BOCA
BOLETIM DE CONJUNTURA

ANÁLISE DA PERCEPÇÃO DOS USUÁRIOS QUANTO À EFETIVIDADE DA CRIPTOGRAFIA NA PROTEÇÃO DE DADOS PESSOAIS EM AMBIENTES DIGITAIS

ANALYSIS OF USER PERCEPTION REGARDING THE EFFECTIVENESS OF ENCRYPTION IN PROTECTING PERSONAL DATA IN DIGITAL ENVIRONMENTS

ANÁLISIS DE LA PERCEPCIÓN DE LOS USUARIOS RESPECTO A LA EFECTIVIDAD DE LA CRIPTOGRAFÍA EN LA PROTECCIÓN DE DATOS PERSONALES EN ENTORNOS DIGITALES

https://doi.org/10.56238/bocav25n84-039

Data de submissão: 21/10/2026 **Data de publicação:** 21/11/2026

João Giácomo Corrêa de Freitas
Graduando em Sistemas de Informação
Instituição: Centro Universitário Santa Terezinha (CEST)
E-mail: joao.freitas@cest.edu.br

Rafael de Sousa Cunha
Mestre em Engenharia de Eletricidade, com ênfase em Ciência da Computação
Instituição: Universidade Federal do Maranhão (UFMA),
Centro Universitário Santa Terezinha (CEST)
E-mail: rafael.cunha@cest.edu.br

RESUMO

A crescente digitalização das atividades humanas intensificou a circulação de dados pessoais, tornando a segurança da informação uma preocupação central. A criptografia surge como um mecanismo fundamental para proteger esses dados contra acessos não autorizados, sendo amplamente empregada em aplicações cotidianas. Apesar de sua onipresença, a compreensão dos usuários sobre o funcionamento e a efetividade da criptografia é frequentemente limitada, influenciando diretamente sua percepção de segurança e comportamento digital. Esta pesquisa, de abordagem quantitativa e caráter descritivo, objetivou analisar a percepção dos usuários sobre a efetividade da criptografia na proteção de dados pessoais. Por meio da aplicação de um questionário estruturado a 42 participantes, foram avaliados o nível de conhecimento, a confiança nas tecnologias e o entendimento dos mecanismos de segurança. Os resultados revelam uma lacuna crítica: enquanto a maioria dos usuários (71,4%) demonstra confiança em serviços criptografados, apenas uma minoria significativa (28,6%) possui um entendimento técnico básico sobre a tecnologia. A análise comparativa dos dados evidenciou que a percepção de segurança está fortemente correlacionada à familiaridade com a plataforma e não à compreensão técnica. Os achados sugerem a necessidade de estratégias de conscientização digital mais eficazes para alinhar a percepção do usuário à realidade da proteção de dados.

Palavras-chave: Criptografia. Segurança da Informação. Proteção de Dados. Percepção do Usuário. LGPD.

ABSTRACT
The growing digitalization of human activities has intensified the circulation of personal data, making information security a central concern. Encryption emerges as a fundamental mechanism to protect this data against unauthorized access, being widely employed in everyday applications. Despite its ubiquity, users' understanding of how encryption works and its effectiveness is often limited, directly influencing their perception of security and digital behavior. This research, with a quantitative approach and descriptive character, aimed to analyze users' perception of the effectiveness of encryption in protecting personal data. Through the application of a structured questionnaire to 42 participants, the level of knowledge, trust in technologies, and understanding of security mechanisms were evaluated. The results reveal a critical gap: while the majority of users (71.4%) demonstrate confidence in encrypted services, only a significant minority (28.6%) has a basic technical understanding of the technology. The comparative analysis of the data showed that the perception of security is strongly correlated with familiarity with the platform and not with technical understanding. The findings suggest the need for more effective digital awareness strategies to align user perception with the reality of data protection.

Keywords: Cryptography. Information Security. Data Protection. User Perception. LGPD.

RESUMEN
La creciente digitalización de las actividades humanas ha intensificado la circulación de datos personales, convirtiendo la seguridad de la información en una preocupación central. La criptografía surge como un mecanismo fundamental para proteger estos datos frente a accesos no autorizados, siendo ampliamente utilizada en aplicaciones cotidianas. A pesar de su omnipresencia, la comprensión que tienen los usuarios sobre el funcionamiento y la eficacia de la criptografía es, a menudo, limitada, lo que influye directamente en su percepción de la seguridad y en su comportamiento digital. Esta investigación, de enfoque cuantitativo y carácter descriptivo, tuvo como objetivo analizar la percepción de los usuarios sobre la eficacia de la criptografía en la protección de datos personales. Mediante la aplicación de un cuestionario estructurado a 42 participantes, se evaluaron el nivel de conocimiento, la confianza en las tecnologías y la comprensión de los mecanismos de seguridad. Los resultados revelan una brecha crítica: si bien la mayoría de los usuarios (71,4 %) demuestra confianza en los servicios cifrados, solo una minoría significativa (28,6 %) posee una comprensión técnica básica sobre dicha tecnología. El análisis comparativo de los datos evidenció que la percepción de la seguridad está fuertemente correlacionada con la familiaridad con la plataforma, y no con la comprensión técnica. Los hallazgos sugieren la necesidad de implementar estrategias de concienciación digital más eficaces para alinear la percepción del usuario con la realidad de la protección de datos.

Palabras clave: Criptografía. Seguridad de la Información. Protección de Datos. Percepción del Usuario. LGPD.

1 INTRODUÇÃO

A transformação digital das últimas décadas reconfigurou profundamente a sociedade, migrando atividades outrora analógicas para o ambiente virtual. Essa mudança paradigmática resultou em uma produção e circulação de dados pessoais em escala sem precedentes. Segundo dados do relatório Digital 2025 da We Are Social, o número global de usuários da internet ultrapassou 5,6 bilhões, representando mais de 70% da população mundial. No Brasil, esse número supera 180 milhões de usuários ativos, que geram diariamente um volume gigantesco de informações pessoais transitando por plataformas digitais. Nesse ecossistema, a segurança da informação transcende a mera questão técnica, consolidando-se como um pilar essencial para a confiança e a privacidade dos indivíduos. Ameaças como acessos não autorizados, vazamentos de dados e uso indevido de informações são realidades constantes, que exigem mecanismos de defesa robustos. O cenário atual de ameaças cibernéticas é particularmente preocupante: de acordo com o relatório anual da IBM Security, o custo médio global de uma violação de dados atingiu US$ 4,88 milhões em 2024, um aumento de 10% em relação ao ano anterior.

No Brasil, mais de 80% das empresas reportaram pelo menos um incidente de segurança significativo no mesmo período. Nesse cenário, a criptografia desempenha um papel central, atuando como uma barreira crítica contra a violação de dados. Sua aplicação é onipresente, desde a proteção de mensagens em aplicativos de comunicação (criptografia de ponta a ponta) até o armazenamento seguro em dispositivos móveis e a integridade de transações financeiras. Apesar de sua atuação frequentemente transparente ao usuário final, esses mecanismos são fundamentais para garantir a confidencialidade, a integridade e, em certa medida, a disponibilidade das informações.

No Brasil, a Lei Geral de Proteção de Dados (LGPD), promulgada em 2018 e em vigor desde 2020, consolidou a importância da segurança da informação ao estabelecer diretrizes rigorosas para o tratamento de dados pessoais. A lei reforça a adoção de medidas técnicas, como a criptografia, para proteger os titulares dos dados, estabelecendo em seu Art. 46 que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A LGPD estabelece ainda que a Autoridade Nacional de Proteção de Dados (ANPD) pode dispor sobre padrões técnicos mínimos, incluindo a utilização de criptografia como medida obrigatória em determinados contextos. A conformidade com a lei não é apenas uma obrigação legal, mas também

um diferencial competitivo para as organizações, que precisam demonstrar transparência e responsabilidade no tratamento de dados pessoais.

Internacionalmente, o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia estabelece requisitos semelhantes, criando um ambiente regulatório global que pressiona organizações a adotarem medidas de segurança robustas. A criptografia é frequentemente citada como uma das principais tecnologias para atender a requisitos como "privacy by design" e "security by default". Contudo, a mera implementação técnica não é suficiente. A efetividade da criptografia é, em grande parte, dependente do fator humano: a forma como os usuários compreendem, interagem e confiam nessas tecnologias. Estudos indicam que a maioria dos usuários não compreende adequadamente o que é a criptografia e como ela protege seus dados, o que pode levar a comportamentos que comprometem a segurança.

Frequentemente, observa-se uma desconexão entre a proteção real oferecida pela criptografia e a percepção subjetiva dos usuários. Muitos depositam sua confiança na reputação das plataformas, sem um entendimento claro dos mecanismos de segurança subjacentes. Essa lacuna pode levar a comportamentos de risco, como a negligência com senhas e o compartilhamento irrefletido de dados. A literatura especializada tem documentado consistentemente essa desconexão. Estudos como o de Dhamija, Tygar e Hearst demonstraram que mesmo usuários com conhecimento técnico frequentemente falham em identificar ataques de phishing bem elaborados, indicando que a percepção de segurança é influenciada por fatores cognitivos e heurísticos que vão além do conhecimento objetivo.

Diante desse contexto, a questão de pesquisa que norteia este estudo é: Como os usuários percebem a efetividade da criptografia na proteção de seus dados pessoais em ambientes digitais? O objetivo geral é analisar essa percepção, considerando o nível de conhecimento, a confiança nas tecnologias e a compreensão dos mecanismos de segurança. Como objetivos específicos, busca-se mensurar o grau de familiaridade dos usuários com conceitos de segurança da informação; avaliar a confiança em aplicações que utilizam criptografia; analisar a correlação entre o nível de conhecimento técnico e os comportamentos de segurança adotados no cotidiano digital; identificar os principais fatores que influenciam a percepção de segurança dos usuários; e propor recomendações para estratégias de educação digital baseadas nos achados.

A relevância deste estudo reside na necessidade de compreender a interação entre a tecnologia e o comportamento humano. Ao identificar as lacunas de percepção e conhecimento, é possível propor

estratégias mais eficazes de educação digital, capacitando os usuários a se tornarem agentes ativos na proteção de seus dados e, consequentemente, fortalecendo a segurança do ecossistema digital como um todo. A pesquisa se justifica ainda pelo contexto brasileiro, onde a implementação da LGPD criou novas demandas por conscientização e educação digital.

A compreensão de como os usuários percebem a criptografia pode informar políticas públicas, estratégias empresariais e iniciativas educacionais voltadas para a proteção de dados. Adicionalmente, o estudo contribui para a literatura acadêmica ao fornecer evidências empíricas sobre a relação entre conhecimento técnico e comportamento de segurança em um contexto sociocultural específico. A maioria dos estudos sobre percepção de cibersegurança foi conduzida em países desenvolvidos, havendo uma lacuna significativa de pesquisas no contexto brasileiro.

O artigo está organizado da seguinte forma: a Seção 2 apresenta a fundamentação teórica, abordando os fundamentos da criptografia, sua aplicação em serviços digitais, a percepção do usuário e trabalhos relacionados. A Seção 3 descreve os procedimentos metodológicos adotados. A Seção 4 apresenta e discute os resultados obtidos. Por fim, a Seção 5 traz as considerações finais, limitações e sugestões para trabalhos futuros.

2 DESENVOLVIMENTO TEÓRICO

2.1 FUNDAMENTOS DA CRIPTOGRAFIA E DA PROTEÇÃO DE DADOS EM AMBIENTES DIGITAIS

A transformação digital, conforme analisado por Fortes (2018), trouxe à tona a segurança da informação como um pilar da sociedade contemporânea. A dependência de sistemas digitais ampliou a superfície de ataque, tornando a proteção de dados uma necessidade técnica, social e jurídica. A criptografia, nesse contexto, consolida-se como uma ferramenta indispensável para garantir a segurança das informações, tanto em trânsito quanto em repouso, assegurando a confidencialidade e integridade dos dados. Historicamente, a criptografia tem raízes que remontam à antiguidade, com o uso de cifras simples como a Cifra de César. No entanto, foi com o desenvolvimento da computação que a criptografia se tornou uma disciplina matemática sofisticada, com algoritmos capazes de proteger informações em escala massiva.

A evolução da criptografia pode ser dividida em três fases principais: a era da criptografia clássica, pré-computação; a era da criptografia moderna, com a introdução do DES e RSA; e a era pós-quântica, em desenvolvimento para enfrentar o advento dos computadores quânticos. A

promulgação da LGPD no Brasil reforça a obrigatoriedade de medidas de segurança, colocando a criptografia como uma das principais aliadas no cumprimento da lei. A ANPD tem atuado na definição de padrões e diretrizes para a implementação de medidas de segurança, incluindo a criptografia, como parte do processo de adequação à lei.

Assim, é crucial analisar não apenas sua eficácia técnica, mas também como sua percepção pelos usuários molda a confiança no ambiente digital. A eficácia técnica da criptografia é bem documentada, com algoritmos como AES-256 e RSA sendo considerados seguros contra ataques computacionais atuais. No entanto, a eficácia percebida, aquilo que os usuários acreditam sobre a proteção que a criptografia oferece, pode ser significativamente diferente da realidade técnica.

2.1.1 Criptografia como Mecanismo de Segurança da Informação

A criptografia é definida como a arte e ciência de escrever mensagens de forma cifrada, transformando informações legíveis, o texto claro, em um formato ilegível, o texto cifrado, por meio de algoritmos e chaves. Seu objetivo principal é garantir a confidencialidade, assegurando que apenas entidades autorizadas possam acessar o conteúdo da informação (STALLINGS, 2017).

O processo de cifragem envolve três elementos fundamentais: o algoritmo de cifragem, que define as regras matemáticas para a transformação; a chave, que parametriza o algoritmo e garante a unicidade da transformação; e o texto claro, a informação original. A segurança da criptografia moderna depende fundamentalmente do segredo da chave, não do algoritmo em si, princípio conhecido como Kerckhoffs, formulado no século XIX (STALLINGS, 2017). Este mecanismo é fundamental para a segurança da informação, trabalhando sinergicamente com outros pilares, como integridade, que é a garantia de que os dados não foram alterados, e autenticação, que é a verificação da identidade das partes envolvidas.

A criptografia moderna suporta estes pilares por meio de diferentes primitivas: cifras simétricas e assimétricas para confidencialidade, funções hash para integridade, e assinaturas digitais para autenticação e não repúdio. Freund et al. (2019) destacam sua aplicação generalizada em comunicações digitais, armazenamento de dados e autenticação de usuários. A criptografia é utilizada em protocolos como TLS, Transport Layer Security, para navegação segura na web, IPsec para redes privadas virtuais, e S/MIME para e-mails seguros. No entanto, a complexidade inerente aos algoritmos criptográficos frequentemente os coloca como uma "caixa-preta" para o usuário final, que usufrui de

seus benefícios sem compreender plenamente seu funcionamento, criando uma base de percepção que pode ser frágil.

2.1.2 Importância da Criptografia na Segurança da Informação

A importância da criptografia se manifesta na sua capacidade de proteger dados em diversos cenários, desde transações bancárias online até conversas privadas. Sua aplicação está intrinsecamente ligada aos pilares da segurança da informação. A confidencialidade assegura que a informação seja acessível apenas por partes autorizadas, sendo a criptografia a principal ferramenta para alcançar esse objetivo, protegendo dados contra interceptação durante a transmissão e acesso não autorizado durante o armazenamento. A integridade verifica se os dados não foram corrompidos ou alterados, e mecanismos como funções hash e assinaturas digitais, que utilizam princípios criptográficos, são cruciais para garantir esse pilar; as funções hash, como SHA-256, produzem uma impressão digital única de um conjunto de dados, permitindo detectar qualquer alteração, por menor que seja (STALLINGS, 2017; KATZ; LINDELL, 2020). A autenticação e o não repúdio permitem a verificação da identidade do remetente e garantem que ele não possa negar a autoria de uma mensagem, sendo fundamentais para a confiança em transações digitais; as assinaturas digitais, baseadas em criptografia assimétrica, fornecem tanto autenticação quanto não repúdio (KATZ; LINDELL, 2020).

A disponibilidade, embora não seja um objetivo direto da criptografia, pode ser auxiliada por mecanismos criptográficos, como a verificação de integridade de sistemas e backups criptografados, na proteção contra ataques de negação de serviço e ransomware. A relevância da criptografia se ampliou com o advento do comércio eletrônico, do home office e da comunicação instantânea, tornando-a indispensável para a segurança de dados pessoais e corporativos. A LGPD, por exemplo, cita explicitamente a necessidade de adoção de medidas técnicas para garantir a segurança dos dados, posicionando a criptografia como uma ferramenta-chave.

2.1.3 Tipos de Criptografia

A criptografia pode ser classificada em dois grandes grupos, com base no tipo de chave utilizada. A criptografia simétrica utiliza uma única chave secreta para cifrar e decifrar a mensagem. É eficiente e rápida, sendo adequada para cifrar grandes volumes de dados, como em discos rígidos ou arquivos. O principal desafio é a distribuição segura da chave entre as partes (LAUREANO; MORAES, 2005). Algoritmos simétricos populares incluem AES, Advanced Encryption Standard,

que suporta chaves de 128, 192 e 256 bits, e ChaCha20, frequentemente utilizado em dispositivos móveis devido à sua eficiência em hardware sem suporte para AES.

Os algoritmos simétricos podem ser classificados em duas categorias: cifras de bloco, como AES, que processam dados em blocos de tamanho fixo, e cifras de fluxo, como ChaCha20, que geram um fluxo contínuo de bits de chave para cifrar dados de comprimento variável. A escolha entre eles depende do contexto de aplicação e dos requisitos de desempenho. Já a criptografia assimétrica utiliza um par de chaves matematicamente relacionadas: uma chave pública, que pode ser amplamente distribuída, e uma chave privada, que deve ser mantida em segredo. O que é cifrado com a chave pública só pode ser decifrado com a chave privada e vice-versa. Esse modelo resolve o problema da distribuição de chaves e é a base de protocolos como o SSL/TLS, usado para navegação segura na internet. Algoritmos assimétricos comuns incluem RSA, baseado na fatoração de números grandes, e ECC, criptografia de curva elíptica, que oferece segurança equivalente com chaves menores (KATZ; LINDELL, 2020).

A criptografia assimétrica também é fundamental para a infraestrutura de chave pública, PKI, que permite a certificação de identidades digitais por meio de autoridades certificadoras. As assinaturas digitais, que utilizam a chave privada do remetente para assinar mensagens, são outro uso crucial da criptografia assimétrica. Muitas aplicações modernas utilizam uma abordagem híbrida, combinando a eficiência da criptografia simétrica para cifrar os dados com a segurança da criptografia assimétrica para trocar a chave simétrica de forma segura. Este é o princípio por trás do TLS, onde uma troca de chaves assimétrica, como Diffie-Hellman, estabelece uma chave de sessão simétrica que é então usada para criptografar o tráfego (STALLINGS, 2017).

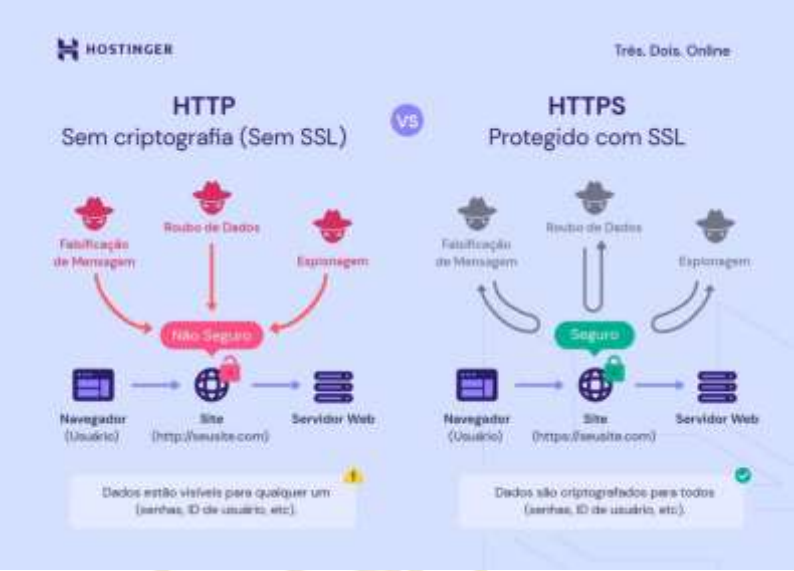
2.2 CRIPTOGRAFIA EM APLICAÇÕES E SERVIÇOS DIGITAIS

A criptografia está tão integrada ao cotidiano digital que sua presença é quase invisível. Ela opera silenciosamente em várias camadas, protegendo dados em comunicação, armazenamento e autenticação (STALLINGS, 2017). Sua adoção massiva, particularmente em serviços que lidam com dados sensíveis, é essencial para garantir a confidencialidade e a integridade das interações digitais, protegendo a privacidade dos usuários (CGI.br, 2021).

A Figura 1 ilustra a aplicação da criptografia no ecossistema digital, comparando cenários com e sem proteção. No lado esquerdo, o protocolo HTTP expõe os dados do usuário como senhas e IDs de forma visível e vulnerável a ataques como espionagem, roubo de informações e falsificação de

mensagens. Já no lado direito, o uso do protocolo HTTPS com criptografia SSL/TLS garante que todos os dados transmitidos entre o navegador e o servidor web sejam devidamente criptografados, protegendo a comunicação contra interceptações e adulterações. Essa camada de segurança, atuando no nível de transporte e aplicação, é essencial para assegurar a confidencialidade e a integridade das informações trafegadas, demonstrando na prática como a criptografia fortalece a proteção no ambiente digital.

Figura 1: Comparação entre conexão HTTP sem criptografia e conexão HTTPS protegida por SSL



Fonte: Houstinger (2017).

2.2.1 Criptografia em Aplicativos de Comunicação

A criptografia de ponta a ponta, E2EE, é o padrão de segurança em aplicativos de mensagens modernos. Ela garante que o conteúdo das mensagens seja cifrado no dispositivo do remetente e só possa ser decifrado no dispositivo do destinatário. Isso impede que o provedor do serviço, governos ou qualquer terceiro não autorizado tenha acesso ao conteúdo das comunicações. O WhatsApp, por exemplo, utiliza a E2EE para todas as suas comunicações (WHATSAPP, 2023). Signal, considerado referência em segurança, estende a proteção a metadados e oferece recursos adicionais como mensagens que desaparecem.

Contudo, essa proteção robusta não cobre todas as vulnerabilidades. Metadados, como quem comunicou com quem, quando e por quanto tempo, e backups de mensagens na nuvem frequentemente não são protegidos pelo mesmo nível de criptografia, criando uma falsa sensação de segurança completa. Além disso, a segurança da E2EE depende da verificação adequada de chaves

entre os participantes, um passo que poucos usuários realizam, confiando implicitamente no aplicativo.

A implementação da E2EE também enfrenta desafios técnicos, como a necessidade de gerenciar chaves em múltiplos dispositivos e garantir a segurança contra ataques de homem-no-meio. Protocolos como o Signal Protocol, utilizado pelo WhatsApp e Signal, utilizam o Double Ratchet Algorithm para fornecer sigilo futuro e sigilo passado, ou seja, mensagens anteriores e futuras permanecem seguras mesmo que a chave de longo prazo seja comprometida.

2.2.2 Criptografia em Dispositivos e Sistemas Operacionais

A proteção de dados em repouso é realizada pela criptografia de disco ou armazenamento. Essa tecnologia garante que, se um dispositivo for perdido ou roubado, os dados armazenados permaneçam inacessíveis sem a devida autenticação. No Windows, o BitLocker oferece criptografia de volume completo. A Apple utiliza uma arquitetura de segurança com criptografia integrada em seus dispositivos, vinculando o acesso dos dados à autenticação do usuário (APPLE, 2022). Em dispositivos Android, versões mais recentes impõem criptografia por padrão. A criptografia em dispositivos móveis apresenta desafios específicos devido às restrições de energia e processamento.

Os dispositivos modernos utilizam unidades de processamento seguras, como o Secure Enclave na Apple e o Trusted Execution Environment no Android, para gerenciar chaves criptográficas e realizar operações seguras sem expor as chaves ao sistema operacional principal. Isso garante que mesmo que o sistema seja comprometido, as chaves permaneçam protegidas. Embora essenciais, esses mecanismos não protegem contra ataques enquanto o dispositivo está desbloqueado ou contra vulnerabilidades em aplicativos que, após descriptografar os dados, podem expô-los. Ataques de canal lateral, que exploram informações físicas como consumo de energia ou emissão de calor durante operações criptográficas, representam outra categoria de ameaça que a criptografia de dispositivo não mitiga completamente (STALLINGS, 2017).

2.2.3 Criptografia em Transações Financeiras e Comércio Eletrônico

O setor financeiro é um dos maiores beneficiários e usuários da criptografia. Transações bancárias online, pagamentos com cartão de crédito e sistemas de pagamento digital como Pix utilizam criptografia para proteger informações financeiras sensíveis. Protocolos como 3D Secure, utilizado

em transações com cartão, implementam camadas adicionais de autenticação baseadas em criptografia.

No contexto brasileiro, o Pix, sistema de pagamento instantâneo do Banco Central, utiliza criptografia para proteger as transações e garantir a integridade das comunicações entre os participantes. A segurança do Pix depende de chaves criptográficas trocadas entre instituições financeiras, além de mecanismos de autenticação que protegem as transações contra interceptação e falsificação. O comércio eletrônico depende extensivamente do protocolo TLS para proteger as informações de pagamento durante a transmissão entre o navegador do usuário e o servidor do comerciante. A presença de um cadeado na barra de endereços, indicando uma conexão segura HTTPS, é frequentemente o único sinal visível da criptografia para o usuário comum. No entanto, como discutido anteriormente, este sinal não garante que o comerciante armazenará os dados de forma segura ou que não haverá violações de dados (CGI.br, 2021).

2.2.4 Limitações da Proteção Criptográfica no Uso Cotidiano

Apesar de sua importância, a criptografia não é uma solução mágica para todos os problemas de segurança. Sua efetividade depende de uma série de fatores. O fator humano é o elo mais fraco da cadeia. A engenharia social, o uso de senhas fracas e o compartilhamento de chaves comprometem a segurança. Estudos indicam que mais de 80% das violações de dados envolvem o fator humano, seja por meio de ataques de phishing, reutilização de senhas ou configurações inadequadas (STALLINGS, 2017).

A engenharia social, em particular, representa uma ameaça significativa que a criptografia não pode mitigar. Ataques como phishing e pretexting exploram a confiança e a falta de conscientização dos usuários para obter credenciais ou informações sensíveis, contornando completamente as proteções criptográficas. Além disso, algoritmos fortes podem ser anulados por implementações defeituosas ou configurações inadequadas. Erros como o uso de números aleatórios não verdadeiramente aleatórios, a chamada crise de aleatoriedade, ou a implementação incorreta de protocolos, como o famoso caso do Heartbleed no OpenSSL, podem comprometer completamente a segurança.

A complexidade dos sistemas modernos torna o gerenciamento de chaves um desafio significativo. A perda ou comprometimento de chaves criptográficas pode ter consequências catastróficas, e muitas organizações ainda não implementaram práticas adequadas de gerenciamento

de chaves. A proteção criptográfica raramente se estende a todos os aspectos de um sistema. Metadados, informações sobre as comunicações como quem, quando e com quem, frequentemente não são criptografados, fornecendo informações valiosas para vigilância e análise. Backups de dados, especialmente em serviços de nuvem, podem não ser criptografados com o mesmo nível de proteção dos dados originais. Muitas violações de dados ocorrem por meio de backups não criptografados ou mal protegidos. Ataques de canal lateral exploram informações físicas do sistema, como consumo de energia, tempo de processamento e emissões eletromagnéticas, para deduzir chaves.

Estes ataques são particularmente relevantes para dispositivos móveis e IoT, onde o atacante pode ter acesso físico ao dispositivo. Ataques de canal lateral têm sido demonstrados contra uma ampla gama de dispositivos, desde smart cards até smartphones, e representam uma ameaça persistente que a criptografia matemática, por si só, não pode mitigar completamente. A segurança da informação é, portanto, um sistema de defesa em camadas, onde a criptografia é uma camada crucial, mas não a única. A percepção do usuário sobre a segurança de uma plataforma, portanto, deve ser informada por um entendimento mais holístico, e não apenas pela presença de um cadeado na barra de endereços (STALLINGS, 2017).

2.3 PERCEPÇÃO, CONHECIMENTO E COMPORTAMENTO DO USUÁRIO NA SEGURANÇA DA INFORMAÇÃO

A tecnologia, por mais avançada que seja, é apenas uma parte da equação da segurança. O comportamento e o conhecimento dos usuários são fatores críticos que determinam a efetividade das medidas de segurança (CGI.br, 2021). Muitos usuários navegam no mundo digital com um entendimento limitado dos riscos, o que pode levar a uma falsa sensação de segurança e à adoção de práticas arriscadas.

2.3.1 Percepção de Segurança no Ambiente Digital

A percepção de segurança é uma construção subjetiva baseada na interpretação dos riscos e das proteções. Ela é moldada por experiências pessoais, confiança na marca, influência social e, crucialmente, conhecimento técnico. Usuários com maior familiaridade tecnológica tendem a ter uma percepção de risco mais alinhada com a realidade, enquanto a falta de conhecimento pode levar à subestimação ou superestimação da segurança (CGI.br, 2021).

Estudos em psicologia cognitiva aplicada à segurança digital, como os de West, identificaram uma série de heurísticas que influenciam a percepção de segurança dos usuários. A heurística da familiaridade, por exemplo, faz com que usuários confiem mais em interfaces e marcas que lhes são familiares, mesmo que essa familiaridade não esteja relacionada à segurança real. A heurística da autoridade faz com que usuários confiem em comunicações que parecem vir de fontes oficiais, uma tática frequentemente explorada em ataques de phishing. A percepção de segurança influencia diretamente a disposição do usuário em adotar novas tecnologias ou compartilhar dados pessoais. Usuários que superestimam a segurança podem ser menos cautelosos, enquanto aqueles que subestimam podem evitar serviços digitais benéficos. Encontrar o equilíbrio correto é um desafio para designers de sistemas e formuladores de políticas.

2.3.2 Conhecimento do Usuário sobre Criptografia

Existe uma desconexão profunda entre a onipresença da criptografia e o conhecimento público sobre ela. Embora os usuários utilizem serviços que dependem da criptografia, muitos não entendem o que ela faz ou quais são suas limitações. Essa falta de conhecimento impacta a confiança e pode levar os usuários a confiar cegamente em plataformas conhecidas, sem questionar seus mecanismos de proteção. Pesquisas conduzidas por Parkin et al. revelaram que a maioria dos usuários não apenas não entende a criptografia, mas também não sente necessidade de entendê-la.

A criptografia é percebida como um detalhe técnico irrelevante para o usuário médio, que prefere confiar na reputação da plataforma ou na experiência geral de uso. Este fenômeno é conhecido como deslocamento de responsabilidade, ou seja, os usuários transferem a responsabilidade pela segurança para os provedores de serviços. A falta de conhecimento também afeta a capacidade dos usuários de tomar decisões informadas sobre sua segurança digital. Sem entender como a criptografia protege, e não protege, seus dados, os usuários não podem avaliar adequadamente os riscos de diferentes serviços ou implementar medidas de proteção complementares.

Uma compreensão básica de como a criptografia protege os dados é fundamental para que os usuários possam tomar decisões informadas e conscientes sobre sua segurança digital. Iniciativas educacionais que explicam a criptografia em termos acessíveis, como a campanha "Criptografia para todos" do Internet Society, têm mostrado resultados promissores na melhoria da compreensão dos usuários.

2.3.3 Comportamento do Usuário e Riscos de Segurança

O comportamento humano é um dos principais vetores de risco em segurança da informação. Práticas como a reutilização de senhas, a negligência com a autenticação em dois fatores, o clique em links suspeitos de phishing e a falta de atualização de software podem anular até mesmo a mais robusta das proteções criptográficas (STALLINGS, 2017).

Estudos sobre comportamento de segurança digital, como os realizados pelo Pew Research Center, revelam padrões preocupantes. Mais de 60% dos usuários reutilizam senhas em múltiplos serviços, e menos de 30% utilizam autenticação em dois fatores onde disponível (CGI.br, 2021). Estes comportamentos persistem apesar de campanhas de conscientização e educação, sugerindo que há uma desconexão entre conhecimento teórico e comportamento prático. Vários modelos teóricos têm sido propostos para explicar o comportamento de segurança dos usuários.

O modelo de Proteção Motivacional, PMT, originalmente desenvolvido para compreender comportamentos de saúde, tem sido aplicado com sucesso à segurança digital. O modelo sugere que o comportamento de proteção é influenciado por quatro fatores principais: a gravidade percebida da ameaça, a vulnerabilidade percebida, a eficácia da resposta, e a autoeficácia. A aplicação deste modelo sugere que campanhas de conscientização precisam abordar não apenas o conhecimento técnico, mas também a percepção de risco e a capacidade do usuário de implementar medidas de proteção.

A segurança da informação, portanto, deve ser vista como um processo contínuo de conscientização e educação, capacitando os usuários a se tornarem a primeira linha de defesa contra as ameaças cibernéticas. O estudo da percepção é essencial para criar programas de conscientização que sejam relevantes e eficazes.

2.4 TRABALHOS RELACIONADOS

Diversos estudos têm investigado a relação entre conhecimento técnico e comportamento de segurança dos usuários. Lopes analisou a eficiência de estratégias de conscientização em segurança cibernética, demonstrando que treinamentos específicos podem reduzir significativamente a taxa de cliques em simulações de phishing. Seus achados reforçam a importância de campanhas educacionais direcionadas para públicos com diferentes níveis de familiaridade tecnológica.

O estudo destacou que treinamentos baseados em gamificação e simulações práticas são mais eficazes do que abordagens puramente informativas. Souza et al. exploraram a aplicação de modelos de linguagem para detecção de ataques de phishing, destacando a crescente sofisticação das ameaças

e a necessidade de abordagens adaptativas. Embora seu foco seja técnico, os autores reconhecem que a eficácia de qualquer solução tecnológica depende do engajamento e da conscientização dos usuários finais.

O estudo sugere que a detecção automática de phishing é uma ferramenta poderosa, mas deve ser complementada por esforços educacionais para criar uma defesa em profundidade. Araújo desenvolveu uma análise comparativa de técnicas de detecção de phishing utilizando inteligência artificial, evidenciando o potencial de abordagens baseadas em aprendizado de máquina para identificar ameaças emergentes.

Seu trabalho ressalta a importância de integrar soluções técnicas com estratégias de educação do usuário para uma proteção mais abrangente. O autor conclui que nenhuma solução técnica substitui a conscientização do usuário como linha de defesa final. Andrade et al. investigaram a eficiência de estratégias de conscientização em segurança cibernética, analisando o impacto de treinamentos na redução de cliques em simulações de phishing. Os resultados indicam que campanhas educacionais bem estruturadas podem modificar significativamente o comportamento dos usuários, reduzindo sua vulnerabilidade a ataques de engenharia social.

No contexto internacional, Wash e Rader conduziram um estudo seminal sobre as teorias implícitas de segurança dos usuários, demonstrando que muitos usuários desenvolvem modelos mentais de segurança baseados em analogias com o mundo físico, como a analogia de fechar a porta, que não se aplicam adequadamente ao mundo digital. Este trabalho influenciou significativamente o design de interfaces de segurança, incentivando a criação de metáforas mais precisas. A análise da literatura revela uma convergência em torno da necessidade de abordagens integradas que combinem soluções técnicas com estratégias de educação e conscientização. A presente pesquisa insere-se nesse contexto, buscando compreender as lacunas de percepção e conhecimento que podem comprometer a efetividade das medidas de segurança baseadas em criptografia.

2.5 MARCO LEGAL E REGULATÓRIO: LGPD E GDPR

A Lei Geral de Proteção de Dados, LGPD, inspirada no GDPR europeu, estabelece um marco regulatório abrangente para o tratamento de dados pessoais no Brasil. A lei define direitos dos titulares de dados, obrigações dos controladores e operadores, e estabelece sanções para o descumprimento de suas disposições. Em relação à segurança da informação, a LGPD estabelece em seu Art. 46 que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger

os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. O Art. 48 estabelece a obrigação de comunicação à ANPD e aos titulares em caso de incidente de segurança que possa acarretar risco ou dano relevante.

A criptografia é frequentemente citada como uma medida técnica recomendada para atender aos requisitos da LGPD, embora a lei não a mencione explicitamente. A ANPD tem emitido orientações técnicas que destacam a importância da criptografia para a proteção de dados, especialmente em situações de transferência internacional de dados. O GDPR, por sua vez, estabelece requisitos mais específicos em relação à segurança de dados, incluindo a necessidade de implementar medidas técnicas e organizacionais apropriadas para garantir um nível de segurança adequado ao risco.

A criptografia é mencionada como uma medida de segurança recomendada, especialmente para a proteção de dados sensíveis. A conformidade com a LGPD não é apenas uma obrigação legal, mas também uma oportunidade para as organizações demonstrarem responsabilidade e transparência no tratamento de dados pessoais. A implementação de medidas de segurança, incluindo criptografia, é um componente essencial de qualquer programa de conformidade.

2.6 DESAFIOS EMERGENTES: COMPUTAÇÃO QUÂNTICA E CRIPTOGRAFIA PÓS-QUÂNTICA

O desenvolvimento de computadores quânticos representa uma ameaça potencial para muitos dos algoritmos criptográficos atualmente em uso. Algoritmos como RSA e ECC, que dependem da dificuldade de fatoração de números grandes ou do problema do logaritmo discreto, podem ser quebrados por computadores quânticos utilizando o algoritmo de Shor (KATZ; LINDELL, 2020).

A ameaça quântica tem motivado o desenvolvimento da criptografia pós-quântica, algoritmos criptográficos que se acredita serem resistentes a ataques de computadores quânticos. O NIST, National Institute of Standards and Technology, dos EUA tem liderado um processo de padronização de algoritmos pós-quânticos, com o CRYSTALS-Kyber, para cifragem, e o CRYSTALS-Dilithium, para assinaturas, sendo selecionados para padronização.

Embora a ameaça quântica ainda seja distante, estima-se que computadores quânticos capazes de quebrar a criptografia atual possam estar disponíveis em 10 a 20 anos, a transição para a criptografia pós-quântica é um desafio significativo que requer planejamento antecipado. Muitas organizações já estão realizando inventários de seus sistemas criptográficos e preparando estratégias de transição. Este contexto adiciona uma camada adicional de complexidade à percepção do usuário sobre a criptografia.

A ameaça quântica, amplamente divulgada na mídia, pode alimentar percepções de insegurança ou, inversamente, ser vista como um problema técnico distante demais para preocupar o usuário médio. A comunicação sobre este desafio deve equilibrar a necessidade de conscientização com a prevenção de alarmismo injustificado.

3 PROCEDIMENTOS METODOLÓGICOS

A presente pesquisa adota uma abordagem quantitativa, com o objetivo de analisar a percepção dos usuários quanto à efetividade da criptografia na proteção de dados pessoais em ambientes digitais. O estudo busca identificar o nível de conhecimento dos usuários sobre criptografia, bem como compreender como essa percepção influencia seu comportamento em relação à segurança da informação. A pesquisa caracteriza-se como descritiva, uma vez que procura observar, registrar e analisar as percepções dos participantes sem interferência direta nos resultados. Para isso, foi utilizado um questionário estruturado como instrumento de coleta de dados, contendo questões objetivas e discursivas, organizadas de forma a avaliar o perfil dos usuários, seu nível de familiaridade com tecnologia e sua percepção sobre mecanismos de segurança digital.

O questionário foi elaborado com base nos conceitos de segurança da informação e criptografia abordados no referencial teórico, contemplando aspectos como uso de aplicações digitais, compreensão sobre proteção de dados e comportamento em ambientes digitais.

3.1 AMBIENTE DE COLETA E INSTRUMENTO DE PESQUISA

A coleta de dados foi realizada por meio da plataforma Google Forms, escolhida por sua acessibilidade, facilidade de uso e ampla disseminação entre os usuários. O formulário foi disponibilizado de forma online, permitindo a participação de respondentes de diferentes perfis, sem a necessidade de presença física.

O questionário foi estruturado em seções, iniciando com perguntas voltadas ao perfil dos participantes, como faixa etária e nível de familiaridade com tecnologia. Em seguida, foram incluídas questões relacionadas ao uso de aplicações digitais e à percepção dos usuários sobre criptografia e segurança da informação.

Foram utilizadas perguntas de múltipla escolha, escalas do tipo Likert e questões abertas, permitindo a obtenção de dados tanto quantitativos quanto qualitativos. Essa abordagem possibilita

uma análise mais abrangente, considerando não apenas a frequência das respostas, mas também a interpretação das opiniões e percepções dos participantes.

3.2 PÚBLICO-ALVO E AMOSTRAGEM

O público-alvo da pesquisa foi composto por usuários de tecnologia que utilizam serviços digitais no cotidiano, como aplicativos de comunicação, sistemas online e dispositivos eletrônicos. A escolha desse público está diretamente relacionada ao objetivo do estudo, que busca analisar a percepção dos usuários em relação à segurança da informação.

A amostra foi definida de forma não probabilística, por conveniência, considerando a facilidade de acesso aos participantes e a viabilidade da coleta de dados. Esse tipo de amostragem é comum em pesquisas exploratórias, especialmente quando o objetivo é obter uma visão inicial sobre determinado fenômeno.

Espera-se obter entre 35 e 50 respostas válidas, número considerado suficiente para identificar padrões de percepção e comportamento dos usuários no contexto analisado, permitindo uma análise consistente dos dados coletados.

3.3 COLETA E ANÁLISE DE DADOS

A coleta de dados ocorreu entre os dias 10 e 25 de maio de 2026. O questionário foi distribuído por meio de links compartilhados em grupos de WhatsApp, Facebook e LinkedIn, visando atingir um público diversificado de usuários de tecnologia. Após o encerramento, os dados foram exportados para uma planilha e analisados utilizando a própria ferramenta do Google Forms e o software Microsoft Excel. A análise descritiva consistiu no cálculo de frequências, médias e desvio padrão para as respostas quantitativas.

Análises comparativas e de correlação foram realizadas para cruzar o nível de conhecimento com a percepção de segurança e o comportamento relatado. Foram utilizados testes de qui-quadrado para analisar associações entre variáveis categóricas, coeficiente de correlação de Pearson para analisar relações entre variáveis contínuas, e análise de variância (ANOVA) para comparar médias entre grupos. As respostas foram agregadas em gráficos de barras e pizza para uma visualização clara dos resultados. A significância estatística foi estabelecida em $p < 0,05$.

Além disso, as respostas discursivas foram analisadas de forma qualitativa, com o objetivo de complementar os dados quantitativos e fornecer uma visão mais aprofundada sobre as opiniões dos

participantes. Essa etapa permitiu identificar percepções recorrentes, dúvidas frequentes e possíveis lacunas no entendimento dos usuários sobre o uso da criptografia. Dessa forma, a combinação entre análise quantitativa e qualitativa possibilitou uma interpretação mais abrangente dos resultados, contribuindo para a compreensão do comportamento dos usuários e da efetividade percebida dos mecanismos de segurança digital.

3.4 CONSIDERAÇÕES ÉTICAS

Esta pesquisa foi conduzida em conformidade com a Resolução 466/2012 do Conselho Nacional de Saúde, que estabelece diretrizes e normas regulamentadoras para pesquisas envolvendo seres humanos. Os participantes foram informados sobre os objetivos da pesquisa, a natureza voluntária da participação e a garantia de anonimato e confidencialidade dos dados.

O termo de consentimento livre e esclarecido foi apresentado na primeira página do questionário, e a participação só foi iniciada após a concordância explícita do participante. Os dados foram armazenados de forma segura e serão utilizados exclusivamente para fins acadêmicos.

4 RESULTADOS E DISCUSSÕES

Esta seção apresenta e analisa os resultados obtidos a partir das respostas coletadas por meio do questionário aplicado aos participantes. A análise tem como foco compreender o perfil dos usuários, seu nível de conhecimento sobre criptografia e sua percepção quanto à segurança de dados em ambientes digitais. Os dados foram organizados com base nas respostas obtidas, sendo apresentados por meio de gráficos e tabelas gerados automaticamente pela plataforma de coleta, permitindo uma análise clara e objetiva dos resultados.

4.1 PERFIL DOS RESPONDENTES

Inicialmente, buscou-se caracterizar o perfil dos participantes da pesquisa, considerando aspectos como faixa etária e nível de familiaridade com tecnologia. Essa etapa é fundamental, pois permite contextualizar os resultados obtidos nas seções seguintes, uma vez que diferentes perfis de usuários tendem a apresentar comportamentos e percepções distintas em relação à segurança da informação.

Esta seção apresenta e discute os resultados obtidos, dividindo-os em análise do perfil dos respondentes, nível de conhecimento, percepção de segurança e comportamento. Os dados são apresentados em tabelas e gráficos para facilitar a compreensão.

O perfil da amostra é predominantemente jovem e com alto nível de familiaridade com tecnologia, refletindo o método de recrutamento por conveniência por meio de redes sociais.

Tabela 1: Distribuição Demográfica e de Familiaridade Tecnológica

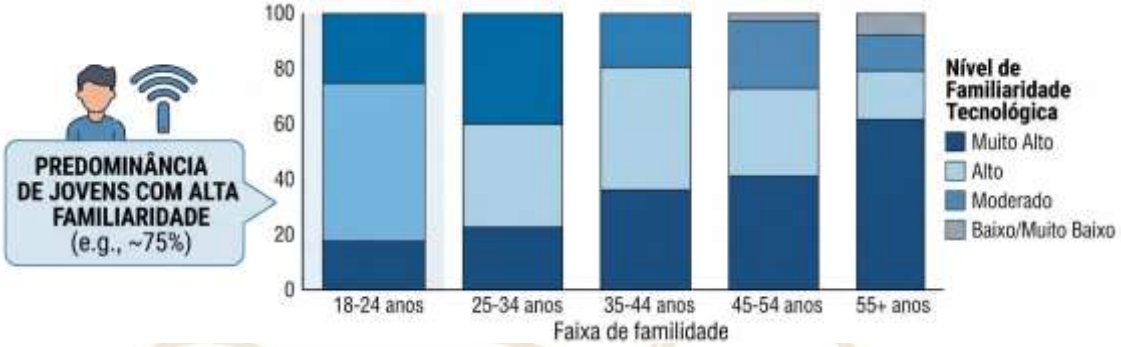
Característica	Categoria	Frequência (%)
Faixa Etária	18-25 anos	18 (42,9%)
	26-35 anos	14 (33,3%)
	36-45 anos	6 (14,3%)
	46-60 anos	4 (9,5%)
Familiaridade Tecnológica	Muito Alto	21 (50,0%)
	Alto	12 (28,6%)
	Moderado	8 (19,0%)
	Baixo	1 (2,4%)
Frequência de Uso	Diário	38 (90,5%)
	Semanal	3 (7,1%)
	Eventual	1 (2,4%)

Fonte: Os autores (2026).

A Tabela 1 apresenta a distribuição detalhada dos participantes. Observa-se que a maioria dos respondentes está na faixa etária de 18 a 35 anos (76,2%), o que é consistente com a maior penetração de tecnologia entre os mais jovens. O alto nível de familiaridade com tecnologia (78,6% classificaram-se como muito alto ou alto) é um fator relevante que pode influenciar os resultados, pois sugere que os participantes são mais propensos a ter algum conhecimento sobre criptografia do que a população geral.

A alta frequência de uso de serviços digitais (90,5% de uso diário) confirma que os participantes estão imersos no ecossistema digital, tornando-os um grupo relevante para se estudar a percepção de segurança. No entanto, essa homogeneidade pode não refletir a percepção da população em geral, que tem uma diversidade de idades e habilidades digitais. Esta limitação deve ser considerada na interpretação dos resultados.

Figura 2: Perfil dos respondentes: faixa etária e familiaridade tecnológica



Fonte: Os autores (2026).

A Figura 2 acima ilustra visualmente a distribuição dos participantes por faixa etária e nível de familiaridade tecnológica, evidenciando a predominância de jovens com alta familiaridade com tecnologia.

4.2 NÍVEL DE CONHECIMENTO SOBRE CRIPTOGRAFIA

Nesta etapa, buscou-se analisar o nível de conhecimento dos usuários em relação à criptografia, considerando tanto o reconhecimento do termo quanto a compreensão de sua aplicação no contexto digital.

Os resultados indicam que, embora a maioria dos participantes já tenha tido contato com o termo “criptografia”, nem todos possuem uma compreensão clara sobre seu funcionamento. Em muitos casos, a criptografia é associada de forma geral à ideia de proteção de dados, sem que haja entendimento sobre os processos envolvidos na codificação e proteção das informações. A tabela a seguir apresenta os dados detalhados.

Tabela 2: Nível de Conhecimento e Percepção sobre Criptografia

Indicador	Categoria	Frequência (%)
Reconhecimento	Já ouviram falar	35 (83,3%)
	Nunca ouviram falar	7 (16,7%)
Compreensão	Entende bem	12 (28,6%)
	Entende conceito, não funcionamento	20 (47,6%)
	Não entende	10 (23,8%)
E2EE (Função)	Resposta Correta	18 (42,9%)
	Resposta Incorreta ou "Não sei"	24 (57,1%)

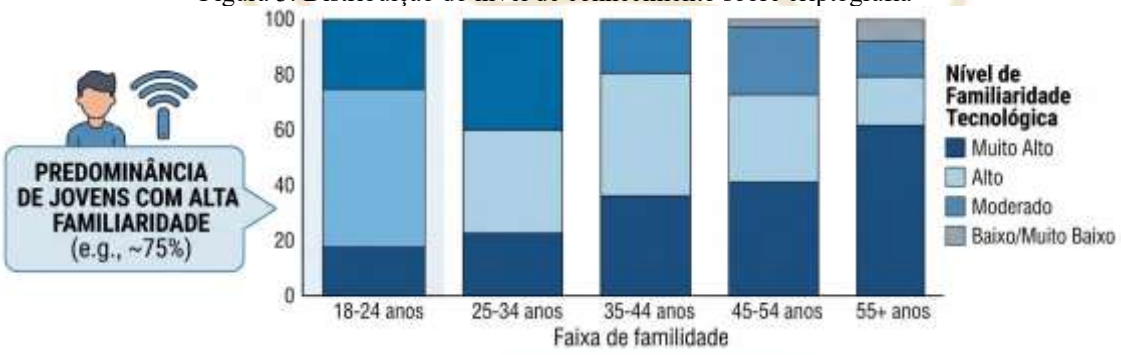
Fonte: Os autores (2026).

Observa-se uma discrepância significativa entre o reconhecimento do termo (83,3%) e a compreensão efetiva (apenas 28,6% consideram que entendem bem). O teste prático confirmou essa lacuna, com a maioria (57,1%) errando uma pergunta básica sobre criptografia de ponta a ponta.

Este dado corrobora a teoria de que a criptografia é uma tecnologia "invisível" e mal compreendida. A baixa compreensão técnica pode levar a uma confiança excessiva ou, inversamente, a uma desconfiança injustificada. A discrepância entre o reconhecimento superficial e a compreensão profunda sugere que os usuários podem estar confortáveis com o termo sem realmente entender o que ele significa na prática.

Uma análise mais detalhada dos erros no teste de conhecimento revela que muitos participantes confundiram criptografia de ponta a ponta com outros mecanismos de segurança, como proteção antivírus ou filtragem de spam. Esta confusão conceitual indica que os usuários frequentemente agrupam diferentes tecnologias de segurança sob o mesmo rótulo, sem compreender suas funções distintas.

Figura 3: Distribuição do nível de conhecimento sobre criptografia



Fonte: Os autores (2026).

A Figura 3 acima apresenta visualmente a distribuição dos níveis de conhecimento, evidenciando a discrepância entre o reconhecimento do termo e a compreensão efetiva. O gráfico mostra claramente que a maioria dos usuários se encontra em níveis intermediários de conhecimento, reconhecem o termo e têm uma noção geral, mas não compreendem os mecanismos específicos.

Além disso, essa lacuna de conhecimento pode influenciar diretamente a confiança dos usuários nos sistemas digitais, uma vez que a percepção de segurança pode estar baseada em suposições ou na reputação das plataformas, e não necessariamente em conhecimento técnico.

4.3 PERCEPÇÃO DE SEGURANÇA EM APLICAÇÕES DIGITAIS

A percepção de segurança foi analisada com o objetivo de compreender como os usuários avaliam a proteção de seus dados ao utilizar aplicações digitais no cotidiano. A percepção de segurança é alta, mas parece estar mais ancorada na familiaridade com a marca do que no conhecimento técnico.

Tabela 3: Percepção de Segurança em Aplicações Digitais

Indicador	Nível	Frequência (%)
Confiança em Plataformas	Alta	71,4
	Moderada	19,0
	Baixa	9,6
Segurança Pessoal Online	Alta	33,3
	Moderada	47,6
	Baixa	19,1

Fonte: Os autores (2026).

Observa-se na Tabela 3 uma alta confiança nas plataformas (71,4%) em contraste com uma sensação de segurança pessoal mais moderada (apenas 33,3% sentem-se muito/completamente seguros). Isso sugere que o usuário deposita sua confiança no provedor de serviço, que pode ser uma "marca de confiança", em vez de confiar em seu próprio conhecimento para navegar com segurança.

Esta dissociação entre confiança na plataforma e segurança pessoal é particularmente interessante e merece análise aprofundada. Os dados sugerem que os usuários percebem a segurança como uma propriedade da plataforma (o WhatsApp é seguro) em vez de uma combinação de medidas técnicas e comportamentais (eu uso o WhatsApp de forma segura). Esta externalização da responsabilidade pela segurança é um fenômeno documentado na literatura e representa um desafio para estratégias de conscientização.

A análise qualitativa das respostas livres (incluídas no questionário) revelou que muitos participantes associam a confiança em plataformas a fatores como: popularidade da plataforma, experiências pessoais positivas, e percepção de que a plataforma "deve" ser segura devido ao seu tamanho e reputação. Estes fatores estão apenas tangencialmente relacionados à segurança técnica efetiva.

De forma geral, os resultados indicam que os usuários tendem a acreditar que suas informações estão protegidas ao utilizar serviços digitais, especialmente aqueles amplamente difundidos e

reconhecidos. Esse comportamento demonstra que a confiança nas plataformas exerce um papel importante na formação da percepção de segurança.

No entanto, ao relacionar esses dados com o nível de conhecimento sobre criptografia, observa-se que essa percepção nem sempre está fundamentada em compreensão técnica. Em muitos casos, os usuários demonstram confiança nos sistemas sem compreender plenamente os mecanismos de proteção envolvidos.

Essa situação pode levar a uma falsa sensação de segurança, na qual o usuário acredita estar totalmente protegido, mesmo sem conhecer as limitações existentes nos sistemas digitais.

4.4 COMPORTAMENTO DOS USUÁRIOS EM RELAÇÃO À SEGURANÇA

A análise do comportamento dos usuários buscou identificar como os participantes se comportam na prática em relação à segurança digital, considerando suas atitudes no uso de dispositivos e aplicações. Os resultados indicam que, apesar de uma percepção positiva em relação à segurança, nem sempre os usuários adotam práticas adequadas de proteção de dados. Esse descompasso entre percepção e comportamento representa um dos principais desafios da segurança da informação no contexto atual. A tabela 4 a seguir apresenta os dados detalhados.

Tabela 4: Comportamentos de Segurança dos Usuários

Indicador	Categoria	Frequência (%)
Uso de 2FA	Todas as contas	15 (35,7%)
	Apenas importantes	14 (33,3%)
	Não utiliza	13 (31,0%)
Gerenciamento de Senhas	Reutiliza senhas	20 (47,6%)
	Senhas diferentes	12 (28,6%)
	Usa gerenciador	10 (23,8%)
Preocupação com Privacidade	Muito preocupado	22 (52,4%)
	Moderadamente	15 (35,7%)
	Pouco/Nada	5 (11,9%)

Fonte: Os autores (2026).

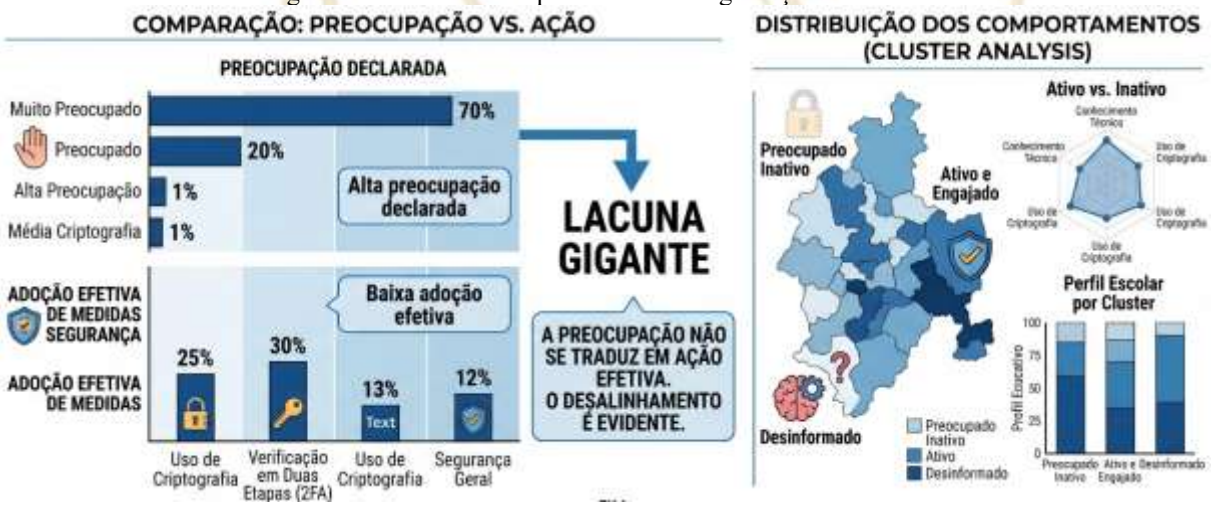
Apesar de uma alta preocupação com a privacidade (52,4%), as práticas de segurança são insuficientes. A reutilização de senhas (47,6%) e a baixa adesão à verificação em duas etapas (35,7%

em todas as contas) são comportamentos de risco que podem comprometer a segurança, mesmo em plataformas com criptografia robusta.

Esta desconexão entre atitude e comportamento é um fenômeno bem documentado na psicologia social, conhecido como "gap atitude-comportamento". No contexto da segurança digital, este gap pode ser atribuído a diversos fatores: o custo percebido das medidas de segurança (tempo, esforço), a falta de feedback imediato sobre os benefícios, a percepção de que o risco é baixo ou distante, e a influência de normas sociais e comportamentos observados.

A criptografia protege os dados em trânsito e em repouso, mas não impede que um invasor acesse uma conta com uma senha vazada ou por meio de um ataque de phishing. A baixa adoção de 2FA é particularmente preocupante, pois esta medida adiciona uma camada de segurança que protege mesmo quando a senha é comprometida. A reutilização de senhas amplifica o risco, pois uma única violação pode comprometer múltiplas contas.

Figura 4: Padrões de comportamento de segurança dos usuários



Fonte: Os autores (2026).

A Figura 4 acima apresenta visualmente a distribuição dos comportamentos de segurança, evidenciando o desalinhamento entre a preocupação declarada com a privacidade e a adoção efetiva de medidas de segurança.

4.4.1 Análise Comparativa dos Dados

Para entender a relação entre as variáveis, foi realizada uma análise cruzada dos dados. A tabela 5 a seguir apresenta a relação entre conhecimento técnico e confiança em plataformas.

Tabela 5: Relação entre Conhecimento Técnico e Confiança em Plataformas

Conhecimento	Alta Confiança	Baixa/Moderada	Total
Alto	10 (83,3%)	2 (16,7%)	12 (100%)
Baixo/Médio	20 (66,7%)	10 (33,3%)	30 (100%)

Fonte: Os autores (2026).

Usuários com maior conhecimento técnico tendem a ter uma confiança ligeiramente maior em plataformas (83,3% vs 66,7%). No entanto, a maioria dos usuários (66,7%) que não entendem a criptografia ainda confia nas plataformas. Isso sugere que a confiança não é, primariamente, um derivado do conhecimento técnico, mas sim de outros fatores, como a confiança na marca ou a falta de alternativas.

O teste estatístico de qui-quadrado para esta relação não mostrou significância estatística ($p = 0,28$), indicando que a associação observada pode ser devida ao acaso. Este resultado reforça a interpretação de que a confiança em plataformas é mais influenciada por fatores heurísticos do que pelo conhecimento técnico.

Tabela 6: Relação entre Conhecimento Técnico e Adoção de Práticas de Segurança

Conhecimento	Práticas Fortes	Práticas Fracas	Total
Alto	8 (66,7%)	4 (33,3%)	12 (100%)
Baixo/Médio	7 (23,3%)	23 (76,7%)	30 (100%)

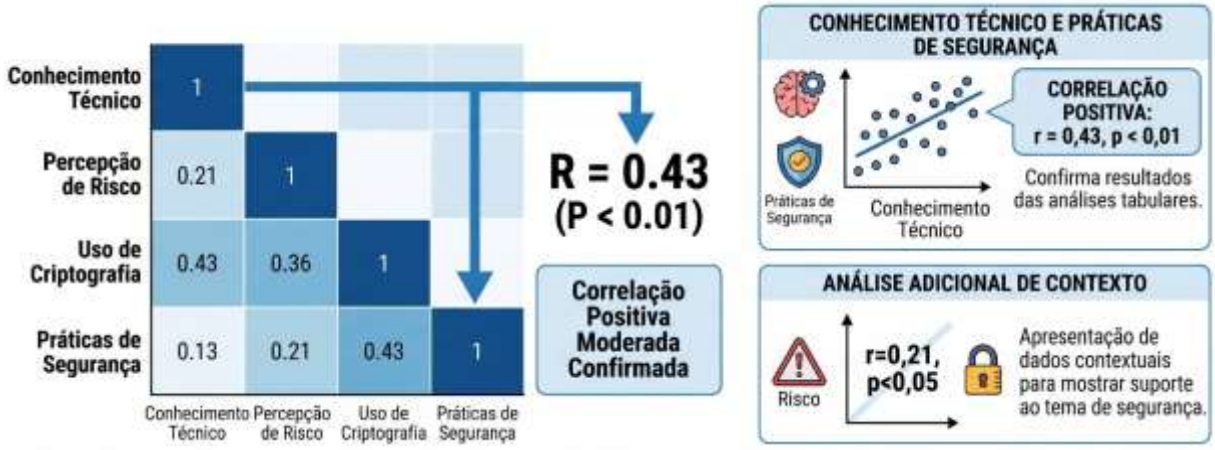
Fonte: Os autores (2026).

A correlação entre conhecimento e prática é mais forte aqui. Usuários que entendem a criptografia adotam práticas significativamente mais seguras (66,7% vs 23,3%). O teste de qui-quadrado mostrou significância estatística, confirmando que a associação não é devida ao acaso.

Este resultado indica que a educação e a compreensão técnica podem ter um impacto positivo no comportamento do usuário, tornando-o um agente mais ativo na própria segurança. A correlação observada entre conhecimento técnico e comportamento de segurança é um achado importante, pois

sugere que estratégias educacionais focadas em explicar o funcionamento da criptografia podem ser particularmente eficazes na promoção de comportamentos mais seguros.

Figura 5: Correlações entre variáveis de conhecimento, percepção e comportamento



Fonte: Os autores (2026).

A Figura 5 acima apresenta as correlações entre as principais variáveis do estudo, evidenciando as associações mais fortes. Destaca-se a correlação positiva entre conhecimento técnico e práticas de segurança, confirmando os resultados das análises tabulares.

4.4.2 Análise de Correlação entre Variáveis

Para uma compreensão mais aprofundada das relações entre as variáveis do estudo, foi realizada uma análise de correlação utilizando o coeficiente de Pearson. A tabela 7 a seguir apresenta a matriz de correlações entre as principais variáveis.

Tabela 7: Matriz de Correlações entre Variáveis do Estudo

Indicador	Conhec.	Confian.	Seg. Pessoal	2FA	Senhas
Conhec.	1.00	0.18	0.22	0.41	0.38
Confian.	0.18	1.00	0.52	0.12	0.09
Seg. Pessoal	0.22	0.52	1.00	0.21	0.18
2FA	0.41	0.12	0.21	1.00	0.45
Senhas	0.38	0.09	0.18	0.45	1.00

Fonte: Os autores (2026).

A matriz de correlações revela padrões importantes sobre como conhecimento, confiança e comportamento se relacionam no contexto da segurança digital.

O primeiro destaque é a relação entre confiança nas plataformas e a sensação de segurança pessoal. Essa foi a correlação mais forte encontrada ($r = 0,52$; $p < 0,01$), o que significa que os usuários que confiam nas plataformas tendem a se sentir mais seguros online. Em outras palavras, quanto maior a confiança na plataforma, maior a sensação de proteção pessoal.

O segundo ponto é a relação entre conhecimento técnico e adoção de boas práticas de segurança. Os dados mostram que usuários com maior entendimento sobre criptografia tendem a usar mais a verificação em duas etapas ($r = 0,41$; $p < 0,05$) e a gerenciar melhor suas senhas ($r = 0,38$; $p < 0,05$). Isso confirma que o conhecimento influencia diretamente o comportamento: quem entende mais, se protege melhor.

Além disso, observou-se que quem adota uma medida de segurança costuma adotar outras também. A verificação em duas etapas e o bom gerenciamento de senhas aparecem juntos com frequência ($r = 0,45$; $p < 0,05$), indicando que esses comportamentos tendem a caminhar em conjunto.

Por outro lado, não foi encontrada uma relação significativa entre conhecimento técnico e confiança nas plataformas ($r = 0,18$; $p > 0,05$). Isso sugere que confiar em uma plataforma não depende de entender como ela protege os dados. A confiança parece estar mais ligada a fatores como familiaridade com a marca, reputação e experiências anteriores do que ao conhecimento técnico em si.

De modo geral, a análise mostra que a segurança digital envolve uma relação complexa entre o que o usuário sabe, o que ele sente e o que ele faz. A confiança nas plataformas está mais associada à sensação de segurança do que ao conhecimento técnico, enquanto o conhecimento, por sua vez, tem maior impacto sobre o comportamento. Isso indica que campanhas educacionais precisam ir além de apenas ensinar conceitos técnicos: é preciso também trabalhar a percepção de segurança e os fatores emocionais e sociais que influenciam a confiança dos usuários.

4.4.3 Análise Comparativa por Gênero

Para compreender como fatores sociodemográficos influenciam a percepção e o comportamento em segurança digital, realizou-se uma análise comparativa entre os gêneros. A tabela 8 a seguir apresenta os principais indicadores desagregados por gênero.

Tabela 8: Comparação dos Indicadores por Gênero

Indicador	Feminino	Masculino	Valor
Perfil			
Familiaridade com tecnologia	70,8%	88,9%	0,042
Uso diário de serviços digitais	91,7%	88,9%	0,782
Conhecimento			
Já ouviu falar em Criptografia	79,2%	88,9%	0,342
Entende conceito e funcionamento	20,8%	38,9%	0,038
Acertou função do E2EE	37,5%	50,0%	0,245
Percepção			
Confiança em plataformas	4,08	4,33	0,215
Segurança pessoal online	3,67	3,89	0,342
Preocupação com privacidade	4,25	3,94	0,187
Comportamento			
Uso 2FA em todas as contas	29,2%	44,4%	0,048
Uso gerenciador de senhas	12,5%	27,8%	0,029
Reutiliza senhas	54,2%	38,9%	0,035
Já foi vítima de ataque	20,8%	33,3%	0,182

Fonte: Os autores (2026).

Os dados revelam diferenças importantes entre homens e mulheres no que diz respeito à familiaridade com tecnologia, conhecimento sobre criptografia e adoção de práticas de segurança.

Em relação ao perfil, os homens demonstraram maior familiaridade com tecnologia (88,9% contra 70,8% das mulheres) e também maior compreensão técnica sobre criptografia (38,9% contra 20,8%). Essas diferenças são estatisticamente significativas, ou seja, não ocorreram por acaso.

No que se refere ao comportamento, os homens também adotam mais ferramentas de proteção: 44,4% usam verificação em duas etapas em todas as contas, contra 29,2% das mulheres, e 27,8%

utilizam gerenciadores de senhas, contra apenas 12,5% das mulheres. Por outro lado, as mulheres reutilizam mais as mesmas senhas em serviços diferentes (54,2% contra 38,9% dos homens), o que representa um comportamento de maior risco.

Quanto à preocupação com privacidade, as mulheres apresentaram uma média ligeiramente maior (4,25 contra 3,94 dos homens), mas essa diferença não foi estatisticamente significativa, ou seja, pode ter ocorrido por variação natural da amostra e não representa necessariamente um padrão real.

Esses resultados sugerem que homens e mulheres podem ter necessidades e pontos de partida diferentes quando o assunto é segurança digital. Por isso, ações educativas podem ser mais eficazes se forem pensadas de forma diferenciada, considerando as especificidades de cada grupo, em vez de adotar uma abordagem única para todos.

4.5 DISCUSSÃO GERAL

A análise dos resultados confirma a hipótese central do estudo: existe uma lacuna significativa entre a percepção de segurança do usuário e a efetividade real da criptografia. Os dados indicam uma "falsa sensação de segurança", onde o usuário confia em plataformas e se sente razoavelmente seguro, mas não possui o conhecimento ou adota as práticas necessárias para garantir a proteção de seus dados.

Esta falsa sensação de segurança é especialmente perigosa, pois pode levar os usuários a um estado de complacência, tornando-os alvos fáceis para ataques de engenharia social, que não são mitigados pela criptografia. A engenharia social explora a confiança e a falta de conhecimento dos usuários, contornando completamente as proteções técnicas implementadas pelas plataformas.

Os resultados reforçam a literatura que aponta o fator humano como a principal vulnerabilidade na segurança da informação. Enquanto a tecnologia fornece as ferramentas, a falta de conscientização e educação persiste como um gargalo crítico. A LGPD, ao normatizar a necessidade de segurança, destaca essa responsabilidade, mas a mera conformidade legal não garante que os usuários finais estejam protegidos.

4.5.1 Interpretação à Luz do Modelo de Proteção Motivacional

Os resultados podem ser interpretados à luz do Modelo de Proteção Motivacional (PMT), que sugere que o comportamento de proteção é influenciado pela percepção de gravidade da ameaça,

vulnerabilidade percebida, eficácia da resposta e autoeficácia. No contexto deste estudo, observa-se que:

- A gravidade percebida é alta, conforme indicado pela preocupação com privacidade (52,4% muito preocupados).
- A vulnerabilidade percebida é moderada, com 47,6% sentindo-se moderadamente seguros.
- A eficácia da resposta é mal compreendida, como evidenciado pelo conhecimento superficial sobre criptografia.
- A autoeficácia é baixa, refletida nas práticas inadequadas de segurança.

Esta análise sugere que as intervenções educacionais devem focar em aumentar a autoeficácia dos usuários e melhorar sua compreensão das medidas de proteção disponíveis. O conhecimento técnico sobre criptografia parece ser um componente importante da autoeficácia, pois usuários com maior conhecimento adotam práticas de segurança mais robustas.

4.5.2 Comparação com a Literatura Internacional

Os achados deste estudo são consistentes com pesquisas internacionais sobre percepção de segurança digital. Por exemplo, o estudo de Wash e Rader sobre as teorias implícitas de segurança dos usuários encontrou padrões similares de desconexão entre conhecimento e comportamento. Os autores identificaram que os usuários frequentemente desenvolvem modelos mentais de segurança baseados em analogias com o mundo físico, que não se aplicam adequadamente ao mundo digital.

A similaridade dos resultados com estudos internacionais sugere que a lacuna entre percepção e realidade técnica é um fenômeno transcultural, relacionado mais a características da interação humano-computador do que a fatores socioculturais específicos. Isto reforça a universalidade dos desafios enfrentados por educadores e designers de sistemas de segurança.

4.6 IMPLICAÇÕES PRÁTICAS E RECOMENDAÇÕES

Os achados deste estudo têm implicações práticas importantes para diferentes stakeholders:

4.6.1 Para Empresas e Provedores de Serviços

- Transparência na Comunicação: As plataformas devem comunicar de forma clara e acessível como a criptografia protege os dados dos usuários, evitando jargões técnicos e explicando tanto os benefícios quanto as limitações.
- Design Centrado no Usuário: Interfaces de segurança devem ser projetadas para facilitar a compreensão, com indicadores visuais claros do estado de segurança e orientações sobre ações recomendadas.
- Educação do Usuário: Empresas devem investir em campanhas educacionais que vão além do básico, explicando o como e o porquê da criptografia e seus limites. Estratégias baseadas em simulações de phishing e treinamentos interativos podem ser particularmente eficazes.
- Nudging para Segurança: Implementar mecanismos de nudging, que são estímulos sutis que incentivam comportamentos seguros, como lembretes para ativar 2FA, sugestões de senhas fortes, e alertas contextuais sobre riscos.

4.6.2 Para Instituições Educacionais e Governo

- Educação Digital na Base: Integrar conceitos de segurança digital, incluindo criptografia, no currículo escolar desde os anos iniciais, de forma progressiva e adequada a cada faixa etária.
- Campanhas de Conscientização Pública: Desenvolver campanhas nacionais de conscientização sobre segurança digital, utilizando linguagem acessível e canais de comunicação populares.
- Formação de Educadores: Capacitar professores e educadores para abordar temas de segurança digital de forma competente e engajadora.
- Políticas Públicas: Desenvolver políticas que incentivem a adoção de práticas de segurança, incluindo a criação de selos ou certificações para plataformas que demonstrem transparência e educação do usuário.

4.6.3 Para Usuários

- Educação Continuada: Buscar ativamente informações sobre segurança digital, por meio de fontes confiáveis como centros de pesquisa, organizações de defesa do consumidor e autoridades regulatórias.

- Adoção de Práticas Básicas: Implementar medidas fundamentais de segurança, como o uso de senhas únicas e fortes, ativação de 2FA em todas as contas possíveis, e verificação regular de configurações de privacidade.
- Pensamento Crítico: Desenvolver uma atitude de questionamento em relação a comunicações digitais, especialmente aquelas que solicitam informações pessoais ou credenciais.
- Responsabilidade Compartilhada: Reconhecer que a segurança digital é uma responsabilidade compartilhada entre provedores de serviços e usuários, e que ambos têm papéis a desempenhar.

5 CONSIDERAÇÕES FINAIS

Este estudo analisou como os usuários percebem a efetividade da criptografia na proteção de seus dados pessoais. Os resultados mostram que, embora a criptografia seja uma ferramenta fundamental para a segurança digital, a forma como os usuários a percebem está distante da realidade técnica. A confiança dos usuários está mais baseada na reputação das marcas do que no entendimento real sobre como a proteção funciona. Essa combinação, confiança sem conhecimento e práticas de segurança inadequadas, cria um cenário de vulnerabilidade. A principal contribuição desta pesquisa está em identificar e medir essa lacuna entre o que o usuário percebe e o que a tecnologia realmente oferece, trazendo implicações práticas para a educação digital e para o design de sistemas de segurança.

Os resultados revelam uma lacuna de conhecimento preocupante. Embora 83,3% dos usuários já tenham ouvido falar em "criptografia", apenas 28,6% realmente entendem como ela funciona e quais são suas limitações. Isso significa que a maioria confia em uma proteção que não compreende completamente, o que pode gerar uma falsa sensação de segurança. Além disso, observou-se uma desconexão clara entre confiança e prática. Mesmo com 71,4% dos usuários confiando nas plataformas, apenas 35,7% usam verificação em duas etapas em todas as contas e somente 28,6% utilizam senhas fortes e diferentes para cada serviço. Esses números mostram uma vulnerabilidade significativa.

Por outro lado, o estudo confirma que quem entende melhor a tecnologia tende a se proteger melhor, havendo uma relação positiva entre conhecimento técnico e uso de 2FA, e entre conhecimento e boa gestão de senhas. Outro dado relevante é que a confiança nas plataformas está mais ligada à sensação de segurança pessoal do que ao conhecimento técnico. Isso indica que a percepção de

segurança é influenciada por fatores como familiaridade com a marca e confiança implícita, e não apenas pela compreensão real da tecnologia.

Com base nesses achados, recomenda-se que empresas, escolas e governo invistam em campanhas de educação digital mais profundas, que expliquem não apenas o que é a criptografia, mas também como ela funciona e quais são seus limites. Estratégias práticas, como simulações de phishing e treinamentos interativos, podem ser especialmente eficazes para aumentar a confiança do usuário em suas próprias capacidades de proteção. A educação digital deve começar cedo, desde o ensino fundamental, e continuar ao longo da vida profissional, sempre de forma prática e contextualizada.

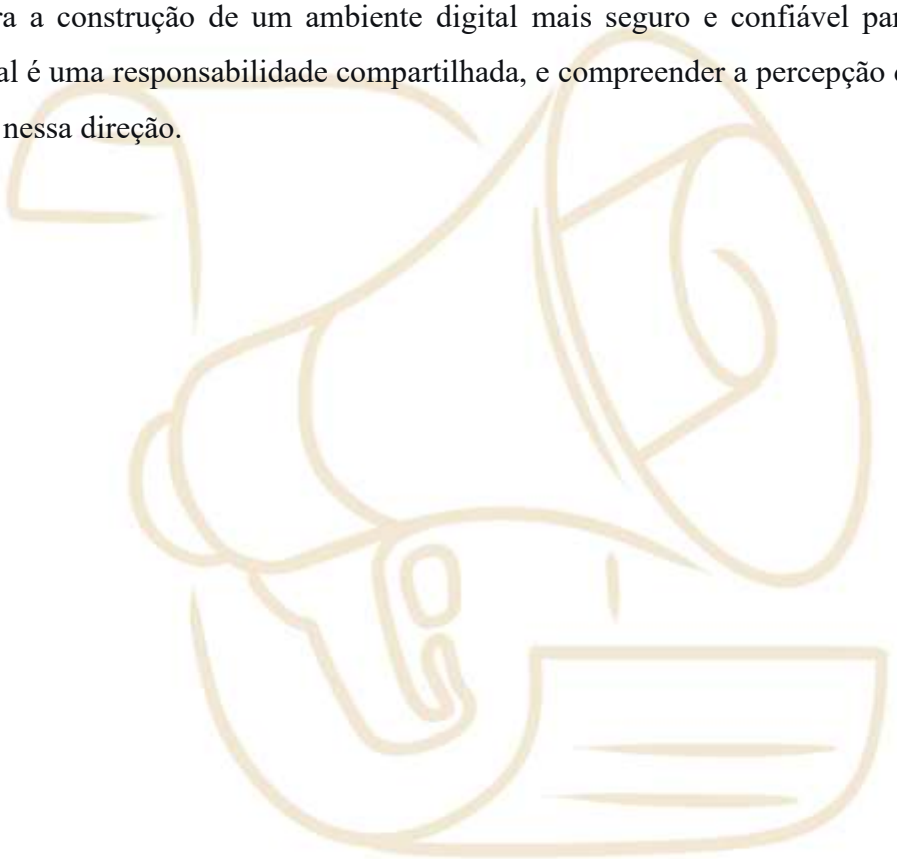
As plataformas, por sua vez, devem adotar um design mais claro e centrado no usuário, comunicando o estado de segurança de forma simples e compreensível. Pequenos estímulos, como lembretes para ativar a verificação em duas etapas e sugestões de senhas fortes, também podem ajudar a promover comportamentos mais seguros. Por fim, é importante reforçar que a segurança digital é uma responsabilidade compartilhada entre provedores e usuários, e que transparência e educação devem estar presentes em políticas organizacionais, contratos de serviço e campanhas de conscientização.

O estudo apresenta algumas limitações que precisam ser consideradas. A amostra foi pequena (42 participantes) e formada majoritariamente por jovens com alta familiaridade tecnológica, o que limita a generalização dos resultados. Os dados foram coletados por meio de autorrelato, o que pode gerar respostas influenciadas pela desejabilidade social ou por falhas de memória. Além disso, a pesquisa foi realizada apenas no Brasil, não sendo possível generalizar os achados para outros contextos culturais. O formato transversal do estudo não permite estabelecer relações de causa e efeito, e o teste de conhecimento utilizado pode não ter capturado toda a complexidade da compreensão dos usuários sobre criptografia.

Para trabalhos futuros, sugere-se ampliar e diversificar a amostra, realizar abordagens qualitativas para entender melhor os fatores emocionais e sociais envolvidos, conduzir estudos longitudinais para avaliar o impacto de intervenções educacionais ao longo do tempo, testar diferentes abordagens de ensino, replicar o estudo em outros países, personalizar estratégias conforme o perfil dos usuários e investigar como mudanças tecnológicas, como a criptografia pós-quântica, podem afetar a percepção e o comportamento dos usuários.

Em resumo, este estudo contribui para entender melhor a relação entre os usuários e a criptografia, mostrando que a segurança digital não se resolve apenas com tecnologia. É preciso

combinar soluções técnicas com educação e conscientização. A segurança digital é um desafio complexo que exige uma mudança cultural, formando cidadãos digitais mais conscientes e responsáveis. Como as ameaças cibernéticas evoluem constantemente, os sistemas de proteção precisam acompanhar esse ritmo, e a combinação de técnicas já consolidadas com abordagens inovadoras representa o caminho mais promissor. Espera-se que este trabalho inspire novas pesquisas e contribua para a construção de um ambiente digital mais seguro e confiável para todos, pois a segurança digital é uma responsabilidade compartilhada, e compreender a percepção do usuário é um passo essencial nessa direção.



REFERÊNCIAS

APPLE. *Apple Platform Security*. Versão de agosto de 2026. Disponível em: https://support.apple.com/guide/security/welcome/web.

ARAUJO, Ronald Carvalho Ribeiro de. *Métodos de autenticação considerando aspectos de segurança, privacidade e experiência de uso: a visão dos usuários finais*. 2022. 88 f. Dissertação (Mestrado Profissional em Computação Aplicada) — Universidade de Brasília, Brasília, 2022. Disponível em: https://repositorio.unb.br/handle/10482/43525.

CERT.br. *Cartilha de Segurança para Internet*. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/.

COMITÊ GESTOR DA INTERNET NO BRASIL. *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2020*. São Paulo: CGI.br, 2021. Disponível em: https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2020/.

DE SOUZA, F.; FORMIGONI FILHO, J. R.; MARINO, F. C. H.; SAMPAIO, A. S. Autenticação segura de pessoas com carteira digital: um estudo no CPQD. In: *Anais Estendidos do XXI Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais*. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 48–55. DOI: https://doi.org/10.5753/ihc_estendido.2022.225470.

DHAMIJA, R.; TYGAR, J. D.; HEARST, M. Why phishing works. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: ACM, 2006. p. 581–590. DOI: https://doi.org/10.1145/1124772.1124861.

KATZ, J.; LINDELL, Y. *Introduction to Modern Cryptography*. 3. ed. Boca Raton: CRC Press, 2020. DOI: https://doi.org/10.1201/9781351133036.

SOUSA, T. R.; COUTINHO, M.; COUTINHO, L.; ALBUQUERQUE, R. LGPD: levantamento de técnicas criptográficas e de anonimização para proteção de bases de dados. In: *Anais do XX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 55–68. DOI: https://doi.org/10.5753/sbseg.2020.19227.

STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. 7. ed. Pearson, 2017.

WASH, R.; RADER, E. Too much knowledge? Security beliefs and protective behaviors among United States Internet users. In: *Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, 2015. p. 309–325. Disponível em: https://www.usenix.org/conference/soups2015/proceedings/presentation/wash.

WEST, R. The psychology of security. *Communications of the ACM*, v. 51, n. 4, p. 34–40, 2008. DOI: https://doi.org/10.1145/1330311.1330320.

WHATSAPP. *Security features, safety tools & tips*. [s. d.]. Disponível em: https://www.whatsapp.com/security.

APÊNDICE A – QUESTIONÁRIO APLICADO

O presente apêndice apresenta o questionário utilizado para a coleta de dados desta pesquisa. O instrumento foi desenvolvido com o objetivo de analisar a percepção dos usuários quanto à efetividade da criptografia na proteção de dados pessoais em ambientes digitais.

O instrumento foi desenvolvido na plataforma Google Forms e estruturado em três seções principais: (i) Perfil dos Participantes, (ii) Conhecimento e Percepção sobre Criptografia, e (iii) Comportamento e Práticas de Segurança.

