REVISTA DA MICRO E PEQUENA EMPRESA
Vol. 19, No. 1, Jan-Abr 2025, p.139-154
ISSN: 2237-3713

Engenharia social no ambiente acadêmico: vulnerabilidade humana e estratégias de conscientização em instituições de ensino superior*

Social engineering in the academic environment: human vulnerability and awareness strategies in higher education institutions

Matheus Almeida de Carvalho
Universidade Federal Fluminense
ac_matheus18@hotmail.com

Júlio César Ferreira Pedrini
Universidade de Vassouras
juliocesarfp8@gmail.com

RESUMO

A transformação digital das instituições de ensino superior (IES) ampliou o volume de recursos e interações digitais e, com isso, a exposição a ameaças que exploram não apenas falhas técnicas, mas o comportamento dos próprios usuários. Este artigo analisa, a partir de revisão bibliográfica e análise documental de fontes técnicas e institucionais, como a engenharia social se manifesta no ambiente acadêmico, quais os seus principais vetores, os ativos potencialmente afetados e as estratégias de conscientização e mitigação discutidas na literatura. A análise indica que *phishing*, *spear phishing* e *pretexting* constituem os mecanismos mais estudados nesse contexto, com evidências empíricas internacionais mostrando suscetibilidade diferenciada entre estudantes, docentes e técnico-administrativos. A literatura converge, ainda, quanto à insuficiência de medidas exclusivamente tecnológicas: políticas institucionais, capacitação continuada e desenvolvimento de competências digitais aparecem como componentes complementares e necessários. Conclui-se que a mitigação da engenharia social em IES depende de uma abordagem integrada entre tecnologia, processos e formação, e que a ausência de estudos empíricos brasileiros específicos representa uma lacuna relevante para pesquisas futuras.

Palavras-chave: Transformação digital. Segurança da informação. Ensino superior. Gestão de riscos. Cultura de segurança.

ABSTRACT

The digital transformation of higher education institutions (HEIs) has expanded the volume of digital resources and interactions, increasing exposure to threats that exploit not only technical flaws but user behavior itself. Drawing on a bibliographic review and documentary analysis of technical and institutional sources, this article examines how social engineering manifests in academic settings, its main attack vectors, the assets potentially affected, and the awareness and mitigation strategies discussed in the literature. The analysis indicates that phishing, spear phishing, and pretexting are the most studied mechanisms in this context, with international

* Recebido em 10 de junho de 2025, aprovado em 10 de agosto de 2025, publicado em 31 de agosto de 2025.

empirical evidence showing differentiated susceptibility among students, faculty, and administrative staff. The literature also converges on the insufficiency of purely technological measures: institutional policies, ongoing training, and digital competency development emerge as necessary complementary components. The study concludes that mitigating social engineering in HEIs requires an integrated approach combining technology, processes, and education, and that the absence of Brazil-specific empirical studies represents a relevant gap for future research.

Keywords: Digital transformation. Information security. Higher education. Risk management. Security culture.

1. INTRODUÇÃO

A transformação digital das instituições de ensino superior (IES) reorganizou boa parte das atividades acadêmicas e administrativas. Ambientes virtuais de aprendizagem, sistemas de gestão acadêmica, correio eletrônico institucional e plataformas de colaboração passaram a mediar rotinas de ensino, pesquisa, extensão e gestão. Esse processo amplia a capacidade das instituições de produzir e compartilhar informação, mas também aumenta o número de ativos digitais e de interações que precisam ser protegidos.

A digitalização não deve ser entendida apenas como aquisição de tecnologia. Batista, Arouca e Lobato (2024), ao estudarem estratégias de digitalização comunicacional em micro e pequenas empresas, constataram que a disponibilidade de ferramentas digitais nessas organizações vinha acompanhada de barreiras ligadas à falta de treinamento e de tempo para planejamento estratégico. O contexto investigado pelos autores é empresarial, não acadêmico, e o estudo não trata de segurança da informação; ainda assim, ele sustenta um argumento conceitual pertinente a este artigo: a presença de infraestrutura digital não garante, por si só, que os usuários desenvolvam as competências necessárias para utilizá-la com segurança.

Essa observação ganha relevância quando a digitalização é analisada sob a ótica da segurança da informação. A ampliação das interações digitais cria oportunidades de ataque que não dependem exclusivamente de falhas técnicas, mas da manipulação dos próprios usuários. A engenharia social pode ser descrita como o conjunto de estratégias empregadas para induzir uma pessoa a revelar informações, executar ações ou adotar comportamentos que comprometam a segurança, por meio de persuasão, engano ou exploração de relações de confiança (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, [s.d.]).

Entre essas estratégias, o *phishing* ocupa posição central na literatura. Desolda et al. (2022), em revisão sistemática sobre fatores humanos em ataques de *phishing*, mostram que a

compreensão desse tipo de ataque exige considerar como os usuários percebem riscos, mensagens e sinais de fraude, e não apenas o conhecimento técnico que possuem. Os autores defendem que os fatores humanos precisam ser tratados como parte constitutiva das estratégias de defesa, ao lado dos controles técnicos.

A relevância do fenômeno se acentua no contexto universitário. Diferentemente de ambientes corporativos comparativamente mais homogêneos, as IES reúnem estudantes, docentes, pesquisadores, técnicos administrativos, gestores e prestadores de serviço, com níveis distintos de experiência, competência digital e responsabilidade sobre ativos informacionais. A própria natureza da atividade acadêmica, que depende de comunicação e compartilhamento constantes de informação, amplia as oportunidades de interação legítima que podem ser exploradas por agentes maliciosos.

Estudos internacionais fornecem evidência empírica dessa vulnerabilidade específica. Broadhurst et al. (2019), em estudo quase experimental com 138 estudantes de uma universidade australiana, testaram a resposta a mensagens fraudulentas genéricas, personalizadas e direcionadas (“*spear*”). Estudantes internacionais e calouros foram enganados por um número significativamente maior de mensagens do que estudantes nacionais e veteranos; mensagens personalizadas tenderam a gerar mais engajamento, embora nem todas as diferenças observadas tenham sido estatisticamente significativas. Casagrande et al. (2023), em avaliação de *phishing* conduzida em uma universidade europeia com 1.508 participantes, encontraram taxas de clique de 30%, 11% e 13% em três campanhas sucessivas e verificaram que estudantes foram mais suscetíveis do que professores e pessoal técnico-administrativo. Diaz, Sherman e Joshi (2020), em experimento com 1.350 estudantes de graduação da *University of Maryland, Baltimore County*, associaram a suscetibilidade a *phishing* a fatores como progressão acadêmica, treinamento prévio em segurança e tempo de uso do computador. Em conjunto, esses estudos indicam que a vulnerabilidade não pode ser explicada por um único fator individual, mas resulta da interação entre perfil do usuário, contexto e características da mensagem.

A resposta institucional a esse cenário não se resume à identificação de comportamentos vulneráveis: depende também da capacidade de transformar informação sobre segurança em conhecimento efetivamente aplicado. Essa ideia pode ser aproximada, ainda que de modo indireto, da noção de capacidade absortiva discutida por Joanella e Laimer (2023). Em ensaio teórico sobre compartilhamento de conhecimento, inovação e desempenho organizacional, os

autores argumentam que a capacidade de adquirir e transformar conhecimento externo é condição para que esse conhecimento produza resultados. O estudo não investiga segurança da informação nem instituições de ensino, de modo que não deve ser tomado como evidência sobre eficácia de treinamentos de cibersegurança; sua contribuição para este artigo é conceitual, ao sugerir que disponibilizar informação sobre segurança não equivale a fazer com que ela seja compreendida e utilizada.

Essa consideração é pertinente às IES, nas quais a formação é atividade central. Rodrigues et al. (2024), em levantamento com 300 estudantes de uma universidade pública brasileira, verificaram que elementos do ecossistema empreendedor, incluindo a própria universidade, influenciam positivamente antecedentes atitudinais da intenção empreendedora, e destacaram o papel de práticas de aprendizagem experiencial. O objeto do estudo é a intenção empreendedora, não a segurança digital; seus resultados oferecem, ainda assim, evidência contextual de que o ambiente universitário participa da formação de atitudes e competências dos estudantes, o que é relevante para pensar a conscientização em segurança como processo formativo contínuo, e não como ação isolada.

A questão central deste artigo situa-se, portanto, na interseção entre digitalização, comportamento humano e segurança institucional no ambiente acadêmico. Existe literatura consolidada sobre engenharia social e *phishing* em organizações; permanece relevante, contudo, integrar como esse fenômeno se manifesta especificamente nas IES, considerando a diversidade de seus usuários e o valor dos ativos informacionais envolvidos.

Uma advertência conceitual é necessária. É comum descrever o usuário como o “elo mais fraco” da segurança da informação. Tomada de forma literal, essa expressão tende a individualizar um problema que também é organizacional: comportamentos inseguros podem ser condicionados por processos mal desenhados, interfaces confusas, comunicação institucional deficiente, ausência de treinamento e falhas no desenho dos próprios sistemas. A literatura sobre fatores humanos em *phishing* sustenta essa leitura sociotécnica, segundo a qual a segurança resulta da interação entre indivíduos e o contexto em que atuam (DESOLDA et al., 2022).

A relevância deste estudo decorre da concentração, nas IES, de informações pessoais, acadêmicas, administrativas e de pesquisa. Um ataque de engenharia social bem-sucedido pode ultrapassar o comprometimento de uma única conta e atingir sistemas compartilhados e fluxos de informação institucionais.

A questão também tem dimensão formativa. A digitalização exige que estudantes, docentes e servidores desenvolvam não apenas competência para operar plataformas digitais, mas também capacidade de reconhecer situações potencialmente fraudulentas e de agir de acordo com políticas de segurança. A literatura sobre digitalização organizacional indica que treinamento e desenvolvimento de habilidades são condições relevantes para o aproveitamento efetivo de tecnologias (BATISTA; AROUCA; LOBATO, 2024), argumento que, por aproximação conceitual, também se aplica à segurança institucional.

Por essas razões, o enfrentamento da engenharia social não deve ser reduzido à instalação de ferramentas técnicas. A proteção depende da articulação entre tecnologia, processos organizacionais e formação de usuários, entendimento que a literatura específica sobre fatores humanos em *phishing* também sustenta (DESOLDA et al., 2022).

O objetivo geral deste estudo é analisar os impactos da engenharia social no ambiente acadêmico a partir da literatura científica e de fontes técnicas disponíveis.

Como objetivos específicos, busca-se:

- identificar as principais técnicas de engenharia social discutidas na literatura em relação à comunidade acadêmica;
- descrever os tipos de dados, informações e sistemas potencialmente visados nesse contexto;
- discutir os impactos associados a esses ataques conforme relatado pela literatura examinada; e
- discutir diretrizes de conscientização e mitigação de risco aplicáveis a instituições de ensino superior.

2. REVISÃO DE LITERATURA

2.1 Segurança da informação, engenharia social e fatores humanos

A engenharia social distingue-se de ataques puramente técnicos por explorar mecanismos de influência, persuasão e engano para induzir uma pessoa a agir de modo favorável ao atacante (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, [s.d.]). A tecnologia costuma funcionar como canal de comunicação nesse processo, mas o elemento explorado diretamente é a tomada de decisão do usuário.

O *phishing*, definido como a tentativa de obter informações sensíveis por meio de comunicação que simula uma entidade legítima (NATIONAL INSTITUTE OF STANDARDS

AND TECHNOLOGY, [s.d.]), constitui a manifestação mais estudada desse fenômeno. Desolda et al. (2022) mostram, em revisão da literatura sobre o tema, que a compreensão da vulnerabilidade a *phishing* exige considerar percepção, comportamento e interação do usuário com mensagens e interfaces, e não apenas o conhecimento técnico disponível. Os autores também argumentam que os fatores humanos precisam ser incorporados às estratégias de defesa, e não tratados como uma categoria residual em relação aos controles técnicos.

Essa literatura recomenda cautela diante de explicações que atribuem a vulnerabilidade exclusivamente à falta de conhecimento. O comportamento diante de uma tentativa de *phishing* resulta da interação entre fatores individuais, organizacionais e contextuais, o que é particularmente relevante em ambientes, como o acadêmico, em que diferentes categorias de usuários têm diferentes responsabilidades e padrões de uso dos sistemas.

2.2 Digitalização, competências e segurança institucional

A digitalização altera não apenas os instrumentos disponíveis às organizações, mas também as competências necessárias para utilizá-los. Batista, Arouca e Lobato (2024), em pesquisa bibliográfica, documental e pesquisa-ação conduzida junto a micro e pequenas empresas de Santarém, identificaram que a disponibilidade de tecnologias digitais não era acompanhada de seu aproveitamento pleno, em razão de barreiras como falta de treinamento e insuficiência de tempo para planejamento estratégico. Os autores concluem que ganhos de competitividade dependem de planejamento e de desenvolvimento de habilidades, não apenas de aquisição tecnológica.

Esse resultado não trata de cibersegurança nem de IES; sua utilização neste artigo é, portanto, uma inferência conceitual, e não uma extensão empírica do estudo original. A inferência é a seguinte: assim como a digitalização comunicacional em pequenas empresas depende de competência de uso, a segurança institucional também depende de que usuários compreendam e apliquem procedimentos, e não apenas de que a instituição disponha de controles tecnológicos.

A relação entre ambiente institucional e formação de competências também encontra respaldo contextual em Rodrigues et al. (2024), que analisaram o ecossistema empreendedor de uma universidade pública brasileira por meio de levantamento com 300 estudantes e modelagem de equações estruturais. Os resultados indicaram influência positiva do ecossistema empreendedor sobre antecedentes atitudinais da intenção empreendedora e destacaram a relevância de práticas de aprendizagem experiencial. Esse achado não permite afirmar que a aprendizagem experiencial reduz *phishing* ou outros incidentes; sustenta, de modo mais limitado, que processos educacionais e características do ambiente institucional participam da formação de atitudes e competências dos estudantes, o que é relevante para discutir programas de conscientização em segurança como componentes permanentes da formação acadêmica.

2.3 Compartilhamento e absorção do conhecimento organizacional

A segurança da informação também envolve processos de produção, compartilhamento e aplicação de conhecimento: políticas, alertas e treinamentos precisam ser compreendidos e incorporados às práticas institucionais, não apenas disponibilizados.

Joanella e Laimer (2023) discutem, em ensaio teórico, a relação entre compartilhamento de conhecimento, inovação e desempenho organizacional, atribuindo à capacidade absortiva o papel de moderar essa relação: a capacidade interna de adquirir e transformar conhecimento externo é o que permite que esse conhecimento produza resultados. Sua contribuição para este trabalho é oferecer uma lente organizacional para um problema recorrente na literatura de segurança: a disponibilização de informação não é suficiente, por si só, para produzir mudança de comportamento.

Essa perspectiva sugere que programas de conscientização em segurança sejam concebidos não como simples transmissão de conteúdo, mas como processos de aprendizagem nos quais o usuário precisa reconhecer, interpretar e aplicar o conhecimento em situações concretas.

2.4 Vetores de engenharia social no contexto acadêmico

A literatura permite distinguir modalidades de engenharia social conforme a estratégia utilizada para induzir o comportamento da vítima. Entre os vetores discutidos com maior frequência em relação ao ambiente acadêmico estão o *phishing*, o *spear phishing*, o *pretexting* e o *baiting* (ADU-MANU et al., 2023; MATYOKUREHWA et al., 2022). A descrição a seguir permanece em nível conceitual e não constitui orientação operacional para a execução desses ataques.

2.4.1 *Phishing*

O *phishing* consiste em uma tentativa fraudulenta de obter informações sensíveis por meio de comunicação que simula uma entidade legítima, tendo como alvos usuais credenciais e dados pessoais. No ambiente acadêmico, essa estratégia costuma assumir a forma de mensagens que imitam comunicações de setores institucionais, como secretaria, tecnologia da informação ou biblioteca, explorando situações rotineiras, como atualização cadastral ou acesso a plataformas.

O risco não é hipotético: Broadhurst et al. (2019) encontraram maior associação entre engano e o perfil de estudante internacional ou calouro; Casagrande et al. (2023) identificaram maior suscetibilidade entre estudantes em comparação com professores e pessoal técnico-administrativo; Cuchta et al. (2019), em campanhas de *phishing* e *spear phishing* conduzidas em uma universidade norte-americana envolvendo estudantes, docentes e funcionários, registraram taxa de clique de 44,3% e inserção de credenciais válidas por 18,6% dos participantes. Esses resultados, obtidos em contextos institucionais distintos, não devem ser generalizados automaticamente para as IES brasileiras, mas evidenciam a heterogeneidade da suscetibilidade entre grupos da comunidade acadêmica.

2.4.2 *Spear phishing*

O *spear phishing* corresponde a uma modalidade direcionada, em que a mensagem é personalizada para um indivíduo ou grupo específico a partir de informações públicas ou previamente obtidas sobre a vítima. Essa modalidade tem relevância particular para universidades porque parte de seus membros tem acesso privilegiado a dados de pesquisa, informações administrativas e documentos institucionais. A afirmação de que o *spear phishing* necessariamente resulta em roubo de propriedade intelectual deve ser tratada como possibilidade.

Os resultados de Broadhurst et al. (2019) mostram que mensagens personalizadas tendem a produzir maior engajamento, embora os próprios autores ressaltem que nem todas as diferenças observadas foram estatisticamente significativas. A personalização deve, portanto, ser entendida como característica potencialmente relevante da estratégia de ataque, e não como garantia de maior eficácia em qualquer contexto.

2.4.3 *Pretexting*

O *pretexting* utiliza um cenário ou identidade fictícia para obter informações ou induzir determinada ação, com o atacante apresentando-se, por exemplo, como funcionário de suporte técnico ou membro da administração. No contexto acadêmico, essa estratégia pode explorar relações de autoridade, urgência ou colaboração, como em solicitações que aparentam estar relacionadas à manutenção de conta ou ao compartilhamento de documentos.

A literatura sustenta a relevância desses mecanismos de manipulação (ADU-MANU et al., 2023), entretanto, em termos de frequência, ainda não se pode afirmar como mais recorrente do que outras modalidades no ambiente acadêmico brasileiro, tratando-se de uma questão em aberto, a ser respondida por estudos empíricos comparativos entre vetores.

2.4.4 *Baiting*

O *baiting* utiliza uma “isca”, como um arquivo ou dispositivo aparentemente atraente, para despertar curiosidade ou expectativa de benefício. No ambiente universitário, essa estratégia poderia, em tese, assumir a forma de arquivos ou dispositivos associados a conteúdos de interesse acadêmico. Não foi localizada, na literatura examinada, documentação suficiente para caracterizar o *baiting* como um dos principais vetores especificamente nas IES brasileiras; sua presença deve ser compreendida como uma possibilidade relevante dentro da taxonomia da engenharia social, e não como resultado de prevalência demonstrado por este estudo.

2.5 Instituições de ensino superior como contexto específico de mitigação

Parte da literatura sobre engenharia social já se volta especificamente para o ambiente universitário. Matyokurehwa et al. (2022) desenvolveram e validaram, por meio de técnica Delphi com 25 especialistas de três instituições de ensino superior, um framework de mitigação de engenharia social fundamentado na teoria do controle equilibrado de Dhillon. Os autores identificaram que conscientização sobre engenharia social, política organizacional de segurança e segurança de dispositivos conectados (IoT) contribuem para reduzir esse tipo de ataque em contextos acadêmicos, resultado que reforça a necessidade de tratar a mitigação como problema multidimensional, e não apenas tecnológico.

3. METODOLOGIA

3.1 Delineamento da pesquisa

Este estudo foi desenvolvido a partir de revisão bibliográfica e de análise documental de relatórios técnicos e institucionais relacionados à engenharia social e à segurança da informação no ambiente acadêmico. A estratégia buscou integrar evidências da literatura científica com informações documentadas por organizações do setor de segurança da informação.

Como estratégia de busca completa por base de dados, registro de operadores booleanos, fluxograma de seleção e avaliação formal da qualidade dos estudos incluídos. Por esse motivo, e em atenção ao rigor terminológico exigido em publicações científicas, este trabalho é classificado como revisão bibliográfica narrativa, estruturada por eixos temáticos, complementada por análise documental.

3.2 Estratégia de busca

A revisão consultou as bases Scopus, SciELO e Google Scholar, além de repositórios institucionais e sítios de organizações de referência em segurança da informação, considerando majoritariamente publicações do período de 2018 a 2025. Os descritores utilizados incluíram "engenharia social", "*social engineering*", "ambiente acadêmico", "*higher education*", "*phishing*" e "segurança da informação". A combinação desses termos permitiu localizar estudos na interseção entre comportamento humano, ataques de engenharia social e segurança no contexto educacional.

3.3 Critérios de análise

Os materiais localizados foram examinados considerando três dimensões: tipo de ataque (*phishing*, *spear phishing*, *pretexting* e *baiting*), impacto potencial (financeiro, operacional e reputacional) e tipo de ativo ou dado potencialmente comprometido (credenciais, informações pessoais e informações institucionais). Essas três dimensões constituem uma estrutura analítica adotada pelos autores para organizar a discussão, e não uma taxonomia consolidada e universalmente aceita na literatura de segurança da informação.

Este artigo não apresenta estatísticas de frequência sobre a prevalência de vetores de ataque na literatura revisada, e concentra-se, em vez disso, na análise qualitativa dos achados descritos por cada fonte.

4. RESULTADOS E DISCUSSÃO

A análise indica que a engenharia social constitui uma dimensão relevante da superfície de ataque das IES, sobretudo porque a transformação digital amplia, simultaneamente, a disponibilidade de serviços, a circulação de informação e o número de interações mediadas por sistemas digitais. O risco associado não decorre exclusivamente de vulnerabilidades técnicas, mas também da interação entre usuários, processos institucionais e tecnologias.

Esse argumento encontra respaldo em estudos que analisam a segurança da informação a partir de perspectiva organizacional. Aramuni e Maia (2020) discutem a engenharia social como ameaça à segurança da informação corporativa e destacam a necessidade de compreender vulnerabilidades ligadas ao modo como as organizações utilizam e protegem seus ativos informacionais. O estudo tem orientação corporativa, e sua aplicação ao ambiente universitário deve ser entendida como aproximação conceitual, não como evidência empírica específica sobre IES.

A especificidade do ambiente acadêmico relaciona-se, entre outros fatores, à intensa circulação de informação entre estudantes, docentes, pesquisadores, gestores e equipes técnico-administrativas, que a digitalização amplia. Batista, Arouca e Lobato (2024) mostram, em contexto empresarial, que disponibilidade de tecnologia não implica, por si só, seu uso adequado; a mesma lógica sustenta que a expansão da infraestrutura digital não deve ser interpretada automaticamente como aumento proporcional de vulnerabilidade. O que a literatura permite sustentar é que a digitalização cria novas oportunidades de interação e, com isso, novas situações em que decisões humanas passam a integrar o processo de segurança.

No âmbito específico do ensino superior, estudos empíricos mostram que usuários acadêmicos constituem uma superfície de ataque relevante. Cuchta et al. (2019) realizaram campanhas de phishing e spear phishing envolvendo estudantes, docentes e funcionários de uma universidade norte-americana e registraram taxas expressivas de interação com as mensagens fraudulentas. Casagrande et al. (2023), em avaliação com 1.508 participantes de uma instituição europeia, observaram diferentes níveis de suscetibilidade entre grupos de usuários e entre diferentes desenhos de mensagem. Esses resultados reforçam a pertinência de investigar o comportamento humano no contexto universitário, embora não devam ser generalizados automaticamente para as IES brasileiras, para as quais não foram localizados estudos experimentais equivalentes.

Relatórios setoriais recentes indicam que instituições educacionais têm sido alvo crescente de ataques baseados em engenharia social. O relatório *Cyber Signals*, da Microsoft (2024), aponta o setor educacional como alvo relevante de campanhas de *phishing*, embora, por se tratar de fonte técnica e não de estudo científico revisado por pares, deva ser utilizado como informação contextual sobre tendências de ameaça, e não como evidência estatística equivalente a um estudo primário. Assim, não foi possível, confirmar a existência de casos brasileiros específicos com números verificáveis de contas ou equipamentos comprometidos;

por isso, afirmações desse tipo foram deliberadamente omitidas e a discussão permanece no nível qualitativo sustentado pelas fontes efetivamente verificadas.

4.1 Impactos potenciais da engenharia social nas IES

Os impactos da engenharia social sobre as IES não se restringem a perdas financeiras diretas. Com base na estrutura analítica apresentada na seção 3.3, é possível organizar esses impactos em três categorias amplas, apresentadas no Quadro 1 a título de integração de informações.

Quadro 1: Categorias de impacto potencial da engenharia social em IES.

Categoria	Exemplos de manifestação	Possíveis consequências
Financeira	Custos de remediação de incidentes, exposição a sanções por violação de dados pessoais, risco a financiamentos de pesquisa	Realocação de recursos orçamentários, prejuízo a projetos em andamento
Operacional	Interrupção de serviços essenciais, como e-mail, sistemas de matrícula ou ambientes virtuais de aprendizagem	Atraso em atividades acadêmicas e administrativas
Reputacional	Exposição pública de incidentes, perda de confiança de parceiros, alunos e financiadores	Dificuldade de atração de talentos, parcerias e recursos

Essa categorização deve ser lida como ferramenta organizadora da discussão, construída a partir da literatura geral sobre impactos de incidentes de segurança da informação, e não como taxonomia empiricamente derivada de um levantamento quantitativo específico sobre IES brasileiras. Em nível mais descritivo, Souza Pereira, Vicentine e Rizo (2022) associam a engenharia social a impactos como venda de informação sensível, espionagem, distribuição de malware e exposição de dados pessoais; os autores tratam do contexto organizacional em geral, sem abordar especificamente instituições de ensino, de modo que sua contribuição a este artigo é ilustrativa das categorias de dano descritas na literatura.

4.2 Vetores de engenharia social identificados na literatura

Entre os mecanismos discutidos, o phishing ocupa posição central por combinar comunicação eletrônica, impersonação e manipulação psicológica. O relatório setorial *Cyber Signals* (MICROSOFT, 2024) também identifica o phishing como vetor inicial recorrente em

ataques ao setor educacional, embora reconheça variação entre fontes quanto às estimativas de frequência.

No contexto universitário, o *phishing* pode assumir diferentes formatos: mensagens em massa que simulam comunicações institucionais e mensagens de spear phishing, direcionadas a indivíduos ou grupos específicos com base em informação previamente coletada. O pretexting, por sua vez, depende da construção de uma narrativa que confere legitimidade à solicitação do atacante, explorando relações de confiança, autoridade percebida ou urgência, mais do que características técnicas da mensagem. O baiting, embora presente na taxonomia geral da engenharia social, não pôde ser caracterizado, nesta revisão, como vetor de prevalência comprovada especificamente nas IES brasileiras.

O aumento do uso de plataformas digitais não torna, isoladamente, uma instituição mais vulnerável; o risco depende de como essas tecnologias são implementadas, utilizadas e governadas. Batista, Arouca e Lobato (2024) mostram, em outro contexto organizacional, que disponibilidade tecnológica sem desenvolvimento de competências não garante aproveitamento adequado, argumento que se aproxima do problema tratado neste artigo: a transformação digital das IES precisa ser acompanhada do desenvolvimento de capacidades humanas e organizacionais correspondentes.

4.3 Conhecimento, aprendizagem e cultura de segurança

A construção de uma cultura institucional de segurança depende da circulação efetiva de conhecimento sobre riscos e procedimentos, não apenas de sua disponibilização formal. O argumento de Joanella e Laimer (2023) sobre capacidade absortiva, embora não trate de cibersegurança, oferece uma lente útil para esse problema: uma instituição pode disponibilizar políticas e alertas sobre phishing sem que os usuários necessariamente incorporem essas informações ao comportamento cotidiano, o que sugere a necessidade de mecanismos que favoreçam aprendizagem, retenção e aplicação prática, e não apenas divulgação.

Essa leitura dialoga com os resultados de Rodrigues et al. (2024), segundo os quais o ambiente universitário participa da formação de atitudes e comportamentos por meio de experiências educacionais estruturadas. Sem transformar esse achado em evidência sobre treinamento de cibersegurança, é possível sustentar, a partir dele, que a educação em segurança tende a ser mais efetiva quando incorporada a processos educacionais contínuos, e não estruturada como campanha pontual.

4.4 Implicações para prevenção e mitigação

Os resultados da revisão indicam que a mitigação da engenharia social não deve ser estruturada exclusivamente como problema tecnológico. Autenticação multifatorial, filtros de mensagens e mecanismos automatizados de detecção são importantes, mas não eliminam a necessidade de preparar usuários para reconhecer e comunicar situações suspeitas (ADU-MANU et al., 2023).

O framework validado por Matyokurehwa et al. (2022) para instituições de ensino superior, discutido na seção 2.5, aponta que conscientização sobre engenharia social, política organizacional de segurança e segurança de dispositivos conectados atuam de forma combinada na redução desse tipo de ataque, resultado que reforça a necessidade de estratégias multidimensionais nesse contexto específico. De modo convergente, Adu-Manu et al. (2023), em revisão sobre phishing e engenharia social, argumentam que soluções exclusivamente técnicas são insuficientes e defendem a combinação entre compreensão do comportamento humano, políticas organizacionais e mecanismos técnicos de detecção.

Para a operacionalização de programas de conscientização, ferramentas como a NIST Phish Scale (DAWKINS; JACOBS, 2023) oferecem um recurso metodológico relevante, ao permitir estimar a dificuldade de identificação de uma mensagem de phishing e, com isso, calibrar programas de treinamento e simulação de forma mais criteriosa do que a simples aplicação de campanhas padronizadas.

No ambiente universitário, uma estratégia de mitigação mais consistente combinaria, portanto, ao menos quatro dimensões: capacitação contínua, adaptada aos diferentes perfis de usuários; mecanismos técnicos de proteção, incluindo autenticação multifatorial e filtragem de mensagens; processos institucionais claros para comunicação de incidentes e validação de solicitações sensíveis; e aprendizagem baseada em situações práticas, incluindo simulações conduzidas com critérios éticos e finalidade predominantemente educativa.

Não foi localizado, estudo experimental específico que permita afirmar, com segurança metodológica, que um programa determinado de treinamento produziu redução estatisticamente significativa de incidentes em instituições de ensino brasileiras; essa lacuna é registrada como direção relevante para pesquisas futuras.

5. CONSIDERAÇÕES FINAIS

A análise da literatura científica e das fontes técnicas examinadas evidencia que a engenharia social constitui um desafio que ultrapassa os limites da segurança tecnológica, pois explora comportamentos humanos inseridos em contextos institucionais específicos. *Phishing* e outras modalidades de engenharia social figuram entre os principais vetores identificados, mas a vulnerabilidade não pode ser atribuída exclusivamente às características individuais dos usuários. Políticas institucionais, processos organizacionais, tecnologias adotadas e oportunidades de aprendizagem influenciam as possibilidades de tomada de decisão segura. Nesse sentido, uma perspectiva sociotécnica permite compreender o comportamento humano como parte de um sistema de segurança mais amplo, no qual as condições institucionais podem favorecer ou dificultar práticas seguras.

Os estudos examinados também indicam que a transformação digital das instituições de ensino superior precisa ser acompanhada pelo desenvolvimento de capacidades humanas e organizacionais. A incorporação de tecnologias, por si só, não elimina barreiras relacionadas à capacitação, ao planejamento e à utilização adequada dos recursos disponíveis. Da mesma forma, a formação de comportamentos seguros depende de oportunidades contínuas de aprendizagem e da capacidade dos usuários de compreender e aplicar conhecimentos em situações concretas. A mitigação da engenharia social deve, portanto, articular mecanismos técnicos, políticas institucionais, processos de comunicação e ações permanentes de conscientização, reconhecendo que a segurança resulta da interação entre pessoas, tecnologias e processos organizacionais.

Nesse contexto, programas de conscientização podem contemplar o reconhecimento de mensagens suspeitas, práticas adequadas de autenticação e gerenciamento de credenciais, além de procedimentos institucionais para comunicação de incidentes. Simulações de phishing também podem ser utilizadas como recurso complementar de avaliação e aprendizagem, desde que conduzidas de maneira ética, transparente e com finalidade predominantemente educativa. Entretanto, os resultados desta revisão não permitem afirmar que treinamentos ou simulações reduzam necessariamente a ocorrência de incidentes em instituições de ensino superior brasileiras. As evidências disponíveis ainda são insuficientes para estabelecer essa relação no contexto nacional, o que reforça a necessidade de pesquisas empíricas capazes de avaliar diferentes estratégias de conscientização em condições institucionais diversas.

A principal contribuição deste estudo consiste em integrar diferentes dimensões da engenharia social no ambiente acadêmico, contemplando seus principais vetores, a participação do fator humano, os ativos potencialmente afetados e as estratégias de mitigação discutidas na literatura. A partir dessa síntese, evidencia-se a necessidade de compreender a segurança das instituições de ensino superior como uma questão que envolve simultaneamente tecnologia, processos, governança e desenvolvimento de competências. Pesquisas futuras podem avançar na investigação de conhecimentos, atitudes e comportamentos de diferentes grupos de usuários, na comparação entre estratégias de capacitação e na análise da relação entre cultura organizacional, aprendizagem e práticas de segurança. A produção dessas evidências será fundamental para verificar como estratégias de prevenção podem ser adaptadas às características das instituições brasileiras e para fortalecer a construção de ambientes acadêmicos mais preparados para enfrentar ameaças baseadas na exploração do comportamento humano.

6. REFERÊNCIAS

ADU-MANU, Kwasi Sarpong; AHIABLE, Richard Kwasi; APPATI, Justice Kwame; MENSAH, Emmanuel Essel. Phishing attacks in social engineering: a review. **Journal of Cyber Security**, v. 4, n. 4, p. 239-267, 2023. DOI: 10.32604/jcs.2023.041095.

ARAMUNI, João Paulo Carneiro; MAIA, Luiz Cláudio. O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa. **AtoZ: novas práticas em informação e conhecimento**, v. 7, n. 1, p. 31-37, 2020. DOI: 10.5380/atoz.v7i2.64640.

BATISTA, Alessandra Giselle Silva; AROUCA, Marcia Waimer Spinola; LOBATO, Fábio Manoel França. Estratégias de digitalização comunicacional para Micro e Pequenas Empresas como promotoras da inovação e competitividade. **Revista da Micro e Pequena Empresa**, v. 18, n. 3, p. 60-79, 2024.

BROADHURST, Roderic; SKINNER, Katie; SIFNIOTIS, Nicholas; MATAMOROS-MACIAS, Bryan; IPSEN, Yuguang. Phishing and cybercrime risks in a university student community. **International Journal of Cybersecurity Intelligence and Cybercrime**, v. 2, n. 1, p. 4-23, 2019.

CASAGRANDE, Marco; CONTI, Mauro; FEDELI, Monica; LOSIOUK, Eleonora. Alpha Phishing fraternity: phishing assessment in a higher education institution. **Journal of Cybersecurity Education, Research and Practice**, v. 2022, n. 2, art. 2, 2023.

CUCHTA, Tom; BLACKWOOD, Brian; DEVINE, Thomas R.; NIICHEL, Robert J.; DANIELS, Kristina M.; LUTJENS, Caleb H.; MAIBACH, Sydney; STEPHENSON, Ryan J. Human risk factors in cybersecurity. In: SIGITE ’19: THE 20TH ANNUAL CONFERENCE ON INFORMATION TECHNOLOGY EDUCATION, 20., 2019, Tacoma. **Proceedings of the 20th Annual SIG Conference on Information Technology Education**. New York: ACM, 2019. p. 87-92. DOI: 10.1145/3349266.3351407.

DAWKINS, Sharon; JACOBS, Jessica. **NIST Phish Scale User Guide**. Gaithersburg: National Institute of Standards and Technology, 2023. (NIST Technical Note 2276). DOI: 10.6028/NIST.TN.2276.

DESOLDA, Giuseppe; FERRO, Lauren S.; MARRELLA, Andrea; CATARCI, Tiziana; COSTABILE, Maria Francesca. Human factors in phishing attacks: a systematic literature review. **ACM Computing Surveys**, v. 54, n. 8, p. 1-35, 2022. DOI: 10.1145/3469886.

DIAZ, Alejandra; SHERMAN, Alan T.; JOSHI, Anupam. Phishing in an academic community: a study of user susceptibility and behavior. **Cryptologia**, v. 44, n. 1, p. 53-67, 2020. DOI: 10.1080/01611194.2019.1623343.

JOANELLA, Fabio; LAIMER, Claudionor Guedes. O efeito moderador da capacidade absortiva entre o compartilhamento de conhecimento, a inovação e o desempenho da empresa. **Revista da Micro e Pequena Empresa**, v. 17, n. 3, p. 86-102, 2023. DOI: 10.48099/1982-2537/2023v17n3p86102.

MATYOKUREHWA, Kanos; RUDHUMBU, Norman; GOMBIRO, Cross; CHIPFUMBU-KANGARA, Colletor Tendeukai. Enhanced social engineering framework mitigating against social engineering attacks in higher education. **Security and Privacy**, v. 5, n. 5, e237, 2022. DOI: 10.1002/spy2.237.

MICROSOFT. Cyber Signals, 8ª edição: Educação sob cerco, como os cibercriminosos têm como alvo escolas. Redmond: Microsoft, 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Social engineering. Gaithersburg**: NIST, [s.d.]. NIST Computer Security Resource Center Glossary.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Phishing. Gaithersburg**: NIST, [s.d.]. NIST Computer Security Resource Center Glossary.

RODRIGUES, Henrique Geraldo; VASCONCELOS, Andréa Costa Van Herk; OLIVEIRA, Márcia Freire de; CARRIJO, Michelle de Castro; MAEMURA, Marcia Mitie Durante; FERNANDES, Vivian Duarte Couto. A influência do ecossistema empreendedor na formação da intenção empreendedora de estudantes universitários: um estudo em uma universidade pública brasileira. **Revista da Micro e Pequena Empresa**, v. 18, n. 3, 2024.

SOUZA PEREIRA, Lucas Avanci de; VICENTINE, Augusto Luciano; RIZO, Andre Castro. Impactos da Engenharia Social na Segurança da Informação**. Revista Brasileira em Tecnologia da Informação**, v. 4, n. 1, p. 48-58, 2022.