# Falhas de Cibersegurança em Instituições Educacionais: Uma Revisão Sistemática

**Marcelo Santos da Cruz**[1], **Júlia Rocha Valverde**[1],
**Filippi Reis Menezes**[1], **Luiz Felipe Oliveira Carregosa**[1],
**Jordan Santos de Jesus**[1], **Gilton José Ferreira da Silva**[2]

[1]Departamento de Computação (DCOMP)
Universidade Federal de Sergipe (UFS)
Av. Marechal Rondon, s/n – Jardim Rosa Elze – CEP 49100-000
São Cristóvão – SE – Brazil

[2]Programa de Pós-Graduação em Ciência da Computação - (PROCC)
Universidade Federal de Sergipe (UFS)
Av. Marechal Rondon, s/n – Jardim Rosa Elze – CEP 49100-000
São Cristóvão – SE – Brazil

marcelo.cruz@dcomp.ufs.br, juliarvalverde@academico.ufs.br

filippirm@academico.ufs.br, luizfelipecarregosa@academico.ufs.br

jordansdj@academico.ufs.br, gilton@dcomp.ufs.br

***Abstract.*** *The COVID-19 pandemic has accelerated the digitalization of virtual teaching and interactions. While it brings benefits such as greater access to education, it also presents challenges in terms of cybersecurity. With increasing digitalization, vulnerability to attacks and data leaks increases. The purpose of this article is to explore the intersection between technological advancement and cybersecurity failures in educational environments. It proposes to achieve this through a systematic review of the literature, highlighting emerging challenges and analyzing measures to mitigate these growing threats. In conclusion, this systematic review highlights the critical importance of cybersecurity in educational institutions, especially amid the rapid advancement of the digital environment. It was identified that internal failures, lack of adequate awareness and training, and increased exposure due to the adoption of distance learning are significant factors that expose institutions to cyber attacks. Data leakage methods include a variety of attacks, highlighting the need for robust preventative measures such as cybersecurity awareness and implementing secure authentication practices. Additionally, human factors play an important role, highlighting the need for ongoing education and training in cybersecurity. Therefore, it is crucial to take proactive measures to address identified vulnerabilities and ensure the protection of institutions' data and systems against cyber threats.*

***Resumo.*** *A pandemia de COVID-19 acelerou a digitalização do ensino e das interações virtuais. Embora traga benefícios, como maior acesso à educação, também apresenta desafios em termos de segurança cibernética. Com a crescente digitalização, aumenta a vulnerabilidade a ataques e vazamentos de dados. O objetivo deste artigo é explorar a interseção entre o avanço tecnológico*

*e as falhas de segurança cibernética em ambientes educacionais. Ele propõe alcançar isso por meio de uma revisão sistemática da literatura, destacando os desafios emergentes e analisando medidas para mitigar essas crescentes ameaças. Em conclusão, esta revisão sistemática ressalta a importância crítica da segurança cibernética nas instituições educacionais, especialmente em meio ao rápido avanço do ambiente digital. Identificou-se que falhas internas, falta de conscientização e treinamento adequados, e o aumento da exposição devido à adoção do ensino a distância são fatores significativos que expõem as instituições a ataques cibernéticos. Os métodos de vazamento de dados incluem uma variedade de ataques, destacando a necessidade de medidas preventivas robustas, como conscientização sobre segurança cibernética e implementação de práticas de autenticação seguras. Além disso, os fatores humanos desempenham um papel importante, destacando a necessidade de educação contínua e treinamento em segurança cibernética. Portanto, é crucial adotar medidas proativas para abordar as vulnerabilidades identificadas e garantir a proteção dos dados e sistemas das instituições contra ameaças cibernéticas.*

## 1. Introdução

Com o avanço da tecnologia e a aceleração dos ambientes digitais impulsionados pela pandemia de COVID-19 em 2021, o mundo testemunhou uma rápida transformação na forma como interagimos virtualmente, principalmente em ambientes educacionais, onde tornou-se cada vez mais necessário a digitalização do ensino.

No entanto, junto com essas mudanças positivas, emergem desafios significativos em termos de segurança cibernética. À medida que mais aspectos da nossa vida cotidiana se tornam digitalizados, aumenta a vulnerabilidade a ataques cibernéticos e vazamentos de dados.

Este artigo explora a interseção entre o avanço tecnológico e as falhas de segurança cibernética em ambientes educacionais, através de uma revisão sistemática da literatura, destacando os desafios emergentes e analisando medidas para mitigar essas ameaças crescentes.

Nas próximas seções do estudo, exploraremos os principais assuntos que norteiam o tema em questão, os passos da metodologia utilizada e as questões de pesquisa promovidas pelo trabalho.

## 2. Fundamentação Teórica

A cibersegurança pode ser definida como um conjunto de atividades destinadas a proteger computadores, redes de computadores, hardwares relacionados softwares, outros dispositivos eletrônicos envolvidos com acesso ao ciberespaço e as informações que eles contêm e comunicam, incluindo softwares e dados, contra ataques, interrupções e outras ameaças [Fischer 2014].

Além disso, o autor também aborda a cibersegurança como uma corrida armamentista entre atacantes e defensores, já que, ao mesmo tempo que os invasores estão constantemente buscando falhas e brechas em sistemas para que se possam atacá-los, os indivíduos que buscam proteger esses sistemas estão buscando formas de proteger esses pontos fracos.

Nas próximas subseções, definiremos alguns assuntos que norteiam a cibersegurança e que serão abordados ao longo deste artigo.

### 2.1. Hacking

É de suma importância conceituar o termo ”Hacking”, pois essa prática abrange uma ampla gama de atividades que podem variar significativamente em sua natureza e intenção. Estabelecer uma definição clara e precisa de Hacking no contexto específico do estudo, auxilia a evitar diferentes interpretações, garantindo que a definição de hacking estabelece os limites do escopo do estudo, delineando claramente quais tipos de atividades estão sendo consideradas e quais estão fora do escopo.

Segundo [Aman Gupta 2017] Hacking é a técnica explorar os elos fracos ou lacunas encontrados nos sistemas de computador ou nas redes, afim de obter acesso não autorizado a dados ou para alterar os recursos dos sistemas de computador ou redes tidas como alvo.

[Aman Gupta 2017] ressalta ainda que o termo Hacking descreve modificações tanto em hardware quanto software ou redes do computador afim de atingir objetivos que não estão alinhados com as finalidades da aplicação . Em contraste o autor também define como, invasões de segurança roubar dados pessoais ou secretos, como números de telefone, detalhes de cartão de crédito, endereços, senhas de bancos on-line, etc.

### 2.2. Engenharia Social

No trabalho de [Wang et al. 2020], é citado como a engenharia social tem sido uma prática prevalente ao longo da história e é provável que continue a ser uma ameaça no futuro. [Wang et al. 2020] também mencionam como a engenharia social envolve a manipulação de indivíduos para tomar decisões que podem não ser do seu melhor interesse, uma tática que tem paralelos com estratégias enganosas usadas ao longo da história.

No campo da cibersegurança, [Wang et al. 2020] descrevem a engenharia social como um tipo de ataque que se aproveita das fraquezas humanas através da interação social, com o objetivo de comprometer a segurança cibernética. O que pode ocorrer com ou sem a exploração de falhas técnicas.

A ameaça da engenharia social decorre da inevitabilidade das vulnerabilidades humanas na cibersegurança. Não existe um sistema de computador que não dependa de humanos. Esses elementos humanos são inerentemente vulneráveis, a ponto de suas vulnerabilidades ofuscarem a eficácia de outras medidas de segurança. Isso significa que essa fraqueza de segurança é universal e independente de plataforma, software, rede ou idade do equipamento [Wang et al. 2020].

### 2.3. Consciência em Cibersegurança

[Shaw et al. 2009] define consciência em cibersegurança como o grau de compreensão dos usuários sobre a importância da segurança da informação e das responsabilidades de seus atos na execução do controle de segurança da informação para proteger dados e redes.

Segundo [Zwilling et al. 2022], muitos internautas não possuem consciência suficiente acerca dos riscos cibernéticos que correm e, por causa disso, não tomam as devidas medidas protetoras de segurança cibernética.

De acordo com [Furnell et al. 2006], embora ferramentas de proteção, como antivírus, estejam instaladas em computadores e em outros dispositivos, eles não mitigam completamente as violações de segurança cibernética. [Anwar et al. 2017] explica que isso ocorre, pois o ponto mais fraco da segurança cibernética é o humano erro.

[Zwilling et al. 2022] classifica os níveis de consciência em segurança cibernética em baixo, médio e alto. O nível baixo inclui comportamentos como não dar a devida atenção ou negligenciar alertas de segurança fornecidos por programas, aplicativos ou sistemas e acessar redes wifi gratuitas com seus dispositivos. No nível médio, o autor define como aqueles indivíduos que negligenciam o uso correto das tecnologias e, no alto nível, aqueles que possuem alto conhecimento em segurança cibernética e que são capazes de tomar ações de prevenção.

## 3. Metodologia

Após definir o tema proposto, elaborou-se questões de pesquisa para objetivar os temas a serem pesquisados. Baseado no título escolhido, definiu-se as palavras-chave e seus sinônimos na língua inglesa para formar a string de busca que viria ser utilizada nas bases de pesquisa escolhidas. Acessando as bases pelo portal Periódicos Capes, buscou-se, pela string, artigos e estudos que foram exportados para a plataforma Parsifal que nos serviu de ferramenta para conduzir a pesquisa. Com os artigos exportados, definiu-se critérios de inclusão e exclusão para que pudéssemos selecionar os estudos que seriam úteis para a pesquisa.

A seguir, tem-se as informações da metodologia de forma mais detalhada.

### 3.1. Questões de Pesquisa

Nessa pesquisa, buscou-se responder algumas questões relacionadas à cibersegurança dentro do ambiente educacional. Primeiramente, buscou-se entender, de forma geral, as principais vulnerabilidades de segurança cibernética que o setor educacional enfrenta (QP1), em seguida, o que leva esse setor a ser vítima dos ataques cibernéticos (QP2). Após isso, procuramos entender as questões técnicas envolvidas nos vazamentos e invasões ocorridos no setor (QP3). Também buscamos entender, além das questões técnicas, os fatores humanos ligados às invasões e vulnerabilidades (QP4) e, por fim, quais as medidas e soluções que podem ser implementadas para mitigar o problema (QP5).

A seguir, as questões de pesquisa:

1. Quais as principais falhas e brechas que levam a invasões no setor educacional?;
2. Quais as principais motivações para a invasão de sistemas e redes institucionais?;
3. Como ocorrem os vazamentos de dados das instituições?;
4. Como os fatores humanos contribuem para as falhas de cibersegurança nas instituições educacionais?;
5. Quais medidas podem ser tomadas pelas instituições de ensino para lidar com o problema em questão?

### 3.2. Palavras-chave

Na Tabela 1 são apresentadas as Palavras-Chave utilizadas utilizadas para formar a *string* de busca.

Na Tabela 2 é apresentada a *string* utilizada para as buscas nas bases:

**Tabela 1. Palavras-Chave utilizadas na *string* de busca**

| Palavra chave | Sinônimo em Inglês |
|---|---|
| falhas | failures, breaches, errors |
| cibersegurança | cybersecurity |
| instituição educacional | educational institution, educational sector, higher education, school, university |

**Tabela 2. *String* utilizada para realizar as buscas nas bases**

| **((”Educational Institution”OR ”Educational Sector”OR ”Higher Education” OR ”School”OR ”University”) AND (”Cybersecurity”) AND (”Failures”OR ”Breaches”OR ”Errors”))** |
|---|

### 3.3. Bases utilizadas na pesquisa

Para selecionar as bases de pesquisa que utilizamos no estudo, optamos por bases comuns dentro da área de computação.

Foram utilizadas as seguintes bases científica para a pesquisa:

- Scopus <http://www.scopus.com>;
- Web of Science <https://www.webofknowledge.com/>.

### 3.4. Critérios

A seguir os Critérios de Inclusão:

1. Artigos que abordam falhas de cibersegurança em ambientes educacionais.

A seguir os Critérios de Exclusão:

1. Artigos Duplicados;
2. Artigos de Revisão;
3. Artigos publicados antes de 2018;
4. Artigos que não abordem falhas de cibersegurança em ambientes educacionais;
5. Artigos que não estão nem em Inglês ou nem em Português;
6. Artigos sem acesso completo;
7. Livros completos.

## 4. Resultados e Discussão

Nesta seção, exploraremos os artigos selecionados e responderemos às questões de pesquisa.

### 4.1. Resultados

Para ler os artigos, adotamos a estratégia de ler o seu título e, em seguida, o seu resumo. Após a verificação dos assuntos abordados nos artigos, realizou-se a seleção destes por meio dos critérios de seleção. Com os artigos selecionados, estes foram lidos de início ao fim para que se pudesse extrair o máximo de informações relevantes.

A Figura 1 apresenta um fluxo descrevendo o processo de extração dos artigos desde a base até a análise.

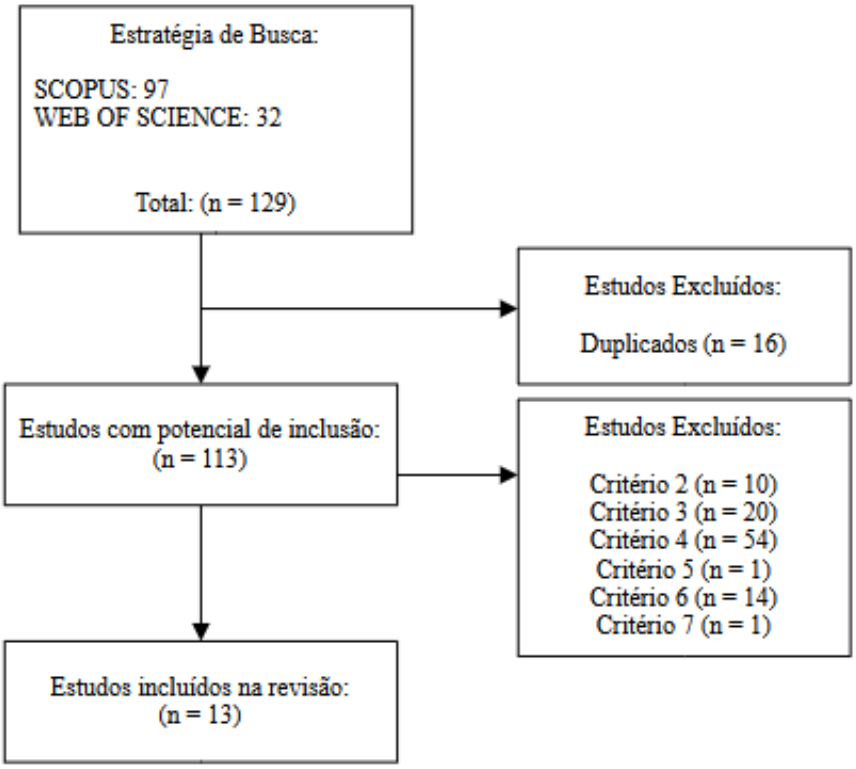


**Figura 1. Gráfico de prisma com a extração de dados**

### 4.2. Resumos das publicações

O estudo de [Basha et al. 2022] tem como objetivo compreender o nível de consciência e a atitude dos alunos de uma universidade em Bangalore, na Índia, a respeito de cibersegurança no ambiente de aprendizagem online, a pesquisa foi feita através de um questionário.

O estudo de [Abdulla et al. 2023] tem como objetivo analisar a consciência dos ataques de engenharia social entre indivíduos na área acadêmica e avaliar os desafios do uso da internet por esses indivíduos com ataques de segurança cibernética. A pesquisa foi realizada através de questionário online com estudantes de graduação, pós-graduação e docentes da Universidade de Sulaimani, no Iraque.

O estudo de [Singh and Naveenkumar 2023] tem como objetivo desenhar um modelo para proteção de vazamento de dados de acordo com as falhas de segurança mais frequentes.

O estudo de [Althobaiti 2021] tem como objetivo investigar os níveis de conscientização dos usuários em relação à ameaças cibernéticas e a capacidade de identificar e-mails de phishing e spam, visando sites educacionais. A pesquisa foi realizada através de questionário e da observação do comportamento de estudantes da Universidade Taif, na Arábia Saudita, após experimentos realizados pelos autores do artigo.

O estudo de [Liu et al. 2020] tem como objetivo estudar como o grau de tomada de decisão centralizada afeta a probabilidade de violações da segurança cibernética.

O estudo de [Yusif and Hafeez-Baig 2023] tem como objetivo desenvolver uma estrutura teórica para uma estratégia eficaz de conformidade de segurança cibernética nas instituições de ensino superior.

O estudo de [Li et al. 2023] investiga empiricamente os fatores que influenciam os riscos de falha de segurança no contexto do ensino superior de acordo com a teoria da oportunidade de crime e a teoria da rotina ativa.

O estudo de [Christopher et al. 2019] descreve os desafios e a solução para modificar um cluster HPC existente para oferecer suporte à computação de dados confidenciais, com o objetivo de mostrar que é possível e prático tomar essa abordagem em vez de construir um novo ambiente.

O estudo de [Canham et al. 2021] tem como objetivo determinar se existem tipos diferentes de funcionários organizacionais no que diz respeito ao seu comportamento em relação com os ataques de phishing e assim, fornecer informações sobre como melhorar a segurança na rede da organização.

O estudo de [Mykola et al. 2020] tem como objetivo simplificar o processo de tomada de decisão em cibersegurança usando técnicas de Soft Computing combinadas com planejamento estratégico.

O estudo de [DJEKI et al. 2021] tem como objetivo investigar as ameaças, as vulnerabilidades e os riscos de segurança cibernética no espaço de aprendizagem digital.

O estudo de [Fouad 2022] tem como objetivo discutir a necessidade da intervenção estatal nos processos de aquisição de sistemas de educação para garantir a segurança cibernética e responsabilizar os fornecedores por questões de falhas na segurança.

O estudo de [Chhillar and Shrivastava 2021] tem o objetivo de discutir a importância da gestão de vulnerabilidades em uma rede de computadores Universitária(UCN).

### 4.3. Quais as principais falhas e brechas que levam a invasões no setor educacional?

Segundo [DJEKI et al. 2021] As principais falhas de segurança relatadas que acabam expondo vulnerabilidades são falhas internas, onde ocorrem vazamentos ocasionados por configurações não implementadas nas áreas de rede, segurança, criptografia e autenticação, além da exibição de dados desnecessários, diretórios expostos e falta de validações de autorização, o que torna o ecossistema digital extremamente vulnerável a ataques externos.

Há ainda vazamentos de dados e falhas intencionais ou acidentais realizadas por ameaças internas, como mostra o estudo de [Singh and Naveenkumar 2023], que aborda diversos fatores humanos como credenciais comprometidas, fracas ou com padrões previsíveis, comprometimento com aplicações de terceiros e computação em nuvem mal configurada, além de fatores já citados anteriormente como configurações imprecisas de rede e segurança, outros fatores humanos abordados por [Li et al. 2023] relacionados a falhas de segurança em instituições de ensino são senhas fracas, exploits e falta de validações para funcionalidades de uploads de arquivos.

Outros estudos como o artigo publicado por [Abdulla et al. 2023] apontam a falta de capacitação de alunos e funcionários para lidar com engenharia social como uma fa-

lha grave e que põe em risco a segurança das instituições, além de realizar experimentos que relataram que seus participantes não tinham conhecimento básico de ferramentas de segurança como firewalls, além de não possuírem ferramentas antivírus e não conseguirem reconhecer e-mails maliciosos. Essa vertente que aponta o fator humano como principal causador de falhas é reforçada ainda mais por [Fouad 2022], que trata da falta de práticas de ciber-higiene citando senhas fracas e falta de atualizações de segurança.

### 4.4. Quais as principais motivações para a invasão de sistemas e redes institucionais?

O artigo de [Basha et al. 2022] não aborda esse tema diretamente em seu estudo, no entanto é citado no artigo que as ameaças cibernéticas geralmente ocorrem com a intenção de acessar, modificar e até mesmo destruir informações e dados sensíveis [Rubens 2014].

O estudo de [Althobaiti 2021] aponta que o campo do ensino superior pode ser alvo regular para ataques de engenharia social por ter uma grande população de usuários frequentes da internet.

O artigo de [Yusif and Hafeez-Baig 2023] aponta que, por serem ricas em dados populacionais e privados e, também, abrigam não apenas grandes e importantes dados biográficos, dados financeiros, mas também dados sobre pesquisa e desenvolvimento de ponta de tecnologias emergentes e novas [Gearhart et al. 2019] [Aliyu et al. 2020], as instituições de ensino superior atraem um número bastante substancial e diversas formas de ataques.

O estudo de [Li et al. 2023] aborda que, por geralmente ter uma carência de segurança competente, às instituições de ensino se tornam alvos mais acessíveis para hackers com motivações criminosas que buscam roubar informações valiosas.

Já o artigo de [DJEKI et al. 2021] aborda a difusão do ensino a distância como motivação para invasões no ambiente educacional. Como o ensino remoto depende do ambiente virtual para realização das atividades, instituições e indivíduos que fazem uso desse recurso são mais suscetíveis a sofrerem ataques cibernéticos se não houver uma boa proteção.

Com base nas informações apresentadas, é possível perceber que existem diversas motivações que culminam em ataques e invasões às instituições de ensino. Tendo em vista a grande variedade de motivos para esse ambiente ser vítima de ataques cibernéticos, surge também a necessidade de explorar diferentes maneiras de combater esse inimigo para que possa-se suprir as diversas causas e lados do problema.

### 4.5. Como ocorrem os vazamentos de dados das instituições?

O estudo de [Abdulla et al. 2023] mencionou os seguintes métodos utilizados por invasores para acessar dados não autorizados: Phishing e Spear Phishing: O Phishing é o método de ataque mais frequente e tem como objetivo obter dados pessoais, sendo uma técnica sofisticada e considerada a mais perigosa dos últimos anos, já o Spear Phishing é mais específico e tem como alvo principalmente usuários da internet, pessoas e grupos ou organizações, por meio de e-mails maliciosos [Alzahrani 2020] [Breda et al. 2017] [Airehrour et al. 2018]; Smashing: é muito semelhante ao Phishing, porém utiliza-se de

mensagens SMS em vez de e-mails [Alzahrani 2020]; Baiting: utiliza uma isca mais personalizada, baseada nos interesses da vítima [Airehrour et al. 2018]; Ataque de Pretexto: nele o invasor cria um cenário e uma narrativa falsa para chamar a atenção da vítima e envolvê-la [Conteh and Schmick 2021]; Quid Pro Quo: os invasores se passam por profissionais de TI para roubar dinheiro e informações das vítimas [Conteh and Schmick 2021].

O artigo de [Singh and Naveenkumar 2023] menciona exploração de vulnerabilidades, malware e ameaças internas como formas de invasão para o roubo de dados. Os autores definem exploração de vulnerabilidade como hackers que estão constantemente buscando brechas e pontos fracos em sistemas e explorando-os sempre que encontram; dentro de malware, os autores abordam principalmente a categoria de ransonware, que é utilizada maioritariamente para benefício monetário, nessa categoria os invasores roubam dados e realizam criptografia nos sitemas para depois exigir resgate das organizações, porém, se não houver um resgate, os dados são vazados; por fim, ao mencionar ameaças internas, os autores referem-se a agentes de dentro da organização, como funcionários insatisfeitos ou fornecedores, que podem ter acesso à dados sensíveis e os divulgam.

O estudo de [Althobaiti 2021] menciona o phishing e o spam como métodos de vazamento de dados. Dentro do artigo, o autor cita que processo de phishing geralmente é concebido por web designers especializados que criam sites que parecem ser legítimos; então, eles roubam informações pessoais quando as vítimas acessam e interagem com tais sites. Além disso, outra tática de phishing comumente usada, envolve o envio de um e-mail como primeira tentativa de roubar dados confidenciais e informações valiosas, como identidade e dados bancários, pedindo à vítima que clique em um link ou baixe um arquivo, esses e-mails geralmente são projetados para parecerem legítimos para o usuário [Arachchilage et al. 2013]. Já o spam pode incluir anúncios sem sentido através de e-mails, mensagens ou comunicações de mídia social, no entanto, eles também podem conter malware ou vírus maliciosos que foram criados para acessar as informações confidenciais dos destinatários [Broadhurst et al. 2018].

O artigo de [Yusif and Hafeez-Baig 2023] também menciona phishing, ramsonware e malware, além disso, os autores falam de invasões por problemas de senhas e de Bring Your Own Device (BYOD). Os problemas de senha geralmente são ocasionados pela utilização de senhas fracas ou repetidas, tornando mais fácil o acesso não autorizado por ”força bruta”ou malware. Já os problemas relacionados a BYOD estão relacionados ao fato de alunos e professores utilizarem seus dispositivos pessoais conectados à rede institucional, o que pode abrir portas para invasões dentro da rede institucional, por meio da instalação de softwares maliciosos e malwares.

Dadas as informações obtidas, percebe-se que o phishing é a forma de ataque mais comum vivenciada pelas instituições educacionais. Por ser um ataque maioritariamente relacionado à engenharia social, evidencia-se que o ambiente educacional é pobre em conhecimento de cibersegurança, já que esse tipo de ataque depende fortemente de decisões humanas. Apesar disso, outras formas mais técnicas de ataque também se demonstraram perigosas no setor, sendo de extrema importância que as instituições educacionais providenciem, além de mecanismos para aumentar a consciência dos indivíduos relacionados à elas sobre a segurança cibernética, formas de combater os métodos de ataque que exigem mais conhecimento técnico.

### 4.6. Como fatores humanos contribuem para as falhas de cibersegurança nas instituições educacionais?

O artigo de [DJEKI et al. 2021] Aponta diversas falhas humanas relacionadas a vulnerabilidades de cibersegurança, dentre elas, Falhas de criptografia, Design não seguro, Componentes vulneráveis e depreciados, Falhas de identificação e autenticação, Falhas de integridade de sistemas e dados, Falhas de segurança de auditoria e monitoramento, Códigos fora do limite, Neutralização imprópria de inputs durante a geração de páginas web, Leitura fora do limite, Validação inapropriada de inputs, Neutralização inapropriada de elementos especiais utilizados em sistemas operacionais, Neutralização inapropriada de elementos especiais usados em SQL, Limitação inapropriada de nomenclatura de diretórios.

O estudo de [Abdulla et al. 2023] explica que a engenharia social utiliza o erro humano para obter dados não autorizados de pessoas e organizações e, por isso, é um método que requer menos conhecimento técnico, tornando essencial o conhecimento sobre engenharia social para minimizar o impacto de seus ataques. Fundamentalmente, o ataque de engenharia social é o ato de explorar o comportamento humano para obter o acesso não autorizado à informações sensíveis.

Já os estudos de [Basha et al. 2022] e de [Fouad 2022] procuram aprofundar no fator humano, no caso o conhecimento em cibersegurança como um forte fator para evitar vazamentos de dados e para evitar vulnerabilidades. O estudo mostra a importância de alunos principalmente, mas também professores e funcionários de instituições educacionais, junto a falta de conscientização sobre as questões de segurança cibernética, possuírem esse conhecimento para tomarem as devidas medidas para prevenir o vazamento de seus dados dentro da instituição em um contexto de aulas online, como também evitar invasões às salas de aula online através do compartilhamento de links e dados de acesso.

Os estudos de [Singh and Naveenkumar 2023] e [Li et al. 2023] apontam que as vulnerabilidades relacionadas a falhas humanas estão fortemente ligadas a credenciais comprometidas, credenciais fracas ou com padrões, rede mal estruturada, configurações de segurança erradas, comprometimento com terceiros, nuvem mal configurada.

Os artigos de [Canham et al. 2021] e de [Althobaiti 2021] demonstram que os fatores de como os usuários reagem ao receber um ataque de phishing. mostrando que é necessário que funcionários, alunos e professores necessitam ter um treinamento voltado para esses casos, atribuindo uma maneira correta para que eles reajam da melhor maneira possível em possíveis golpes de violação de dados sensíveis.

O artigo de [Yusif and Hafeez-Baig 2023] aponta que os aspectos técnicos da cibersegurança não são uma panaceia completa para garantir a segurança dos ativos de sistemas de informação e prevenir ciberataques. As restantes questões de segurança cibernética dependem de fatores humanos no contexto da conformidade.

A análise dos artigos referenciados demonstra que os fatores humanos desempenham um papel crucial nas falhas de segurança cibernética nos ambientes educacionais. Durante a revisão dos artigos foram definidas as fragilidades humanas mais recorrentes nas falhas de segurança.

A engenharia social é uma falha de grande ameaça por explorar especificamente a fragilidade e falha humana para obter o acesso aos dados sensíveis. A falta de conhecimento sobre a engenharia social é um fator agravante, e por isso torna-se necessário aumentar a consciência sobre esse aspecto de um modo geral.

Em ademais, a falta de conhecimentos básicos em segurança cibernética entre professores, alunos e funcionários contribuem de maneira direta para criação de novas vulnerabilidades, tais como as fugas de dados e a pirataria informática nos ambientes virtuais de educação, isso acaba destacando ainda mais a necessidade da criação de programas de educação nas áreas de cibersegurança.

O uso de configurações julgadas como inadequadas e credenciais comprometidas também foram identificadas como algumas das principais causas de vulnerabilidades nesse meio. Erros na configuração de redes, credenciais com baixa qualidade de segurança ou até comprometidas junto a controles inadequados acabam por fomentar o risco iminente de exploração das falhas por invasores. Isso, junto a forma como os usuários e utilizadores reagem frente a ataques de phishing tem um grande impacto diretamente na segurança cibernética.

O estudo sugere que para uma melhor eficiência da segurança nos meios educacionais, torna-se necessário cursos e treinamentos para os usuários reconhecerem esses ataques e responderem adequadamente a eles.

### 4.7. Quais medidas podem ser tomadas pelas instituições de ensino para lidar com o problema em questão?

Para [Liu et al. 2020], as instituições de ensino devem implementar uma governança centralizada de TI. Isso pode ajudar no estabelecimento de políticas de controle uniformes e de segurança em toda a organização, melhorando o alinhamento estratégico e a responsabilização. Promover a conformidade universal com protocolos de segurança, facilita a implementação e o cumprimento desses protocolos em toda instituição.

Os autores do estudo [Abdulla et al. 2023] sugerem que as instituições acadêmicas forneçam workshops de conscientização sobre engenharia social e ferramentas de segurança e forneçam também pacotes de antivírus para seus estudantes e funcionários. Além disso, contratar profissionais adicionais de segurança cibernética para cada departamento da universidade também ajudaria a combater as ameaças mais facilmente, sem sobrecarregar o departamento de TI.

É necessário que as instituições de ensino invistam na educação dos alunos sobre segurança cibernética, especialmente em áreas como proteção de redes com firewall, políticas de senha forte e controle de mídia removível, além de sugestões para investimentos em hardware e software para proteger redes e firewalls[Basha et al. 2022].

O estudo [Mykola et al. 2020] discute a implementação de um modelo que utiliza inteligência artificial e planejamento estratégico para auxiliar na tomada de decisões em cibersegurança, sem detalhar outras medidas preventivas ou de resolução de problemas. É importante mencionar o uso de ferramentas de varredura e avaliação de vulnerabilidades, análise dos resultados para identificar vulnerabilidades e priorização da remediação com base nas varreduras e análises[Chhillar and Shrivastava 2021].

No estudo [Christopher et al. 2019], é destacado a importância de implementar controles técnicos de segurança e documentação de processos e auditorias para garantir uma computação segura em clusters HPC ou máquinas virtuais em nuvem. [Fouad 2022] sugere medidas como intervenção estatal no processo de aquisição de tecnologia educacional para garantir a segurança cibernética e a implementação de padrões de segurança por parte dos fornecedores de tecnologia educacional.

No artigo [Singh and Naveenkumar 2023], é proposto medidas como design de infraestrutura segura, pesquisa de vulnerabilidades, minimização de dados e redesenho do sistema considerando falhas de segurança. Destacar a importância da conscientização sobre riscos de segurança e controles para melhorias no desenvolvimento de controle e desempenho em segurança da informação[Yusif and Hafeez-Baig 2023].

Por fim, o artigo [Canham et al. 2021] propoe medidas preventivas e corretivas baseadas no padrão de comportamento identificado nos funcionários, alocação de recursos de segurança com base nas fraquezas e forças relativas, programas de conscientização em segurança cibernética, além de treinamento em segurança da informação[Li et al. 2023].

Esses estudos fornecem uma visão abrangente das medidas necessárias para fortalecer a segurança cibernética nas instituições acadêmicas, destacando a importância da educação, investimento em tecnologia e implementação de políticas e práticas de segurança eficazes.

### 4.8. Discussões a respeito das publicações

Neste estudo, exploramos as falhas e vulnerabilidades de segurança cibernética nas instituições educacionais. As falhas internas, incluindo configurações inadequadas de rede, criptografia e autenticação, bem como a exposição de dados desnecessários, são fatores significativos que expõem as instituições a ataques externos. Além disso, a falta de conscientização e treinamento adequado entre alunos e funcionários é uma preocupação proeminente.

As motivações por trás dos ataques cibernéticos às instituições educacionais são diversas e multifacetadas. Entre elas, destaca-se o potencial de acesso a informações sensíveis, incluindo dados pessoais, financeiros e de pesquisa. Além disso, a crescente adoção de ensino a distância durante a pandemia da COVID-19 aumentou a exposição das instituições a ataques cibernéticos devido à dependência de ambientes virtuais para atividades educacionais.

Os métodos de vazamento de dados identificados pelos estudos incluem uma variedade de ataques cibernéticos, como phishing, ransomware, malware e exploração de vulnerabilidades. Esses métodos destacam a importância de medidas preventivas robustas, incluindo conscientização sobre segurança cibernética e implementação de práticas de autenticação seguras.

Os fatores humanos desempenham um papel significativo nas falhas de segurança cibernética nas instituições educacionais. As vulnerabilidades decorrentes de erros humanos, como falhas de criptografia, design inseguro e falta de autenticação adequada, destacam a necessidade de educação contínua e treinamento em segurança cibernética para alunos e funcionários.

Em conclusão, esta revisão sistemática destaca a importância crítica da segurança

cibernética nas instituições educacionais, especialmente diante do crescente ambiente digital impulsionado pela pandemia da COVID-19. As descobertas destacam a necessidade de medidas proativas para abordar as vulnerabilidades identificadas e garantir a proteção dos dados e sistemas das instituições contra ameaças cibernéticas.

## 5. Ameaças à validade

O assunto escolhido para este trabalho se mostrou ainda pouco discutido, já que menos da metade dos artigos retornados tinham ligação com o tema proposto; além disso, a maioria dos artigos estudados tinham muitas limitações na pesquisa, tornando as informações deles tiradas mais restritas àquele ambiente estudado.

## 6. Considerações Finais

Esta pesquisa realizou uma revisão sistemática da literatura, a fim de estudar falhas de cibersegurança no setor educacional, buscando identificar os ocorridos mais frequentes nesse âmbito e como eles ocorrem, bem como investigar as causas e os fatores que levam a ocorrer invasões e roubos de dados neste ambiente e, por fim, identificar as medidas e intervenções que podem ser realizadas nas instituições para resolver o problema.

Para isso, foram estudados diversos trabalhos relacionados ao tema para que se pudesse tirar informações para responder às 5 perguntas de pesquisa e, dessa forma, entender o cenário atual do tema proposto.

Em nossa metodologia, definimos as palavras chaves para fazer uma string de busca para fazer a pesquisa nas bases escolhidas. Em seguida, exportou-se os artigos retornados para a plataforma Parsifal, onde fez-se a seleção dos artigos utilizando métodos de inclusão e exclusão e, após isso, realizou-se a extração de dados por meio da leitura dos artigos selecionados.

Por ser um tema ainda pouco estudado, havia poucos trabalhos disponíveis para a realização da pesquisa e, ainda, os estudos selecionados era maioritariamente limitados em sua pesquisa também.

Apesar dessas limitações, informações importantes foram coletadas nesta pesquisa, que poderá servir de base para futuros trabalhos sobre o tema.

## Contribuição dos autores:

- Marcelo Santos da Cruz: Pesquisa, correções e escrita do manuscrito;
- Júlia Rocha Valverde: Pesquisa, correções e escrita do manuscrito;
- Filippi Reis Menezes: Pesquisa, correções e escrita do manuscrito;
- Luiz Felipe Oliveira Carregosa: Pesquisa, correções e escrita do manuscrito;
- Jordan Santos de Jesus: Pesquisa, correções e escrita do manuscrito;
- Gilton José Ferreira da Silva: Coordenação do trabalho, correções e direcionamentos da pesquisa.

## Referências

[Abdulla et al. 2023] Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., and Rashid, T. A. (2023). Analysis of social engineering awareness among students and lecturers. *IEEE Access*.

[Airehrour et al. 2018] Airehrour, D., Vasudevan Nair, N., and Madanian, S. (2018). Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model. *Information*, 9(5):110.

[Aliyu et al. 2020] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., and Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the united kingdom. *Applied Sciences*, 10(10):3660.

[Althobaiti 2021] Althobaiti, M. M. (2021). Assessing user's susceptibility and awareness of cybersecurity threats. *Intelligent Automation & Soft Computing*, 28(1).

[Alzahrani 2020] Alzahrani, A. (2020). Coronavirus social engineering attacks: Issues and recommendations. *International Journal of Advanced Computer Science and Applications*, 11(5).

[Aman Gupta 2017] Aman Gupta, A. A. (2017). Ethical hacking and hacking attacks. *International Journal Of Engineering And Computer Science*, 6(4):21042–21050.

[Anwar et al. 2017] Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69:437–443.

[Arachchilage et al. 2013] Arachchilage, N. A. G., Namiluko, C., and Martin, A. (2013). A taxonomy for securely sharing information among others in a trust domain. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pages 296–304. IEEE.

[Basha et al. 2022] Basha, M. S. A., Christina, S., Devi, A. U., Sucharitha, M. M., and Maheshwari, A. (2022). A study on student cyber safety consciousness in the light of online learning. In *2022 IEEE 19th India Council International Conference (INDICON)*, pages 1–6. IEEE.

[Breda et al. 2017] Breda, F., Barbosa, H., and Morais, T. (2017). Social engineering and cyber security. In *INTED2017 Proceedings*, pages 4204–4211. IATED.

[Broadhurst et al. 2018] Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., and Ipsen, Y. (2018). Phishing and cybercrime risks in a university student community. *Available at SSRN 3176319*.

[Canham et al. 2021] Canham, M., Posey, C., Strickland, D., and Constantino, M. (2021). Phishing for long tails: Examining organizational repeat clickers and protective stewards. *SAGE Open*, 11(1):2158244021990656.

[Chhillar and Shrivastava 2021] Chhillar, K. and Shrivastava, S. (2021). Vulnerability scanning and management of university computer network. In *2021 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON)*, pages 01–06. IEEE.

[Christopher et al. 2019] Christopher, J., Jung, G., and Doane, C. (2019). Making it more secure: The technical and social challenges of expanding the functionality of an existing hpc cluster to meet university and federal data security requirements. In *Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning)*, pages 1–5.

[Conteh and Schmick 2021] Conteh, N. Y. and Schmick, P. J. (2021). Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In *Ethical hacking techniques and countermeasures for cybercrime prevention*, pages 19–31. IGI Global.

[DJEKI et al. 2021] DJEKI, E., DEGILA, J., BONDIOMBOUY, C., and ALHASSAN, M. H. (2021). Security issues in digital learning spaces. In *2021 IEEE International Conference on Computing (ICOCO)*, pages 71–77. IEEE.

[Fischer 2014] Fischer, E. A. (2014). Cybersecurity issues and challenges: In brief.

[Fouad 2022] Fouad, N. S. (2022). The security economics of edtech: vendors' responsibility and the cybersecurity challenge in the education sector. *Digital Policy, Regulation and Governance*, 24(3):259–273.

[Furnell et al. 2006] Furnell, S. M., Jusoh, A., and Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1):27–35.

[Gearhart et al. 2019] Gearhart, G. D., Abbiatti, M. D., and Miller, M. T. (2019). Higher education's cyber security: Leadership issues, challenges and the future. *International Journal on New Trends in Education and Their Implications*, 10(2):11–18.

[Li et al. 2023] Li, J., Xiao, W., and Zhang, C. (2023). Data security crisis in universities: identification of key factors affecting data breach incidents. *Humanities and Social Sciences Communications*, 10(1):1–18.

[Liu et al. 2020] Liu, C.-W., Huang, P., and Lucas Jr, H. C. (2020). Centralized it decision making and cybersecurity breaches: Evidence from us higher education institutions. *Journal of Management Information Systems*, 37(3):758–787.

[Mykola et al. 2020] Mykola, T., Svitlana, T., Andrii, Y., Oleksandr, T., Kateryna, K., and Mykola, K. (2020). Protection of information in assessing the factors of influence. In *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, pages 285–289. IEEE.

[Rubens 2014] Rubens, P. (2014). Anti-malware software can't spot all malicious code. is isolating end-user tasks through virtualization a better approach to security?

[Shaw et al. 2009] Shaw, R. S., Chen, C. C., Harris, A. L., and Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1):92–100.

[Singh and Naveenkumar 2023] Singh, R. G. and Naveenkumar, D. (2023). Are we undermining data breaches? protecting education sector from data breaches. In *2023 International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3)*, pages 1–6. IEEE.

[Wang et al. 2020] Wang, Z., Sun, L., and Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access*, 8:85094–85115.

[Yusif and Hafeez-Baig 2023] Yusif, S. and Hafeez-Baig, A. (2023). Cybersecurity policy compliance in higher education: a theoretical framework. *Journal of Applied Security Research*, 18(2):267–288.

[Zwilling et al. 2022] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., and Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1):82–97.