CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

A LACUNA NA CONSCIENTIZAÇÃO SOBRE GOLPES CIBERNÉTICOS:

Entre a Disseminação Preventiva e a Ação dos Usuários de Smartphones.

THE GAP IN CYBERSCAM AWARENESS:

Between Preventative Dissemination and Smartphone User Action.

Roger L. S. Munhoz – munhoz.roger@bol.com.br

Orientador: Arnaldo Napolitano Sanches – Arnaldo.sanches@fatec.sp.gov.br

RESUMO

A crescente presença dos smartphones na sociedade contemporânea, embora traga inúmeros benefícios, também expôs os usuários a um aumento significativo de golpes cibernéticos. Diante desse cenário, este trabalho tem como objetivo investigar o nível de conscientização dos usuários de smartphones em relação à segurança digital e avaliar a percepção sobre a efetividade das campanhas informativas, com base na aplicação de um questionário estruturado a participantes de diferentes perfis sociodemográficos, cuja análise evidenciou lacunas relevantes no conhecimento e na adoção de medidas básicas de proteção, bem como a percepção de que as campanhas existentes são insuficientes ou pouco acessíveis, reforçando a necessidade de ações educativas mais eficazes, acessíveis e contínuas para reduzir a distância entre informação e prática e, assim, fortalecer a segurança digital individual e coletiva.

Palavras-chave: Segurança digital. Smartphones. Conscientização. Campanhas informativas. Educação tecnológica.

ABSTRACT

The growing presence of smartphones in contemporary society, although it brings numerous benefits, has also exposed users to a significant increase in cyber scams. Given this scenario, this study aims to investigate the level of awareness of smartphone users regarding digital security and to evaluate their perception of the effectiveness of information campaigns, based on the application of a structured questionnaire to participants with different sociodemographic profiles, whose analysis highlighted relevant gaps in knowledge and adoption of basic protection measures, as well as the perception that existing campaigns are insufficient or not very accessible, reinforcing the need for more effective, accessible and continuous educational actions to reduce the gap between information and practice and, thus, strengthen individual and collective digital security.

Keywords: Digital security. Smartphones. Awareness. Informational campaigns. Digital education.

Junho/2025

1. INTRODUÇÃO

A transformação digital que marca a sociedade contemporânea trouxe incontáveis benefícios, conectando pessoas, simplificando serviços e integrando atividades pessoais e profissionais em um único dispositivo: o smartphone. Contudo, esse avanço também abriu portas para novas ameaças. Golpes digitais, como fraudes bancárias, clonagem de chips (SIM Swap) e ataques de *phishing*, tornaram-se cada vez mais comuns, atingindo usuários das mais diversas idades e perfis.

Apesar da crescente sofisticação das ameaças, muitas pessoas ainda desconhecem os mecanismos básicos de proteção disponíveis em seus próprios aparelhos. Medidas simples, como bloqueio por senha, autenticação em dois fatores, antivírus e atualizações regulares, poderiam mitigar boa parte desses riscos. No entanto, a ausência de uma cultura de segurança digital no cotidiano da população evidencia um problema mais amplo: a distância entre a informação e a ação.

Escolas, mídias sociais, veículos de comunicação e órgãos públicos deveriam ser protagonistas na promoção da conscientização digital. Ainda assim, observa-se uma atuação dispersa, muitas vezes limitada a campanhas pontuais e com linguagem excessivamente técnica. Como resultado, parcela significativa da população permanece vulnerável – não necessariamente por desinteresse, mas por falta de acesso a informações claras, acessíveis e contextualizadas.

A importância do tema se intensifica quando consideramos o impacto que a perda ou o roubo de um smartphone pode causar. Os danos vão além do valor do dispositivo. Informações bancárias, documentos, registros pessoais e profissionais passam a correr risco, causando prejuízos financeiros, emocionais e práticos.

Diante desse cenário, este trabalho busca compreender se há uma relação direta entre o nível de conscientização promovido por campanhas informativas e a adoção efetiva de medidas de segurança pelos usuários. A partir da aplicação de um questionário estruturado, voltado a diferentes faixas etárias e níveis de escolaridade, pretende-se identificar padrões de comportamento, lacunas de conhecimento e percepções sobre a eficácia dessas campanhas.

Mais do que apenas diagnosticar o problema, este estudo tem como propósito contribuir para a discussão sobre estratégias mais eficazes de comunicação em segurança

digital, capazes de transformar informação em ação e promover uma cultura de proteção mais presente no dia a dia das pessoas.

2. REFERENCIAL TEÓRICO

2.1 A Era da Mobilidade e a Centralidade dos Smartphones

A digitalização da vida cotidiana transformou os smartphones em dispositivos multifuncionais, integrando comunicação, entretenimento, transações financeiras e acesso a documentos pessoais. De acordo com dados da Anatel (2023), o número de smartphones em uso no Brasil já ultrapassa a população nacional, consolidando a centralidade desses dispositivos na rotina dos brasileiros. Com essa expansão, cresce também a superfície de exposição a riscos cibernéticos.

Além de sua versatilidade, os smartphones oferecem conectividade constante à internet, o que os torna vetores preferenciais para ataques cibernéticos. A mobilidade, por mais conveniente que seja, traz consigo uma nova série de vulnerabilidades. A dependência desses dispositivos para tarefas cotidianas, como o acesso a serviços bancários, e-mails e sistemas de autenticação, amplia as consequências de uma falha de segurança. Segundo estudo publicado por Alves et al. (2014), o uso intensivo de smartphones sem a devida conscientização sobre segurança torna o usuário final o elo mais fraco da cadeia digital.

É importante destacar que o conceito de segurança da informação não se restringe apenas a barreiras tecnológicas, mas também envolve aspectos comportamentais e sociais. A ausência de práticas básicas de proteção — como o uso de senhas fortes, autenticação multifatorial e cuidados com redes públicas — ainda é frequente, revelando uma lacuna entre o avanço técnico e a preparação dos usuários. Conforme aponta Cravo (2023), essa lacuna reflete, em parte, a ausência de uma política nacional sólida voltada à cibersegurança.

Outro aspecto preocupante é o número crescente de pessoas que usam smartphones sem compreender as implicações de privacidade e segurança. Muitos utilizam aplicativos sem revisar permissões, ignoram atualizações de sistema e desconhecem a existência de configurações de segurança disponíveis. Isso demonstra que, mesmo em um ambiente altamente conectado, a informação crítica nem sempre chega ao usuário de forma compreensível.

Por fim, cabe observar que os smartphones deixaram de ser apenas objetos de uso pessoal e se tornaram ferramentas de trabalho. Com o crescimento do trabalho remoto e da mobilidade corporativa, o risco cibernético se expande também para o ambiente empresarial,

o que exige uma abordagem mais sistemática e articulada sobre a segurança desses dispositivos.

2.2 Ameaças Cibernéticas em Dispositivos Móveis

A gama de ameaças digitais direcionadas a smartphones é ampla e em constante evolução. Dentre os ataques mais comuns estão o *phishing*, o SIM Swap, a instalação de aplicativos espiões (*spyware*) e o uso de redes Wi-Fi públicas para interceptação de dados. A sofisticação desses golpes cresce em paralelo à disseminação de tecnologias móveis, tornando cada vez mais difícil a distinção entre um ambiente seguro e um ambiente comprometido.

O *phishing*, por exemplo, continua sendo uma das formas mais eficazes de ataque. Por meio de links maliciosos enviados por e-mail, SMS ou aplicativos de mensagens, cibercriminosos induzem o usuário a fornecer informações confidenciais. Em dispositivos móveis, esses ataques se tornam ainda mais perigosos devido à dificuldade de verificar a autenticidade de sites e links em telas pequenas. Cravo (2023) argumenta que a engenharia social aplicada nesses casos é extremamente eficaz porque explora diretamente a confiança e a rotina do usuário.

Outro ataque recorrente é o SIM Swap, no qual o criminoso transfere o número da vítima para outro chip SIM, ganhando controle sobre contas bancárias e plataformas de autenticação em dois fatores. Esse tipo de ataque foi responsável por grandes prejuízos financeiros nos últimos anos, inclusive no Brasil, sendo tema de campanhas pontuais promovidas por instituições financeiras e pela Anatel.

Além disso, a instalação inadvertida de aplicativos maliciosos representa um vetor silencioso de invasão de privacidade. Muitos aplicativos aparentemente inofensivos coletam dados sensíveis dos usuários, incluindo localização, lista de contatos, fotos e até registros de chamadas. Estudos indicam que usuários frequentemente aceitam permissões desnecessárias por não entenderem as implicações de segurança envolvidas (ALVES et al., 2014).

Vale destacar também a utilização de redes Wi-Fi públicas sem criptografia, um dos riscos mais comuns e menos percebidos. Em ambientes como cafeterias, aeroportos e praças, os usuários frequentemente se conectam a redes inseguras, tornando seus dados suscetíveis à interceptação. Esse comportamento evidencia a necessidade de uma educação digital contínua e mais acessível.

O cenário descrito demonstra que a segurança de dispositivos móveis exige tanto soluções técnicas quanto campanhas de conscientização. A simples existência de recursos de

proteção não garante sua adoção. É preciso informar, motivar e orientar os usuários sobre a importância de utilizá-los de forma correta e constante.

2.3 Conscientização em Segurança da Informação

A conscientização em segurança da informação é considerada, atualmente, um dos pilares da proteção digital. Ainda que haja um número crescente de ferramentas e soluções técnicas para mitigar riscos cibernéticos, especialistas apontam que nenhuma medida é totalmente eficaz se o comportamento do usuário não for orientado para a segurança. A fronteira entre o digital e o real se torna cada vez mais tênue, exigindo que a educação incorpore, desde cedo, práticas de conscientização e formação voltadas à segurança da informação (IPEA, 2023).

Um dos maiores desafios enfrentados na promoção da conscientização é a transformação da informação técnica em conhecimento acessível e aplicável. Estudos recentes que analisaram um conjunto significativo de publicações científicas na área de segurança da informação ressaltam que uma comunicação eficaz depende da utilização de uma linguagem que seja, ao mesmo tempo, clara e suficientemente detalhada. Além disso, reforçam a importância de adaptar as mensagens de segurança ao contexto do público-alvo, considerando tanto seu nível de familiaridade com a tecnologia quanto suas necessidades específicas. Personalizar o conteúdo, portanto, é um elemento estratégico para promover uma real mudança de comportamento entre os usuários (Zimmeck et al., 2024).

De acordo com Alves et al. (2014), a conscientização deve ser entendida como um processo contínuo e contextualizado, não limitado a ações pontuais ou esporádicas. A eficácia das campanhas depende de sua repetição, da qualidade do conteúdo e da forma como são disseminadas. Campanhas unilaterais, focadas apenas na transmissão de mensagens, tendem a ser menos eficazes do que aquelas que envolvem o usuário em processos participativos, como oficinas, simulações de ataques e conteúdos interativos.

Segundo Eisenstein (2023), a alfabetização digital é uma das estratégias mais eficazes para minimizar os riscos de ataques virtuais. Ensinar crianças, jovens e adultos a reconhecer sinais de fraude, configurar adequadamente a privacidade de seus dispositivos e entender a importância de senhas seguras é essencial para que possam se proteger.

Além disso, a percepção de risco tem papel central na mudança de comportamento. De acordo com uma pesquisa realizada pelo C6 Bank em parceria com o Ipec (2023), usuários que já sofreram golpes digitais tendem a adotar medidas de proteção com maior rigor. O

estudo revelou que 68% passaram a ter mais cautela ao clicar em links suspeitos e 48% reforçaram suas senhas após o incidente, indicando uma mudança significativa de comportamento motivada pela experiência negativa. A prevenção, portanto, deve ser incentivada antes da experiência negativa. Como resume Marcel Stolz; Louise Axon (2023, p. 59)**:**

"Uma mentalidade de cibersegurança consiste em valores, atitudes e práticas – incluindo hábitos de usuários individuais, especialistas e outros atores – no ecossistema de segurança cibernética que aumentam a capacidade dos usuários de se protegerem on-line."

2.4 Campanhas Informativas e Políticas Públicas

As campanhas informativas voltadas à segurança digital têm como objetivo principal a conscientização da população quanto aos riscos envolvidos no uso cotidiano de tecnologias conectadas. No entanto, no Brasil, observa-se uma carência de políticas públicas consistentes e articuladas que deem suporte a essas campanhas de forma contínua. Conforme destaca Cravo (2023), a inexistência de uma estratégia nacional consolidada para a cibersegurança compromete a eficácia das ações educativas e deixa a população desassistida frente a ameaças cada vez mais sofisticadas.

Outro ponto crítico é a centralização dessas campanhas em órgãos governamentais, sem articulação com outras esferas sociais. A ausência de parcerias consistentes entre governo, setor privado, escolas e universidades resulta em ações isoladas, muitas vezes redundantes ou mal direcionadas. Iniciativas da Anatel e do Banco Central, como a campanha #FiqueEsperto, são exemplos de tentativas de orientação digital, mas sua divulgação e penetração social ainda são limitadas (ANATEL, 2023).

Políticas públicas eficazes devem, portanto, superar o modelo tradicional de campanhas instrutivas e migrar para modelos formativos, que envolvam educação digital desde a escola básica, capacitação de professores, formação continuada de profissionais e inclusão digital crítica.

2.5 A Relação entre Informação e Ação

Apesar da crescente disseminação de informações sobre segurança digital, muitos usuários ainda mantêm práticas vulneráveis, como o uso de senhas fracas, o compartilhamento de dados pessoais e a ausência de autenticação em dois fatores. Esse descompasso entre o que se sabe e o que se faz no ambiente digital tem sido abordado por

pesquisadores da área de ciberpsicologia e segurança da informação (BADA; SASSE; NURSE, 2019).

Além disso, há uma tendência comportamental de priorizar a conveniência em detrimento da segurança. Usuários preferem manter logins automáticos e não ativar recursos como autenticação em dois fatores, por acreditarem que esses mecanismos dificultam o uso cotidiano. Isso indica que, mesmo diante do conhecimento, a adoção de práticas protetivas depende de fatores motivacionais e contextuais (Marcel Stolz; Louise Axon , 2023)

Para superar essa lacuna entre saber e agir, é essencial que campanhas de conscientização em segurança digital não apenas informem, mas incentivem a mudança de comportamento. A construção de mensagens claras, adaptadas ao cotidiano e que demonstrem valor prático à proteção digital são estratégias que potencializam a efetividade das ações educativas (CARREIRA et al., 2025).

A transformação da cultura digital requer mais do que instruções técnicas: exige mobilização social, envolvimento institucional e ações contínuas de educação digital que transformem conhecimento em hábito e segurança em valor cultural.

3. METODOLOGIA

3.1 Tipo de Pesquisa

Este trabalho é uma pesquisa aplicada, com abordagem quantitativa e qualitativa. O objetivo é entender o quanto os usuários de smartphones estão conscientes sobre segurança digital e o que pensam sobre a efetividade de campanhas informativas, quando estas existem, por parte de mídias sociais, escolas e até mesmo do governo sobre o tema.

3.2 Planejamento da pesquisa

Foi feito um levantamento de dados por meio de um questionário estruturado, baseado em temas levantados por alunos de segurança da informação da Fatec de Araraquara, auxiliado por professores. O questionário foi criado para coletar dados objetivos sobre hábitos, conhecimentos e opiniões dos participantes.

A coleta foi feita de forma online, usando um formulário enviado por redes sociais e e-mail. Esse método foi escolhido por ser prático, rápido e por alcançar pessoas de diferentes perfis. Os dados foram coletados com respeito ao anonimato e aos princípios éticos.

3.3 População e Amostra

O público da pesquisa foi formado por usuários de smartphones, com foco na região de Araraquara, com diferentes idades e escolaridade. A amostra foi composta por pessoas acessíveis ao autor e que aceitaram participar voluntariamente.

Mesmo que os dados não possam ser generalizados para toda a população, a amostra serve bem para identificar padrões e tendências dentro de um contexto específico (MARCONI; LAKATOS, 2017).

3.4 Instrumento de Coleta de Dados

O questionário foi elaborado pelo autor e dividido em blocos:

- Perfil do participante: idade, gênero, escolaridade;
- Hábitos de segurança: uso de senhas, autenticação em dois fatores, atualizações e antivírus;
- Conhecimento sobre riscos: golpes como *phishing*, SIM Swap e clonagem de WhatsApp;
- Campanhas educativas: se já viu alguma, onde viu, clareza e impacto.

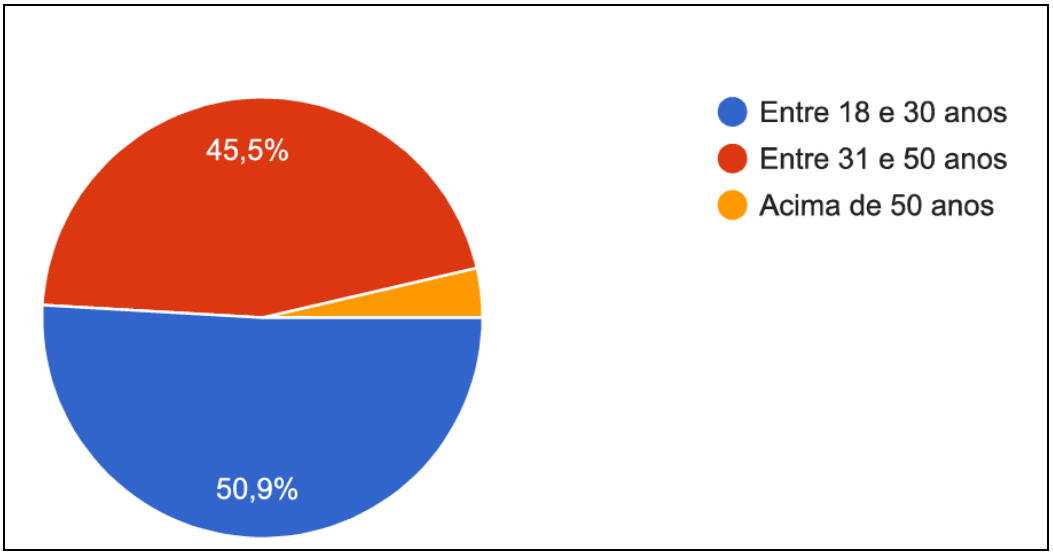
4. RESULTADOS E DISCUSSÕES

A análise dos dados coletados revelou importantes padrões comportamentais relacionados à segurança digital no uso de smartphones. A seguir, os principais achados são discutidos de forma integrada, utilizando gráficos explicativos e análise crítica dos dados.

4.1 Perfil dos Participantes

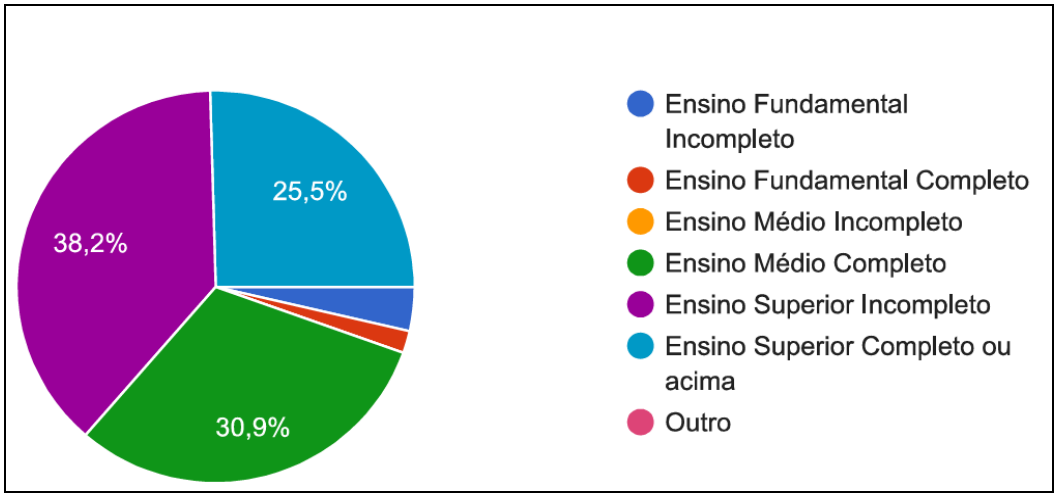
A maioria dos respondentes pertence à faixa etária entre 18 e 50 anos, conforme Gráfico 1, com predominância de escolaridade em nível superior (incompleto ou completo), conforme Gráfico 2. Esse perfil aponta para um público teoricamente mais familiarizado com tecnologia, o que torna os resultados ainda mais relevantes ao evidenciar lacunas de comportamento seguro.

Gráfico 1: Idade dos entrevistados



Fonte: Elaborado pelo autor (2025)

Gráfico 2: Nível de escolaridade dos entrevistados



Fonte: Elaborado pelo autor (2025)

4.2 Uso de Ferramentas de Bloqueio x Aplicativo 'Celular Seguro'

Observa-se que, de forma unânime, os entrevistados consideram importante a existência de uma ferramenta oficial do governo para o bloqueio rápido do celular (Gráfico 3). No entanto, a maioria desconhecia o aplicativo 'Celular Seguro' até o momento da pesquisa (Gráfico 4), e uma parcela significativa dos participantes não utiliza recursos de bloqueio remoto em casos de perda ou roubo do aparelho (Gráfico 5). Esses dados evidenciam a fragilidade na divulgação de iniciativas governamentais, reforçando a constatação de Cravo (2023) sobre a inexistência de uma estratégia nacional de comunicação em cibersegurança.

Gráfico 3:é importante ter ferramenta do governo

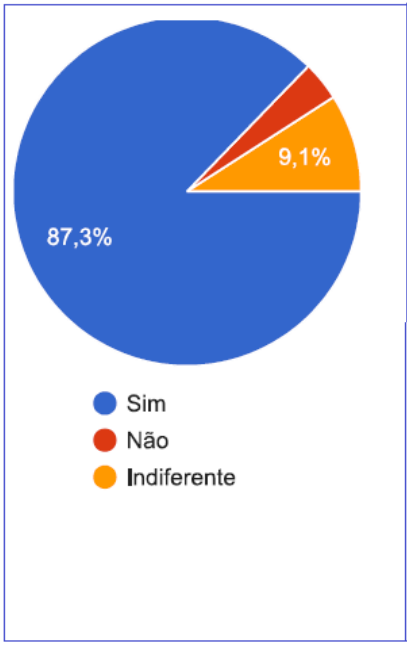


Gráfico 4: conhecia o aplicativo 'Celular Seguro'

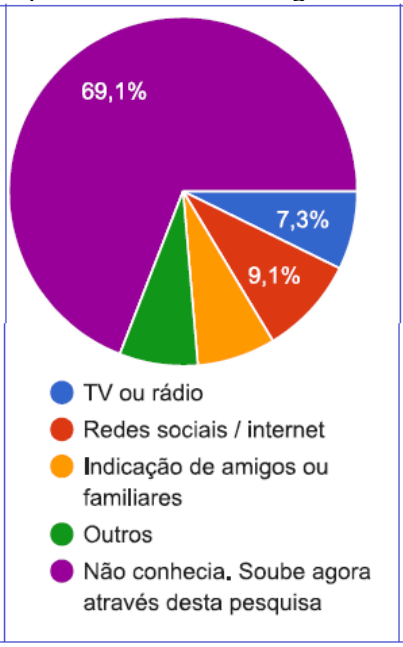
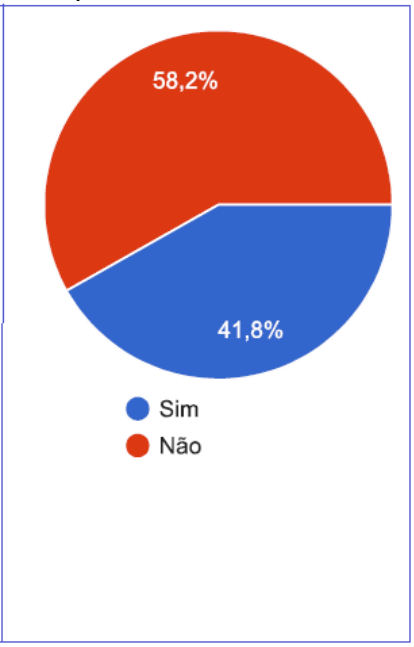


Gráfico 5: utiliza recursos de bloqueio remoto

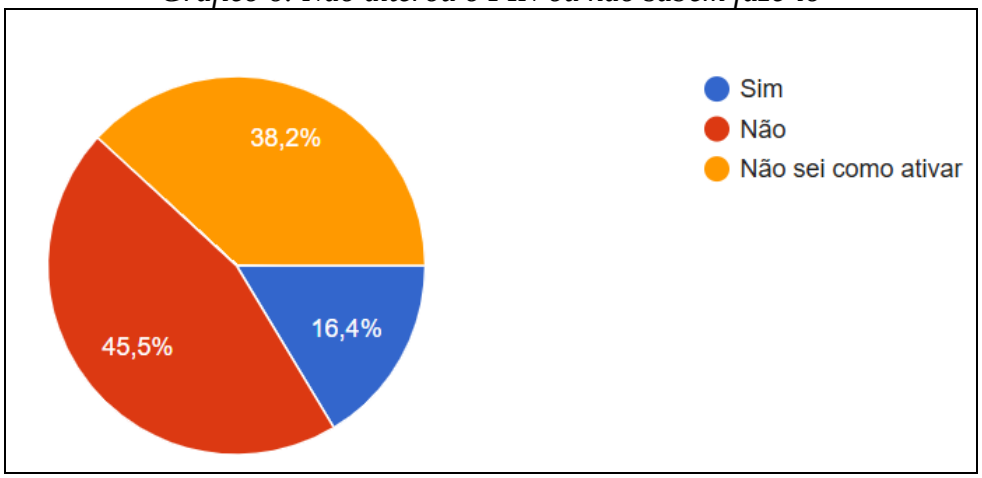


Fonte: Elaborado pelo autor (2025)

4.3 PIN, PUK e Segurança Básica (Sim Swape)

As respostas mostram que muitos usuários não alteraram o PIN padrão de seus chips, ou não sabem como fazê-lo, conforme se observa no Gráfico 6. Tal fragilidade expõe o usuário a ataques como o SIM Swap, uma ameaça séria de golpes no Brasil, conforme relatado por Redação (2023).

Gráfico 6: Não alterou o PIN ou não sabem fazê-lo



Fonte: Elaborado pelo autor (2025)

4.4 Segurança no Whatsapp

Embora o WhatsApp seja um dos aplicativos mais utilizados no Brasil conforme divulgado por Dourado (2025), os dados da pesquisa revelam que uma parcela significativa dos usuários ainda não ativou a verificação em duas etapas (Gráfico 7), nem restringiu a visualização da foto de perfil (Gráfico 8). Tais medidas são fundamentais para prevenir o chamado "golpe do novo número", no qual criminosos se passam por contatos conhecidos, alegando terem trocado de número e solicitando transferências financeiras ou dados pessoais. Esses resultados indicam que o uso frequente de um aplicativo não implica, necessariamente, o domínio de suas funcionalidades de segurança, evidenciando a necessidade de campanhas educativas que orientem os usuários quanto à configuração segura de mensageiros instantâneos.

Gráfico 7: Utiliza verificação em 2 etapas whatsapp

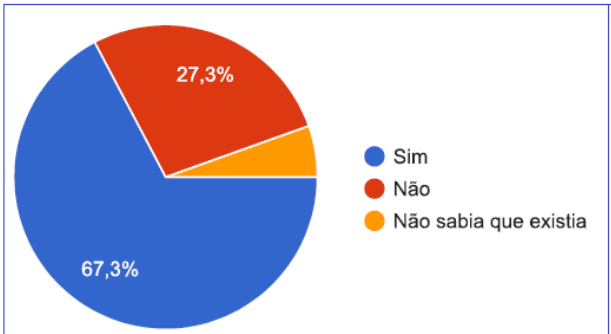
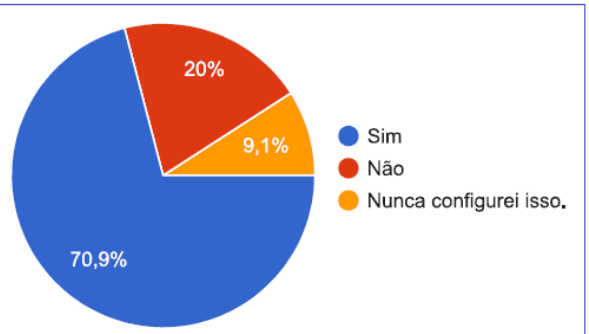


Gráfico 8: Não restringiu a visualização da foto de perfil whatsapp

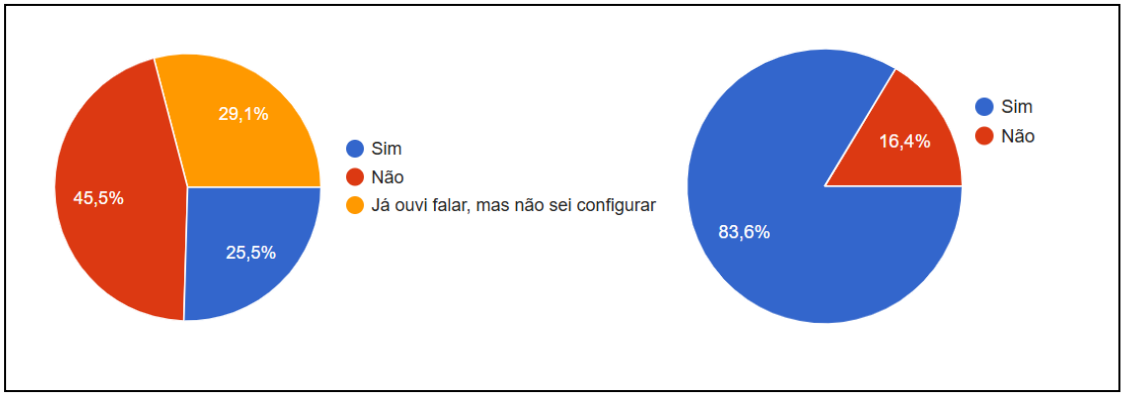


Fonte: Elaborado pelo autor (2025)

4.5 Recursos de Emergência: SOS e Contatos

Embora muitos não conheçam ou não saibam configurar o botão SOS, conforme Gráfico 9, houve interesse unânime em saber como utilizá-lo e concordância com sua utilidade em casos de emergências, conforme Gráfico 10. Isso reforça a importância de campanhas práticas, ilustrativas e acessíveis e que o problema não é de desinteresse, mas de acesso e clareza das informações — ponto também discutido por Zimmeck et al. (2024).

Gráfico 9: Não conhece / Não sabem configurar *Gráfico 10: Interesse em aprender*



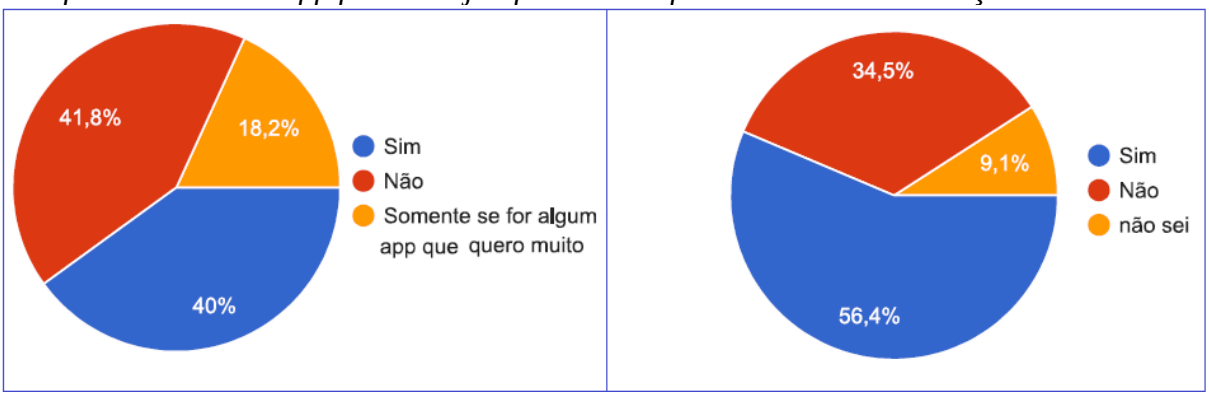
Fonte: Elaborado pelo autor (2025)

4.6 Android Seguro - Atualizações e Aplicativos de Origem Duvidosa

Os dados da pesquisa indicam que uma parcela expressiva dos participantes ainda realiza o download de aplicativos fora das lojas oficiais, como Google Play ou App Store (Gráfico 11), ignorando alertas sobre permissões excessivas e riscos associados a malwares. Além disso, observou-se que poucos usuários demonstram consciência sobre os riscos de manter o sistema operacional desatualizado (Gráfico 12), o que pode comprometer seriamente a segurança do dispositivo.

Esse conjunto de comportamentos reforça a urgência de campanhas educativas que orientem os usuários sobre os perigos dos aplicativos de origem duvidosa, a importância das atualizações regulares e o uso de soluções complementares de proteção, como antivírus e firewalls móveis.

Gráfico 11: Instalou app fora da loja oficial *Gráfico 12: Possui atualizações automáticas*



Fonte: Elaborado pelo autor (2025)

4.7 Percepção das Campanhas Informativas

Os participantes consideram que:

- O governo brasileiro não investe de forma satisfatória em campanhas sobre segurança digital (Gráfico 12).

- As mídias sociais trazem conteúdo, mas ainda de forma insuficiente (Gráfico 13).

- As escolas podem e devem ter papel mais ativo nessa educação (Gráfico 14).

- A iniciativa da Fatec Araraquara foi amplamente aprovada e valorizada, indicando que ações institucionais locais têm forte potencial de impacto (Gráfico 15).

Gráfico 12: Acreditam que o governo investe em campanhas

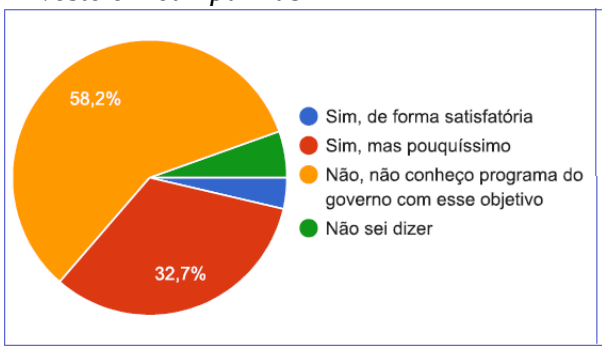
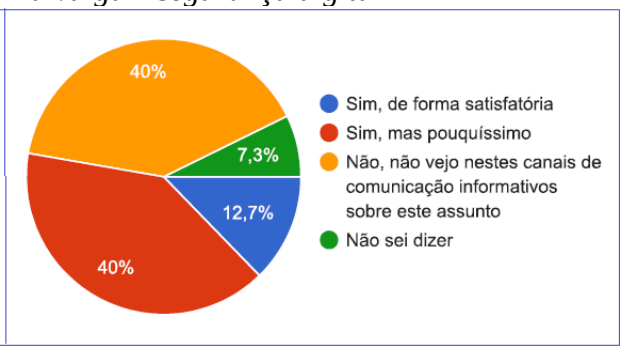


Gráfico 13: Acreditam que as mídias divulgam segurança digital



Fonte: Elaborado pelo autor (2025)

Gráfico 14: Acreditam que escolas podem contribuir em campanhas

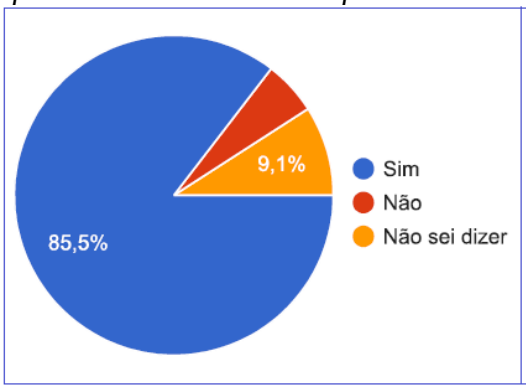


Gráfico 15: Aprovam a iniciativa da Fatec em campanhas de segurança digital

Fonte: Elaborado pelo autor (2025)

5. CONSIDERAÇÕES FINAIS

A presença crescente dos smartphones na sociedade contemporânea, embora traga inúmeros benefícios, também expôs os usuários a um aumento significativo de golpes cibernéticos. Diante desse cenário, este estudo buscou investigar o nível de conscientização dos usuários de smartphones em relação à segurança digital e avaliar a percepção sobre a efetividade das campanhas informativas.

A pesquisa revela uma realidade preocupante: mesmo entre usuários com bom nível de escolaridade e acesso a tecnologias, as práticas de segurança digital ainda são insuficientes. Há um abismo entre o que se sabe ser importante e o que realmente é feito no cotidiano — um reflexo da lacuna entre informação e ação.

Campanhas pontuais e tecnicamente engessadas não são suficientes. O estudo mostra que os usuários estão abertos a aprender, mas precisam de conteúdos mais acessíveis, audiovisuais, práticos e contínuos.

Diante disso, este trabalho propõe que:

- As escolas passem a incluir temas de segurança digital em seus currículos desde a educação básica.
- O governo promova campanhas multicanais, com linguagem acessível e recursos visuais.
- Instituições como a Fatec continuem a produzir conteúdo gratuitos, explorando vídeos tutoriais, oficinas e parcerias com a comunidade.

Conclui-se que a chave da proteção digital não está apenas na tecnologia, mas na educação e na capacidade de traduzir conhecimento técnico em ações simples e práticas para o usuário comum.

REFERÊNCIAS

ALVES, V. F. et al. Segurança Cibernética e Políticas Públicas no Brasil. Anais do SEGeT – **Simpósio de Excelência em Gestão e Tecnologia,** 2014. Disponível em: https://www.aedb.br/seget/arquivos/artigos14/38620415.pdf. Acesso em: 2 maio. 2025.

ANATEL. Evento online apresenta práticas para proteção contra golpes virtuais. **Agência Nacional de Telecomunicações**, 2023. Disponível em: https://www.gov.br/anatel. Acesso em: 5 maio. 2025.

BADA, M.; SASSE, A. M.; NURSE, J. R. C. **Cyber Security Awareness Campaigns: Why do they fail to change behaviour?** arXiv, janeiro 2019. Disponível em: <https://arxiv.org/abs/1901.02672>. Acesso em: 10 maio 2025.

C6 BANK; IPEC. **68% dos brasileiros mudaram comportamento para se proteger de golpes digitais**. Security Leaders, 11 abr. 2023. Disponível em: https://securityleaders.com.br/68-dos-brasileiros-mudaram-comportamento-para-se-proteger-de-golpes-digitais/. Acesso em: 5 maio. 2025.

CARREIRA, C.; MENDES, A.; FERREIRA, J. F.; CHRISTIN, N. **A Systematic Review of Security Communication Strategies: Guidelines and Open Challenges**. arXiv, abril 2025. Disponível em: <https://arxiv.org/abs/2504.02109>. Acesso em: 15 maio 2025.

CRAVO, V. C. **Em busca de uma estratégia nacional de segurança cibernética: marco legal e autoridade nacional de segurança cibernética**. 2023. Tese (Doutorado em Estudos Estratégicos Internacionais) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023.

DOURADO, B. **Ranking: as redes sociais mais usadas no Brasil e no mundo em 2023, com insights, ferramentas e materiais - RD Station Blog API**. Disponível em: <https://www.rdstation.com/blog/marketing/redes-sociais-mais-usadas-no-brasil/>. Acesso em: 22 maio 2025.

EISENSTEIN, Evelyn. Crianças, adolescentes e a era digital: benefícios e riscos. **Revista Acadêmica Licencia&acturas**, v. 11, n. 1, p. 7-14, 2023.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA (IPEA). **O papel da segurança cibernética no universo digital**. In: Digitalização e tecnologias transformadoras: implicações para o desenvolvimento nacional. Brasília: IPEA, 2023. Cap. 9, p. 319–332. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/13148/1/Digitalizacao_e_tecnologias_Capitulo_9.pdf. Acesso em: 8 maio 2025

MARCONI, M. A.; LAKATOS, E. M. **Metodologia do trabalho científico.** 7. ed. São Paulo: Atlas, 2017.

REDAÇÃO. **Phishing e SIM Swap estão entre os quatro principais golpes mobile em 2023 - Security Leaders.** Disponível em: <https://securityleaders.com.br/phishing-e-sim-swap-estao-entre-os-quatro-principais-golpes-mobile-em-2023/>. Acesso em: 22 maio 2025.

STOLZ, Marcel; AXON, Louise. **Revisão das capacidades de segurança cibernética do Brasil 2023.** Brasília: GSI-PR, 2023. Disponível em: <https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber/cmm-report-brazil-2023_final_pt.pdf>. Acesso em: 15 maio 2025.

ZIMMECK, Sebastian et al. **A systematic review of security communication: Exploring how to effectively convey security information to users**. arXiv, [S. l.], 2024. Disponível em: https://arxiv.org/pdf/2504.02109v1. Acesso em: 9 maio. 2025.