CIBERSEGURANÇA PARA USUÁRIOS LEIGOS: DESAFIOS, VULNERABILIDADES E A IMPORTÂNCIA DA EDUCAÇÃO PARA A PROTEÇÃO DA INFORMAÇÃO

Gleissel Florisbelo Alves[1], Glaicon Florisbelo Alves[2]

[1]Universidade Federal de Uberlândia (UFU), Uberlândia, Brasil (gleissel@gmail.com)
[2]Universidade Federal de Uberlândia (UFU), Uberlândia, Brasil (glaicon.florisbelo@gmail.com)

Resumo: A crescente digitalização ampliou o acesso às tecnologias, mas também a exposição de usuários leigos a ameaças cibernéticas, como golpes, fraudes e vazamento de dados. Este estudo analisa os principais desafios da segurança digital e destaca a educação em cibersegurança como estratégia de prevenção. Com base em revisão bibliográfica, conclui que o fator humano permanece como a principal vulnerabilidade, reforçando a importância da alfabetização digital para proteger dados, privacidade e promover a cidadania digital.

Palavras-chave: Cibersegurança; Alfabetização Digital; Cidadania Digital.

INTRODUÇÃO

A sociedade contemporânea vivencia um intenso processo de transformação impulsionado pelas tecnologias digitais da informação e comunicação. A expansão da internet, da computação em nuvem, dos dispositivos móveis, das redes sociais, da inteligência artificial e dos serviços digitais modificou profundamente a maneira como as pessoas aprendem, trabalham, comunicam-se e realizam atividades cotidianas. Atualmente, operações bancárias, compras, consultas médicas, processos educacionais e diversos serviços públicos são executados por meio de plataformas digitais, tornando a conectividade elemento essencial da vida moderna.

Segundo Castells (2022), a sociedade em rede caracteriza-se pela centralidade da informação e pela interconexão global entre indivíduos, organizações e instituições, promovendo profundas mudanças econômicas, sociais e culturais. Nesse contexto, a informação assume papel estratégico, tornando-se um dos principais ativos da economia do conhecimento.

Entretanto, o avanço tecnológico também ampliou significativamente os riscos associados ao ambiente digital. À medida que cresce o volume de informações compartilhadas na internet, aumentam igualmente as oportunidades para ações criminosas voltadas ao roubo de dados, fraudes financeiras, espionagem, extorsão digital e invasão de sistemas computacionais. Dessa forma, a segurança da informação passou a constituir um dos principais desafios da sociedade conectada.

De acordo com Schneier (2015), a segurança não depende exclusivamente da tecnologia empregada, mas principalmente do comportamento humano diante dos riscos existentes. Para o autor, muitos ataques bem-sucedidos ocorrem porque criminosos exploram falhas cognitivas, emocionais e comportamentais das pessoas, utilizando estratégias de manipulação conhecidas como engenharia social.

Essa perspectiva é corroborada por Stallings (2018), ao afirmar que o fator humano continua sendo o elo mais vulnerável da segurança da informação. Mesmo organizações que possuem infraestrutura tecnológica avançada podem sofrer incidentes de segurança quando seus usuários desconhecem procedimentos básicos de proteção.

Nesse cenário, observa-se que usuários leigos apresentam maior suscetibilidade aos ataques cibernéticos. Muitas pessoas utilizam senhas fracas, repetem credenciais em diferentes plataformas, compartilham informações pessoais em excesso nas redes sociais, clicam em links suspeitos e desconhecem mecanismos de autenticação em dois fatores. Essas práticas aumentam significativamente a exposição a golpes digitais e comprometem a proteção dos dados pessoais.

Entre as ameaças mais recorrentes destacam-se o **phishing**, caracterizado pelo envio de mensagens fraudulentas com o objetivo de obter informações confidenciais; o **ransomware**, que sequestra dados mediante criptografia e exige pagamento para sua liberação; os **malwares**, programas desenvolvidos para comprometer dispositivos; os ataques de engenharia social; a clonagem de contas em aplicativos de mensagens; além das fraudes financeiras realizadas por meio de sistemas de pagamento instantâneo.

Além das consequências individuais, ataques cibernéticos provocam impactos econômicos e sociais expressivos, afetando empresas, órgãos públicos e instituições educacionais. O vazamento de informações sensíveis pode comprometer a privacidade dos cidadãos, gerar prejuízos financeiros, afetar a reputação das organizações e comprometer a confiança da sociedade nas tecnologias digitais.

Nesse contexto, a educação em cibersegurança emerge como elemento estratégico para o fortalecimento da cultura de proteção da informação. A conscientização dos usuários constitui uma das principais recomendações das normas de gestão da segurança da informação. A ABNT NBR ISO/IEC 27002:2022 destaca a importância da conscientização, da educação e do treinamento em segurança da informação como mecanismos para reduzir vulnerabilidades humanas e fortalecer a proteção dos ativos informacionais (ABNT, 2022).

Sob a perspectiva educacional, Kenski (2012) argumenta que a incorporação das tecnologias ao cotidiano exige novas competências relacionadas ao uso ético, crítico e seguro dos recursos digitais. Da mesma forma, Lévy (2010) ressalta que a cibercultura amplia as possibilidades de construção coletiva do conhecimento, mas demanda responsabilidades proporcionais quanto ao uso das informações e à proteção dos ambientes digitais.

A educação crítica proposta por Freire (2021) também oferece importantes contribuições para a compreensão da cibersegurança como prática social. Para o autor, educar significa desenvolver autonomia, consciência crítica e capacidade de tomar decisões fundamentadas. Aplicada ao contexto digital,

essa perspectiva implica formar cidadãos capazes de identificar riscos, avaliar informações, proteger seus dados pessoais e utilizar as tecnologias de maneira ética e responsável.

Outro aspecto relevante refere-se à crescente importância da proteção dos dados pessoais. No Brasil, a promulgação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), estabeleceu princípios, direitos e responsabilidades relacionados ao tratamento de dados pessoais, reforçando a necessidade da adoção de medidas técnicas e administrativas voltadas à segurança da informação. Embora a legislação represente um importante avanço no campo da proteção de dados, sua efetividade depende diretamente do nível de conscientização dos usuários e das organizações quanto às boas práticas de segurança da informação e de proteção digital (BRASIL, 2018).

Nesse cenário, torna-se evidente que a cibersegurança ultrapassa os limites da tecnologia, constituindo um desafio educacional, social, econômico e cultural. O desenvolvimento de uma cultura de segurança requer investimentos contínuos em formação, campanhas educativas e políticas públicas que promovam o uso seguro das tecnologias digitais.

A partir dessas considerações, este estudo tem como propósito analisar os principais desafios enfrentados pelos usuários leigos na utilização segura das tecnologias digitais, bem como compreender de que maneira a educação em cibersegurança pode contribuir para a redução das vulnerabilidades no ambiente digital.

O objetivo geral consiste em analisar os desafios da cibersegurança para usuários leigos no mundo digital, enfatizando a importância da conscientização e da educação digital na prevenção de incidentes de segurança. Como objetivos específicos, busca-se identificar as principais ameaças cibernéticas que afetam os usuários comuns; discutir os fatores humanos associados às vulnerabilidades digitais; analisar o papel da educação em cibersegurança e do letramento digital na promoção da segurança da informação; e apresentar boas práticas capazes de fortalecer a cultura de cibersegurança na sociedade contemporânea.

MATERIAL E MÉTODOS

Esta pesquisa caracteriza-se como qualitativa, de natureza exploratória e descritiva, desenvolvida por meio de revisão bibliográfica. Esse tipo de investigação possibilita compreender determinado fenômeno a partir da análise crítica da produção científica existente, permitindo identificar conceitos, tendências, desafios e contribuições relacionadas ao objeto de estudo.

Foram consultadas obras que abordam segurança da informação, cultura digital, educação tecnológica, proteção de dados pessoais e comportamento do usuário no ambiente virtual. A fundamentação teórica compreendeu autores como Castells (2022), Lévy (2010), Kenski (2012), Schneier (2015), Stallings (2018), Sêmola (2014) e Freire (2021), além de documentos técnicos publicados pelo Comitê Gestor da Internet no Brasil (CGI.br, 2024), da ABNT NBR ISO/IEC 27002:2022 (ABNT, 2022) e da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018).

A análise buscou identificar os principais desafios enfrentados pelos usuários leigos diante das ameaças cibernéticas, bem como estratégias educativas voltadas à promoção da segurança digital.

RESULTADOS E DISCUSSÃO

A revisão da literatura evidencia que a rápida transformação digital trouxe benefícios significativos para a sociedade, mas também ampliou os riscos associados ao uso das tecnologias da informação. A crescente dependência de dispositivos conectados, redes sociais, aplicativos de mensagens, serviços bancários digitais e plataformas em nuvem aumentou a superfície de exposição aos ataques cibernéticos.

Segundo Castells (2022), a sociedade em rede reorganizou profundamente as relações sociais, econômicas e institucionais, fazendo da informação um recurso estratégico. Essa nova configuração ampliou a conectividade global, porém também criou oportunidades para diferentes modalidades de crimes digitais. Nesse contexto, observa-se que os usuários leigos figuram entre os grupos mais vulneráveis, pois frequentemente desconhecem princípios básicos de segurança

da informação. Essa realidade demonstra que a proteção digital não depende apenas da infraestrutura tecnológica, mas principalmente do comportamento dos indivíduos.

Nesse cenário, os estudos de Schneier (2015) demonstram que a maioria dos ataques cibernéticos não ocorre exclusivamente por falhas técnicas, mas pela exploração de comportamentos humanos. Em vez de atacar diretamente sistemas altamente protegidos, os criminosos buscam convencer as vítimas a fornecer voluntariamente informações confidenciais. Essa prática caracteriza a chamada engenharia social, conjunto de técnicas que utiliza manipulação psicológica para obter senhas, códigos de autenticação, dados bancários e outras informações sensíveis.

Stallings (2018) afirma que o usuário representa o elo mais vulnerável da cadeia de segurança da informação, sobretudo quando não recebe treinamento adequado. Mesmo organizações que investem em tecnologias avançadas permanecem suscetíveis a incidentes quando seus colaboradores desconhecem procedimentos básicos de proteção. Entre os fatores humanos mais frequentemente observados destacam-se a utilização de senhas fracas, a reutilização da mesma senha em diferentes serviços, o compartilhamento excessivo de informações pessoais, a confiança em mensagens aparentemente legítimas, a ausência de autenticação em dois fatores, o desconhecimento sobre atualizações de segurança e a instalação de aplicativos provenientes de fontes não confiáveis. Essas práticas favorecem ataques de engenharia social, comprometendo a confidencialidade, a integridade e a disponibilidade das informações.

A literatura também identifica diversas modalidades de ataques cibernéticos direcionados ao público em geral. O phishing permanece entre as ameaças mais frequentes. Nesse tipo de golpe, criminosos enviam mensagens eletrônicas que simulam comunicações oficiais de bancos, empresas ou órgãos públicos com o objetivo de induzir a vítima ao fornecimento de informações sigilosas. Outra ameaça crescente é o ransomware, caracterizado pelo sequestro de arquivos

mediante criptografia. Após bloquear o acesso aos dados, os criminosos exigem pagamento para disponibilizar a chave de recuperação.

Além dessas ameaças, destacam-se os malwares, spywares, trojans, a clonagem de contas de aplicativos de mensagens, o roubo de identidade digital, o vazamento de dados pessoais, as fraudes em compras eletrônicas e os golpes envolvendo sistemas de pagamento instantâneo.

Segundo dados do CGI.br (2024), o crescimento dessas ameaças está diretamente relacionado à intensificação da transformação digital e ao aumento da circulação de dados pessoais em ambientes digitais. Conforme Sêmola (2014), grande parte dos incidentes de segurança decorre de falhas humanas e do desconhecimento de práticas adequadas de proteção da informação, evidenciando que ações contínuas de conscientização e capacitação dos usuários contribuem significativamente para a redução dos riscos no ambiente digital.

Diante desse contexto, os resultados da revisão indicam consenso entre os autores quanto ao papel fundamental da educação na promoção da segurança digital. Kenski (2012) argumenta que a utilização das tecnologias exige o desenvolvimento de competências que ultrapassam o domínio técnico, envolvendo pensamento crítico, responsabilidade e autonomia. Na perspectiva de Freire (2021), educar significa promover a capacidade de compreender criticamente a realidade e agir de forma consciente diante dos desafios sociais. Essa concepção pode ser aplicada à cibersegurança ao incentivar usuários a reconhecerem ameaças, avaliarem informações e adotarem práticas preventivas.

Lévy (2010) destaca que a cibercultura amplia extraordinariamente as possibilidades de compartilhamento do conhecimento. Contudo, essa mesma dinâmica exige responsabilidade coletiva quanto à proteção das informações e ao uso ético das tecnologias. Sob essa perspectiva, a alfabetização digital deve contemplar conteúdos relacionados à segurança da informação desde os primeiros níveis da educação formal, favorecendo a construção de hábitos seguros ao longo da vida.

Outro aspecto relevante identificado na literatura refere-se à proteção jurídica dos dados pessoais. A promulgação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), representou um importante avanço na regulamentação do tratamento de dados pessoais no Brasil. A lei estabelece princípios como finalidade, adequação, necessidade, transparência, segurança e responsabilização, determinando que organizações públicas e privadas adotem medidas técnicas e administrativas para proteger os dados sob sua responsabilidade (BRASIL, 2018).

Entretanto, a legislação, por si só, não elimina os riscos existentes. Usuários que desconhecem seus direitos ou não adotam medidas básicas de proteção continuam vulneráveis a fraudes e vazamentos de informações. Isso evidencia que a efetividade da legislação depende diretamente da formação de uma cultura de proteção de dados, envolvendo educação, conscientização e participação ativa da sociedade.

A literatura consultada apresenta ainda diversas recomendações capazes de reduzir significativamente os riscos associados ao uso das tecnologias digitais, conforme apresentado no Tabela 1. Observa-se que grande parte dessas medidas pode ser implementada sem custos financeiros elevados, dependendo principalmente da conscientização dos usuários.

Tabela 1**:** Boas práticas de cibersegurança para usuários leigos.

Prática recomendada	Objetivo	Benefício esperado
Utilizar senhas longas e exclusivas	Proteger contas	Dificulta invasões
Ativar autenticação em dois fatores	Reforçar autenticação	Reduz acesso não autorizado
Atualizar sistemas operacionais	Corrigir vulnerabilidades	Maior proteção contra ataques
Manter antivírus atualizado	Detectar códigos maliciosos	Redução de infecções

Realizar backups periódicos	Preservar informações	Recuperação em casos de ransomware
Verificar remetentes de mensagens	Evitar phishing	Proteção contra golpes
Evitar redes Wi-Fi públicas sem proteção	Preservar dados	Redução de interceptações
Compartilhar menos informações pessoais	Preservar privacidade	Menor exposição a fraudes
Capacitar-se continuamente	Desenvolver consciência digital	Fortalecimento da cultura de segurança

Fonte: Autores (2026).

Por fim, os resultados indicam que a cibersegurança não pode ser compreendida como responsabilidade exclusiva dos profissionais de tecnologia. Governos, instituições educacionais, empresas, organizações da sociedade civil e cidadãos compartilham responsabilidades na construção de ambientes digitais mais seguros. Campanhas educativas, programas de treinamento, políticas públicas e investimentos em alfabetização digital constituem elementos essenciais para reduzir vulnerabilidades e fortalecer a cultura da segurança da informação. Assim, a revisão bibliográfica evidencia que o principal desafio contemporâneo não consiste apenas em desenvolver tecnologias mais sofisticadas, mas em formar usuários conscientes, críticos e preparados para atuar de maneira segura no ambiente digital.

CONCLUSÃO

A transformação digital modificou profundamente a forma como indivíduos, organizações e governos produzem, compartilham e utilizam informações. O crescimento da conectividade proporcionou avanços significativos nas áreas da educação, saúde, comércio, comunicação e prestação de serviços públicos. Entretanto, essa evolução tecnológica também ampliou a incidência de ameaças cibernéticas, tornando a proteção da informação um dos principais desafios da sociedade contemporânea.

A análise desenvolvida neste estudo evidenciou que os usuários leigos representam um dos grupos mais vulneráveis aos ataques cibernéticos. A baixa familiaridade com práticas de segurança digital, aliada ao aumento da sofisticação das estratégias utilizadas por criminosos virtuais, favorece a ocorrência de incidentes como phishing, engenharia social, roubo de identidade, infecção por malware, ransomware, vazamento de dados pessoais e fraudes financeiras. Esses riscos demonstram que a segurança digital não depende apenas da adoção de tecnologias avançadas, mas também da formação de usuários capazes de reconhecer ameaças e agir preventivamente.

A revisão bibliográfica confirmou o entendimento de Schneier (2015) e Stallings (2018) de que o fator humano permanece como a principal vulnerabilidade dos sistemas de informação. Em muitos casos, os ataques exploram comportamentos cotidianos, como reutilização de senhas, compartilhamento excessivo de informações pessoais, ausência de autenticação multifator e dificuldade para identificar comunicações fraudulentas. Assim, o fortalecimento da cultura de segurança deve priorizar não apenas soluções técnicas, mas também ações educativas permanentes.

Outro aspecto relevante identificado refere-se ao papel da educação na promoção da cibersegurança. Conforme discutido por Kenski (2012), Lévy (2010) e Freire (2021), a formação para o uso das tecnologias deve contemplar competências relacionadas ao pensamento crítico, à ética, à autonomia e ao exercício consciente da cidadania digital. Nesse sentido, a alfabetização digital deve incorporar conteúdos voltados à proteção de dados, à privacidade, ao reconhecimento de golpes virtuais e ao uso responsável das tecnologias, preparando os indivíduos para enfrentar os desafios de uma sociedade cada vez mais conectada.

Também se verificou que instrumentos normativos, como a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) e a ABNT NBR ISO/IEC 27002:2022 (ABNT, 2022), representam importantes avanços na consolidação de uma cultura de proteção da informação. Contudo, a efetividade dessas normas depende diretamente da capacidade das organizações e dos cidadãos

de compreender e aplicar seus princípios no cotidiano. A existência de legislações e normas técnicas, embora essencial, não elimina os riscos decorrentes do desconhecimento dos usuários, reforçando a necessidade de programas contínuos de conscientização.

Os resultados da pesquisa indicam que práticas relativamente simples, como a criação de senhas robustas, a utilização da autenticação multifator, a atualização periódica de softwares, a realização de cópias de segurança (backups), a verificação da autenticidade de mensagens eletrônicas e o cuidado no compartilhamento de dados pessoais, podem reduzir significativamente a exposição aos ataques cibernéticos. Essas medidas, quando associadas à educação permanente, contribuem para o fortalecimento da resiliência digital tanto em ambientes domésticos quanto institucionais.

Além disso, observou-se que a cibersegurança deve ser compreendida como responsabilidade compartilhada entre governo, instituições de ensino, empresas e sociedade civil. A implementação de políticas públicas voltadas à educação digital, aliada à promoção de campanhas de conscientização e ao incentivo à pesquisa na área, constitui estratégia fundamental para ampliar a capacidade de prevenção e resposta às ameaças cibernéticas.

Diante desse cenário, conclui-se que a educação em cibersegurança representa um elemento indispensável para a consolidação de uma cultura de segurança da informação. Mais do que proteger equipamentos ou sistemas computacionais, trata-se de formar cidadãos conscientes, críticos e preparados para atuar de maneira ética, segura e responsável no ambiente digital. Assim, investir em alfabetização digital e em programas permanentes de conscientização não apenas reduz vulnerabilidades individuais, mas também fortalece a confiança nas tecnologias e contribui para a construção de uma sociedade digital mais segura, resiliente e inclusiva.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 27002:2022: Segurança da informação, segurança cibernética e proteção da privacidade - Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 jun. 2026.

CASTELLS, Manuel. A sociedade em rede. 24. ed. São Paulo: Paz e Terra, 2022.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios *2023*. São Paulo: CGI.br, 2024. Disponível em: https://cetic.br/media/analises/tic_domicilios_2023_coletiva_imprensa.pdf. Acesso em: 18 jun. 2026.

FREIRE, Paulo. Pedagogia da autonomia: saberes necessários à prática educativa. 84. ed. Rio de Janeiro: Paz e Terra, 2021.

KENSKI, Vani Moreira. Educação e tecnologias: o novo ritmo da informação. 8. ed. Campinas: Papirus, 2012.

LÉVY, Pierre. Cibercultura. 3. ed. São Paulo: Editora 34, 2010.

SCHNEIER, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton, 2015.

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. Rio de Janeiro: Elsevier, 2014.

STALLINGS, William. Segurança de redes: princípios e práticas. 6. ed. São Paulo: Pearson, 2018.