SEGURANÇA DA INFORMAÇÃO: PERCEPÇÃO DO PÚBLICO EM GERAL

INFORMATION SECURITY: GENERAL PUBLIC PERCEPTION

Kaick Juscelino Silva

Bacharelando em Engenharia da Computação pelo Centro Universitário de Tecnologia de Curitiba (UNIFATEC)

Instituição: Centro Universitário de Tecnologia de Curitiba (UNIFATEC)

Endereço: R. Itacolomi, 449, Portão, Curitiba - PR, CEP: 81070-150

E-mail: Kaickjuscelino12@gmail.com

Marjori Klinczak

Mestre em Computação Aplicada pela Universidade Tecnológica Federal do Paraná (UTFPR)

Instituição: Centro Universitário de Tecnologia de Curitiba (UNIFATEC)

E-mail: marjori.klinczak@unifatecpr.com.br

RESUMO

Este trabalho tem como objetivo analisar a percepção do público em geral em relação à segurança da informação, tema cada vez mais relevante diante do crescimento do uso de dispositivos digitais e do aumento das ameaças cibernéticas. A pesquisa busca compreender o nível de conhecimento, atitudes e visão dos usuários no que se refere à proteção de dados e à adoção de medidas preventivas. Para isso, foi aplicado um questionário entre os dias 25 e 28 de maio de 2025 para um grupo diversificado de participantes, abordando aspectos como o uso de senhas, atualizações de sistemas, reconhecimento de ameaças e comportamento em ambientes digitais.

Palavras-chave: Segurança da Informação, Proteção de Dados, Ameaças Cibernéticas, Comportamento Digital.

ABSTRACT

This study aims to analyze the general public's perception regarding information security, a topic that is becoming increasingly relevant due to the growing use of digital devices and the rise in cyber threats. The research seeks to understand users' level of knowledge, attitudes, and perspectives related to data protection and the adoption of preventive measures. To this end, a questionnaire was administered between May 25 and 28, 2025, to a diverse group of participants, addressing aspects such as password

usage, system updates, threat recognition, and behavior in digital environments. Keywords: Information Security, Data Protection, Cyber Threats, Digital Behavior.

1 INTRODUÇÃO

Em levantamento produzido pela TIC Domicílios 2023 e noticiado pelo G1, mostrou-se que 84% da população brasileira com 10 anos ou mais tem acesso à internet, o que representa 156 milhões de usuários, o mesmo cenário no ano anterior era de 81%.

Diante dessa realidade, esta pesquisa tem como ponto de partida uma pergunta essencial: *Como o público em geral percebe a segurança da informação?*

O principal objetivo é realizar um estudo preliminar, a partir de uma amostra e compreender essa percepção por meio da aplicação de um questionário, onde será feito o cruzamento de dados obtidos por meio do formulário online e feita uma análise, como por exemplo, qual faixa etária é mais cuidadosa com dados, qual grupo o mais participativo etc.

A motivação para este estudo preliminar nasce da crescente onda de ameaças digitais enfrentadas por usuários, onde cada vez mais surgem notícias sobre vazamentos de dados. Casos como o da Netshoes, que em 2018 teve dados de aproximadamente dois milhões de clientes expostos (KASPERSKY, 2023), ilustram bem os riscos envolvidos.

Esse cenário ganha contornos ainda mais preocupantes quando se olha para os números: de acordo com Oliveira (2022), “o Brasil registou um aumento de 94% nos ataques cibernéticos apenas no primeiro semestre de 2022, com cerca de 31,5 bilhões de tentativas de invasão, sendo o segundo país mais visado da América Latina”.

Com os dados recolhidos por meio da pesquisa, espera-se identificar pontos de fragilidade na percepção e nos comportamentos dos usuários, o que em trabalhos futuros permitirá sugerir ações concretas de conscientização e estudo.

2 REFERENCIAL TEÓRICO

A segurança da informação está profundamente conectada à maneira como os sistemas de informação são estruturados e utilizados nas organizações, eles são a espinha dorsal da gestão de dados e processos internos. Como explica Risco (2024), um

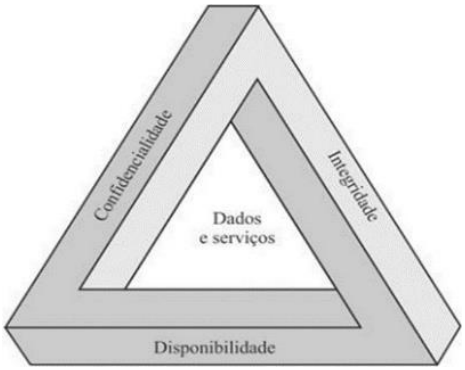
sistema de informação pode ser entendido como a combinação de elementos que se interligam para formar um todo funcional, podendo assumir formas concretas ou abstratas.

Um sistema de informação é, basicamente, um conjunto de elementos que colaboram entre si para recolher, tratar, guardar e partilhar informações, ajudando as pessoas e as organizações a tomar decisões com mais segurança e eficiência.

Entre os diferentes tipos de sistemas, Rezende (2005, p. 34) propõe uma classificação clara: os Sistemas de Informação Operacionais (SIO), voltados para o controle de atividades essenciais da organização; os Sistemas de Informação Gerenciais (SIG), que sintetizam dados para apoiar decisões estratégicas de gestores; e os Sistemas de Informação Estratégicos (SIE), que atuam em uma visão mais ampla, analisando informações considerando o ambiente organizacional interno e externo.

No que se refere à segurança da informação, são muitas as abordagens e ferramentas disponíveis para garantir que os dados estejam protegidos. Stallings e Brown (2014) apontam que toda estratégia de proteção deve estar fundamentada na chamada tríade CID: Confidencialidade, Integridade e Disponibilidade. Esses três pilares formam a base da segurança digital, como apresentado na Figura 1, garantindo que as informações estejam acessíveis apenas para quem deve, permaneçam íntegras e estejam disponíveis sempre que necessário.

Figura 1: Tríade de requisitos de segurança



Fonte: Stallings e Brown, 2014.

Segurança da Informação e Ataques Cibernéticos

Como explicam Stallings e Brown (2014), a confidencialidade garante que apenas pessoas autorizadas possam acessar determinadas informações; a integridade

assegura que os dados permaneçam inalterados sem consentimento; e a disponibilidade refere-se à acessibilidade dos dados e serviços para quem de fato tem permissão de uso.

É o que aponta Batista (2004), ao destacar que apenas após o "primeiro acidente" é que as organizações passam a perceber a real importância da proteção da informação. Essa fragilidade é aproveitada por criminosos digitais. Segundo Almeida (2018), "crackers utilizam a internet para espalhar *malwares* com o objetivo de obter informações ou ganhos financeiros".

Tipos de Ataques Cibernéticos

O *phishing* é um tipo de golpe cada vez mais comum e sofisticado. Olivo (2010) define essa prática como uma forma de *engenharia social*, que visa enganar a vítima para obter informações pessoais ou financeiras. Assolini, da Kaspersky (apud KASPERSKY, 2023), afirma que esse é o ataque mais popular justamente por ser barato e fácil de executar. Microsoft (2022) alerta para sinais típicos: links suspeitos, erros de ortografia e remetentes estranhos, que devem ser reconhecidos por todos os colaboradores da empresa, e não apenas pelos profissionais de TI.

Os *malwares* são softwares desenvolvidos com a intenção de prejudicar sistemas, roubar dados ou comprometer o funcionamento de dispositivos. Valenga (2018) define *malware* como um código malicioso que afeta diretamente o desempenho e a segurança de computadores, *smartphones* e outros equipamentos. Segundo a Kaspersky (2023), o Brasil regista mais de 1.500 tentativas de infecção por minuto, o que evidencia a necessidade de medidas preventivas como o uso de antivírus, *firewalls* e a conscientização dos utilizadores.

Entre os ataques mais destrutivos, destaca-se o *ransomware*, que "sequestra" dados e exige pagamento para sua liberação. Kaspersky (2023) relata que esse tipo de ataque utiliza criptografia para bloquear arquivos e sistemas inteiros, impedindo o acesso até que a vítima pague o resgate. Para Valenga (2018), o caso do WannaCry, que afetou empresas globalmente em 2017, é um marco que deixou clara a dimensão desse tipo de ameaça.

Já o ataque DDoS (*Distributed Denial of Service*) é voltado para interromper serviços. Chavez (2022) explica que esse ataque consiste em enviar milhares de requisições simultâneas a um servidor, fazendo com que ele fique sobrecarregado e saia

do ar. Os cibercriminosos utilizam *botnets* redes de computadores infectados — para coordenar essas ações, como descreveram McCarty (2003b) e Freiling et al. (2005). Existem variações como Flood, UDP Flood e NTP Flood, conforme destaca Ariane (2023).

Os ataques do tipo *Flood* se caracterizam por um volume anormal de solicitações enviadas a um servidor, com a intenção de sobrecarregar sua capacidade de resposta e torná-lo inacessível aos usuários legítimos (STAMMERS, 2019). Entre as variações desse tipo de ataque, destaca-se o *UDP Flood*, que explora o protocolo de datagramas do usuário (UDP) um meio de comunicação que permite o envio rápido de pacotes, mas sem estabelecer uma conexão formal. Essa característica é explorada para sobrecarregar o servidor, enviando um grande volume de solicitações até que ele fique extremamente lento ou pare de funcionar por completo.

Outra forma bastante conhecida é o *NTP Flood*, que também se baseia no envio massivo de pacotes, mas com um agravante: esses pacotes são aparentemente válidos, porém têm seus endereços de origem forjados. Isso gera uma sobrecarga ainda maior, pois o sistema tenta responder a múltiplas solicitações falsas, o que leva ao esgotamento de seus recursos e, muitas vezes, à queda total do serviço por repetidas falhas e reinicializações (SCHEINER, 2020).

3 METODOLOGIA

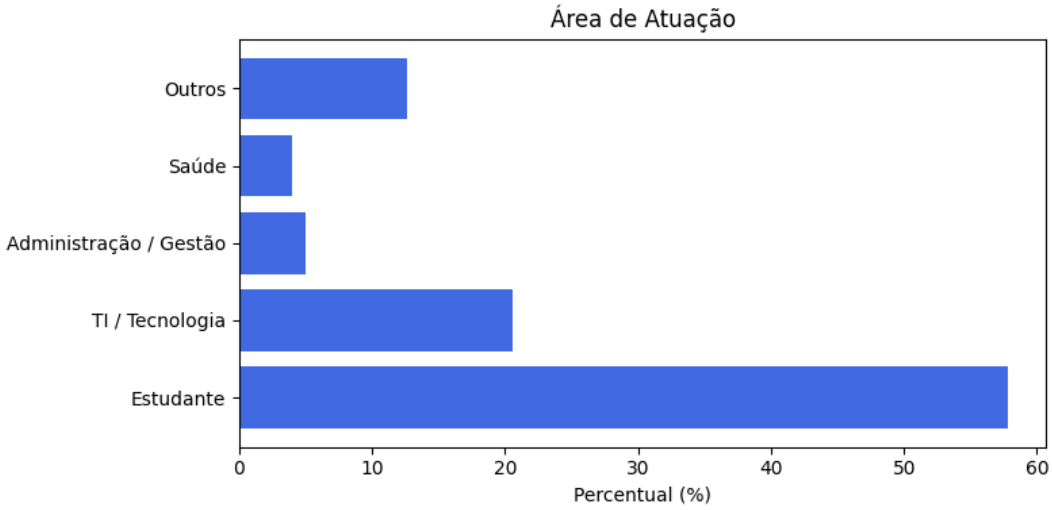
Este estudo preliminar foi baseado em uma mostra e construído a partir de uma metodologia que combinou pesquisa bibliográfica e aplicação de um formulário online entre os dias 25 e 28 de maio de 2025, realizado para o público em geral e compartilhado via redes sociais, onde foram aplicadas 14 questões, 13 delas fechadas e 1 aberta, que visava obter a visão de cada pessoa a respeito da segurança digital, nessa questão foram descartadas 46 respostas, visto que essas não apresentavam conteúdo para análise. Ao total foram recolhidas 102 respostas que ajudaram no desenvolvimento da análise. A respeito das 13 questões fechadas buscou-se respostas como: faixa etária, sexo, nível de conhecimento em tecnologia, utilização de autenticação em dois fatores, conhecimento sobre ataque *phishing,* se o usuário compartilha a senha com terceiros, se são cuidadosas com dados, entre outras questões, todas as respostas do formulário foram obtidas de maneira anônima, protegendo todos os voluntários.

Além disso, a escolha pelo questionário se justifica pela capacidade dessa abordagem em investigar fenômenos atuais dentro de seus contextos reais, como explica Yin (2015), sendo, portanto, adequada para análises aprofundadas.

4 ANÁLISE DAS RESPOSTAS

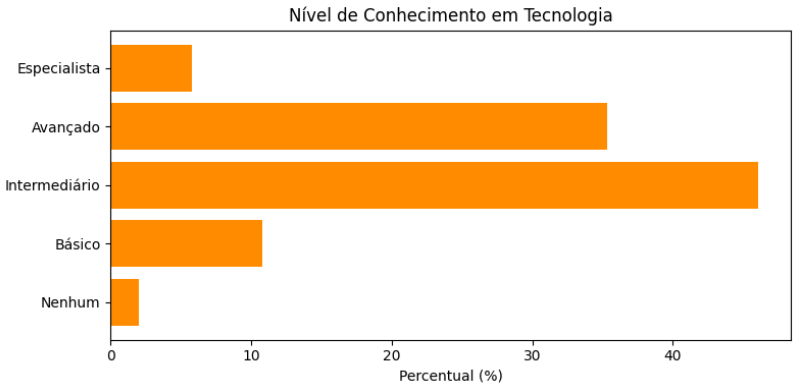
Foi aplicada uma pesquisa com voluntários com o objetivo de avaliar o nível de conhecimento dos usuários sobre segurança da informação. Utilizando a plataforma Google Forms, o questionário foi enviado e aberto para respostas entre os dias 25 e 28 de maio de 2025, com retorno de 102 respostas. Os respondentes pertenciam a diferentes grupos etários e atuantes em diferentes setores da sociedade como: Estudante, Tecnologia, Administração e Gestão, Saúde, Professor Ambiental, Perito Grafotécnico, Militar da FAB, entre outros, como demonstrado na Figura 2, em que a maior parte considerou seu conhecimento em tecnologia como básico (47 respostas, equivalente a 46,1%) como apresentado na Figura 3. Algumas perguntas buscaram identificar o grau de familiaridade dos usuários com práticas seguras no ambiente digital, como por exemplo, apenas 29,4% das pessoas que responderam utilizam da autenticação em 2 fatores em todas as contas importantes e 43,1% utilizam em apenas algumas contas, como apresentada na Figura 4.

Figura 2. Gráfico área de atuação dos usuários



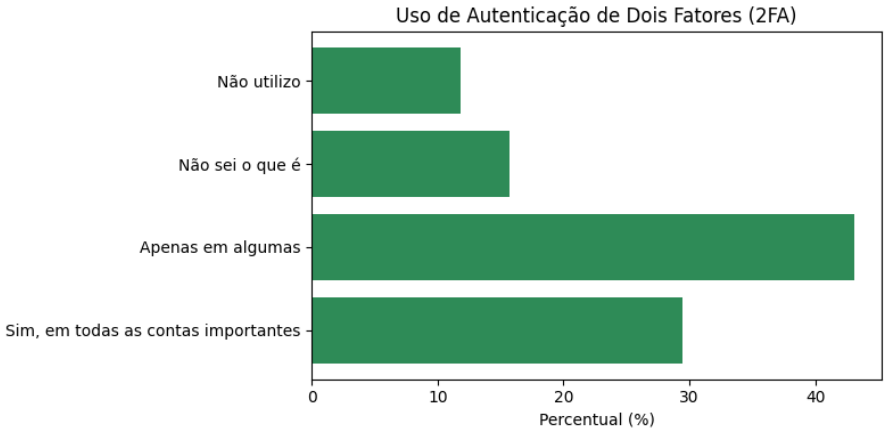
Fonte: O Autor, 2025

Figura 3. Nível de conhecimento em tecnologia



Fonte: O Autor, 2025

Figura 4. Utilização autenticação em dois fatores



Fonte: O Autor, 2025

Após a análise dos dados, observou-se uma correlação direta entre o nível de conhecimento em tecnologia e o uso mais consistente da autenticação em dois fatores, na Figura 5 vê-se de maneira clara. Entre os respondentes com conhecimento básico, observou-se que a maioria (18 pessoas) utiliza a 2FA apenas em algumas contas, enquanto 10 afirmaram utilizá-la em todas. No entanto, um número significativo de pessoas desse grupo ainda não utiliza (7 respostas) ou sequer conhece o recurso (8 respostas), indicando uma carência de informação e conscientização.

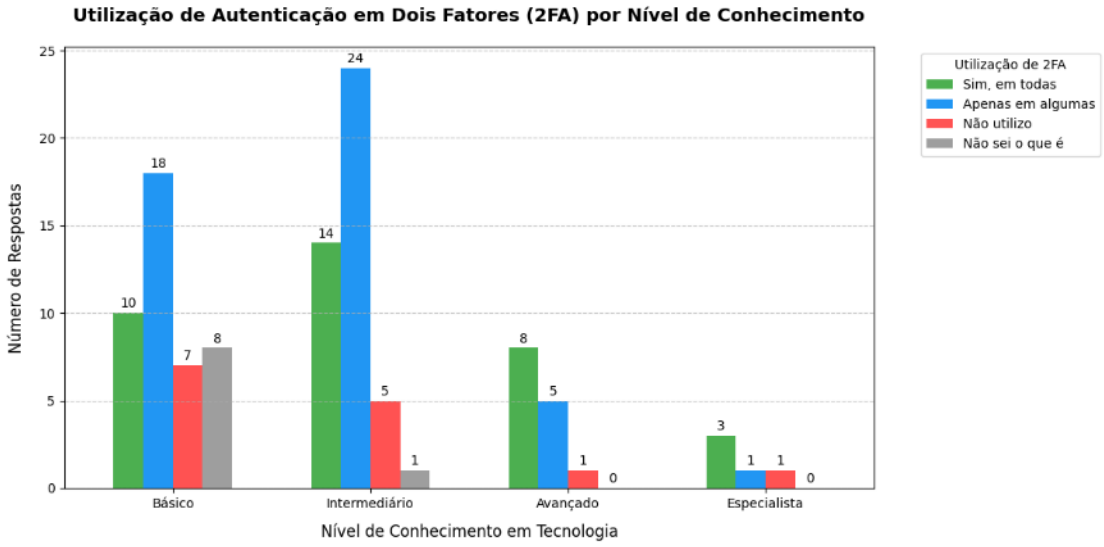
No grupo intermediário, há uma melhora notável: 14 pessoas utilizam a 2FA em todas as contas e 24 em algumas, com apenas 5 não utilizando e 1 alegando não saber o que é. Esse dado sugere que, à medida que o usuário adquire maior familiaridade com a tecnologia, cresce sua percepção sobre a importância de práticas de segurança digital.

Entre os usuários com nível avançado, há uma mudança no padrão: 8 utilizam a

2FA em todas as contas e apenas 5 em algumas. Esse grupo representa uma parcela mais consciente e engajada com a proteção de suas credenciais digitais. Apenas um respondente deste grupo declarou não utilizar 2FA, e nenhum alegou desconhecê-la.

O grupo especialista, embora com menor número de respondentes, segue o padrão esperado: 3 afirmaram utilizar a 2FA em todas as contas, e apenas um declarou utilizá-la em algumas e outro não a utiliza. O desconhecimento do recurso foi inexistente entre os especialistas.

Figura 5: Utilização autenticação em 2 fatores x Nível de Conhecimento

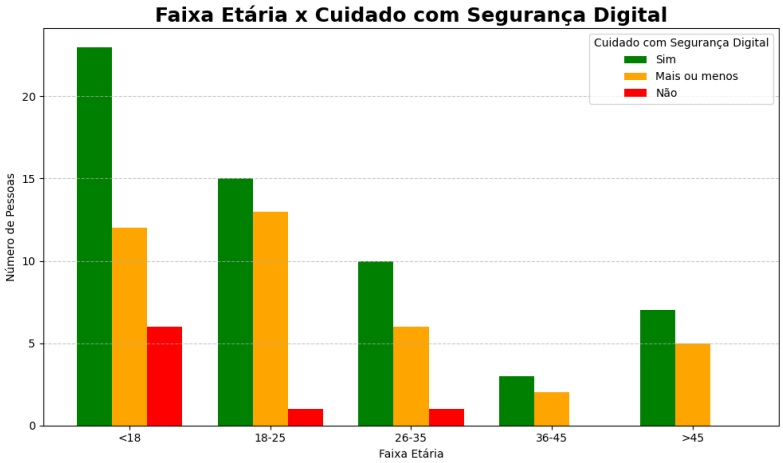


Fonte: O Autor, 2025

Observando a Figura 6, nota-se que a maioria dos respondentes tem menos de 18 anos. Nessa faixa, a maior parte diz se preocupar com segurança digital, mas uma parcela dos respondentes admite só tomar alguns cuidados, enquanto uma minoria afirma não se proteger muito. Na faixa de 18 a 25 anos, a divisão é mais equilibrada: tem quase o mesmo número de pessoas que se consideram cuidadosas e as que só seguem práticas de segurança de vez em quando, com poucos admitindo descuido total.

Na faixa dos 26 aos 35 anos, o número de participantes cai, mas a maioria ainda mostra preocupação com segurança digital. Entre os de 36 a 45 anos, as respostas são ainda menos numerosas, mas quase todos marcaram "Sim" quando questionados sobre cuidados, sem nenhum "Não" registrado. Por fim, o grupo acima de 45 anos teve poucos participantes, mas todos relataram algum nível de atenção com a segurança digital, sendo que o “Sim” foi a resposta mais selecionada.

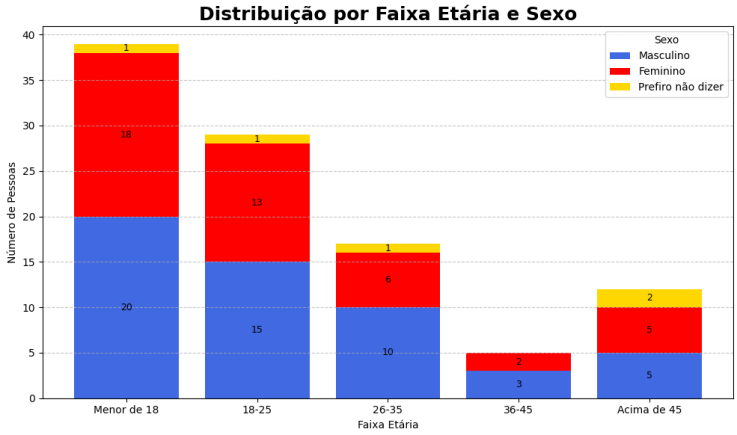
Figura 6. Relação Faixa Etária x Cuidado com a Segurança Digital



Fonte: O Autor, 2025

O gráfico presente na Figura 7 mostra a distribuição dos participantes por faixa etária e sexo, usando cores para diferenciar: azul (masculino), vermelho (feminino) e amarelo (quem preferiu não informar). A faixa menos de 18 anos formou o maior grupo, com 41 respondentes, a proporção entre homens e mulheres foi bem equilibrada, com um caso optando por não revelar o gênero. Em seguida, a faixa de 18 a 25 anos aparece como a segunda mais representativa, também com uma distribuição parecida entre os gêneros, embora os homens tenham sido mais numerosos, essas duas parcelas representaram 68,6% dos respondentes, isso pode ser um reflexo do maior contato com tecnologia ou da disposição em participar desse tipo de estudo. Na faixa dos 26 a 35 anos, o número de participantes cai, mas ainda assim há um equilíbrio entre homens e mulheres. Quando chegamos nas idades acima disso (36 a 45 anos e mais de 45), a participação cai, esses dois grupos representam 14,7%.

Figura 7. Relação Faixa Etária x Sexo

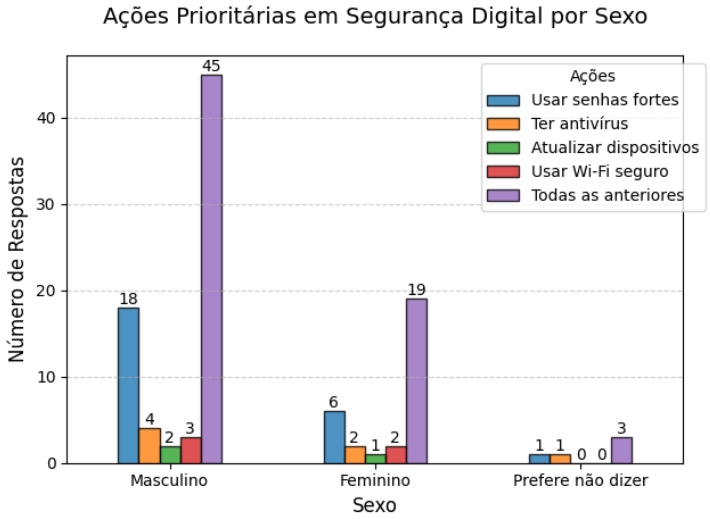


Fonte: O Autor, 2025

Na Figura 8, o grupo masculino que contou com 72 respostas escolheu em maior parte que todas as ações propostas são importantes, com 62,5%, seguido do uso de senhas fortes (25%), no grupo feminino a tendência se manteve a mesma, com 63,3% das respostas sendo relacionada a todas as alternativas, vemos que os três grupos reconhecem que segurança digital requer múltiplas ações integradas (evidenciado pela dominância de "Todas as anteriores").

As mulheres proporcionalmente atribuíram ligeiramente que ter um antivírus (6,6%) é mais importante que os homens que atribuíram apenas 5,5%, uma diferença pequena, que pode ser maior ou menor dependendo do nível de amostragem.

Figura 8: Sexo x Ações por usuários



Fonte: O Autor, 2025

Após remoção das respostas não pertinentes da pergunta aberta *"Deixe sua opinião sobre segurança digital"* foi gerada uma nuvem de palavras que revelou os temas mais mencionados pelos participantes. A Figura 9 mostra, de forma visual, o que mais preocupa e chama a atenção das pessoas quando o assunto é proteção online. As palavras mais mencionadas foram: "segurança", "dados", "importante", "digital", "proteger" e "essencial". Isso mostra de forma clara que, para a maioria, a segurança digital é algo importante para preservar informações pessoais e corporativas.

Outros termos como "tecnologia", "cuidado", "ameaças" e "dia" mostram que as pessoas enxergam a segurança como uma necessidade diária, algo que deve acompanhar o uso constante da internet e dos dispositivos. Além disso, expressões como "deveríamos nos proteger mais" e "cuidado pessoal" sugerem que muitos

reconhecem sua própria responsabilidade na proteção dos dados. Por fim, palavras como "acesso", "confidencialidade", "corporativo" e "internet" mostram que o entendimento sobre segurança digital vai além de algo banal, as pessoas pensam tanto no uso pessoal quanto nos riscos profissionais.

No geral, a nuvem de palavras apresentada na Figura 9 confirma que há uma consciência forte sobre a importância da segurança digital. No entanto, o nível de conhecimento sobre como se proteger pode variar de pessoa para pessoa. O que fica claro é que, na visão dos participantes, estar seguro online não é opcional, é uma necessidade do mundo conectado de hoje.

Figura 9: Nuvem de Palavras



Fonte: O Autor, 2025

5 CONCLUSÃO

Este estudo preliminar surgiu da necessidade de entender como as pessoas comuns encaram os riscos digitais em um momento em que o Brasil vive uma verdadeira explosão no uso da internet. O principal objetivo foi realizar uma investigação inicial, por meio da aplicação de um questionário online, para compreender essa percepção através do cruzamento de dados obtidos. A análise buscou identificar padrões como qual faixa etária se mostra mais cuidadosa com seus dados, quais grupos são mais participativos nas medidas de segurança, entre outros aspectos relevantes.

Com mais brasileiros conectados do que nunca muitos sem o devido preparo para navegar com segurança e o aumento alarmante de golpes e invasões virtuais, a pesquisa buscou mapear como o público em geral lida com essas ameaças no dia a dia. O formulário aplicado tinha como objetivo claro descobrir não só o que as pessoas sabem sobre proteção digital, mas como elas de fato se comportam diante de desafios

como criação de senhas, utilização de ferramentas de segurança e identificação de redes suspeitas.

Os resultados revelam uma realidade preocupante: embora 61,8% dos respondentes afirmem utilizar métodos de proteção como antivírus, senhas fortes e redes seguras, a maioria classifica seu próprio conhecimento como básico. Essa aparente contradição sugere uma fragilidade na navegação digital, onde muitos usuários reconhecem a importância da segurança, mas sentem que seus esforços não são totalmente suficientes. Essa percepção fica evidente na análise das respostas e se reflete na nuvem de palavras gerada a partir dos comentários.

O *phishing* emerge como uma das maiores preocupações. Curiosamente, 70,6% dos participantes acreditam nunca ter sofrido esse tipo de ataque, mas considerando que se trata de um método extremamente comum, a probabilidade real de exposição é significativamente maior - especialmente para profissionais que lidam constantemente com links e arquivos externos. A análise detalhada dos dados revela que jovens adultos (18-25 anos) são os mais afetados por *phishing*, seguidos por adolescentes. Essa vulnerabilidade decorre da combinação perigosa entre comportamentos de risco e falta de conhecimento técnico específico.

Os números e depoimentos coletados permitem concluir que o grupo de 18 a 25 anos é o mais exposto aos riscos digitais, situação agravada por três fatores principais: hábitos inseguros, falta de conscientização adequada e intensa atividade online. Já os menores de 18 anos apresentam vulnerabilidades distintas, relacionadas principalmente à inexperiência digital. Entre os participantes acima de 26 anos, observa-se maior adoção de medidas protetivas, embora ainda existam lacunas importantes a serem abordadas.

A solução para esse cenário exige ação coordenada em três níveis complementares. No plano individual, é urgente que cada usuário revise e melhore seus hábitos digitais, adotando medidas práticas de proteção no cotidiano. No âmbito educacional, torna-se imprescindível incorporar o ensino de segurança digital desde os primeiros anos escolares, além de promover a conscientização familiar. Por fim, organizações e instituições precisam assumir sua responsabilidade, implementando políticas robustas de proteção de dados e privacidade. Somente através dessas ações será possível construir uma cultura digital verdadeiramente consciente e protegida, capaz de acompanhar o ritmo acelerado da transformação digital no país.

REFERÊNCIAS

ALMEIDA, Claúdia. A Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço. Instituto da Defesa Nacional, 2018.

ALMEIDA, Júlio. *Crackers e suas táticas no ambiente digital*. Revista de Segurança Digital, São Paulo, 2018.

AMAZON. *Amazon Web Services – Cloud Computing Services*. 2023. Disponível em: https://aws.amazon.com. Acesso em: 16 maio 2025.

ARIANE, G. *Entenda os diferentes tipos de ataques DDoS*. Segurança e TI, 2023.

ARIANE, Paula. *Cibersegurança na prática: ameaças e defesas digitais*. Porto: DigitalTech, 2023.

BATISTA, Emerson de Oliveira. *Sistemas de Informação: o uso consciente da tecnologia para o gerenciamento*. São Paulo: Saraiva, 2004.

BEJTLICH, R. *The practice of network security monitoring: understanding incident detection and response*. San Francisco: No Starch Press, 2014.

BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 1, 15 ago. 2018.

CHAVEZ, Juan José Santos. *Ataques DDoS: Qué son, cómo identificarlos y cómo prevenirlos*. Disponível em: <https://www.deltaprotect.com/blog/ataques-ddos-que-son> Acesso em: 18/02/2024

CHAVEZ, Marcelo. *O que é um ataque DDoS?* Blog CloudDefender, 2022.

CHAVEZ, Rodrigo. *Guia prático de segurança cibernética: proteção em ambientes digitais*. São Paulo: Nova Era, 2022.

CHIAVENATO, Idalberto. *Administração: teoria, processo e prática*. 4. ed. Rio de Janeiro: Elsevier, 2014.

CHIAVENATO, Idalberto. Gestão de pessoas: O novo papel dos recursos humanos nas organizações. São Paulo: Editora Manole, 2014.

CONVERGÊNCIA DIGITAL. *92% dos CEOs vão investir em TI e 37,5% em segurança da informação*. 2023. Disponível em: https://convergenciadigital.uol.com.br. Acesso em: 16 maio 2025. Disponível em: <https://softwarelab.org/pt/melhores-antivirus/>. Acesso em16/05/25.

FREILING, Felix C.; HOLZ, Thorsten; WICHERSKI, Georg. *Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks*. In: Proceedings of the 10th European Symposium on Research in Computer Security, 2005.

FREILING, Felix C.; HOLZ, Thorsten; WICHERSKI, Georg. Botnet tracking: exploring a root-cause methodology to prevent distributed denial-of-service attacks. In: *Proceedings of the 10th European Symposium on Research in Computer Security*. Berlim: Springer, 2005. p. 319–335.

G1. Acesso à internet cresce no Brasil e chega a 84% da população em 2023, diz pesquisa. *G1*, 16 nov. 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/11/16/acesso-a-internet-cresce-no-brasil-e-chega-a-84percent-da-populacao-em-2023-diz-pesquisa.ghtml. Acesso em: 28 maio 2025.

GIL, A. C. *Métodos e técnicas de pesquisa social*. 7. ed. São Paulo: Atlas, 2019.

IBM. *Cost of a Data Breach Report*. 2020. Disponível em: https://www.ibm.com/security/data-breach. Acesso em: 16 maio 2025.

INFORMAÇÃO. *In*: DICIO, Dicionário Online de Português. Porto: 7Graus, 2024. Disponível em: <https://www.dicio.com.br/informacao/>. Acesso em: 16/05/25.

KASPERSKY. *Os 5 melhores antivírus para empresas*. 2023. Disponível em: https://www.kaspersky.com.br. Acesso em: 16 maio 2025.

KASPERSKY. *Relatório anual de ameaças cibernéticas 2023*. Moscovo: Kaspersky Lab, 2023. Disponível em: https://www.kaspersky.com. Acesso em: 27 maio 2025.

KOTLER, P. **Administração de Marketing: A edição do Novo Milênium**.São Paulo:Prentice Hall, 2000.

MARCONI, M. A.; LAKATOS, E. M. *Fundamentos de metodologia científica*. 8. ed. São Paulo: Atlas, 2017.

McCarty, B. (2003b). **Botnets: Big and bigger. IEEE Security and Privacy.** Disponível em: < https://doi.ieeecomputersociety.org/10.1109/MSECP.2003.1219079> Acesso em: 16/05/25

MCCARTY, B. Botnets: Big and Bigger. *IEEE Security & Privacy Magazine*, v. 1, n. 4, p. 87–90, jul./ago. 2003b.

McCARTY, Brad. *Botnets and the new threat landscape*. Network Security Journal, 2003b.

MICROSOFT. *Como identificar e evitar phishing*. Microsoft Security Blog, 2022. Disponível em: https://www.microsoft.com/security

OLIVEIRA, Ingrid. **Levantamento Mostra que Ataques Cibernéticos no BrasilCresceram 94%.** CNN Brasil. Disponível em: < https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/>. Acesso em 16/05/25

OLIVEIRA, M. *Brasil é o segundo país mais atacado da América Latina*. CNN Brasil, 2022. Disponível em: https://www.cnnbrasil.com.br. Acesso em: 16 maio 2025.

OLIVO, C.K. **Avaliação de características para detecção de phishing de e-mail.** Dissertação (mestrado), Pontifícia Universidade Católica do Paraná, Curitiba: 2010.

OLIVO, Nelson. *Segurança da Informação e Engenharia Social*. Curitiba: Appris, 2010.

REZENDE, Denis Alcides. **Engenharia de Software e Sistemas de Informação.** 3ª ed. Rio de Janeiro: Brasport, 2005.

REZENDE, Denis Alcides. *Planejamento de sistemas de informação e informática: guia prático para planejar a informática integrada ao planejamento estratégico empresarial*. 3. ed. São Paulo: Atlas, 2005.

RISCO. *Dicionário Online Risco*. 2024. Disponível em: https://www.dicionarioris.com. Acesso em: 16 maio 2025.

SCHEINER, L. *Ataques DDoS: como funcionam e como se proteger*. São Paulo: Novatec, 2020.

SISTEMA. *In*: DICIO, Dicionário Online de Português. Porto: 7Graus, 2024. Disponível em:<https://www.dicio.com.br/sistema/>. Acesso em: 26/01/2024

STAIR, Ralph M.; REYNOLDS, George W. **Princípios de sistemas de informação.** 14ª ed. São Paulo: Cengage Learning, 2021.

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores: Princípios e Práticas.** 2ª ed. Rio de Janeiro: Elsevier Editora Ltda., 2014.

STALLINGS, William; BROWN, Lawrie. *Segurança em redes de computadores: princípios e prática*. 2. ed. São Paulo: Pearson, 2014.

STAMMERS, R. *Cybersecurity for Beginners*. London: CyberSafe Publishing, 2019.

STJ – SUPERIOR TRIBUNAL DE JUSTIÇA. *Lei Geral de Proteção de Dados Pessoais (LGPD) entra em vigor*. 2020. Disponível em: https://www.stj.jus.br. Acesso em: 16 maio 2025.

VALENGA, Danilo. *Ataques cibernéticos: estudo de caso do WannaCry e suas implicações globais*. Curitiba: Editora Universitária UFPR, 2018.

VALENGA, Guilherme. *Cibersegurança nas organizações: uma necessidade contínua*. Revista de Tecnologia em Informação, 2018.

VALENGA, Gustavo. **Malware, riscos e métodos de proteção.** Disponível em: <https://www.centralpress.com.br/artigo-malware-riscos-e-metodos-de-protecao/ >. Acesso em: 16/05/25

YIN, R. K. *Estudo de caso: planejamento e métodos*. 5. ed. Porto Alegre: Bookman, 2015.

ZIMMER, Kelvin. **Hackers x Empresas Quais os ataques cibernéticos mais comuns**. Disponível em: <https://www.lumiun.com/blog/hackers-empresas-quais-os-ataques-ciberneticos-mais-comuns/>. Acesso em 19/07/2023.