artigo de revisão

PERCEPÇÃO DOS RISCOS CIBERNÉTICOS NA ERA DIGITAL:
Um estudo sobre o conhecimento dos usuários de internet da cidade de Pelotas/RS acerca das vulnerabilidades a que estão expostos

PERCEPTION OF CYBER RISKS IN THE DIGITAL AGE:
A study on the knowledge of internet users in the city of Pelotas, RS, regarding the vulnerabilities to which they are exposed

Carolina Paz da Cruz[1]
https://orcid.org/0009-0008-1173-6749
Larissa Medianeira Bolzan [2]
https://orcid.org/0000-0002-3257-7096

RESUMO
Este estudo teve como objetivo analisar a percepção dos riscos cibernéticos entre os usuários de internet da cidade de Pelotas/RS, considerando fatores sociodemográficos e comportamentais que podem influenciar a segurança digital. Para isso, foi realizada uma pesquisa quantitativa por meio da aplicação de um questionário estruturado, que contou com a participação de 416 respondentes. Os dados coletados foram analisados por meio de estatísticas descritivas e técnicas de análise multivariada. Os resultados indicaram que a percepção dos riscos cibernéticos varia de acordo com características individuais, como idade, escolaridade, renda e tempo de acesso à internet. Observou-se que usuários com maior exposição ao ambiente digital tendem a demonstrar maior consciência sobre segurança online, embora práticas seguras nem sempre sejam adotadas uniformemente. Além disso, diferenças foram identificadas entre gêneros na percepção sobre a segurança de dispositivos e contas, assim como entre diferentes grupos de renda e escolaridade. Conclui-se que, embora haja um conhecimento crescente sobre os riscos cibernéticos, ainda existem lacunas na adoção de medidas eficazes de segurança digital. Os achados reforçam a necessidade de campanhas de conscientização e educação digital voltadas a diferentes perfis de usuários, promovendo um ambiente online mais seguro e resiliente.

Palavras-Chave: Segurança Digital. Riscos Cibernéticos. Percepção de Risco.

ABSTRACT
This study aimed to analyze the perception of cyber risks among internet users in the city of Pelotas/RS, considering sociodemographic and behavioral factors that may influence digital security. To achieve this, a quantitative survey was conducted using a structured questionnaire, with the participation of 416 respondents. The collected data were analyzed through descriptive statistics and multivariate analysis techniques. The results indicated that the perception of cyber risks varies according to individual characteristics such as age,

Artigo submetido em 17/10/2015 e aceito para publicação em 311/07/2026.

[1]Aluna do Curso de graduação em Engenharia de Produção da Universidade Federal de Pelotas (UFPel), carolinapazc@outlook.com
[2]Professora Adjunta da Universidade Federal de Pelotas (UFPel), larissambolzan@gmail.com

education level, income, and time spent on the internet. It was observed that users with greater exposure to the digital environment tend to demonstrate higher awareness of online security, although safe practices are not always uniformly adopted. Additionally, differences were identified between genders in the perception of device and account security, as well as among different income and education level groups. It is concluded that, although there is a growing awareness of cyber risks, gaps still exist in the adoption of effective digital security measures. The findings reinforce the need for awareness campaigns and digital education tailored to different user profiles, promoting a safer and more resilient online environment.

Keywords: *Digital Security. Cyber Risks. Risk Perception.*

1 INTRODUÇÃO

A internet, considerada uma das inovações tecnológicas mais significativas do século XX, tornou-se uma ferramenta indispensável na vida moderna, oferecendo um vasto conjunto de serviços e informações (Castells, 2019). Desde a sua criação, a internet tem desempenhado um papel transformador na sociedade, influenciando diversos aspectos da vida cotidiana, incluindo a comunicação, a educação, o comércio e o entretenimento (Kritzinger; Von Solms, 2010). Segundo dados do Comitê Gestor da Internet no Brasil (CGI, 2022) aproximadamente 81% da população brasileira tem acesso à internet, o que representa cerca de 146 milhões de pessoas conectadas.

Frente a esse cenário, importante considerar que o ambiente digital é permeado por diversas ameaças que vão desde ataques cibernéticos, como *phishing* e *malware*, até fraudes financeiras e roubo de identidade (Amar; Kumar, 2023). Os ataques de *phishing*, por exemplo, são caracterizados pelo envio de comunicações fraudulentas que parecem vir de uma fonte confiável, com o objetivo de enganar as vítimas para que divulguem informações pessoais, como senhas e dados bancários (Ivanov *et al.,* 2021). *Malware*, por sua vez, refere-se a *softwares* maliciosos destinados a causar danos a um computador, servidor ou rede de computadores (Rohith; Kaur, 2021). Essas ameaças são acentuadas pela crescente sofisticação das técnicas utilizadas por cibercriminosos, que frequentemente conseguem burlar as defesas tradicionais (Maiorca; Biggio; Giacinto, 2019).

De acordo com um relatório, de 2024, da Federação Brasileira de Bancos (FEBRABAN), foram registrados cerca de 3,5 milhões de tentativas de golpes e fraudes financeiras no Brasil em 2023, um aumento de 30% em relação ao ano anterior. A FEBRABAN destaca a importância de práticas de segurança, como a

verificação de links antes de clicar, o uso de *softwares* antivírus atualizados e a ativação da autenticação em duas etapas, como formas de mitigar esses riscos.

Torna importante destacar que a segurança cibernética tem impactos diretos na privacidade, na economia e no bem-estar social. Empresas e governos enfrentam riscos que podem comprometer operações críticas, resultando em perdas financeiras e de reputação. No Brasil, o crescimento do *e-commerce*, da digitalização de serviços públicos e a implementação da Lei Geral de Proteção de Dados (LGPD), em 2020, reforçaram a urgência de conscientizar a população e aprimorar práticas de segurança. Estes desafios, aliados às diferenças de percepção entre públicos variados, tornam o tema ainda mais relevante.

Além disso, a falta de conhecimento e a baixa conscientização sobre práticas seguras na internet são considerações significativamente importantes para a analisar a vulnerabilidade dos usuários (Rahman *et al.,* 2020). De acordo com pesquisas da Kaspersky (2023), empresa de segurança cibernética, 65% dos brasileiros admitem não saber identificar se um site é legítimo e 58% utilizam a mesma senha por um longo período e para múltiplas contas, facilitando a ação de cibercriminosos. Os comportamentos citados anteriormente aumentam consideravelmente os riscos de segurança digital, mostrando uma necessidade crítica de educação e treinamento em cibersegurança (Ahmad *et al.,* 2022).

O aumento da conectividade digital no Brasil, enquanto propulsor de desenvolvimento e da inclusão social, também é um fator que se acrescenta aos desafios em termos de segurança (Ahmad *et al*., 2022). A crescente sofisticação dos ataques cibernéticos exige que tanto os indivíduos quanto as organizações adotem práticas robustas de segurança digital. Isso inclui o uso de senhas fortes e únicas, a adoção de autenticação multifator e a constante atualização de *software* para proteger contra vulnerabilidades conhecidas (Marton; David, 2014).

Neste contexto, emerge o seguinte objetivo geral de pesquisa: analisar a percepção dos usuários de internet da cidade de Pelotas/RS acerca dos riscos cibernéticos a que estão expostos. Balizam esse objetivo geral, os seguintes objetivos específicos: (i) avaliar o nível de conhecimento dos usuários de internet da cidade de Pelotas/RS sobre práticas de cibersegurança; (ii) analisar os tipos mais comuns de vulnerabilidades enfrentadas pelos usuários ao navegar na internet; (iii) analisar a relação entre as características dos usuários e a incidência de vulnerabilidades; (iv)

desenvolver recomendações para melhorar o conhecimento de cibersegurança entre os usuários.

2 REFERENCIAL TEÓRICO

Com vistas a dar suporte a compreensão dos resultados, neste tópico, serão abordados os temas: incidentes de cibersegurança e seu impactos; comportamento dos usuários e conscientização sobre cibersegurança; e, medidas de proteção e políticas públicas, a partir de investigações avaliadas por pares e publicadas anteriormente.

2.1 Incidentes de Cibersegurança e seus Impactos

O Brasil tem sido palco de inúmeros incidentes significativos de cibersegurança. Um dos exemplos mais notórios foi o vazamento massivo de dados pessoais ocorrido em janeiro de 2021, onde informações de mais de 223 milhões de registros foram expostas. Embora o número exceda a população brasileira viva estimada pelo IBGE, essa discrepância se deve ao fato de que o vazamento incluiu não apenas dados de pessoas vivas, mas também informações de indivíduos já falecidos, que permaneceram armazenadas nos bancos de dados comprometidos. Entre os dados expostos estavam informações sensíveis como CPF, número de telefone, e até mesmo detalhes de veículos e contas bancárias. Esse incidente revelou não apenas a gravidade das brechas de segurança, mas também a insuficiência das práticas de proteção de dados no país (Pecsen, 2021).

Outro caso significativo ocorreu com a empresa de telefonia Vivo, que, em 2019, teve um vazamento de dados que expôs informações pessoais de seus clientes, incluindo nome, RG, CPF, e-mail, telefone, data de nascimento e o nome da mãe de clientes. O incidente destacou a vulnerabilidade das grandes corporações e a necessidade urgente de aprimorar as práticas de segurança digital (Schaeffer, 2019).

Os incidentes de segurança cibernética não apenas comprometem a privacidade dos usuários, mas acarretam significativos impactos econômicos. Segundo um estudo realizado pela Accenture, em 2021, o custo médio de um ataque cibernético no Brasil foi estimado em cerca de US$1,35 milhão, abrangendo desde a

perda de dados até a interrupção de negócios e danos à reputação das empresas (Accenture, 2021).

Além dos custos diretos, os ataques cibernéticos têm profundas repercussões sociais. A exposição de dados pessoais pode levar ao roubo de identidade, que muitas vezes resulta em fraudes financeiras. Em 2024, a Serasa Experian relatou que o ano de 2023 registrou quase 10 milhões de tentativas de fraude, afetando diretamente a vida financeira de milhões de brasileiros (Serasa Experian, 2024).

Em julho de 2020, um incidente significativo evidenciou as vulnerabilidades de segurança nas redes sociais: contas no Twitter de várias personalidades, incluindo Elon Musk, Bill Gates e Barack Obama, foram *hackeadas* em um golpe de Bitcoin. Os invasores usaram essas contas de alto perfil para promover um esquema de doação de Bitcoin, enganando seguidores e resultando em prejuízos financeiros consideráveis para os usuários que caíram no golpe. Além das perdas econômicas diretas, o ataque gerou grande alarme social, levantando questões sobre a segurança das plataformas digitais e a confiança pública nas redes sociais. Este evento destacou a necessidade urgente de implementar medidas de segurança mais robustas e eficazes para proteger as contas de usuários, especialmente aquelas de figuras públicas com grande influência. O impacto deste ataque também levou a uma análise crítica das práticas de segurança digital e a uma pressão para o fortalecimento das defesas cibernéticas nas plataformas de mídia social (New York State, 2020).

2.2 Comportamento dos usuários e conscientização em cibersegurança

Comportamentos de usuários frequentemente contribuem de forma significativa para aumentar a vulnerabilidade em cibersegurança. O uso de senhas fracas e repetidas é uma prática comum que facilita o trabalho dos *hackers*, pois muitos usuários continuam a utilizar senhas fáceis de adivinhar, como "123456" ou "*password*" e frequentemente utilizam as mesmas senhas em múltiplas contas (Graupner *et al.*, 2016).

Estudos indicam que a conscientização e o comportamento dos usuários são fatores críticos na mitigação de riscos cibernéticos. Uma pesquisa realizada pela empresa de segurança digital Kaspersky, em 2023, revelou que 58% dos brasileiros

utilizam a mesma senha para múltiplas contas, enquanto 65% não sabem identificar se um site é seguro. Esses comportamentos aumentam significativamente a vulnerabilidade dos usuários a ataques como *phishing* e invasão de contas (Ahmad *et al.,* 2022).

A educação em cibersegurança é apontada como uma solução eficaz para esses problemas. Programas de treinamento focados em boas práticas, como a criação de senhas fortes e o reconhecimento de tentativas de *phishing*, têm mostrado resultados promissores. Um estudo conduzido por Ahmad *et al.* (2022) demonstrou que treinamentos regulares podem reduzir a incidência de ataques bem-sucedidos em até 45%.

2.3 Medidas de proteção e políticas públicas

A implementação de políticas públicas robustas é essencial para a proteção cibernética. A Lei Geral de Proteção de Dados (LGPD), que entrou em vigor no Brasil em 2020, estabelece diretrizes claras para a coleta, armazenamento e tratamento de dados pessoais, impondo sanções severas para violações. Estudos sugerem que a LGPD tem potencial para melhorar significativamente a segurança de dados no Brasil, incentivando as empresas a adotarem melhores práticas de cibersegurança (Pinheiro, 2020).

Além das políticas públicas, ferramentas tecnológicas amplamente acessíveis ao público têm desempenhado um papel crucial na proteção de dados pessoais e na conscientização sobre práticas seguras. Os gerenciadores de senhas, por exemplo, ajudam os usuários a criar, armazenar e gerenciar credenciais de maneira segura, reduzindo significativamente os riscos associados ao uso de senhas fracas ou reutilizadas. Essas ferramentas representam um avanço na proteção individual de dados, sendo facilmente adotadas por diferentes perfis de usuários (Oesch; Ruoti, 2019).

Navegadores com foco em privacidade oferecem proteção contra rastreamento e coleta de dados não autorizados, possibilitando maior controle do usuário sobre sua experiência online. Estudos apontam que esses navegadores são eficazes na prevenção de rastreamento por terceiros, embora enfrentem desafios relacionados à compatibilidade com algumas plataformas (Carr; Shahandashti, 2020).

Outra categoria relevante são as soluções de *backup* de dados baseadas em nuvem, que oferecem uma camada adicional de proteção contra perdas acidentais ou ataques cibernéticos. Essas ferramentas têm sido amplamente adotadas por pequenas empresas e usuários domésticos, permitindo o armazenamento seguro de informações e uma recuperação rápida em caso de incidentes (Lemos, 2022).

A Política Nacional de Cibersegurança (PNCiber), lançada pelo Governo Federal em 2023, complementa essas iniciativas ao promover a proteção de infraestruturas críticas, a educação em cibersegurança e a conscientização pública sobre práticas seguras online. A política incentiva a colaboração entre diferentes setores e prevê a criação de um centro nacional de cibersegurança, ampliando as estratégias de defesa e resposta a incidentes (Goldoni *et al.,* 2024).

3 MÉTODO DO TRABALHO

O presente estudo caracteriza-se como uma pesquisa de natureza quantitativa e caracter descritivo. É considerada quantitativa uma vez que utiliza dados numéricos para avaliar a percepção dos riscos cibernéticos entre os usuários de internet da cidade de Pelotas/RS. De acordo com Joseph Hair *et al.* (2024), a análise quantitativa refere-se ao uso de técnicas estatísticas para interpretar grandes volumes de dados. Já a classificação descritiva se dá porque visa descrever e analisar como a população-alvo se comporta diante dos riscos cibernéticos, sem buscar necessariamente identificar relações de causalidade (Gil, 2019).

A técnica de coleta de dados utilizada foi o questionário, que é um instrumento estruturado composto por afirmações e escalas de respostas predefinidas. As afirmações foram construídas a partir de variáveis encontradas na literatura, conforme mostra Quadro 1. Os respondentes deverão indicar seu grau de concordância com a alternativa, utilizando uma Escala Likert de cinco níveis. A escala Likert é amplamente utilizada em pesquisas sociais por sua capacidade de medir atitudes e opiniões de forma prática e padronizada (Hair *et al.*, 2024).

Quadro 1 - Construção do Instrumento para coleta de dados

Afirmativa	**Literatura base para construir a afirmativa**
Eu uso senhas diferentes para diferentes contas.	Ahmad *et al.* (2022)
Minhas senhas contêm uma combinação de letras, números e caracteres/símbolos especiais. (como # ou @).	Ferreira *et al*. (2014)
Eu nunca compartilho minhas senhas com outras pessoas.	Ahmad *et al.* (2022)
Eu uso um aplicativo para criar e salvar minhas senhas.	Ivanov *et al.* (2021)
Eu sei identificar e-mails falsos (fraudulentos) que tentam me enganar.	Sheng *et al.* (2010)
Eu nunca forneço informações pessoais em resposta a e-mails ou mensagens suspeitas.	Abu-Nimeh *et al.* (2007)
Eu sempre desconfio de ofertas que parecem boas demais para ser verdade.	Parsons *et al.* (2015)
Eu sempre verifico se os links são seguros antes de clicar.	Ivanov *et al.* (2021)
Eu mantenho meus dispositivos (celular/computador) com antivírus atualizados.	Ahmad *et al.* (2022)
Eu não abro anexos de e-mails enviados por desconhecidos.	Sheng *et al.* (2010)
Se meu dispositivo (celular/computador) for infectado por um vírus, eu sei o que fazer.	Ivanov *et al.* (2021)
Eu configuro a privacidade das minhas contas online para me proteger.	Rohith e Kaur (2021)
Eu sei proteger meus dados quando uso redes Wi-Fi públicas (como em cafés, praças e aeroportos).	Ferreira *et al.* (2014)
Eu controlo quem pode ver minhas informações pessoais nas redes sociais.	Ahmad *et al.* (2022)
Eu entendo os riscos de compartilhar informações pessoais na internet.	Ivanov (2021)

Fonte: As autoras, 2025.

O questionário foi construído tanto por questões voltadas para temas de vulnerabilidades e segurança digital, como por questões destinadas à coleta de informações socioeconômicas e demográficas. Essas variáveis possibilitaram analisar

possíveis correlações entre as características dos respondentes e suas percepções sobre segurança digital.

O questionário foi aplicado entre novembro e dezembro de 2024, com a utilização da plataforma Google Forms. O público-alvo foi a população da cidade de Pelotas/RS, onde de acordo com o IBGE (2022), residem 325.685 mil habitantes. Assim, para garantir a representatividade da amostra, foi adotado um nível de confiança de 95% e uma margem de erro de 5%, resultando em uma amostra mínima de 385 respondentes. A equação usada para calcular a amostra é apresentada na Equação 1.

Equação 1: Cálculo da amostra com base no nível de confiança.

$$n = \frac{\sigma^2 * z^2}{D^2}$$

Onde:

n = tamanho da amostra.

σ = desvio padrão da população.

z = valor da distribuição normal padrão para o nível de confiança definido.

D = margem de erro.

A divulgação do questionário foi realizada em grupos de WhatsApp, Instagram e grupos de trabalho, além de abordagens pessoais, buscando alcançar uma diversidade de perfis de usuários de internet.

3.1 Testes usados para Análise dos Dados

A análise dos dados foi realizada com o auxílio do software SPSS (*Statistical Package for the Social Sciences*), utilizando técnicas de estatística descritiva para avaliar a frequência das respostas e identificar padrões de comportamento entre os respondentes. Além disso, para verificar se os dados seguiam uma distribuição normal, foi aplicado o Teste de Shapiro-Wilk. Como a normalidade não foi confirmada, foram utilizados testes não-paramétricos nas análises subsequentes.

A adequação da amostra para a Análise Fatorial Exploratória (AFE) foi avaliada por meio do índice KMO (Kaiser-Meyer-Olkin) e do Teste de Bartlett, que verificaram

a pertinência da estrutura fatorial. Em seguida, foi aplicada a matriz de componentes rotativa para identificar agrupamentos latentes entre as variáveis do questionário. Para avaliar a confiabilidade interna das escalas utilizadas, foi calculado o Alfa de Cronbach.

Adicionalmente, foi empregada a Análise Multivariada de Variância (MANOVA) para investigar possíveis diferenças entre os grupos analisados, considerando múltiplas variáveis dependentes simultaneamente. Quando diferenças significativas fossem identificadas, o Teste de Tukey seria aplicado como análise pós-hoc, permitindo determinar especificamente quais grupos apresentaram variações relevantes entre si.

4 RESULTADOS E DISCUSSÃO

O estudo obteve respostas de uma amostra de 416 indivíduos da cidade de Pelotas/RS. A distribuição etária mostrou, dentre os respondentes, uma predominância de indivíduos entre 25 e 34 anos (33,2%), seguidos pelo grupo de 35 a 44 anos (21,6%). Os respondentes entre 18 e 24 anos representaram 19,2%, enquanto as faixas menos representadas foram menores de 18 anos (1,4%) e maiores de 65 anos (1,9%). Quanto ao gênero, a distribuição demonstra predominância de indivíduos do gênero feminino (66,8%), o gênero masculino corresponde a 32,5% dos respondentes e 0,7% dos participantes se identificaram com o gênero “Outro”.

Quanto ao nível de escolaridade dos participantes, a maior parte possui ensino superior completo 41,6%, seguido por indivíduos com pós-graduação, incluindo mestrado e doutorado, que representam 35,6% da amostra. Os respondentes com ensino médio correspondem a 18,8%, enquanto os do ensino fundamental representam 3,1%. Apenas 1% dos participantes indicaram outra opção de escolaridade.

A análise do nível de escolaridade dos pais dos respondentes revela diferenças importantes entre os grupos. No caso das mães, 29,1% possuem ensino médio completo, seguido de 28,8% com ensino fundamental, 20,9% com ensino superior, 14,7% com pós-graduação, 5,3% em "outro" e 1,2% que indicaram "não sei dizer". Já entre os pais, a maior percentagem corresponde ao ensino fundamental, com 36,1%,

seguido de 32,5% com ensino médio e 16,6% com ensino superior, 6,7% possuem pós-graduação, 3,8% marcaram "outro" e 4,3% indicaram "não sei dizer".

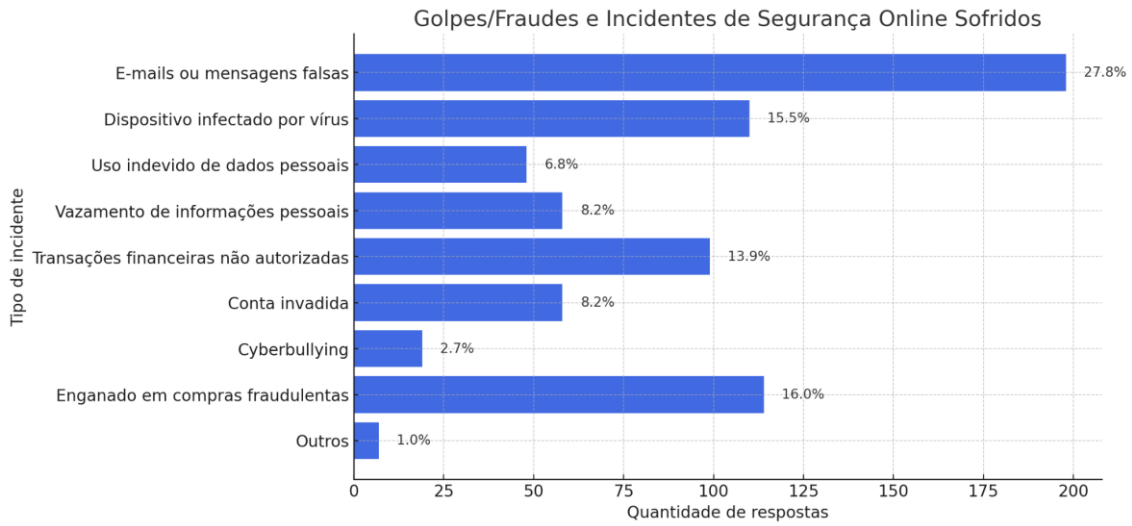
A distribuição ocupacional dos respondentes demonstra que a maior parte dos respondentes da pesquisa é composta por indivíduos economicamente ativos, com 42,1% declarando que "apenas trabalham", seguido por 34,9% que conciliam estudo e trabalho. O grupo que se dedica exclusivamente ao estudo corresponde a 15,9% dos participantes. Já os aposentados representam 4,3% da amostra, enquanto 2,9% indicaram "outro" como ocupação.

A distribuição da renda familiar mensal dos 416 respondentes demonstra uma predominância de faixas intermediárias. A maioria indicou rendimentos entre R$5.001 e R$10.000 (29,8%) e entre R$2.001 e R$5.000 (29,3%). Participantes com rendas entre R$10.001 e R$20.000 representam 20,4% da amostra, enquanto 12,3% declararam renda de até R$2.000. Apenas 3,4% indicaram rendimentos superiores a R$20.000, e 4,8% preferiram não informar sua renda.

Quanto ao comportamento de uso da internet, a maioria correspondendo a 30,5% dos respondentes relatou utilizar a internet por mais de 8 horas/dia. Os respondentes que utilizam a internet entre 5 e 8 horas por dia representam 26,4%, seguidos por 28,1% que indicaram um tempo de uso diário entre 3 e 5 horas. Aqueles que relataram acessar a internet entre 1 e 3 horas correspondem a 13,9%, enquanto apenas 1% declarou utilizar a internet por menos de 1 hora ao dia.

Sobre incidentes de segurança, apenas 8,97% afirmaram não terem sofrido incidentes de segurança online. Os demais incidentes estão listados e apresentados na Figura 1.

Figura 1 - Gráfico que informa os tipos de incidentes e golpes/fraudes sofridos pelos respondentes



Fonte: Dados da pesquisa, 2025.

4.1 Testes de Validação do Questionário

Inicialmente, foram realizados os testes de Shapiro-Wilk e Kolmogorov-Smirnov para verificar a normalidade dos dados. Os resultados indicaram valores de Significância (Sig.) inferiores a 0,05, demonstrando que os dados não seguem uma distribuição normal (Razali; Wah, 2011). Diante disso, optou-se por utilizar testes não-paramétricos nas análises subsequentes.

Em seguida, para verificar a adequação dos dados a Análise Fatorial Exploratória, foram feitos os testes de Kaiser-Meyer-Olkin (KMO) e de esfericidade de Bartlett. O teste KMO avalia a adequação da amostragem, e um valor superior a 0,7 é considerado satisfatório para esse tipo de análise. O KMO inicial foi de 0,781, indicando que os dados eram adequados. O teste de esfericidade de Bartlett apresentou um valor de significância (Sig.) igual a 0,000, confirmando que as variáveis possuem correlações suficientes para justificar a aplicação da Análise Fatorial Exploratória.

O teste de Análise Fatorial Exploratória foi realizada três vezes. Isso porque conforme recomendado por Hair *et al.* (2010), questões cujas cargas fatoriais não alcançam 0,5, na matriz de componente rotativa, devem ser excluídas e um novo teste deve ser realizado sem as variáveis excluídas. Na primeira Análise Fatorial Exploratória, as cargas fatoriais das variáveis presentes nas questões 11 e 14 não

alcançaram o valor mínimo de 0,5. Na segunda Análise Fatorial Exploratória, mais duas variáveis foram excluídas, as presentes nas questões 15 e 24. Na terceira vez que a Análise Fatorial Exploratória foi realizada, 11 variáveis, com cargas fatoriais superiores a 0,5, formaram 3 fatores. Conforme Tabela 2. Aos fatores foram atribuídos os nomes: Segurança de Dispositivos e Contas, Identificação de Ameaças Cibernéticas e Segurança de Senhas e Compartilhamento de Dados.

Tabela 2: Matriz de componente rotativa (4)

	Componente		
	Segurança de Dispositivos e Contas	Identificação de Ameaças Cibernéticas	Segurança de Senhas e Compartilhamento de Dados
19. Eu mantenho meus dispositivos (celular/computador) com antivírus atualizados.	0,739		
21. Se meu dispositivo (celular/computador) for infectado por um vírus, eu sei o que fazer.	0,754		
22. Eu configuro a privacidade das minhas contas online para me proteger.	0,652		
23. Eu sei proteger meus dados quando uso redes Wi-Fi públicas (como em cafés, praças e aeroportos).	0,793		
17. Eu sempre desconfio de ofertas que parecem boas demais para ser verdade.		0,779	
18. Eu sempre verifico se os links são seguros antes de clicar.		0,695	
20. Eu não abro anexos de e-mails enviados por desconhecidos.		0,528	
25. Eu entendo os riscos de compartilhar informações pessoais na internet.		0,612	
16. Eu não forneço informações pessoais em resposta a e-mails ou mensagens suspeitas.			0,629
12. Minhas senhas contêm uma combinação de letras, números e caracteres/símbolos especiais (como # ou @).			0,573
13. Eu não compartilho minhas senhas com outras pessoas.			0,799

Fonte: Dados dos testes estatísticos.

Depois de identificados os 3 fatores, foi verificado o Coeficiente Alfa de Cronbach para analisar a confiabilidade do instrumento. O Coeficiente Alfa de Cronbach apresentou um valor de 0,551, indicando uma confiabilidade substancial. De acordo com Hair *et al.* (2024), valores de Alfa de Cronbach acima de 0,5 são considerados aceitáveis em pesquisas exploratórias, especialmente quando o número de itens é reduzido. Esse resultado sugere que os itens avaliados possuem uma correlação moderada entre si, demonstrando que eles medem de forma consistente o mesmo conceito ou construto.

Assim, um instrumento (mostrado na Tabela 2) para verificar a conhecimento dos usuários de internet da cidade de Pelotas/RS sobre práticas de cibersegurança foi validado, formado por 11 variáveis alocados em 3 fatores.

4.2 Explorando a Percepção dos Usuários de Internet sobre riscos cibernéticos da cidade de Pelotas/RS

Para determinar se é possível aplicar um teste de variância e covariância adequado à análise dos dados, foi realizado o Teste de M de Box. Esse teste avalia se as matrizes de covariância das variáveis dependentes são heterogêneas entre os grupos estudados, requisito para a utilização de alguns testes estatísticos. O valor de significância obtido foi 0,070, superior ao limite crítico de 0,001. Dessa forma, os resultados indicam que os dados permitem a aplicação de testes estatísticos baseados na comparação entre grupos. Assim, foi possível aplicar a Análise Multivariada de Variância (MANOVA) para verificar se há diferenças estatisticamente significativas entre os grupos analisados em relação a um conjunto de variáveis dependentes.

Quanto ao fator faixa etária, a análise dos efeitos entre sujeitos revelou que os fatores A (Segurança de Dispositivos e Contas) e C (Proteção de Dados Pessoais) apresentaram diferenças estatisticamente significativas em relação à faixa etária. O Fator A apresentou um valor de 0,002 e o Fator C, um valor de 0,032, ambos inferiores ao limite crítico de 0,05. Diante desse resultado, torna-se necessário aplicar o Teste de Tukey, um teste pós-hoc utilizado para identificar especificamente quais grupos apresentam diferenças estatisticamente significativas entre si.

Os resultados do Teste de Tukey indicaram que a variável faixa etária não apresentou impacto estatisticamente significativo nas percepções dos respondentes quanto à Segurança de Dispositivos e Contas (Fator A) e à Proteção de Dados Pessoais (Fator C), já que os valores de significância (Sig.) encontrados foram superiores ao nível de 0,05. Isso sugere que, em linhas gerais, a idade não influenciou de maneira determinante as respostas relacionadas à segurança digital.

A análise da variável independente gênero revelou que apenas o Fator A (Segurança de Dispositivos e Contas) apresentou diferenças estatisticamente significativas entre os grupos, com um valor de Sig = 0,001, inferior ao limite crítico de 0,05. Isso indica que o gênero influenciou as respostas sobre percepção de segurança. Por outro lado, os Fatores B (Práticas de Proteção Contra Vírus) e C (Proteção de Dados Pessoais) não apresentaram diferenças estatisticamente significativas, pois os valores de Sig. foram 0,830 e 0,138, respectivamente, superiores ao limite de 0,05, sugerindo que o gênero não impacta as respostas nessas variáveis.

Diante desse resultado, torna-se necessário aplicar o Teste de *Tukey* para o Fator A. Os resultados do Teste de Tukey para o Fator A (Segurança de Dispositivos e Contas) revelam uma diferença estatisticamente significativa entre os grupos masculino (1) e feminino (2), com valor de significância de 0,001, inferior ao limite de 0,05. Essa diferença sugere que as mulheres apresentaram uma maior percepção de segurança em relação à proteção de dispositivos e contas quando comparadas aos homens. Essa percepção ampliada pode estar relacionada a um maior grau de cautela por parte das mulheres no ambiente digital, possivelmente influenciado por experiências anteriores e/ou casos divulgados na mídia, preocupações com segurança pessoal ou um nível de atenção maior a riscos virtuais.

Os resultados do Teste MANOVA da variável independente escolaridade indicam que apenas o Fator B (Práticas de Proteção Contra Vírus) apresentou diferenças estatisticamente significativas entre os grupos, com um valor de Sig. 0,041, inferior ao limite de 0,05. Isso indica que o nível de escolaridade impacta as respostas relacionadas a essa variável.

Diante desse resultado, torna-se necessário aplicar o Teste de *Tukey* ao Fator B. Os resultados do referido teste indicam que não houve diferenças estatisticamente

significativas entre os grupos de diferentes escolaridade, pois as comparações apresentaram valores de Sig. superiores a 0,05.

No que se refere aos resultados do Teste MANOVA da variável independente ocupação, o Fator C (Proteção de Dados Pessoais) apresentou diferenças estatisticamente significativas entre os grupos ocupacionais, com um valor de Sig. 0,002, inferior ao limite de 0,05. Isso sugere que a ocupação dos respondentes influencia suas respostas nessa variável específica.

Diante desse resultado, torna-se necessário aplicar o Teste de *Tukey* acerca do Fator C. Os resultados do referido teste indicaram que a ocupação dos respondentes influenciou significativamente suas percepções sobre esse tema. As comparações entre os grupos revelaram diferenças estatisticamente significativas, especialmente entre os respondentes que estudam e trabalham (grupo 3) e aqueles que apenas trabalham (grupo 2), com valor de significância de 0,012, e entre os que estudam e trabalham (grupo 3) e os aposentados (grupo 4), com valor de 0,031.

Em ambos os casos, os respondentes que conciliam estudo e trabalho apresentaram maior percepção sobre a importância da proteção de dados pessoais. Essa maior sensibilidade pode estar relacionada à exposição constante a conteúdos educacionais em ambientes profissionais, o que pode aumentar sua consciência sobre os riscos digitais e a necessidade de proteger informações pessoais. Por outro lado, aqueles que apenas trabalham ou estão aposentados podem não estar tão imersos em discussões atualizadas sobre segurança da informação, o que pode influenciar uma percepção menos acentuada sobre o tema.

Acerca dos resultados do Teste MANOVA para a variável independente renda familiar mensal, o Fator A (Segurança de Dispositivos e Contas) apresentou um valor de significância de 0,005. Isso sugere que os diferentes níveis de renda podem influenciar a forma como os entrevistados percebem esse fator.

Diante desse resultado, foi necessária a aplicação do Teste de *Tukey.* Os resultados do Teste de *Tukey* para o Fator A, referente à Segurança de Dispositivos e Contas, indicaram que a renda familiar mensal exerce influência significativa sobre a percepção dos respondentes. Foram identificadas diferenças estatisticamente significativas entre alguns grupos de renda. Destaca-se que os participantes com renda entre R$10.001 e R$20.000 apresentaram maior percepção de segurança em

comparação aos respondentes com renda entre R$5.001 e R$10.000, com valor de significância de 0,041.

Da mesma forma, este último grupo, de R$5.001 a R$10.000, também demonstrou percepção mais elevada em relação ao grupo de pessoas que preferiram não informar sua renda, com valor de significância de 0,013. Além disso, foi observada uma diferença relevante entre os grupos de R$10.001 a R$20.000 e acima de R$20.000, também com valor de significância de 0,013. Essa diferença pode sugerir que a percepção de segurança digital não necessariamente aumenta conforme o aumento da renda, mas sim que existe uma maior sensibilidade entre os grupos de renda intermediária e média-alta.

Uma possível interpretação para esse padrão é que pessoas com renda entre R$5.000 e R$20.000 podem estar mais inseridas em atividades digitais relacionadas a consumo, trabalho e educação, estando mais expostas e, por consequência, mais atentas à necessidade de proteger seus dispositivos e contas. Esses achados reforçam a importância de considerar o contexto socioeconômico ao pensar em ações de conscientização e políticas públicas voltadas à segurança digital, com atenção especial aos públicos que, embora estejam mais expostos, podem não perceber plenamente os riscos envolvidos.

Os resultados do Teste MANOVA para a variável independente tempo diário de acesso à internet indicaram uma diferença estatisticamente significativa no Fator C (Proteção de Dados Pessoais), com um valor de significância de 0,011. Isso sugere que o tempo médio de navegação pode influenciar as percepções relacionadas a esse fator.

Dessa forma, foi aplicada uma análise pós-hoc pelo Teste de *Tukey* para identificar quais grupos de tempo de acesso apresentam diferenças estatisticamente significativas entre si em relação ao Fator C. Os resultados do Teste de *Tukey* demonstram que o tempo diário de acesso à internet influencia significativamente a percepção dos usuários sobre segurança digital. Foram identificadas diferenças estatisticamente significativas entre alguns grupos, destacando especialmente aqueles com tempos de uso moderado.

Usuários que acessam a internet entre 1 e 3 horas por dia apresentaram maior percepção sobre proteção de dados pessoais em comparação aos que acessam por 3 a 5 horas por dia, com valor de significância de 0,045, e também em relação aos

que utilizam a internet entre 5 e 8 horas diárias, com significância de 0,005. Esses dados indicam que a exposição excessiva pode estar associada a uma percepção reduzida sobre os riscos à privacidade, talvez pela naturalização do uso constante ou por excesso de confiança em ferramentas tecnológicas.

Além disso, uma diferença significativa foi observada entre os usuários que acessam a internet entre 3 e 5 horas diárias e aqueles com uso superior a 8 horas por dia, com valor de 0,006. Isso reforça a hipótese de que usuários com uso mais controlado e equilibrado da internet tendem a demonstrar maior sensibilidade em relação à proteção de seus dados pessoais.

O Teste MANOVA acerca do nível de escolaridade da mãe indicaram diferenças estatisticamente significativas nos Fatores B (Práticas de Proteção Contra Vírus) e C (Proteção de Dados Pessoais), com valores de significância de 0,005 e 0,004, respectivamente. Esses achados sugerem que o nível de escolaridade materno pode influenciar as respostas associadas a esses fatores.

Diante disso, foi aplicado o Teste de *Tukey.* Os resultados do Teste de *Tukey* para os fatores B e C indicam que a escolaridade materna exerce influência significativa nas percepções dos respondentes sobre práticas de proteção digital. No Fator B (Práticas de Proteção Contra Vírus), observou-se que os participantes cujas mães têm ensino superior apresentaram uma percepção mais elevada em relação à proteção contra vírus quando comparados àqueles cujas mães possuem ensino médio e formações classificadas como 'outro', com diferenças estatisticamente significativas. Esses dados sugerem que, possivelmente, a presença de um ambiente familiar mais escolarizado, com maior acesso a informações e incentivo ao uso consciente da tecnologia, pode refletir na construção de hábitos mais cautelosos quanto à proteção de dispositivos.

No Fator C (Proteção de Dados Pessoais), os respondentes cujas mães possuem ensino médio ou ensino superior apresentaram maior percepção em comparação aos que informaram ensino fundamental e outra escolaridade, sendo também observada uma diferença significativa entre pós-graduação e o grupo classificado como "outro". Essas diferenças reforçam a hipótese de que o nível educacional da mãe pode influenciar a formação da consciência digital dos filhos, especialmente ao longo da infância e adolescência, impactando no modo como esses indivíduos lidam com a segurança e privacidade no ambiente online. Em síntese, os

dados apontam que quanto mais elevado o nível de escolaridade materna, maior tende a ser a percepção do respondente em relação à proteção de dados e à adoção de práticas seguras na internet.

Por últimos, os resultados do Teste MANOVA sobre escolaridade do pai indicam a necessidade de aprofundamento da análise por meio do Teste de *Tukey*. O Fator B (Práticas de Proteção Contra Vírus) apresentou um valor de significância de 0,000, enquanto o Fator C (Proteção de Dados Pessoais) obteve 0,001, ambos abaixo do limiar de 0,05, indicando diferenças estatisticamente significativas entre os grupos analisados.

Diante disso, foi aplicada a análise pós-hoc pelo Teste de *Tukey.* No Fator B (Práticas de Proteção Contra Vírus), o Teste de *Tukey* intensificou diferenças importantes entre os participantes cujos pais possuem ensino médio e aqueles com ensino superior completo, com valor de significância de 0,006, assim como entre ensino médio e pós-graduação, com valor de 0,044. Além disso, os participantes cujos pais têm ensino fundamental também se diferenciaram daqueles com pais com ensino superior e pós-graduação, com valores de 0,008 e 0,026, respectivamente. Esses resultados indicam que a percepção de práticas seguras contra ameaças digitais tende a ser mais elevada entre os indivíduos com pais mais escolarizados, possivelmente em função de um ambiente familiar mais informado, com maior acesso à tecnologia e valorização do uso consciente da internet.

No Fator C (Proteção de Dados Pessoais), também foram observadas diferenças significativas. Os participantes com pais com ensino superior apresentaram maior percepção sobre proteção de dados em comparação aos que possuem pais com ensino fundamental (0,035) e ensino médio (0,044). A mesma tendência foi observada entre os grupos com pais com ensino médio e pós-graduação, com valor de 0,025. Esses achados reforçam que níveis mais elevados de escolaridade paterna estão associados a uma maior percepção dos filhos em relação à proteção digital.

5 CONCLUSÃO

Este estudo teve como objetivo analisar a percepção dos riscos cibernéticos entre os usuários de internet da cidade de Pelotas/RS, a partir da influência de fatores sociodemográficos e comportamentais sobre a segurança digital. Por meio da análise

estatística dos dados coletados, foi possível identificar perfis e padrões que contribuem para a compreensão das vulnerabilidades enfrentadas no ambiente virtual.

Os resultados revelaram que características como tempo de acesso à internet, renda, ocupação e escolaridade dos pais exercem influência sobre a percepção dos usuários, ainda que essa relação não seja uniforme entre todos os grupos. Usuários com maior tempo de exposição à internet tendem a demonstrar menor consciência sobre riscos cibernéticos. A ocupação também se mostrou relevante, sugerindo que o contexto profissional e acadêmico pode impactar diretamente as práticas de segurança adotadas pelos usuários.

A análise revelou ainda que o nível de escolaridade dos pais (tanto da mãe quanto do pai) está associado a uma percepção mais apurada em relação à proteção de dados pessoais e às práticas de prevenção contra ameaças digitais, indicando a importância do ambiente familiar e da formação ao longo da vida na construção de hábitos seguros. Por outro lado, a escolaridade dos próprios respondentes não apresentou influência estatisticamente significativa sobre a maioria dos fatores analisados, o que sugere que a percepção de riscos pode estar mais relacionada a experiências práticas e contextos socioculturais do que apenas ao nível formal de instrução.

A análise por gênero apontou que mulheres apresentaram maior percepção de segurança em relação a dispositivos e contas, evidenciando a necessidade de estratégias de conscientização mais sensíveis às diferenças de perfil dos usuários. Esses achados reforçam a importância de iniciativas educacionais voltadas à segurança digital, promovendo uma maior disseminação de informações e incentivando práticas mais seguras no ambiente online.

Como continuidade desta pesquisa, estudos futuros podem aprofundar os fatores que apresentaram diferenças estatisticamente significativas, utilizando métodos qualitativos que permitam compreender as razões subjacentes às percepções identificadas. Também se sugere a aplicação do estudo em outros contextos geográficos ou segmentos específicos da população, como profissionais de tecnologia, estudantes e idosos, para enriquecer a compreensão das vulnerabilidades e das estratégias de mitigação dos riscos cibernéticos.

Embora limitado geograficamente à cidade de Pelotas/RS, este trabalho oferece contribuições relevantes para o entendimento das diferentes formas como os

usuários percebem os riscos digitais, servindo de base para o desenvolvimento de ações de conscientização e educação digital mais eficazes, com o objetivo de tornar o ambiente online mais seguro e resiliente para todos.

REFERÊNCIAS

ABU-NIMEH, S. *et a*l. Uma comparação de técnicas de aprendizado de máquina para detecção de phishing. **Proceedings of the Anti-Phishing Working Groups 2nd Annual e Crime Researchers Summit**, p. 60–69, 2007.

AHMAD, A.; MAYNARD, S. B.; SHANKS, G. G. Uma análise de caso da gestão de segurança de sistemas de informação no contexto de uma grande organização de saúde. **Australasian Journal of Information Systems**, v. 19, n. 1, p. 97–116, 2022.

AHMAD, Norita *et al*. Uma comunidade educada em segurança cibernética. **IEEE Transactions on Emerging Topics in Computing,** v. 10, n. 3, p. 1456-1463, 2022 .

CARR, Michael; SHAHANDASHTI, Siamak F. Revisiting Security Vulnerabilities in Commercial Password Managers. **In:** IFIP International Conference on ICT Systems Security and Privacy Protection. Cham: Springer International

CASTELLS, Manuel. O Impacto da Internet na Sociedade: Uma Perspectiva Global. **In Change: 19 Ensaios Chave sobre Como a Internet Está Mudando Nossas Vidas**, Madri, BBVA, 2013.

Cyber Threat Intelligence Report. **Accenture,** v. 2, p. 1-27, 2021.

Federação Brasileira de Bancos. Relatório FEBRABAN de Tecnologia Bancária 2024. **FEBRABAN**. São Paulo, 2024

FERREIRA, A. *et a*l. Melhorando a conscientização sobre políticas e procedimentos de segurança dentro das organizações. **Journal of Information Systems Security**, v. 10, n. 3, p. 39-50, 2014.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** Ed. 4, p. 1-176. São Paulo, 2018.

GOLDONI, Luiz Rogério Franco; RODRIGUES, Karina Furtado; MEDEIROS, Breno Pauli. Qual é o futuro da governança de cibersegurança no Brasil? **Cadernos Gestão Pública e Cidadania**, v. 29, p. 1-14, São Paulo, 2024.

GRAUPNER, Hendrik *et al*. Análise e interpretação automatizadas de vazamentos de identidade. **CF '16: Anais da Conferência Internacional da ACM sobre Fronteiras da Computação.** Nova Iorque, 2016.

HAIR, Joseph F. *et al.* **Análise multivariada de dados**. Ed. 6, p. 1-688. Porto Alegre, 2024

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE)**.** Pelotas (RS): população estimada 2022.

IVANOV, Michael A *et al* . Phishing Attacks and Protection Against Them. **Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus),** Moscou, 2021.

IVANOV, V. *et a*l. Gerenciamento de ameaças internas de segurança de TI: estendendo a teoria da dissuasão e o papel do artefato de TI. **Journal of Strategic Information Systems**, v. 30, n. 2, p. 101-664, 2021.

JOHRI, Amar; KUMAR, Shailendra. Explorando a conscientização do cliente em relação à sua segurança cibernética no Reino da Arábia Saudita: um estudo na era da transformação digital bancária, **Comportamento Humano e Tecnologias Emergentes,** v. 2023, n. 1, p. 10, 2023.

KASPERSKY DAILY. 58% dos brasileiros não trocam suas senhas com frequência**. Kaspersky,** Reino Unido, 2023.

KASPERSKY DAILY. 65% dos brasileiros não sabem reconhecer se um site é legítimo. **Kaspersky**, Reino Unido, 2023.

KRITZINGER, Elmarie; VON SOLMS S.H. Segurança cibernética para usuários domésticos: uma nova forma de proteção por meio da aplicação da conscientização. **Computers & Security,** v.29, n.8, p. 840-847, 2010.

LEMOS, Samuel Afonso da Câmara. **Levantamento e avaliação da qualidade das senhas e alternativas de autenticação: uma análise com base em uma pesquisa de survey.** Monografia (Graduação em Informática), Universidade Federal do Rio Grande do Norte, 2022.

MAIORCA, D; BIGGIO, B; GIACINTO, G. Towards Adversarial Malware Detection: Lessons Learned from PDF-based Attacks**. Revista ACM,** v. 52, n.4, p. 1-36, 2019.

MARTON, G; DAVID, A. Considerações de segurança e oportunidades de autenticação de dois fatores em ambientes de e-learning. **IEEE International Conference on Emerging eLearning Technologies and Applications (ICETA),** v. 4, n. 5, p. 319-323, 2014.

OESCH, Sean; RUOTI, Scott. That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers. **29th USENIX Security Symposium**. 2019.

PARSONS, K. *et a*l. Determinando a conscientização dos funcionários usando o Questionário de Aspectos Humanos da Segurança da Informação (HAIS-Q**)**. **Computers & Security**, v. 48, p. 70-79, 2015.

PECSEN, Thaisy. Vazamento em massa expõe número de CPF de milhões de brasileiros, alerta PSafe. **Dfndr Blog - PSafe.** 2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: Comentários à Lei n. 13.709/2018 - LGPD**. São Paulo: Saraiva, 2019. 118 p, 2020.

RAHMAN, Abd *et al*. A importância da educação em segurança cibernética na escola. **International Journal of Information and Education Technolgy.** v. 10, n. 5, p. 378-382, 2020.

RAZALI, Nornadiah Mohd; WAH, Yap Bee. Power comparisons of Shapiro-Wilk, Kolmogorov-Smirnov, Lilliefors, and Anderson-Darling tests. **Journal of Statistical Modeling and Analytics**, v. 2, n. 1, p. 21-33, 2011.

ROHITH, C.; KAUR, G. Um estudo abrangente sobre técnicas de detecção e prevenção de malware usadas por antivírus. **2ª Conferência Internacional sobre Engenharia e Gestão Inteligentes (ICIEM),** Londres, 2021.

ROHITH, S.; KAUR, P. Uma análise abrangente de técnicas de phishing e contramedidas. **Journal of Cybersecurity Research**, v. 8, n. 2, p. 23-34, 2021.

SCHAEFFER, Cesar. Falha de segurança expõe dados de 24 milhões de usuários da Vivo. **Olhar Digital**. 2019.

SERASA EXPERIAN. Quase 10 milhões de tentativas de fraude de identidade foram registradas em 2023. **Serasa Experian**. 2024.

SHANKER, Anusha Kadambari; USHA, G. Cenário de ameaças cibernéticas no ciberespaço. **Conferência Internacional de Eletrônica, Comunicação e Tecnologia Aeroespacial (ICECA),** p. 375-380, 2017.

SHENG, S. *et a*l. Quem cai no phishing? Uma análise demográfica da suscetibilidade ao phishing e eficácia das intervenções. **Proceedings of the SIGCHI Conference on Human Factors in Computing Systems**, p. 373–382, 2010.