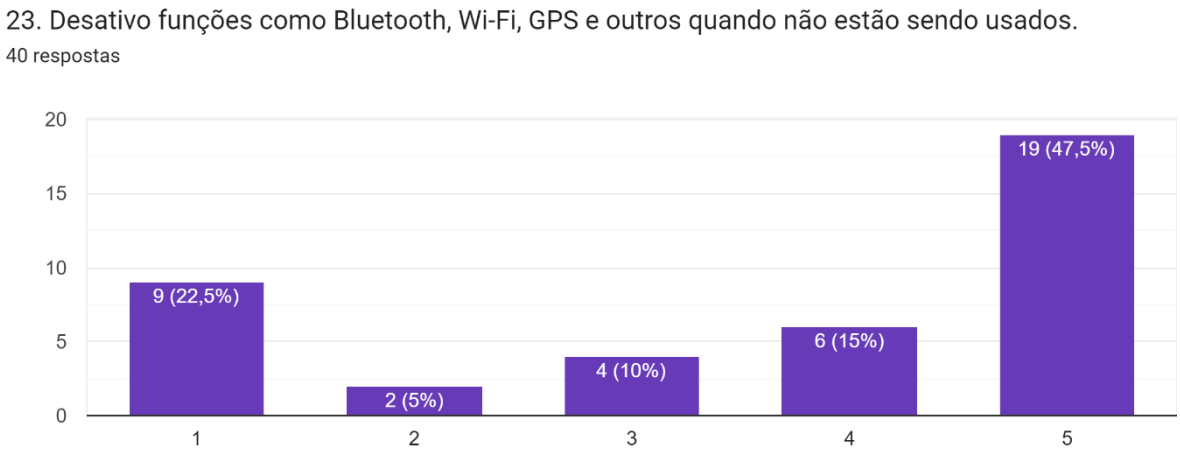
Fonte: Do autor, 2023.

Pode-se observar na Figura 24 que as respostas foram bastante diversas. Cerca de 12,5% dos alunos discordaram fortemente dessa prática, enquanto 30% discordaram levemente. Por

outro lado, 17,5% concordaram levemente e outros 17,5% concordaram completamente, mostrando um nível de preocupação com essa prática de segurança. Surpreendentemente, 22,5% dos alunos ficaram neutros em relação a essa afirmação. Embora a maioria ou afirme não ler ou ficaram em opinião neutra, foi positivo perceber que um número substancial de alunos se mostra preocupado com este benéfico hábito de segurança, o que pode contribuir para uma maior conscientização e proteção digital.

Na pergunta 23, para além dos aplicativos, os estudantes foram indagados sobre como gerenciam algumas funções básicas dos dispositivos móveis (Figura 25). Funções como *Bluetooth*, *Wi-Fi*, *GPS* e outras são bastante úteis, entretanto podem servir de porta de entrada para ataques cibernéticos quando ligadas, além de ainda haver consumo de bateria, portanto, não há razão para deixá-las ativadas quando não estão sendo utilizadas.

Figura 25: Desativação de funções



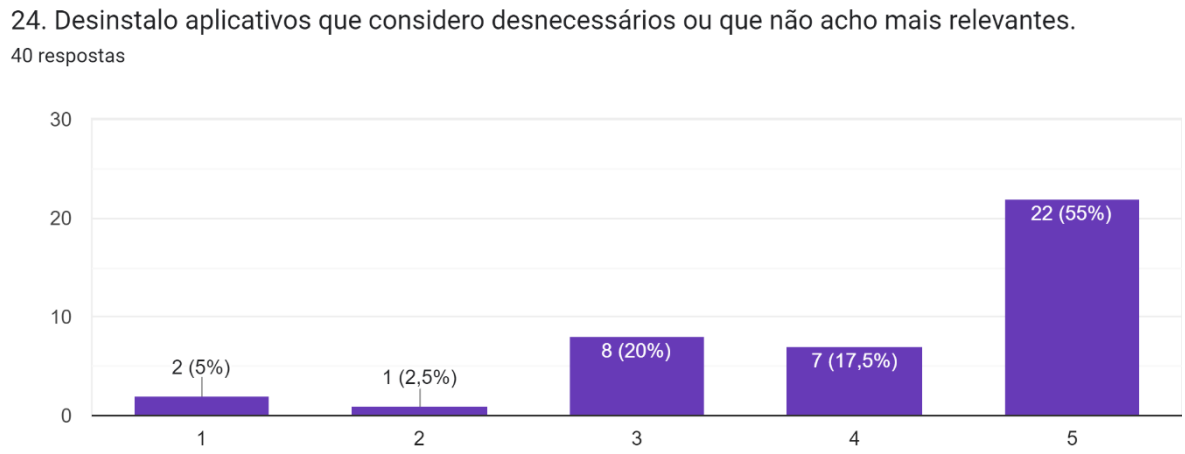
Fonte: Do autor, 2023.

Na figura 25, observou-se que 9 participantes (22,5%) discordaram fortemente, insinuando que mantém estas funções funcionando quando não estão cumprindo nenhum propósito, permitindo brechas para ataques de cibercriminosos. Outros 2 discordaram levemente, 4 (10%) participantes assumiram uma posição neutra, outros 6 (15%) concordaram levemente, enquanto os restantes 19 (47,5%) concordaram fortemente que não mantêm essas funções ativadas quando não estão sendo utilizadas. Pouco mais da metade dos participantes seguem tal boa prática de segurança da informação, reconhecendo os riscos associados a manter

essas funções ligadas desnecessariamente, o que pode contribuir para uma maior proteção contra possíveis ataques cibernéticos e economia de bateria.

Retornando ao tema dos aplicativos, a pergunta 24 verifica se os estudantes concordam em desinstalar aplicativos desnecessários ou que não são mais relevantes para eles.

Figura 26: Desinstalação de aplicativos



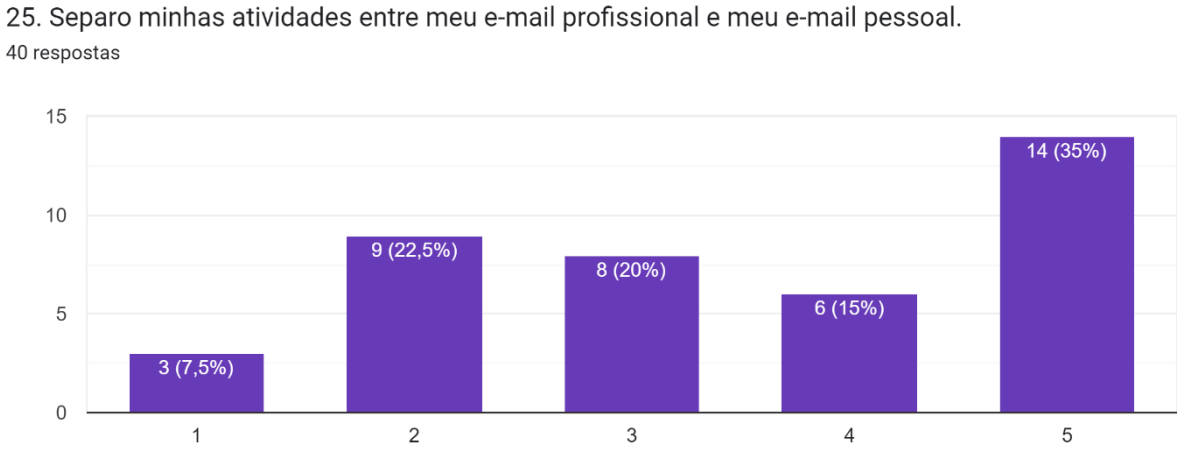
Fonte: Do autor, 2023.

Conforme evidenciado na Figura 26, apenas 2 alunos (5%) discordaram completamente, apenas 1 aluno (2,5%) só discordou levemente, outros 8 (20%) se mantiveram em posição neutra, enquanto 7 (17,5%) concordaram levemente, e por fim, os outros 22 alunos (55%) concordaram completamente. É importante destacar que aplicativos antigos ainda podem continuar coletando dados e monitorando suas atividades dos usuários enquanto ainda estiverem no seu dispositivo. Portanto, é recomendado desinstalá-los quando não servirem mais a nenhum propósito. É encorajador constatar que muitos estudantes parecem aderir a essa prática.

A questão 25 examina como os alunos administram as suas atividades de acordo com o espaço pessoal e profissional nos *e-mails*. Se atentando aos dados da Figura 27, fica visível que 3 participantes (7,5%) discordaram fortemente na separação de atividades entre endereços pessoais e profissionais, mais 9 (22,5%) discordaram levemente, totalizando no mínimo 30% da amostra que mistura atividades destas duas naturezas em suas comunicações digitais. Além disso, outros 8 participantes (20%) se mantiveram de forma neutra. Este é mais um hábito que pode tornar os usuários e funcionários vulneráveis à prática de *phishing*. Aparentemente, 50% dos participantes não sabem ou não se preocupam em adotar essa simples prática que ajuda a

evitar este tipo de ocorrência. Para a outra metade, 6 alunos (15%) concordaram levemente, e os outros 14 (35%) concordaram fortemente com esta divisão, evidenciando que uma parte significativa da amostra reconhece a importância dessa prática.

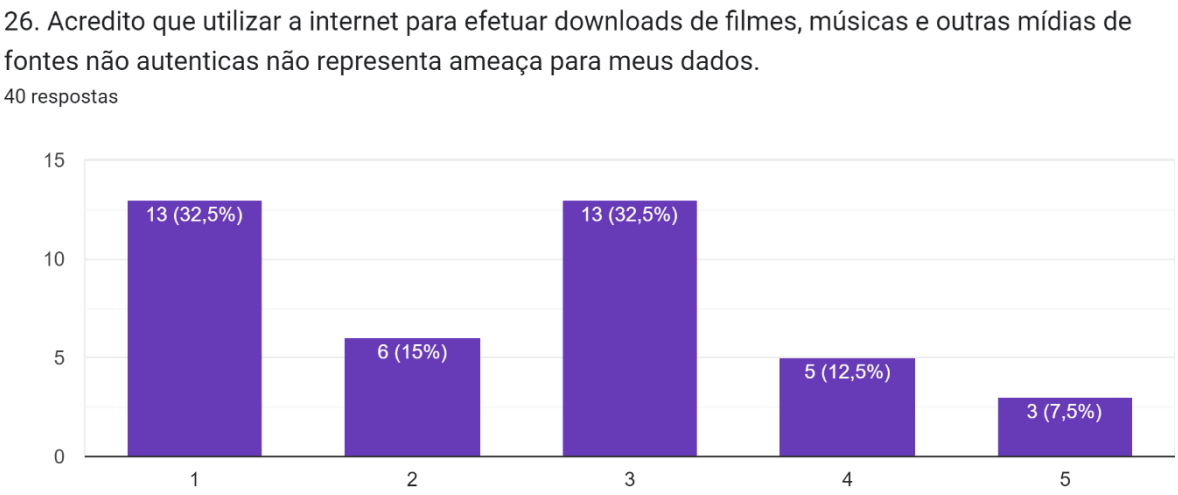
Figura 27: *E-mail* profissional e pessoal



Fonte: Do autor, 2023.

Para a pergunta 26, os estudantes foram questionados sobre como interpretam a possibilidade de ameaças em endereços da *Internet* não-fidedignos. De acordo com a Figura 28, entre os participantes da pesquisa, 13 (32,5%) discordaram fortemente da afirmação, mais 6 (15%) discordaram levemente, reconhecendo a possível ameaça que *downloads* de fontes não-autênticas podem representar para seus dados. Entretanto, 13 alunos (32,5%) assumiram uma posição intermediária, enquanto 5 (12,5%) concordaram levemente e mais 3 (7,5%) concordaram fortemente em não reconhecer quaisquer riscos ou ameaças possíveis aos seus dados ao realizar este tipo de prática. É importante ressaltar que a realização de *downloads* de fontes suspeitas pode expor os usuários a diversos tipos de ameaças, como vírus, cavalos de troia e outras formas de *malware*. Portanto, é recomendável ter cuidado ao lidar com endereços eletrônicos duvidosos ou evitar completamente essa prática.

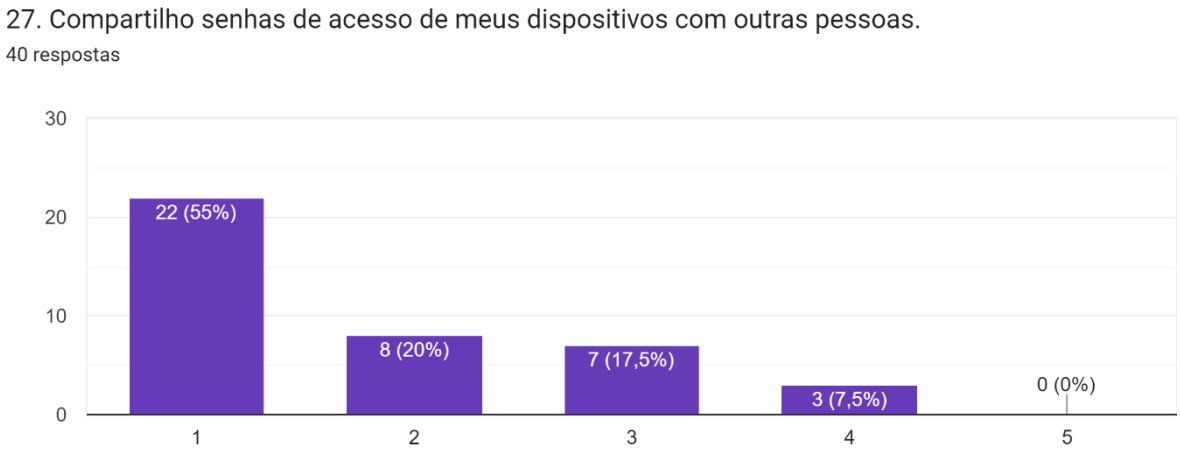
Figura 28: Fontes não autênticas na *Internet*



Fonte: Do autor, 2023.

Conforme verificado anteriormente na questão 19, todos os participantes da amostra afirmam utilizar algum mecanismo de autenticação em seus dispositivos, como senhas de acesso. Essa constatação é positiva, pois indica que os participantes reconhecem a importância de proteger seus dispositivos e informações pessoais por meio do uso de autenticação. Entretanto, na questão 27, foi investigado se os participantes têm o hábito de compartilhar suas senhas de acesso com terceiros. A motivação para esta questão leva em consideração que compartilhar senhas com indivíduos mal-intencionados ou ceder a solicitações de terceiros mediante o uso de técnicas de engenharia social pode comprometer a segurança dos dispositivos e dos dados pessoais dos usuários. A proteção das senhas é essencial para evitar acessos não autorizados e garantir a integridade das informações digitais.

Figura 29: Compartilhamento de senhas

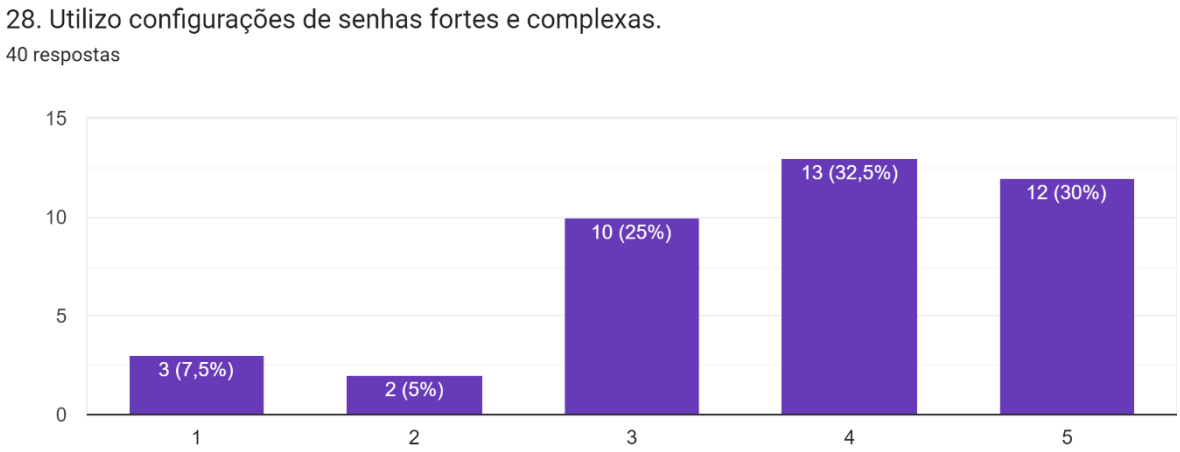


Fonte: Do autor, 2023.

Os resultados apresentados na Figura 29 trazem um cenário favorável para segurança informacional por demonstrar que a maioria dos estudantes tem consciência da importância de manter as senhas pessoais em sigilo. Dentre todos os participantes, 22 alunos (55%), discordam fortemente da afirmação, indicando que são contrários ao compartilhamento de senhas. Além disso, 8 alunos (20%) discordam levemente, outros 7 (17,5%) se mantiveram em posição neutra. Enquanto apenas 3 (7,5%) concordaram levemente, sugerindo que talvez considerem o compartilhamento de senhas em circunstâncias específicas. Em geral, manter informações sobre suas senhas para si mesmo, ou seja, confidenciais, é recomendado, assim como evitar anotá-las em pedaços de papel facilmente acessíveis ou identificáveis. No entanto, pode-se levar em consideração também que algumas pessoas apenas compartilhem suas senhas com pessoas que considerem altamente confiáveis, porém este tipo de informação não foi alvo desta pesquisa.

Essa variação nas atitudes em relação ao compartilhamento de senhas destaca a complexidade do comportamento humano e evidencia uma limitação inerente ao método de pesquisa utilizado. Ainda no que se refere às senhas, a questão 28 foi formulada para investigar as configurações adotadas pelos estudantes em termos de força e complexidade das suas senhas. A definição fornecida para senhas fortes e complexas no questionário foi "senhas que envolvem variação entre letras maiúsculas e minúsculas, uso de elementos numéricos e caracteres especiais".

Figura 30: Configurações de senhas



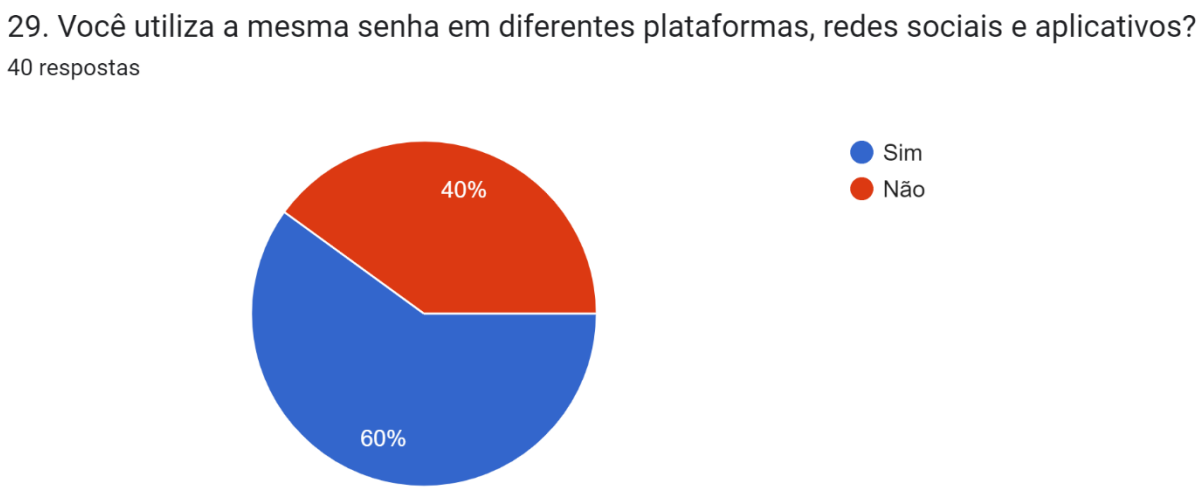
Fonte: Do autor, 2023.

Supondo que os estudantes tenham se atentado a esta descrição, é possível concluir conforme o gráfico da Figura 30, que ao menos 3 alunos (7,5%) que discordaram fortemente, e outros 2 alunos (5%) que discordaram levemente, indicando que possuem senhas fracas e simples. Observa-se ainda que 10 alunos (25%) parecem ter senhas medianas ou se colocam em um cenário neutro entre possuir uma senha forte ou não. Adicionalmente, outros 13 participantes (32,5%) concordam ter senhas mais fortes e complexas, e os últimos 12 (30%) concordam fortemente que usam configurações de senhas muito seguras.

O uso de senhas fracas e simples não é recomendado pois poderiam ser rapidamente sobrepostas pela ameaça da quebra de força bruta mencionada na fundamentação teórica, onde o computador do invasor tenta um alto número de combinações diferentes de caracteres até que encontre a senha correta.

Na questão 29, complementando a questão de concordância anterior, indaga os estudantes sobre a sua variabilidade de senhas, através de diversas plataformas, redes sociais e aplicativos.

Figura 31: Similaridade de senhas

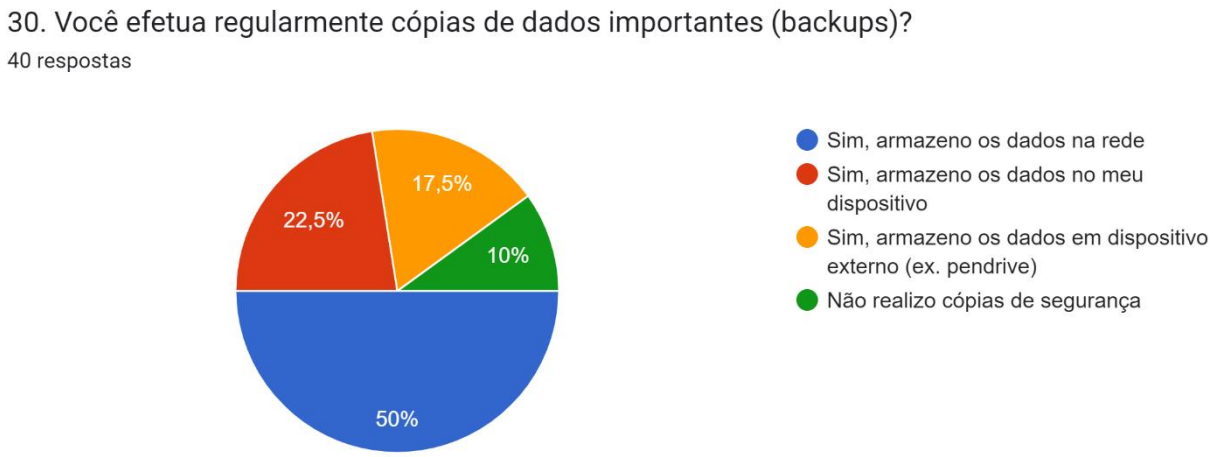


Fonte: Do autor, 2023.

Ao analisar os dados conforme demonstrado no gráfico da Figura 31, nota-se que 24 participantes (60%) responderam que sim, utilizam a mesma senha repetidas vezes em múltiplas contas diferentes como chave de acesso. Esta não é uma prática recomendada por vários especialistas da área, obviamente se um invasor desvendar uma das senhas do usuário terá acesso facilitado a outras contas também. Os outros 16 participantes (40%) responderam que não, uma porção considerável da amostra, mas infelizmente na minoria nesta situação.

A questão 30 trata de *backups*, cópias de dados reserva, e sobre a frequência que os participantes realizam estes para seus próprios dados importantes.

Figura 32: Regularidade de *backups*



Fonte: Do autor, 2023.

De acordo com a coleta de dados (Figura 32), um total de 20 participantes, 50% da amostra, realiza *backups* regularmente e mantém-los armazenados na nuvem (rede), em plataformas como *Google Drive*. Mais 9 (22,5%) fazem o mesmo, porém os armazenam no próprio dispositivo, enquanto outros 7 alunos (17,5%) também fazem *backups*, mas guardando os dados em dispositivos externos, como um *pendrive*. Todas as opções de *backup* são válidas, com suas vantagens e desvantagens, o importante é fazer essas cópias de segurança, e dependendo de sua importância, até guardar cópias em várias dessas mídias. Entretanto, ainda houveram outros 4 estudantes (10%) que não tem o hábito de realizar tais cópias de segurança, isto deixa os dados frágeis e vulneráveis a ataques como de *ransomware*, onde os dados são criptografados por criminosos que exigem uma quantia em dinheiro a ser paga para que ele recupere seus dados. Neste caso, se o usuário tem um *backup* em outro espaço, o ataque pode não se mostrar um problema, exceto a depender da sensibilidade da informação contida nos dados.

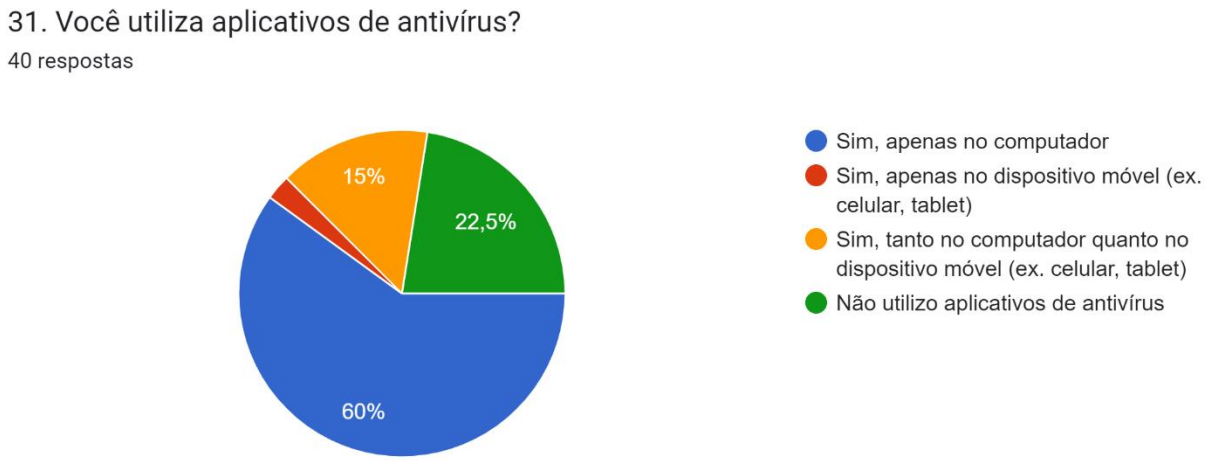
Os *backups* são essenciais para proteger os dados importantes contra perdas, seja devido a falhas de *hardware*, erros humanos, ataques cibernéticos ou desastres naturais. Ao realizar *backups* regularmente, os indivíduos melhoram suas chances de recuperar seus dados caso ocorra algum incidente que comprometa as informações armazenadas em seus dispositivos.

Assim, embora uma parcela considerável dos participantes tenha mostrado preocupação e aderência à prática de realizar *backups*, é importante ressaltar que ainda existe um número significativo de estudantes que não adotam essa medida de segurança. Promover a

conscientização sobre a importância dos *backups* e os benefícios que eles oferecem pode ser um ponto relevante a ser abordado para melhorar a postura de segurança digital dos usuários.

A questão seguinte, de número 31, perguntou aos participantes se eles utilizam quaisquer aplicativos de antivírus em algum de seus dispositivos.

Figura 33: Uso de antivírus

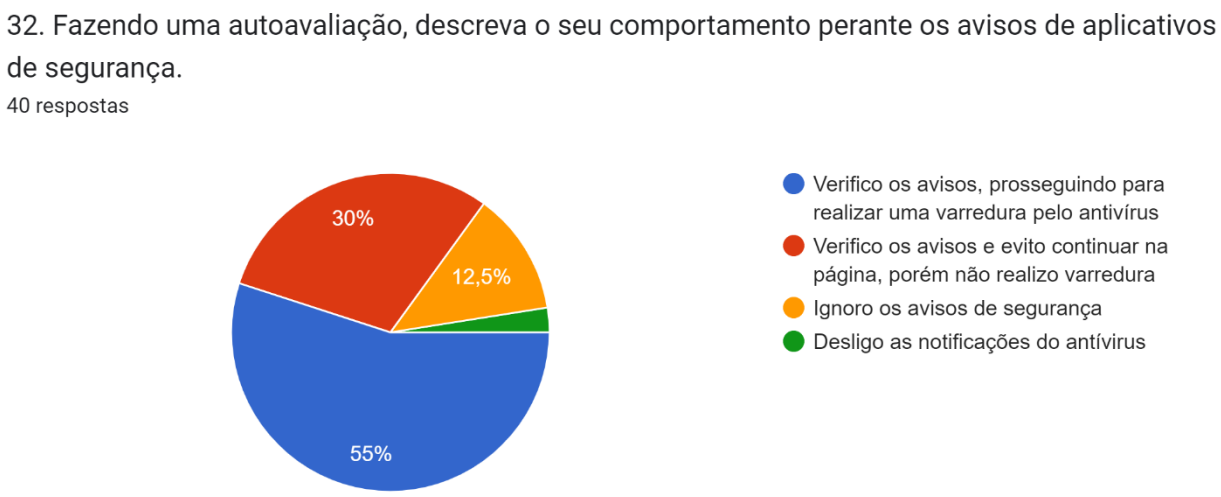


Fonte: Do autor, 2023.

Como pode ser observado na Figura 33, a grande maioria dos estudantes da amostra utiliza algum tipo de programa de antivírus em seus dispositivos. Dentre esses, 24 participantes (60%) usam apenas em seus computadores, outros 6 (15%) usam tanto nos seus computadores quanto em seus dispositivos móveis (como celulares ou tablets), e somente 1 participante (2,5%) utiliza apenas no seu dispositivo móvel. Todavia, um número considerável de estudantes, 9 deles (22,5%), não utilizam qualquer tipo de aplicativo de antivírus em nenhum de seus dispositivos. É importante ressaltar que essa prática não é recomendada, pois expõe os dispositivos e os dados dos usuários a diversas ameaças virtuais. Entretanto, é interessante destacar que esses dados apresentam semelhanças, mas não correspondência exata, com os resultados da questão 15, na qual 11 alunos (27,5%) afirmaram não adotar medidas de segurança contra as diversas ameaças virtuais. Esta pequena divergência pode indicar que alguns estudantes adotam outras medidas de segurança, além do uso de aplicativos de antivírus, ou que possuem percepções diferentes sobre o que constitui uma medida de segurança eficaz.

Na questão seguinte, de número 32, os participantes são requeridos a realizar uma autoavaliação sobre seu comportamento diante dos avisos dos aplicativos de segurança.

Figura 34: Comportamento com avisos de segurança



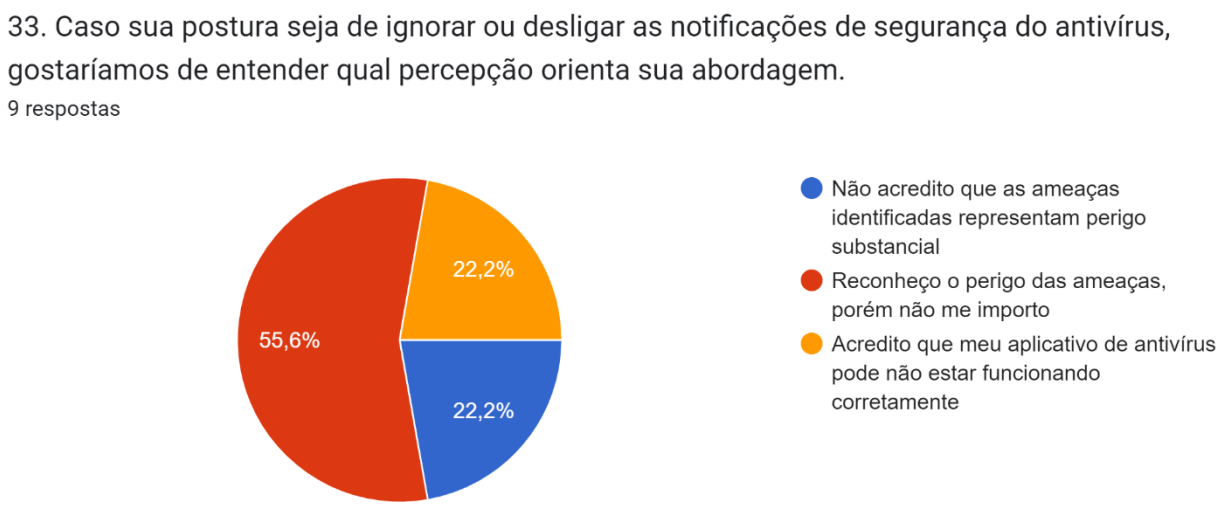
Fonte: Do autor, 2023.

Ao analisar os resultados desta amostra (Figura 34), percebe-se que 22 alunos (55%) adotam a atitude mais segura, verificando os avisos e prosseguindo para realizar varredura com o *software* de antivírus. Outros 12 alunos (30%) verificam os avisos e evitam continuar na página que causou o alerta, porém deixam de realizar as varreduras recomendadas. Nota-se uma minoria de 5 alunos (12,5%) que ignoram os avisos de segurança, e ainda 1 único participante (2,5%) que afirmou desligar as notificações do antivírus.

A respeito desta prática, Modic e Anderson (2014) alertaram sobre o quão comum pode ser o hábito de usuários serem advertidos sobre riscos de segurança por seus antivírus, e mesmo assim sendo ignorados. Os autores também mencionaram que alguns usuários até optam por desligar as notificações por completo. Percebe-se visualizando dos dados desta pesquisa, que a tese de Modic e Anderson (2014) se confirma. Porém vale lembrar que os autores também indicaram que essas notificações deveriam ser simplificadas, a fim de facilitar sua compreensão pelos usuários. Essa sugestão que se mostra relevante para a próxima questão.

A pergunta 33, que é a terceira e última pergunta opcional, os participantes são convidados a fornecer informações sobre o motivo pelo qual optam por ignorar ou desligar as notificações de segurança, conforme mencionado na questão 32. Essa abordagem tem como objetivo compreender as razões por trás dessa escolha específica dos participantes.

Figura 35: Abordagem de ignorar notificações



Fonte: Do autor, 2023.

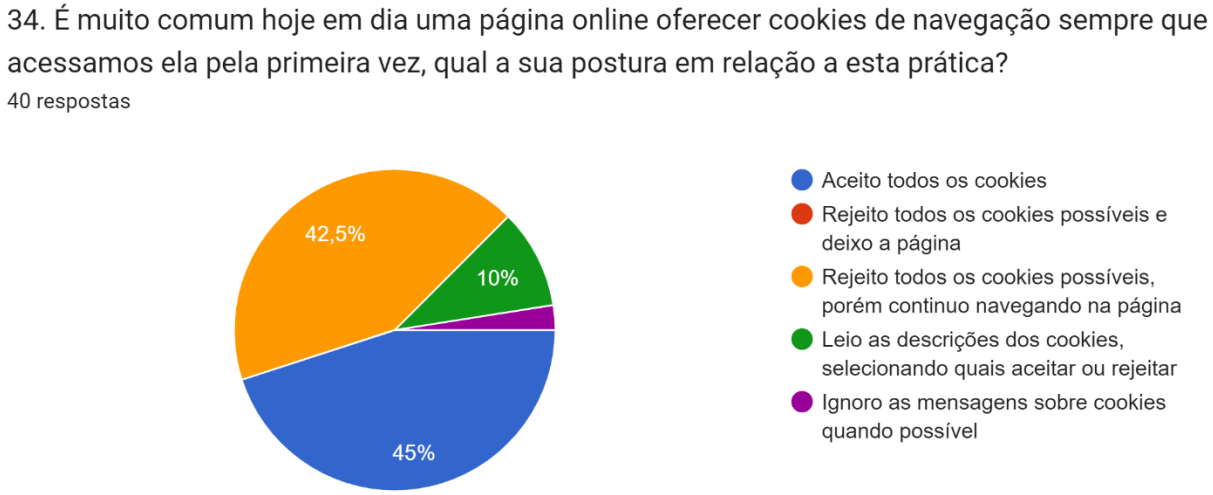
Pode-se observar na Figura 35, que do total de 9 respondentes, 2 alunos (22,2%) afirmaram não acreditar que as ameaças identificadas representam perigo substancial. O problema com esta visão é que mesmo que aparentemente nada esteja errado com o dispositivo, informações podem estar sendo roubadas e espionagem sendo realizada sem mesmo o usuário perceber, nem todas as ameaças se mostram claramente aos usuários. Outros 2 alunos (22,2%) acreditam que o programa antivírus pode não estar funcionando corretamente. Essa opinião ressalta a importância de ter o hábito de manter os aplicativos sempre atualizados, a fim de evitar quaisquer mal funcionamento. Ao mesmo tempo, esta constatação evoca o que Modic e Anderson (2014) apontaram anteriormente, que às vezes as notificações não são claras o suficiente para os usuários.

No entanto, talvez o aspecto mais intrigante seja o grupo de 5 estudantes (55,6%), que afirmam reconhecer o perigo das ameaças, porém não se importam com elas. Este é um comportamento comum entre usuários que adotam hábitos arriscados de segurança. Pode ser resultado de uma falta de educação adequada sobre o assunto, uma falta de compreensão sobre o que está em jogo ou simplesmente uma falta de preocupação com o conteúdo do dispositivo que estão utilizando.

Esses resultados destacam a importância de conscientização e educação sobre segurança digital, a fim de promover comportamentos mais seguros e proteger os usuários contra ameaças cibernéticas.

A penúltima pergunta do questionário, de número 34, levanta o assunto dos *cookies*, uma das ferramentas mais comuns de coleta de dados, e mais eficientes também, rotineiramente usuários são abordados por diversos *sites* com opções de aceitação ou rejeição de instalação de *cookies*. Esta questão busca descobrir qual postura os estudantes adotam quando se deparam com esta prática.

Figura 36: Postura com os *cookies*



Fonte: Do autor, 2023.

Na amostra analisada, e apresentada na Figura 36, observa-se que os participantes adotam diferentes abordagens em relação à aceitação de *cookies*. Observa-se que 18 alunos (45%) aceitam todos os *cookies* que são oferecidos enquanto 17 alunos (42,5%) rejeitam todos os *cookies* possíveis e continuam navegando na página. Por outro lado, 4 alunos (10%) fazem uma seleção cuidadosa dos *cookies*, lendo suas descrições e escolhendo quais aceitar ou rejeitar e apenas 1 único aluno (2,5%) afirmou ignorar mensagens sobre *cookies* quando possível.

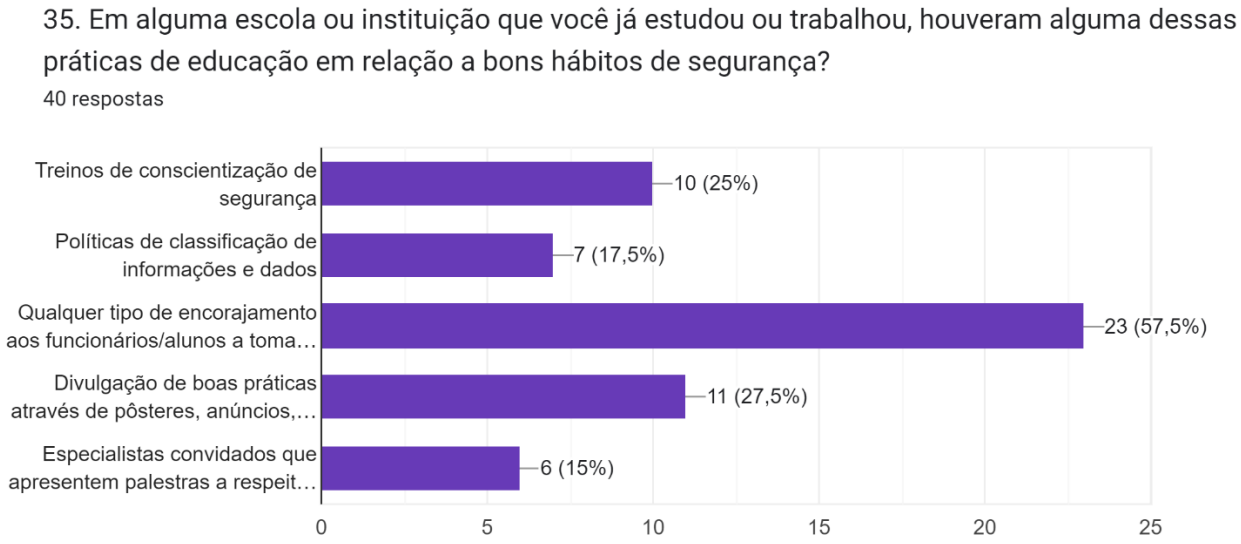
A situação dos *cookies* pode ser complexa, eles são oferecidos sob a proposta de melhorar a experiência do usuário, mas por outro lado também podem ser usados para coletar todo tipo de dados sobre os usuários, invadindo a privacidade dos que não conhecem e daqueles que optam por não ler as descrições. Ao mesmo tempo, em algumas páginas a navegação só é permitida caso o usuário aceite a política de *cookies*. Como Barros (2021) afirma, essas ferramentas podem ser usadas para nos avaliar e descobrir como melhor nos bombardear com anúncios e artigos, a fim de manipular o comportamento e estimular instintos específicos, muitas vezes transformando usuários essencialmente em produtos da indústria de *marketing*.

Mesmo que não seja apresentada aqui uma instrução exata sobre qual seria a atitude mais correta a se adotar, é importante ter cuidado com que tipo de permissões estamos concedendo e que tipo de arquivos estamos baixando para nosso sistema. É fundamental ter consciência dos riscos associados à coleta de dados por meio de *cookies* e tomar decisões informadas sobre quais aceitar ou rejeitar, levando em consideração a privacidade e a segurança de nossas informações.

Uma boa prática a ser adotada, é a limpeza ou remoção de *cookies* periódica. Isso ajuda a manter a privacidade e a segurança dos dados pessoais, além de proporcionar uma experiência de navegação mais controlada. Os *cookies* são armazenados no dispositivo e podem acumular-se ao longo do tempo, registrando informações sobre as atividades *online* do usuário. Ao realizar a limpeza ou remoção destes *cookies*, é possível reduzir a quantidade de dados coletados e armazenados, minimizando o risco de exposição de informações pessoais.

Na última pergunta do questionário (questão 35), os participantes foram questionados sobre as práticas de educação e bons hábitos de segurança da informação que presenciaram em escolas ou outras instituições que frequentaram.

Figura 37: Bons hábitos de segurança



Fonte: Do autor, 2023.

Antes de prosseguir para a análise dos resultados desta questão, é importante apontar um erro que foi cometido em sua formulação. Não foi adicionada a opção para os participantes de responderem que nunca presenciaram nenhuma dessas práticas em qualquer instituição

antes, dado que seria relevante para medir a falta de exposição à temática de cibersegurança. Sendo assim, ainda é interessante notar que as respostas foram variadas, permitindo na análise ao menos se avaliar quais práticas e hábitos de segurança são menos ou mais populares.

Os resultados apresentados na Figura 37 revelaram que a prática mais comum presenciada pelos participantes da pesquisa foi o simples encorajamento da instituição às pessoas de tomarem cuidado com riscos de segurança, foram 23 participantes (57,5%) que selecionaram este item. Essa prática, embora simples, pode ser efetiva na conscientização e prevenção de incidentes de segurança.

A segunda prática mais comum foi a divulgação de boas práticas por meio de pôsteres, anúncios, vídeos e/ou boletins, com um total de 11 alunos (27,5%) que selecionaram esta opção. Esta forma de comunicação visual pode ajudar a disseminar informações importantes sobre segurança da informação.

Logo após, 10 alunos (25%) selecionaram os treinos de conscientização de segurança como uma prática educativa que vivenciaram. Esses treinamentos têm um potencial significativo para evitar incidentes, pois fornecem conhecimento prático e hábitos recomendados aos participantes.

Em penúltimo, apenas 7 alunos (17,5%) destacaram a existência de políticas de classificação de informações e dados nas instituições que frequentaram. Embora seja uma prática importante, pode haver falta de divulgação adequada dessas políticas, resultando em desconhecimento por parte dos indivíduos.

E por fim, a prática de educação em menor evidência foram as palestras por especialistas convidados a respeito de segurança da informação e comportamento do usuário, sendo apontada por apenas 6 (15%) dos participantes. Esta prática pode exigir um esforço maior da instituição, mas talvez possa ser a mais impactante, visto que uma explicação e apresentação mais humanizada pode chamar mais atenção dos usuários do que qualquer outra prática de protocolo ou apenas por escrito.

Esses resultados indicam que existem diferentes práticas de educação em segurança da informação sendo adotadas, mas algumas podem ser mais comuns do que outras. É importante que as instituições continuem aprimorando suas estratégias de educação em segurança da informação, utilizando uma combinação de abordagens para garantir uma conscientização adequada e promover bons hábitos de segurança entre seus funcionários e alunos.

Como a pesquisa não especifica o momento em que as práticas de educação em segurança da informação foram vivenciadas pelos participantes, não é possível afirmar se

ocorreram durante o curso de graduação em Biblioteconomia ou em outro contexto. As informações fornecidas na pesquisa são baseadas nas experiências gerais dos participantes em diferentes instituições que frequentaram, sem distinção específica em relação à área de estudo.

Estas são todas práticas recomendadas por Borkovich e Skovira (2019), mas o principal ponto dessas recomendações é construir uma cultura de segurança de forma geral, o que não é tarefa fácil ou simples. O autor Gonçalves (2019) apontou que para realmente proteger uma organização, são necessários conhecimento, compreensão, aceitação e competência em termos de tecnologia e seguridade.

4.4 Síntese de resultados

A pesquisa abordou questões relacionadas à segurança da informação e hábitos dos estudantes em relação a essa área. Foram coletados dados demográficos dos participantes e dados sobre o uso de senhas, configurações de senhas, realização de *backups*, utilização de aplicativos antivírus, comportamento diante de avisos de segurança, aceitação ou rejeição de *cookies* e práticas de educação em segurança da informação vivenciadas pelos participantes.

Na questão das senhas, verificou-se que a maioria dos estudantes utiliza algum mecanismo de autenticação, como senhas de acesso. No entanto, alguns alunos ainda possuem senhas fracas e simples, o que os torna vulneráveis a ataques de força bruta.

Quanto aos *backups*, constatou-se que a metade dos participantes realiza *backups* regularmente e os armazena na nuvem, enquanto outros optam por dispositivos externos. No entanto, uma parcela significativa não realiza *backups*, o que coloca seus dados em risco.

No que diz respeito aos aplicativos antivírus, a maioria dos estudantes utiliza-os em seus computadores, mas uma proporção considerável não utiliza nenhum tipo de aplicativo de antivírus em seus dispositivos.

A pesquisa também revelou que a atitude dos estudantes diante dos avisos de segurança varia, com alguns verificando e agindo adequadamente, outros evitando a continuidade na página que gerou o alerta, alguns ignorando os avisos e até mesmo desligando as notificações.

No contexto dos *cookies*, observou-se que os participantes têm diferentes posturas, desde aceitar todos até rejeitá-los completamente. Alguns estudantes leem as descrições e selecionam os *cookies* cautelosamente, enquanto outros simplesmente ignoram as mensagens.

Finalmente, em relação às práticas de educação em segurança da informação vivenciadas, destacaram-se em ordem do mais popular até o menos popular: o encorajamento para cuidados de segurança, a divulgação de práticas positivas, os treinos de conscientização,

as políticas de classificação de informações e por último as palestras por especialistas convidados.

Em resumo, diante dos dados coletados, a pesquisa evidencia a importância de medidas de segurança da informação, como o uso de senhas fortes, realização de *backups*, utilização de aplicativos antivírus e cuidados com *cookies*. Além disso, ressalta a relevância da educação em segurança da informação, pelo uso de práticas adotadas por instituições, conscientização dos usuários e divulgação de informações claras e acessíveis.

5 CONSIDERAÇÕES FINAIS

Em suma, se procede para apresentar a recopilação das conquistas, limitações, reconsiderações alcançadas com este estudo, assim como verificar as relações entre os dados e a teoria pesquisada. A presente monografia tinha como objetivo geral identificar o comportamento dos alunos do curso de Biblioteconomia da UnB a respeito da segurança da informação no meio digital. Com base na fundamentação teórica, foi possível identificar as principais ameaças e vulnerabilidades sobre os dados dos usuários da informação, sendo descritos vários programas maliciosos, técnicas de manipulação e os diferentes tipos de cibercriminosos que as empregam. Não apenas ameaças, mas também formas de legislação existentes tanto nacionais quanto internacionais foram identificadas e explicadas. Também foi possível determinar múltiplas práticas que minimizem incidentes de segurança da informação, foram descritas várias práticas positivas, hábitos arriscados que permitem brechas e comprometem a segurança, assim como métodos de construir uma cultura de segurança de forma geral. Ainda através da fundamentação teórica, foram indicados elementos da mente humana e mecanismos de coleta de dados, demonstrando como a própria personalidade dos usuários pode ser utilizada para manipulá-los; os documentários comentados auxiliaram o estudo a identificar algumas das principais ferramentas utilizadas, muitas vezes difundidas pelo uso de propaganda; além do uso de *cookies*, um instrumento poderoso em determinar padrões de comportamento de usuários.

Em outra etapa, pelo auxílio do questionário, a pesquisa foi capaz de identificar as características sociodemográficas dos alunos do curso de Biblioteconomia da UnB, diversos fatores como idade, gênero, traços de personalidade, quais plataformas digitais se engajam e quanto tempo investem nelas foram determinados. Dados a respeito do comportamento dos alunos em relação às atitudes que garantem ou põem em risco a segurança da informação também foram alcançados. Além destes objetivos, o questionário de pesquisa ainda conseguiu determinar quais das principais ameaças e vulnerabilidades os alunos tinham conhecimento, e quais lhe eram desconhecidas, entre outros conhecimentos gerais. Entretanto, apesar destas conquistas, o mecanismo de questionário utilizado teve suas limitações, vez que não era capaz de cruzar dados entre questões diferentes, não sendo possível várias vezes determinar se alunos que responderam de determinada forma em uma questão, responderam de forma condizente em outra questão. Porém, ao menos esta limitação foi um pouco mitigada pelo uso de algumas questões opcionais em momentos específicos do questionário.

Dito isso, ainda sim foi possível verificar as relações entre as teorias estudadas e os resultados quantitativos da pesquisa. Várias vezes foram comprovadas as afirmações realizadas na teoria no estudo prático, por exemplo como Modic e Anderson (2014) alertaram sobre o quão comum era o hábito de usuários ignorarem alertas de segurança dos antivírus, o que foi de fato confirmado por uma porcentagem relevante de respostas nos dados do questionário. Já para exemplificar as limitações na análise das relações entre teorias e dados, podemos dizer que foi possível determinar que 20% da amostra se identificou com traço de personalidade do neuroticismo. Porém não foi possível conectar esse dado com os dados das respostas de questões sobre *phishing*, para verificar se a teoria de Halevi, Lewis e Memon que dizia existir uma relação entre estes fatores, ficaria evidente durante a pesquisa. Outra limitação da pesquisa foi a amostra pequena, possivelmente pela curta janela de tempo em que foi realizada, apenas entre 5 e 16 de junho, assim como o baixo engajamento da população, este segundo fator talvez fosse amenizado se houvesse alguma forma maior de incentivo para a participação.

Para concluir, segue a resposta para a questão inicial de **"como se apresenta o comportamento dos alunos do Curso de Biblioteconomia da UnB sobre segurança da informação e aspectos que a fomentam?"**: em média, os alunos tiveram resultados relativamente positivos, demonstrando certos comportamentos favoráveis em relação à cibersegurança, mesmo que ainda tenham conhecimento superficial sobre algumas questões; entretanto, uma porção substancial de alunos pareceu ter hábitos arriscados em relação à segurança da informação, abrindo caminho para vários incidentes no futuro. De toda forma, o estudo tornou evidente a necessidade de garantir maior atenção e cuidado em relação a esta temática, não apenas por parte dos alunos, mas das instituições também, vez que foi determinado seu papel na construção de uma cultura de segurança durante a fundamentação teórica. Seguem algumas recomendações a seguir, primeiramente aconselha-se a realização de mais pesquisas desta natureza, com instrumentos de pesquisa e coleta de dados mais avançados a fim de alcançar resultados ainda mais detalhados, se possível com maiores amostras; em segundo, sugere-se promover uma maior divulgação e conscientização a respeito desta problemática, através dos diversos métodos e práticas citados ao decorrer da pesquisa; e por último, ainda permanece a recomendação indicada previamente na justificativa, de integrar uma disciplina que trate especificamente da cibersegurança nos cursos da Ciência da Informação. Vez que uma disciplina desta categoria, mesmo que básica e/ou optativa, possivelmente ajudaria a reduzir o número de ocorrências de cibercrimes, auxiliando os alunos não apenas em sua carreira profissional, mas na sua qualidade de vida em geral.

REFERÊNCIAS

33GIGA. **Os 8 tipos mais comuns de ataques hackers.** 2022. Disponível em: Os 8 tipos mais comuns de ataques hackers - 33Giga. Acesso em: 22 maio 2023.

ADVISERA. **Como gerenciar vulnerabilidades técnicas de acordo com o controle A. 12.6.1 da ISO 27001.** 2015. Disponível em: Como gerenciar vulnerabilidades técnicas de acordo com o controle A.12.6.1 da ISO 27001 | 27001Academy (advisera.com). Acesso em: 03 maio 2023.

ALECRIN, E. **Malwares – O Que São E Como Agem.** Disponível em: Malwares: o que são e como agem (infowester.com). Acesso em: 19 abr. 2023

ALURA. **O que é cibersegurança: práticas e as equipes de segurança.** 2022. Disponível em: O que é cibersegurança: práticas e as equipes de segurança | Alura. Acesso em: 03 maio 2023.

ASER. **7 estatísticas de Segurança da Informação que precisam ser acompanhadas.** 2023. Disponível em: 7 estatísticas de Segurança da Informação que precisam ser acompanhadas – Aser Security. Acesso em dia: 16 jan. 2023.

ATLÂNTICO. **Os cinco pilares da segurança da informação.** 2021. 1 imagem. 608x356 pixels. Disponível em: Segurança da Informação - Instituto Atlântico (atlantico.com.br). Acesso em: 17 jan. 2023.

BARCELOS, N. **Os pilares da Segurança da Informação - Quais são e qual sua importância para uma segurança efetiva.** Tripla, 2019. Disponível em: Pilares da Segurança da Informação: o que você precisa saber! (tripla.com.br). Acesso em dia: 17 jan. 2023.

BARROS, B. **Privacidade na *Internet*: Como nossos dados são coletados?** Blog RASUFCG, 2021. Disponível em: Privacidade na *Internet*: Como nossos dados são coletados? - (ieee.org). Acesso em: 21 maio 2023.

BERTOLLI, E. **Conheça as principais estatísticas em segurança digital para 2020.** Varonis, 2019. Disponível em: Conheça as principais estatísticas em segurança digital para 2020 (varonis.com). Acesso em dia: 16 jan. 2023.

BORKOVICH, D. J.; SKOVIRA, R. J. Cybersecurity inertia and social engineering: Who's worse, employees or hackers? **Issues in Information Systems**, v. 20, n. 3, 2019. Disponível em: Cybersecurity-Inertia-and-Social-Engineering-Whos-Worse-Employees-or-Hackers.pdf (researchgate.net). Acesso em dia: 30 mar. 2023.

BRASIL. **Lei Nº 13.709, de 14 de agosto de 2019.** Dispõe sobre a proteção de dados pessoais (LGPD). Diário Oficial da União. Brasília, DF. 2019. Disponível em: L13709 (planalto.gov.br). Acesso em: 16 jan. 2023.

BUGHUNT. **Quais são os principais tipos de hackers?** 2022. Disponível em: Quais são os principais tipos de hackers? (bughunt.com.br). Acesso em: 21 maio 2023.

CREESE, S.; SAUNDERS, J.; AXON, L.; DIXON, W. **Future series: Cybersecurity, emerging technology and systemic risk.** In: World Economic Forum. [S.l.: s.n.], 2020.

DIAS, P. R. S. **Prevenir um Ataque de Phising.** Tese (Doutorado), 2021.

FERNANDES, M. **Modelo Big Five: conheça os cinco fatores da personalidade.** Católica de Pelotas, 2022. Disponível em: Modelo Big Five: conheça os cinco fatores da personalidade! (ucpel.edu.br). Acesso em dia: 29 mar. 2023.

FORTIFIREWALL. **Cinco ciberataques a serem observados em 2022.** Blog Forti Firewall, 2022. Disponível em: Cinco ciberataques a serem observados em 2022 | Blog Forti Firewall. Acesso em: 20 mar. 2023.

GATInfoSec. **5 Pilares da Segurança da Informação.** c2020. Disponível em: 5 Pilares de Segurança da Informação nas Empresas (gatinfosec.com). Acesso em: 21 maio 2023.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 6ª edição. São Paulo: Atlas, 2008.

GONÇALVES, R. S. **O fator humano da cibersegurança nas organizações.** Tese (Doutorado) — Universidade de Lisboa (Portugal), 2019.

GRATIAN, M.; BANDI, S.; CUKIER, M.; DYKSTRA, J.; GINTHER, A. Correlating human traits and cyber security behavior intentions**. Computers Security**, v. 73, p. 345-358, 2018. ISSN 0167-4048. Disponível em: Correlating human traits and cyber security behavior intentions - ScienceDirect. Acesso: 20 mar. 2023.

HADLINGTON, L. **Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours.** Heliyon, Elsevier Ltd, England, v. 3, n. 7, p. e00346-e00346, 2017. ISSN 2405-8440.

HALEVI, T.; LEWIS, J.; MEMON, N. A pilot study of cyber security and privacy related behavior and personality traits. In: **Proceedings of the 22nd international conference on world wide web.** [S.l.: s.n.], 2013. p. 737-744.

LAHCEN, R. A. M.; CAULKINS, B.; MOHAPATRA, R.; KUMAR, M. **Review and insight on the behavioral aspects of cybersecurity.** Cybersecurity, Springer Singapore, Singapore, v. 3, n. 1, p. 1-18, 2020. ISSN 2523-3246.

LéVESQUE, F. L.; CHIASSON, S.; SOMAYAJI, A.; FERNANDEZ, J. M. **Technological and human factors of malware attacks**: A computer security clinical trial approach. ACM Trans. Priv. Secur., Association for Computing Machinery, New York, NY, USA, v. 21, n. 4, jul 2018. ISSN 2471-2566. Disponível em: https://doi.org/10.1145/3210311. Acesso em: 19 abr. 2023

LI, Q. **Mobile Security: Threats and Best Practices.** Hindawi, 2020. Disponível em: Mobile Security: Threats and Best Practices (hindawi.com). Acesso em: 20 mar. 2023.

LINKEDIN. **Desvendando os ataques dos hackers.** 2022. Disponível em: Ataque hacker: veja os principais tipos e como se proteger (linkedin.com). Acesso em: 22 maio 2023.

MARCELO, A.; PEREIRA, M. **A Arte de Hackear Pessoas.** Rio de Janeiro: Brasport. 2005.

MARCONI, M. A.; Lakatos, Eva Maria. **Fundamentos de metodologia científica.** 5ª edição. São Paulo: Atlas, 2003.

MITNICK, K. D.; SIMON, W. L. **A arte de enganar.** 1 ed. São Paulo: Pearson Education do Brasil, 2003.

MODIC, D.; ANDERSON, R. **Reading this may harm your computer**: The psychology of malware warnings. Computers in Human Behavior, v. 41, p. 71-79, 2014. ISSN 0747-5632. Disponível em: Reading this may harm your computer: The psychology of malware warnings - ScienceDirect. Acesso em: 19 abr. 2023

MORESI, E. (Org.). **Metodologia da Pesquisa.** Brasília: [s. n.], 2003. 108 p.

NOBLES, C. **Stress, burnout, and security fatigue in cybersecurity**: A human factors problem. Holistica: Journal of business and public administration, Sciendo, v. 13, n. 1, p. 49-72, 2022. ISSN

2067-9785. Disponível em: (PDF) Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem (researchgate.net). Acesso em: 18 abr. 2023.

NORTON. **O que é um vírus de computador?** Disponível em: O que é um vírus de computador? (norton.com). Acesso em dia: 19 abr. 2023.

O DILEMA das Redes. Direção: Jeff Orlowski. Produção: Larissa Rhodes. Intérpretes: Skyler Gisondo, Kara Hayward, Vincent Kartheiser et al. Estados Unidos: Netflix, 2020.

PALMIERI, M.; SHORTLAND, N.; MCGARRY, P. **Personality and online deviance**: The role of reinforcement sensitivity theory in cybercrime. Computers in human behavior, Elsevier, v. 120, p. 106745, 2021.

PARSONS, K.; CALIC, D.; PATTINSON, M.; BUTAVICIUS, M.; MCCORMAC, A.; ZWAANS, T. **The human aspects of information security questionnaire (hais-q)**: Two further validation studies. Computers Security, v. 66, p. 40-51, 2017. ISSN 0167-4048. Disponível em: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies - ScienceDirect. Acesso em: 22 maio 2023

PEIXOTO, M. C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006.

PERALLIS SECURITY. **A história da segurança da informação: mais de um século protegendo conhecimento.** Disponível em: A história da segurança da informação: mais de um século protegendo conhecimento — Perallis Security. Acesso em dia: 19 jan. 2023.

PRIVACIDADE Hackeada. Direção: Karim Amer, Jehane Noujaim. Produção: Jehane Noujaim, Karim Amer, Pedro Kos, Geralyn Dreyfous, Judy Korin. Intérpretes: Carole Cadwalladr, David Carroll, Brittany Kaiser. et al. Estados Unidos: Netflix, 2019.

RAHMAN, T.; ROHAN, R.; PAL, D.; KANTHAMANON, P. Human factors in cybersecurity: a scoping review. In: **The 12th International Conference on Advances in Information Technology.** [S.l.: s.n.], 2021. p. 1-11.

RAZAQUE, A.; AJLAN, A. A.; MELAOUNE, N.; ALOTAIBI, M.; ALOTAIBI, B.; DIAS, I.; OAD, A.; HARIRI, S.; ZHAO, C. **Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled cybersecurity awareness system.** Applied Sciences, v. 11, n. 17, 2021. ISSN 2076-3417. Disponível em: Applied Sciences | Free Full-Text | Avoidance of Cybersecurity Threats with the Deployment of a Web-Based Blockchain-Enabled Cybersecurity Awareness System (mdpi.com). Acesso em 22 maio 2023

SARACEVIC, T. Information Science**. JASIS – Journal of the American Society for Information Science**, v. 50, n. 12, p. 1051-1063, 1999.

SCHULTZ, E. The human factor in security. **Computers Security**, v. 24, n. 6, p. 425-426, 2005. ISSN 0167-4048. Disponível em: The human factor in security - ScienceDirect. Acesso em: 16 jan. 2023.

SENHASEGURA. **Os pilares da Segurança da Informação.** 2021. Disponível em: Os pilares da Segurança da Informação - senhasegura. Acesso em dia: 17 jan. 2023.

SIKDER, R.; KHAN, M. S.; HOSSAIN, M. S.; KHAN, W. Z. **A survey on android security**: development and deployment hindrance and best practices. TELKOMNIKA (Telecommunication Computing Electronics and Control), v. 18, n. 1, p. 485-499, 2020.

SILVA, D. R. P.; STEIN, L. M. **Segurança da informação**: uma reflexão sobre o componente humano. Ciências & Cognição, Porto Alegre, v. 10, p. 46-53, 12 mar. 2007 1806-5821. Disponível em: Reflexão sobre o componente humano.pdf. Acesso em dia: 15 jan. 2023.

SILVA, E.; MENEZES, E. **Metodologia da pesquisa e elaboração de dissertação.** 4. ed. rev. e atual. Florianópolis: [s. n.], 2005.

UNISYS. **Ataques cibernéticos — O que você precisa saber.** 2023. Disponível em: O que é um ataque cibernético? | Definição de ataque cibernético | Unisys. Acesso em: 03 maio 2023.

UNIVERSIDADE DE BRASÍLIA. FACULDADE DE CIÊNCIA DA INFORMAÇÃO. **Projeto Pedagógico do Curso de Biblioteconomia.** Brasília, 2018. Objetivo geral do curso.

VAULTONE. **Como funciona um ciberataque de RDP (Remote Desktop Protocol).** 2021. Disponível em: Como funciona um ciberataque de RDP (Remote Desktop Protocol) - VaultOne - PAM Vendor. Acesso em: 22 maio 2023.

VERGARA, S. **Projetos e relatórios de pesquisa em administração.** 5. ed. São Paulo: Atlas, 2004. Disponível em: https://unbbr.sharepoint.com/:b:/s/ProjetodeEstudodeUsurios/EVHIagj_2SVOl14KJvuBAHoBSKcX6a-rfilbuowmQ4NDDg?e=ATT1M3. Acesso em: 06 abr. 2022.

WEICHBROTH, P.; ŁYSIK, Ł. **Mobile security**: Threats and best practices. Mobile Information Systems, Hindawi, v. 2020, 2020. Disponível em: Mobile Security: Threats and Best Practices (hindawi.com). Acesso em: 17 jan. 2023.

WENDT, E. JORGE, H. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 2012. Ed. Brasport, Rio de Janeiro.

ZANELLA, L. **Metodologia de pesquisa.** 2. ed. rev. e atual. Florianópolis: Departamento de Ciências da Administração/UFSC, 2011. 134 p. Disponível em: untitled (atfcursosjuridicos.com.br). Acesso em: 05 abr. 2023.

APÊNDICE 1

Pesquisa sobre segurança da informação

Esse questionário faz parte do trabalho de conclusão de curso sobre segurança da informação, desenvolvido pelo aluno Igor Lukas e orientado pela professora Fernanda Farinelli.

Visa coletar dados para a finalização do TCC de Biblioteconomia da UnB, sendo o objetivo identificar o grau de conhecimento dos alunos do curso de Biblioteconomia da UnB sobre segurança da informação, as leis que os protegem e seus direitos.

Caso não seja estudante de Biblioteconomia na UnB, por favor, desconsiderar.

Tempo estimado para responder o formulário: 12 minutos

* Indica uma pergunta obrigatória

Caracterização da amostra

1. 1. Qual sua idade? *

Marcar apenas uma oval.

- ◯ 17 - 19
- ◯ 20 - 22
- ◯ 23 - 25
- ◯ 26+

2. 2. Qual seu gênero? *

Marcar apenas uma oval.

- ◯ Feminino
- ◯ Masculino
- ◯ Outro: _____

3. 3. Em qual semestre você está? *

Marcar apenas uma oval.

- ◯ 1º - 2º semestre
- ◯ 3º - 4º semestre
- ◯ 5º - 6º semestre
- ◯ 7º - 8º semestre
- ◯ 9º+ semestre

4. 4. Em que ano você ingressou no curso de biblioteconomia? *

Marcar apenas uma oval.

- ◯ 2013
- ◯ 2014
- ◯ 2015
- ◯ 2016
- ◯ 2017
- ◯ 2018
- ◯ 2019
- ◯ 2020
- ◯ 2021
- ◯ 2022
- ◯ 2023

5. 5. Quais plataformas digitais você utiliza? *

Marque todas que se aplicam.

- [ ] WhatsApp
- [ ] YouTube
- [ ] Instagram
- [ ] Facebook
- [ ] TikTok
- [ ] LinkedIn
- [ ] Messenger
- [ ] Kwai
- [ ] Pinterest
- [ ] Twitter
- [ ] Nenhuma
- [ ] Outro: _____

6. 6. Quanto tempo diariamente você gasta navegando pelas plataformas digitais? *

Marcar apenas uma oval.

- ◯ Não utilizo
- ◯ Utilizo as plataformas digitais até 1 hora por dia
- ◯ Utilizo as plataformas digitais acima de 1 hora até 2 horas por dia
- ◯ Utilizo as plataformas digitais acima de 2 horas até 5 horas por dia
- ◯ Utilizo acima de 5 horas por dia

7. 7. Existem cinco principais traços de personalidade na psicologia conhecidos como "Big Five", com quais deles você se identifica? *

Marque todas que se aplicam.

- [ ] Abertura à experiencia: determina o interesse por novas vivências, são pessoas aventureiras, curiosas e imaginativas, com ideias incomuns.
- [ ] Conscienciosidade: define o grau de autocontrole sobre emoções e impulsos, são pessoas com comportamento mais planejado, possuem forte autodisciplina e foco nos objetivos.
- [ ] Extroversão: indica a tendência de se envolver com outras pessoas e o mundo exterior, são pessoas sociáveis, animadas e dispostas a criar novas relações.
- [ ] Agradabilidade: aponta o nível de simpatia e cooperação com os outros, costumam ter boas relações e serem respeitosos, amigáveis e prestativos.
- [ ] Neuroticismo: este fator mede a tendência de sentir emoções negativas como raiva, ansiedade e depressão constantemente. Pessoas neuróticas são pessoas reativas e instáveis emocionalmente.

8. 8. Você já foi diagnosticado com Transtorno de Déficit de Atenção (TDAH)? *

Marcar apenas uma oval.

- ◯ Já fui diagnosticado com TDAH
- ◯ Nunca fui diagnosticado com TDAH

9. 9. Qual você considera ser seu grau de atenção durante execução das tarefas do cotidiano? *

Marcar apenas uma oval.

Baixo

1 ⬭

2 ⬭

3 ⬭

4 ⬭

5 ⬭

Alto

Conhecimentos gerais

10. 10. Você conhece o termo cybersegurança (também conhecido como segurança da informação)? *

Marcar apenas uma oval.

⬭ Sim

⬭ Não

11. 11. Caso conheça, qual você diria que é seu grau de conhecimento sobre cybersegurança?

Caso tenha respondido "não" na questão anterior, ignorar esta questão.

Marcar apenas uma oval.

Superficial

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Aprofundado

12. 12. A Lei Geral de Proteção de Dados Pessoais (LGPD) e o Regulamento Geral sobre a Proteção de Dados (GDPR) são algumas formas de legislação vigentes mais importantes para garantir os direitos e a proteção dos dados de cidadãos. Você conhece alguma dessas leis? *

Marcar apenas uma oval.

◯ Nunca ouvi falar de nenhuma dessas leis

◯ Conheço apenas a LGPD

◯ Conheço apenas a GDPR

◯ Conheço ambas as leis citadas

13. 13. Você está ciente dos seus direitos perante a Lei Geral de Proteção de Dados Pessoais (LGPD) a respeito dos seus dados? *

Marcar apenas uma oval.

- ◯ Não, desconheço os direitos garantidos por essa lei
- ◯ Sim, estou ciente dos direitos que tenho através essa lei

14. 14. Quais dessas ameaças virtuais você conhece? *

Marque todas que se aplicam.

- ☐ Vírus
- ☐ Spyware
- ☐ Ramsonware
- ☐ Trojan/cavalo de troia
- ☐ Phishing
- ☐ RDP (Protocolo de Desktop Remoto)
- ☐ Backdoor
- ☐ Keylogger
- ☐ Ataque DoS/DDoS
- ☐ Port Scanning
- ☐ Quebra de força bruta
- ☐ Cryptojacking
- ☐ Zero Day
- ☐ Não conheço nenhuma
- ☐ Outro: _____

15. 15. Você adota medidas para evitar essas ameaças? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

Experiência pessoal

16. 16. Você já sofreu algum tipo de golpe em plataformas digitais? *

São consideradas plataformas digitais e-mail, SMS, redes sociais e ligações telefônicas.

Marque todas que se aplicam.

- [ ] Já fui vítima de golpe que me causou prejuízo financeiro
- [ ] Já fui vítima de golpe que me causou prejuízo material
- [ ] Já fui vítima de golpe que me fez perder acesso à conta de rede social
- [ ] Nunca sofri nenhum tipo de golpe em plataformas digitais

17. 17. Caso você tenha sofrido algum tipo de golpe, por meio de qual plataforma digital este golpe ocorreu?

Caso nunca tenha sofrido golpe em plataformas digitais, ignorar esta questão.

Marque todas que se aplicam.

- [ ] E-mail
- [ ] SMS
- [ ] Rede social
- [ ] Ligação telefônica

18. 18. Você já se viu vítima de algum destes truques de engenharia social (manipulação do comportamento)? *

Marque todas que se aplicam.

- [ ] Pretexto: o criminoso finge ser amigável ou uma figura de autoridade, como um policial ou funcionário de uma grande empresa. Através do disfarce, estabelece confiança com a vítima por meio digital, telefone ou pessoalmente, em seguida tenta extrair dados pessoais ou informações financeiras.
- [ ] Phishing: mensagens que aplicam fingimento, confiança e a vontade de clicar para incentivar os destinatários a divulgar informações pessoais, como palavras passe ou detalhes de cartões de crédito. Essas mensagens podem vir em formato de e-mail, chamadas telefónicas, mensagens de texto ou mensagens de rede social.
- [ ] Isca: faz uso do aliciamento ou medo de falhar (FOMO) para incentivar determinados comportamentos, Como oferecer presentes gratuitos ao usuário de um site caso forneça informações, senhas pessoais ou clique em links ou botões suspeitos.
- [ ] Nunca fui vítima de nenhum destes métodos.

19. 19. Você bloqueia seus dispositivos por meio de algum mecanismo de autenticação (ex. senha, biometria, etc.)? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

Para as questões 20 até 28, marque de acordo com seu nível de concordância com as respectivas afirmações.

20. 20. Considero prudente abrir um e-mail de fonte desconhecida a fim de determinar seu assunto e o conteúdo que ele carrega. *

Marcar apenas uma oval.

Discordo completamente	
1	◯
2	◯
3	◯
4	◯
5	◯
Concordo completamente	

21. 21. Considero prudente clicar/abrir em links, arquivos, vídeos, anexos recebidos de fonte desconhecida. *

Marcar apenas uma oval.

Discordo completamente

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Concordo completamente

22. 22. Tenho a preocupação de ler a respeito das permissões e classificações de aplicativos antes de instala-los. *

Marcar apenas uma oval.

Discordo completamente

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Concordo completamente

23. 23. Desativo funções como Bluetooth, Wi-Fi, GPS e outros quando não estão sendo usados. *

Marcar apenas uma oval.

Discordo completamente

1 ◯
2 ◯
3 ◯
4 ◯
5 ◯

Concordo completamente

24. 24. Desinstalo aplicativos que considero desnecessários ou que não acho mais relevantes. *

Marcar apenas uma oval.

Discordo completamente

1 ◯
2 ◯
3 ◯
4 ◯
5 ◯

Concordo completamente

25. 25. Separo minhas atividades entre meu e-mail profissional e meu e-mail pessoal. *

Marcar apenas uma oval.

Discordo completamente

1 ⬭

2 ⬭

3 ⬭

4 ⬭

5 ⬭

Concordo completamente

26. 26. Acredito que utilizar a internet para efetuar downloads de filmes, músicas e outras mídias de fontes não autenticas não representa ameaça para meus dados. *

Marcar apenas uma oval.

Discordo completamente

1 ⬭

2 ⬭

3 ⬭

4 ⬭

5 ⬭

Concordo completamente

27. 27. Compartilho senhas de acesso de meus dispositivos com outras pessoas. *

Marcar apenas uma oval.

	Discordo completamente
1	
2	
3	
4	
5	
	Concordo completamente

28. 28. Utilizo configurações de senhas fortes e complexas. *

Senhas fortes e complexas seriam senhas com variação entre letras minúsculas e maiúsculas, com uso de elementos numéricos e caracteres especiais.

Marcar apenas uma oval.

	Discordo completamente
1	◯
2	◯
3	◯
4	◯
5	◯
	Concordo completamente

29. 29. Você utiliza a mesma senha em diferentes plataformas, redes sociais e aplicativos? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

30. 30. Você efetua regularmente cópias de dados importantes (backups)? *

Marcar apenas uma oval.

- ◯ Sim, armazeno os dados na rede
- ◯ Sim, armazeno os dados no meu dispositivo
- ◯ Sim, armazeno os dados em dispositivo externo (ex. pendrive)
- ◯ Não realizo cópias de segurança

31. 31. Você utiliza aplicativos de antivírus? *

Marcar apenas uma oval.

- ◯ Sim, apenas no computador
- ◯ Sim, apenas no dispositivo móvel (ex. celular, tablet)
- ◯ Sim, tanto no computador quanto no dispositivo móvel (ex. celular, tablet)
- ◯ Não utilizo aplicativos de antivírus

32. 32. Fazendo uma autoavaliação, descreva o seu comportamento perante os avisos de aplicativos de segurança. *

Marcar apenas uma oval.

- ◯ Verifico os avisos, prosseguindo para realizar uma varredura pelo antivírus
- ◯ Verifico os avisos e evito continuar na página, porém não realizo varredura
- ◯ Ignoro os avisos de segurança
- ◯ Desligo as notificações do antívirus

33. 33. Caso sua postura seja de ignorar ou desligar as notificações de segurança do antivírus, gostaríamos de entender qual percepção orienta sua abordagem. Caso contrário, ignore esta questão.

Marcar apenas uma oval.

- ◯ Não acredito que as ameaças identificadas representam perigo substancial
- ◯ Reconheço o perigo das ameaças, porém não me importo
- ◯ Acredito que meu aplicativo de antivírus pode não estar funcionando corretamente

34. 34. É muito comum hoje em dia uma página online oferecer cookies de navegação sempre que acessamos ela pela primeira vez, qual a sua postura em relação a esta prática? *

Marcar apenas uma oval.

- ◯ Aceito todos os cookies
- ◯ Rejeito todos os cookies possíveis e deixo a página
- ◯ Rejeito todos os cookies possíveis, porém continuo navegando na página
- ◯ Leio as descrições dos cookies, selecionando quais aceitar ou rejeitar
- ◯ Ignoro as mensagens sobre cookies quando possível

35. 35. Em alguma escola ou instituição que você já estudou ou trabalhou, houveram alguma dessas práticas de educação em relação a bons hábitos de segurança? *

Marque todas que se aplicam.

- ☐ Treinos de conscientização de segurança
- ☐ Políticas de classificação de informações e dados
- ☐ Qualquer tipo de encorajamento aos funcionários/alunos a tomarem cuidado com riscos de segurança
- ☐ Divulgação de boas práticas através de pôsteres, anúncios, vídeos e/ou boletins
- ☐ Especialistas convidados que apresentem palestras a respeito de segurança da informação e comportamento do usuário