DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Detecção de Malware em Instituições de Ensino Superior: Uma Revisão Bibliográfica Sistemática das Ameaças de Phishing, Ransomware e DDoS

Carlos Eduardo da Cunha Silva

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Detecção de Malware em Instituições de Ensino Superior: Uma Revisão Bibliográfica Sistemática das Ameaças de Phishing, Ransomware e DDoS

Carlos Eduardo da Cunha Silva

Orientador: Prof. Dr. Daniel Chaves Café, FT/UnB

PUBLICAÇÃO: PPEE.MP.112

BRASÍLIA-DF ABRIL/2026

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Detecção de Malware em Instituições de Ensino Superior: Uma Revisão Bibliográfica Sistemática das Ameaças de Phishing, Ransomware e DDoS

Carlos Eduardo da Cunha Silva

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. Daniel Chaves Café, FT/UnB *Orientador*	_____
Prof. Dr. Carlos Alberto da Silva, UFMS *Examinador Externo*	_____
Prof. Dr. João Souza Neto, FT/UnB *Examinador interno*	_____
Prof. Dr. Vinícius Pereira Gonçalves, FT/UnB *Suplente*	_____

FICHA CATALOGRÁFICA

SILVA, CARLOS EDUARDO DA CUNHA

DETECÇÃO DE MALWARE EM INSTITUIÇÕES DE ENSINO SUPERIOR: UMA REVISÃO BIBLIOGRÁFICA SISTEMÁTICA DAS AMEAÇAS DE PHISHING, RANSOMWARE E DDOS [Distrito Federal] 2026.

xii, 106 p, 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2026).

Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Phishing
2. Ransomware
3. Ataques de DDoS
4. Malware
5. Instituições de Ensino Superior
6. Detecção

I. ENE/FT/UnB

II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

SILVA, C. E. C. DETECÇÃO DE MALWARE EM INSTITUIÇÕES DE ENSINO SUPERIOR: UMA REVISÃO BIBLIOGRÁFICA SISTEMÁTICA DAS AMEAÇAS DE PHISHING, RANSOMWARE E DDOS. Dissertação de Mestrado Profissional, Publicação: PPEE.MP.112 Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 106 p.

CESSÃO DE DIREITOS

AUTOR: Carlos Eduardo da Cunha Silva.

TÍTULO: DETECÇÃO DE MALWARE EM INSTITUIÇÕES DE ENSINO SUPERIOR: UMA REVISÃO BIBLIOGRÁFICA SISTEMÁTICA DAS AMEAÇAS DE PHISHING, RANSOMWARE E DDOS.

GRAU: Mestre em Engenharia Elétrica ANO: 2026

_____

Carlos Eduardo da Cunha Silva

Depto. de Engenharia Elétrica (ENE) - FT

Universidade de Brasília (UnB)

Campus Darcy Ribeiro

CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho, primeiramente à Deus, à minha família, em especial à minha esposa, Gleiciane, aos meus filhos, à minha mãe, Maria Inês, as minhas irmães Paulinha e Pri e ao meu pai, Gilberto (*in memoriam*), cuja memória, ensinamentos e exemplo permanecem como fonte constante de inspiração.

Dedico também à equipe PRC / DIMEQ / da Universidade de Brasília (UnB), pelo apoio institucional, pelo trabalho em conjunto e pela confiança depositada em mim ao longo desta trajetória. Registro meu agradecimento em especial ao Diretor da DIMEQ, Humberto Barbosa, — que me apoiou 100% nesta caminhada — a atual Prefeita, Danielle, pelo incentivo e apoio concedidos e o ex-Prefeito Valdeci que ajudou e proporciono a liberação para estudo.

Estendo esta dedicação aos amigos da Seção Técnica da DIMEQ Antônio Ederson — amigo que me acompanha desde a nomeação do concurso da FUB, Isaias, Vidigal Barbosa — amigo também de caminhada na FUB — , Wanderson, Damião, Ednei — cuja colaboração foi fundamental no desenvolvimento do artigo científico publicado —, Fernando, Bruno, Geraldo, João Victor, Hugo, Igor, Jorge, José Pereira, Seu Anis, Giovani, Seu Antônio Ribeiro, Antônio Mendes (*in memoriam*), Senhor e Mestre Adão, Renato, Diogo, Diego, Edvan, Eduardo, Filipe, Roniere, Ronei, Tauan Cunha, Ana, Gisele, Odara, Thamires, Bruno, Henrique (Baia), Elias, Roberto, Ricardo, bem como aos demais colegas que, de forma direta ou indireta, contribuíram para esta caminhada.

Dedico igualmente aos amigos do curso, em especial Luís Marcos, Ednei Coelho, João Goulart (Jango), Neto e Leonardo, o primeiro do Centro de Ensino a Distância (CEAD), em sequência DIMEQ/Transporte; Dep° de Segurança e outros dois da Faculdade de Tecnologia (FT), e aos demais amigos e professores do programa, pelo compartilhamento de conhecimentos. Aos amigos da graduação de Engenharia Elétrica da FACNET que ainda seguem juntos em especial, Sebastião, João Paulo, Edson (Zé de Brito), Davi, Wesley Junior, Josélia, Diego, Jamir, Anderson, Cristiano, Rodrigo, Eneias, Edinaldo, Luandson, Serjão, Otávio, Pedro, Sóstenys, Windson e os demais amigos que não citei, mas estão presentes em minha jornada.

Por fim, dedico este trabalho aos meus amigos e professores da graduação e pós, Dr° Prof. Francisco de Assis da Silva Ferreira, Dr° Prof. Flavio Ferreira Lima, MsC Brito, Prof. Flávio Nery, Prof. Valdone, e de pós-graduação Professora Dalila Rocha, Dr° Celson, MsC Marcel Anderson, MsC Raylton Carvalho, Dr° Prof. Ten. Cel. CBMDF Professor Rodrigo Almeida, Professor Gilson, Professor Fernando Barbosa, que foram fundamentais na construção da base acadêmica e profissional.

AGRADECIMENTOS

A Deus, nosso pai espiritual, primeiramente, e a toda a minha família – mãe, esposa, filhos, pais e amigos expresso o mais profundo agradecimento pelo carinho, tivemos algumas perdas importantes na família, mas fomos muito bem confortados.

Agradeço também a Direção e à Prefeitura do Campus pela liberação necessária para que eu pudesse me dedicar aos estudos e ao desenvolvimento deste mestrado. Registro também meu sincero reconhecimento aos amigos da DIMEQ, CEAD, FT e STI pelo constante apoio, incentivo e parceria ao longo do percurso acadêmico. Estendo meus agradecimentos aos professores, coordenadores de curso pelos deferimentos de solicitações, equipe de atendimento da secretaria acadêmica PPEE em especial Tayná Gabriela, Ludmila e Julia que sem descanso auxilia nos Discentes com um suporte profissional ético e atencioso.

Manifesto meu agradecimento ao Dr°. Prof. Daniel Chaves Café, pela orientação, atenção, paciência, dedicação e elevado profissionalismo. Sua condução possibilitou transformar um projeto embrionário em um trabalho possível e materializado. A trajetória não foi fácil e nem simples, mas, com empenho e perseverança, concluo este curso com a experiência e a formação de um Docente.

Agradeço igualmente ao Dr°. Prof. João Souza Neto, pela co-orientação e pelos ensinamentos que ultrapassaram o conteúdo técnico ministrado, mostrando que, por meio do estudo contínuo, persistência, resiliência, aperfeiçoamento e trabalho árduo, é possível alcançar destaque e excelência profissional.

Registro ainda meus agradecimentos aos professores Dr°. William Ferreira Giozza e Dr°. Luiz Antônio Ribeiro Junior, cujas contribuições foram fundamentais na disciplina de Metodologia e Pesquisa Científica; à Dra. Edna Dias Canedo, que demonstrou aos discentes a relevância dos fatores humanos na Segurança Cibernética, evidenciando que estes não devem ser negligenciados; ao Dr°. Georges Daniel Amvame Nze, pelos ensinamentos relacionados aos riscos de ataques em redes; e, novamente, ao Dr°. Daniel Chaves Café, na condição de professor da disciplina de Estudo Orientado e Internet das Coisas (IoT), pela valiosa contribuição acadêmica.

Por fim, agradeço o apoio de ferramentas de inteligência artificial, como CHATGPT E COPILOT, utilizadas de forma complementar para aprimorar a redação e a estrutura textual deste trabalho, sem qualquer substituição da autoria intelectual, mantendo-se a responsabilidade integral do autor sobre o conteúdo descrito e apresentado.

“ 90% do sucesso se baseia simplesmente em insistir!!!”

(Woody Allen)

“ Querer vencer significa já ter percorrido a metade do caminho!!!”

(Ignacy Paderewski)

“ Pequenas oportunidades podem ser o começo de grandes oportunidades!!!”

(Demostenes)

“ No mundo dos negócios todos são pagos em duas moedas: dinheiro e experiência. Agarre a experiência que o dinheiro virá depois!!!”

(Harold Genev)

“ Escolher cada batalha que vale apena lutar... O resto é café e vinho!!!”

(Francisco Ferreira)

RESUMO

Nos últimos anos, as instituições de ensino superior se tornou alvo frequente de ataques cibernéticos, comprometendo a confiabilidade, integridade e a disponibilidade de dados acadêmicos, administrativos e científicos. A complexidade dos ambientes universitários, marcada pela diversidade de usuários, dispositivos conectados e sistemas heterogêneos, amplia significativamente a superfície de ataque e exploração de vulnerabilidade pelos agentes criminosos.

Para integrar e consolidar os resultados metodológicos encontrados na literatura, adotou-se a Teoria do Enfoque Meta-Analítico Consolidado (TEMAC) como ferramenta de apoio à revisão sistemática. As buscas foram realizadas nas bases *Web of Science* e *IEEE Xplore*, abrangendo publicações entre 2021 e 2025, utilizando como palavras-chave *phishing*, *ransomware*, ataques DDoS, *malware,* instituições de ensino superior e detecção. Inicialmente, foram coletados 400 artigos na *Web of Science* e 355 na *IEEE Xplore*, totalizando 755 registros. Após o processo de concatenação e remoção de duplicidades, 49 artigos foram excluídos, resultando em 706 trabalhos considerados relevantes para análise.

O estudo destacou cinco artigos com maior impacto em citações e outros sete que apresentaram soluções técnicas aplicáveis à mitigação de ataques cibernéticos em ambientes universitários, totalizando 55 referências essenciais para a fundamentação teórica e metodológica do trabalho. Os resultados reforçam a necessidade de adoção de modelos de segurança mais robustos e adaptativos, capazes de responder à natureza multifacetada das ameaças digitais nas instituições de ensino superior.

Palavras-chave: phishing, ransomware, ataques ddos, malware, instituições de ensino superior e detecção.

ABSTRACT

In recent years, higher education institutions have become frequent targets of cyber attacks, compromising the reliability, integrity, and availability of academic, administrative, and scientific data. The complexity of university environments, marked by the diversity of users, connected devices, and heterogeneous systems, significantly increases the surface area for attack and exploitation of vulnerabilities by criminal agents.

To integrate and consolidate the methodological results found in the literature, the Consolidated Meta-Analytic Approach Theory (TEMAC) was adopted as a tool to support the systematic review. Searches were conducted in the Web of Science and IEEE Xplore databases, covering publications between 2021 and 2025, using the keywords phishing, ransomware, DDoS attacks, malware, higher education institutions, and detection. Initially, 400 articles were collected from Web of Science and 355 from IEEE Xplore, totaling 755 records. After the process of concatenation and removal of duplicates, 49 articles were excluded, resulting in 706 works considered relevant for analysis.

The study highlighted five articles with the greatest impact in citations and seven others that presented technical solutions applicable to the mitigation of cyber attacks in university environments, totaling 55 essential references for the theoretical and methodological foundation of the work. The results reinforce the need to adopt more robust and adaptive security models capable of responding to the multifaceted nature of digital threats in higher education institutions.

Keywords: phishing, ransomware, ddos attacks, malware, higher education institutions and detection.

Sumário

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Agência Nacional de Proteção de Dados
CEAD/UnB	Centro de Educação a Distância da da Universidade de Brasília
COVID-19	Coronavirus Disease 2019
CSF	Cybersecurity Framework
CSV	Comma-Separated Values
DIMEQ	Diretoria de Manutenção de Equipamentos
DGP	Decanato de Gestão de Pessoas
DoS	Denial of Service
DDoS	Distributed Denial of Service
EaD	Ensino a Distância
EDR	Endpoint Detection and Response
FUB	Fundação Universidade de Brasília
FT	Faculdade de Tecnologia
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Inteligência Artificial
IEC	International Electrotechnical Commission
IES	Instituição de Ensino Superior
IEEE	Institute of Electrical and Electronics Engineers
INEP	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
IoT	Internet das Coisas
IP	Internet Protocol
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
WoS	Web of Scinece
SGD	Secretaria de Governo Digital
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
NIST	National Institute of Standards and Technology
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SQL	Structured Query Language
PRP01	Palton's Robot in Python
PPSI	Programa de Privacidade e Segurança da Informação
TEMAC	Teoria do Enfoque Meta-Analítico Consolidado

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

1 – INTRODUÇÃO

As instituições de ensino superior estão enfrentando desafios crescentes e raros em relação à segurança cibernética, tornando-se alvos chaves de ataques devido à grande quantidade de metadados armazenados em seus bancos de dados institucionais. Esses ambientes acadêmicos além de produzirem conteúdos científicos apresentam em seu teor dados pessoais como CPF, e-mails, credenciais de acesso e resultados de trabalhos acadêmicos ainda não publicados.

Com a transformação do ambiente acadêmico e ampliação significativa das dependências das Instituições de Ensino Superior (IES) em relação a tecnologia da informação, cresce exponencialmente o quantitativo de metadados a serem guardados e monitorados. Os maiores consumidores de espaços são os sistemas acadêmicos, plataformas de ensino a distância EaD e base de dados administrativos que também concentram um volume expressivo de informações, incluindo dados pessoais, dados sensíveis e ativos intelectuais e de pesquisas. Elas vêm enfrentando desafios a cada dia mais complexos no campo da segurança cibernética.

Os ataques direcionados aos sistemas das Instituições de Ensino Superior (IES) constituem um dos principais vetores que impulsionam a atuação de cibercriminosos, especialmente no que se refere à obtenção e comercialização de dados pessoais sensíveis. Essas informações, quando comprometidas, passam a ter alto valor no mercado ilícito, incentivando ainda mais a ocorrência de invasões e violações de segurança.

O *Moodle* é um sistema de Gestão de Aprendizagem, ou seja, uma plataforma on-line que proporciona em seu ambiente aulas virtuais e interação dos discente aos docentes através de tarefas e avaliações. Ele armazena dados sensíveis como conteúdo, identificações de alunos, professores e credenciais corporativas. Como é um sistema que armazena metadados sensíveis e de cunho científico e pessoal a segurança automatizada dos dados e de suma relevância. (Nascimento *et al*, 2025)

Segundo Nascimento (2025), a automatização de um sistema robusto como do *Moodle* é necessário para que não ocorra incidências de falhas humanas, retrabalho e vulnerabilidades a scripts maliciosos. O desenvolvimento do PRP01 (*Palton's Robot in Python*) foi programado para integrar o *Moodle* com os sistemas institucionais SIGAA e SIGER através da web *scraping* e autenticação segura.

Em virtude do amplo volume de metadados gerados pelas instituições de ensino, o interesse dos invasores tem se intensificado, já que essas informações incluem pesquisas valiosas e dados

confidenciais de valores inestimáveis.

Segundo Ulver e Wanger (2021), as instituições geram um quantitativo substancial de dados importantes, o que fomenta e deixa atrativo aos cibercriminosos (atacantes). O mercado ilegal financia esses crimes com valores expressivos para obter os dados pessoais e resultados de pesquisas, estimulando ainda mais o fluxo de ataques.

Não é suficiente reduzir de forma significativa os ataques e as práticas de ciberespionagem no atual contexto tecnológico; é igualmente indispensável compreender, de maneira aprofundada, os vetores de ataque, bem como os fatores culturais envolvidos, os quais devem ser devidamente identificados, analisados e amplamente debatidos.

Para reduzir essas ameaças de forma eficaz, é essencial adotar medidas preventivas voltadas ao monitoramento contínuo das tentativas de intrusão, bem como à identificação dos principais tipos de vulnerabilidades e riscos que afetam esses ambientes acadêmicos. (Ulver e Wanger, 2021)

Os estudos recentes investigaram os principais tipos de ameaças digitais enfrentadas pelas universidades, revelando vulnerabilidades críticas em seus sistemas. Entre as ameaças mais recorrentes destacam-se o phishing e a engenharia social reversa, considerados vetores predominantes de invasões externas.

O *ransomware* e ataques envolvendo SQL também se mostram particularmente preocupantes, pois a primeira causa paralisações operacionais e danos aos sistemas, enquanto o segundo injeta códigos maliciosos para obter acesso ilegal a dados confidenciais (Pillay e Sharma, 2023).

De acordo com Pillay e Sharma (2023), ataques envolvendo *phishing, ransomware* e SQL têm preocupado especialistas, que observam um crescimento significativo dessas ocorrências em universidades públicas e privadas, impulsionado pelo valor estratégico do conteúdo armazenado.

Desta forma, a implementação de políticas de segurança da informação como planos de resposta a incidentes, controles de acesso, mecanismos de monitoramento contínuo e programas de conscientização dos usuários torna-se essencial para a mitigar os riscos cibernéticos e garantir a conformidade regulatória. A segurança da informação, aliada à adequação da LGPD, deixa de ser apenas um requisito tecnológico e passa a configurar um elemento estratégico de gestão institucional das IES.

Pillay e Sharma (2023, p. 2) acrescentam um fator importante que,

> [...] visar reitores de universidades ou membros acadêmicos específicos é uma tática alternativa. Essas pessoas podem ter acesso a determinados conjuntos de dados que interessam aos hackers, ou podem simplesmente ser pessoas abastadas. Para escolher a melhor estratégia para ganhara confiança da pessoa-alvo, o hacker examinará o seu comportamento. Essa tática também é conhecida como "*whaling" ou "spear phishing*".

Com isso, torna-se evidente a necessidade de melhoria contínua principalmente no que tange as políticas e práticas de segurança cibernética no ambiente de ensino superior. Aimplementação de medidas robustas, como atualizações regulares de software, protocolos avançados de autenticação e ações permanentes de conscientização dos usuários, é essencial para mitigar riscos e assegurar a continuidade das atividades educacionais e administrativas.

A mitigação desses riscos ligados exige a adoção de uma abordagem estruturada da gestão, alinhada às diretrizes da norma elaborada pela *International Organization for Standardization (ISO) e pela International Electrotechnical Commission (IEC)* que se baseia nos três pilares da segurança da informação conhecido como Tríade CIA (Confiabilidade, Integridade e Disponibilidade) em relação a gestão da segurança das informações.

Em seu escopo traduz a importância dos requisitos da implementação, a manutenção e melhoria contínua do sistema no contexto de uma organização pública ou privada. (ISO/IEC 27001,2022)

Entre as principais medidas destacam-se a segmentação de redes, o controle rigoroso de acessos com autentificação multifator Autenticação Múltiplo Fator (MFA), a gestão contínua de vulnerabilidades de correções de segurança, bem como a criptografia de dados em repouso e em transito.

A implementação de políticas técnicas relacionadas a backup e de recuperação de dados consumidos por algum ataque cibernético configura-se como um pilar estratégico para a garantia da disponibilidade da informação no ambiente institucional. Sob uma perspectiva contemporânea, tais mecanismos não apenas asseguram a continuidade operacional, como também contribuem de forma significativa para a mitigação de riscos, ao reduzir a superfície de ataque e fortalecer a resiliência cibernética dos sistemas das IES. (Cheng e Wang, 2022)

Embora as técnicas de endurecimento dos ambientes tecnológicos (*security hardening*) e automação da segurança desempenham um papel fundamental com o objetivo de prevenir e dificultar as ações dos criminosos digitais. Entretanto a aplicação de princípios como *least privilegie, zero trust,* monitoramento contínuo por meio de *Security Information and Event*

Managemetm (SIEM), o uso de *Endpoint Detection and Response* (EDR) e *Security Orchestration Automation and Response* (SOAR) contribuem para a detecção precoce de atividades suspeitas e resposta rápidas aos incidentes.

Em paralelo a isto, ações de capacitação e conscientização dos usuários, aliados à uma boa governança de dados em conformidade com a norma (ISO/IEC 27701,2022) com orientações da Autoridade Nacional de Proteção de Dados (ANPD), fortalecem a cultura de segurança e privacidade, tornando o ambiente mais robusto, resiliente e com número reduzido a incidências de ataques cibernéticas.

Apesar das vantagens agregadas a esta norma, os desafios da transição são exponenciais principalmente em relação a complexidades jurídicas e visões multidisciplinares, integração com sistemas existentes, mudança cultural e mentalidade e mapeamento identificando onde e como os dados são tratados. (ISO/IEC 27701,2025)

Visto isso, torna-se evidente a necessidade de melhoria contínua principalmente no que tange as políticas e práticas de segurança cibernética no ambiente de ensino superior. A implementação de medidas robustas, como atualizações regulares de software, protocolos avançados de autenticação e ações permanentes de conscientização dos usuários, é essencial para mitigar riscos e assegurar a continuidade das atividades educacionais e administrativas.

O estudo proposto concentra-se nos ataques cibernéticos direcionados às instituições de ensino superior, como ambientes com demandas operacionais, fluxos intensos de informações relativas a área institucional acadêmica e pessoal e a complexidade dos sistemas utilizados. Esses fatores agregados à intensa iteração manual dos usuários internos e externos – incluindo discentes, docentes, técnicos administrativos e prestadores de serviços – ampliam significativamente a exposição e as ameaças digitais.

Neste contexto, a segurança cibernética torna-se elemento estratégico para a proteção dos ativos digitais da academia e integridade dos dados sensíveis. As intrusões ocorridas nas IES estão ligadas as seguintes premissas: sistemas desatualizados, credenciamentos comprometidos, dispositivos pessoais conectados a redes institucionais e a engenharia social reversa.

Em suma, a diversidade de perfis de usuários e a descentralização do acesso aos sistemas tornam as instituições de nível superior alvos atrativos para cibercriminosos, fomentando a estes órgãos políticas robustas de governança digital, monitoramento contínuos e capacitação permanente dos usuários.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

Com o avanço acelerado da digitalização nas instituições de ensino superior o uso da tecnologia computacional ampliou de forma exponencial a dependência de sistemas informatizados para a gestão acadêmica, administrativa e científica, produtos estes, que geram expressivos dados sensíveis e ativos intelectuais de alto valor estratégico. As plataformas de ensino a distância (EaD), sistemas acadêmicos institucionais e bases administrativas concentram um apanhado de informações pessoais, pesquisas cientificas, produções acadêmicas, credencias da instituição e usuários, tornando-se alvos prioritários de cibercriminosos.

Além do valor informacional desses ativos, estudos recentes demostram que os principais vetores de ataques às universidades incluem as práticas de intrusão por *phishing*, engenharia social direta e reversa, *ransomware*, injeções de códigos maliciosos e ataques de negação de serviço distribuído.

A ideia dos criminosos virtuais é explorar as falhas humanas, sistemas desatualizados e controles de segurança inadequados, pois eles sabem que existem uma diversidade de perfis de usuários descentralizados dos acessos ao dispositivo das redes das instituições e com isso ampliam de forma significativa os ataques. Dessa forma, as (IES) trabalham em ambientes extremamente complexos, dinâmicos e altamente expostos a riscos cibernéticos (intrusões) que podem comprometer após um ataque a confiabilidade, integridade e disponibilidade das informações.

Outro panorama, justifica-se a realização deste estudo pela necessidade de compreender de forma sistemática os principais vetores de ataque que afetam as instituições de ensino superior, bem como os fatores tecnológicos, organizacionais e humanos que contribuem para a ampliação das vulnerabilidades.

A pesquisa visa verificar e propor ferramentas de segurança digital mais eficazes, estratégias de mitigação de riscos e práticas de governança digital alinhada às exigências legais do marco regulatório em segurança, contribuindo para o fortalecimento da resiliência cibernética das IES e para a proteção dos dados informacionais essências às atividades educacional, cientifica e administrativa.

1.2 DESAFIOS EM SE MANTER A SEGURANÇA E INTEGRIDADE DAS INFORMAÇÕES

Outro desafio relevante está relacionado à heterogeneidade das infraestruturas tecnológicas presentes nas IES, muitas vezes compostas por sistemas legados, plataformas acadêmicas próprias e soluções terceirizadas. A coexistência de tecnologias distintas dificulta a padronização de políticas de segurança e a aplicação uniforme de controles técnicos, como atualizações, correções de vulnerabilidades e monitoramento contínuo. Essa fragmentação tecnológica favorece a exploração de falhas por agentes maliciosos, especialmente em ataques multifacetados que combinam engenharia social, exploração de vulnerabilidades de softwares e comprometimento de credenciais.

Observa-se que com a crescente sofisticação dos ataques cibernéticos impõe-se desafios constantes à detecção e resposta a incidentes as instituições e melhores ferramentas. Malware como *ransomware*, *phishing* direcionados, movimentação lateral dentro das redes e exploração de dispositivos pessoais conectados às infraestruturas institucionais demandam mecanismos avançados de prevenção muita supervisão e treinamento.

Os modelos tradicionais de segurança perimetral mostram-se insuficientes frente a esse cenário, tornando necessária a adoção de abordagens mais modernas, como defesa em profundidade, Zero Trust, segmentação de redes, autenticação multifator e análise comportamental de acessos. (Santos JR. *et al*, 2024)

A implementação de programas contínuos de capacitação, aliados a políticas institucionais claras e ao uso de frameworks de governança em segurança cibernética, torna-se fundamental para mitigar riscos, fortalecer a resiliência dos sistemas e assegurar a confidencialidade, integridade e disponibilidade das informações institucionais.

1.3 DA NECESSIDADE DE AUTOMATIZAR SISTEMAS E MITIGAR AS INTRUSÕES

O avanço acelerado da transformação digital nas Instituições de Ensino Superior – IES aumentou exponencialmente a dependência de sistemas informatizados para execução das atividades acadêmicas, administrativas e científica, proporcionalmente elevando os riscos associados a ameaças cibernéticas.

Com número reduzido de processos de identificação de intrusões de forma automatizada, a segurança digital dos dados torna-se vulnerável e susceptível a incidentes por criminosos tornando o monitoramento lento e insuficiente. Portanto, é de suma importância a implantação

de sistemas automatizados para garantir a operação contínua e a integridade das informações sensíveis.

Para enfrentar esse tipo de ameaça, modelos de segurança modernos, como o Zero Trust, adotam o princípio de não confiar automaticamente em nenhum usuário ou dispositivo, exigindo verificação contínua de identidades e comportamentos, independentemente da origem do acesso. (Rose. *et al*, 2020)

Para proteger os sistemas institucionais e necessário a correlação de eventos de segurança por meio de plataformas (softwares) *Security Information and Event Management* (SIEM) permitem o monitoramento em tempo real das redes e sistemas, integrando logs de múltiplas fontes para detecção precoce de anomalias. (Caminha e Suzuki, 2024)

Outra solução seria a implantação do sistema *Security Orchestration, Automation and Response* (SOAR) que automatiza a resposta a incidentes reais, otimizando o tempo de contenção de ataques e padronizando procedimentos de mitigação. A adoção desses recursos contribui para uma postura de segurança mais proativa, capaz de reagir de forma rápida e estruturada às tentativas de intrusão. (Machado,2024)

Como base normativa e metodológica, os frameworks do *National Institute of Standards and Technology* (NIST) oferecem diretrizes amplamente reconhecidas para gestão de riscos cibernéticos, identificação de ameaças, proteção de ativos, detecção de incidentes, resposta e recuperação. (Gonçalves, *et al*, 2024)

Quando integrados a práticas automatizadas, esses modelos fortalecem a governança da segurança da informação nas (IES), promovendo maior visibilidade dos tipos de ataques, do tempo de exposição às ameaças e da efetividade das soluções implementadas. Dessa forma, a combinação entre automação, autenticação multifator, monitoramento contínuo e frameworks consolidados configura um caminho essencial para enfrentar ataques no ambiente educacional.

1.4 CONFORMIDADE COM A LEGISLAÇÃO E BOAS PRÁTICAS DE SEGURANÇA

Vários fatores justificam a realização desta pesquisa, incluindo a necessidade de implementar políticas estruturadas de segurança da informação que estejam em conformidade com as exigências legais e as melhores práticas internacionais.

No Brasil, a conformidade normativa desempenha um papel crucial na proteção de dados acadêmicos, administrativos e científicos, especialmente considerando a intensa troca de informações pessoais e sensíveis nas Instituições de Ensino Superior (IES). A adoção de

controles técnicos e organizacionais fortalece a prevenção contra intrusões e garante a responsabilidade institucional em relação a incidentes de segurança.

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) define princípios como finalidade, necessidade, segurança e prevenção, exigindo que as organizações adotem medidas eficazes para proteger as informações que manipulam. Para as IES, isso se traduz na implementação de mecanismos como controle de acesso, autenticação multifatorial e monitoramento contínuo e resposta organizada a incidentes, alinhada aos riscos dos ambientes digitais acadêmicos.

O não cumprimento dessas responsabilidades pode resultar em sanções administrativas e impactos operacionais significativos. Além disso, o Decreto nº 10.332/2020 e a Portaria SGD/MGI nº 852/2023 promovem a modernização dos serviços públicos e a gestão de riscos em cibersegurança no nível federal.

Juntas às boas práticas internacionais do NIST, que organizam a segurança em pilares como identificar, proteger, detectar, responder e recuperar, essas diretrizes ajudam a criar ambientes digitais mais resilientes nas Instituições de Ensino Superior (IES). A combinação entre legislação e frameworks técnicos estabelece uma governança eficaz da segurança da informação, capaz de lidar continuamente com ameaças multifacetadas.

1.5 PROBLEMA DE PESQUISA E OBJETIVOS

O expressivo aumento de ataques cibernéticos contra as Instituições de Ensino Superior (IES) proporcionou a busca ao estudo com intuito de combater ameaças digitais. Entretanto, falta informações sobre métodos de proteção e tecnologias aplicadas as intrusões. A maior dificuldade desta pesquisa foi conseguir organizar, analisar e apresentar de modo claro todo o saber já existente sobre como descobrir ameaças online nas universidades.

Pensando nisso, o objetivo maior do nosso estudo é fazer uma análise completa dos trabalhos já divulgados para achar, comparar e juntar as principais formas de identificar phishing, ransomware, ataques DDoS e outros tipos de malware que atingem as IES. Buscamos entender quais táticas são mais usadas, o quanto funcionam e quais tecnologias estão crescendo, montando um guia para ajudar na escolha de segurança online nas instituições.

Para atingir esses objetivos, foi adotada a Teoria do Enfoque Meta-Analítico Consolidado (TEMAC) como forma de guiar nossa análise, pois ela ajuda a organizar vários estudos além de proporcionar resultados de forma sistêmica. As buscas foram feitas nas bases *Web of Science* e *IEEE Xplore*, olhando publicações entre 2021 e 2025, com palavras-chave como *phishing*,

ransomware, ataques DDoS, malware, instituições de ensino superior e detecção, com intuito de proporcionar um material importante aos anais e repositórios acadêmicos.

De início, coletamos 400 artigos na *Web of Science* e 355 na *IEEE Xplore*, juntos ofereceram um produto de 755 registros. Após a unificação dos dados, foram removidos um total de 49 artigos duplicados, restando 706 documentos importantes para serem analisados de forma detalhada. Esse grupo de pesquisas serviu como base a dissertação que sustentou as discussões sobre os desafios, soluções e progressos na segurança cibernética nas IES.

Diante deste cenário, surgiu a seguinte questão relativa a pesquisa: Como realizar uma automação robusta com o quantitativo de metadados em níveis exponenciais, garantindo segurança, integridade e conformidade com orientações da LGPD por meio da integração de bancos de dados institucionais com investimento regular e suficiente?

As demandas geradas não implicam apenas em criar soluções técnicas eficazes, mas também compreender os aspectos organizacionais, tecnológicos e regimentais, que envolvem a automação segura em ambientes acadêmicos.

1.6 HIPÓTESE DE PESQUISA

Parte-se do princípio de que as IES são bem suscetíveis a invasões virtuais, por causa da forma como seus sistemas são montados, da quantidade de usuários internos e externos que os usa e do acesso facilitado a eles. Um dos problemas que costumam fomentar as invasões está relacionada a maturidade normativa e gestão dos sistemas de tecnologia de informação TI.

Além dos pontos já mencionados, instituições de ensino superior estão expostas a um conjunto amplo de vulnerabilidades que podem comprometer a segurança da informação e a continuidade dos serviços. Entre elas, destacam-se:

a) Infraestrutura tecnológica obsoleta, com servidores e equipamentos sem suporte adequado.
b) Ausência de políticas robustas de segurança da informação ou sua aplicação inconsistente.
c) Falta de segmentação de rede, facilitando a propagação de incidentes entre diferentes setores.
d) Controles de acesso inadequados, com privilégios excessivos para usuários e ausência de revisão periódica.
e) Baixo nível de conscientização dos usuários, tornando a comunidade acadêmica mais suscetível a ataques como phishing.
f) Inexistência ou fragilidade de planos de resposta a incidentes e de continuidade de negócios.
g) Backups inexistentes, desatualizados ou não testados regularmente.

h) Uso de softwares não licenciados ou desatualizados, aumentando a exposição a vulnerabilidades conhecidas.
i) Integração insegura entre sistemas acadêmicos, administrativos e plataformas externas.
j) Falta de auditorias e monitoramento contínuo de eventos de segurança.
k) Crescimento desordenado de dispositivos conectados (BYOD), sem controle adequado.
l) Exposição de dados sensíveis de alunos, professores e pesquisas por falhas de configuração.
m) Dependência de fornecedores externos sem avaliação adequada de segurança.
n) Ausência de cultura organizacional voltada à segurança da informação.

Essas fragilidades, quando combinadas, ampliam significativamente o risco de incidentes cibernéticos, exigindo uma abordagem integrada que envolva tecnologia, processos e capacitação contínua dos profissionais.

Isso tudo faz com que invasores encontrem várias formas de ataque, como phishing, ransomware e ataques DDoS. Acredita-se que essa situação tem feito com que se criem muitas formas de achar programas maliciosos, mas isso tem acontecido de maneira separada nos estudos científicos.

O método TEMAC caracteriza-se como uma abordagem de revisão bibliográfica sistemática orientada pela análise de metadados, priorizando a organização e o mapeamento inicial da produção científica. Diferentemente de métodos mais aprofundados, sua aplicação não se concentra na leitura analítica integral dos estudos desde o início do processo.

Sua principal função é promover uma triagem estruturada, com base em critérios objetivos, permitindo identificar padrões, tendências e lacunas na literatura. A etapa de maior aprofundamento ocorre posteriormente, por meio da análise manual dos trabalhos selecionados como maior relevância.

Por fim, destaca-se que a principal contribuição do método TEMAC reside na etapa final de revisão manual, na qual os artigos previamente selecionados são analisados de forma crítica e aprofundada. É nesse momento que se extraem os elementos teóricos, metodológicos e empíricos essenciais para a construção do referencial teórico da dissertação.

1.7 OBJETIVO GERAL

O propósito central deste estudo é efetuar uma análise sistemática das publicações, através da Teoria do Enfoque Meta-Analítico Consolidado (TEMAC), buscando encontrar, examinar e reunir as mais importantes ações, métodos e estruturas de descoberta contra ameaças usados nas Instituições de Ensino Superior, focando nos perigos de *phishing*, *ransomware* e ataques de negação de serviço distribuído (DDoS), para entender direções, áreas sem pesquisa e ajudas importantes para o aumento da segurança cibernética nesses locais.

1.8 OBJETIVOS ESPECÍFICOS

1. Verificar e informar os mecanismos eficazes que detectam e mitiguem os ataques de *malware* advindos do *phishing, ransomware* e DDoS;
2. Descrever critérios de monitoramento, detecção e correção das tentativas de ataques consumados;

1.9 DELIMITAÇÃO DA PESQUISA

A presente pesquisa dedica-se a estudos científicos voltados à segurança digital em Instituições de Ensino Superior. O foco da pesquisa está relacionado a métodos de detecção de malware e as estratégias de enfrentamento de ameaças cibernéticas. Além disso, investiga-se o desafio de disseminar e consolidar uma cultura prevencionista junto aos discentes, docentes, técnicos administrativos e colaboradores externos. Tal dificuldade evidencia a necessidade de abordagens mais eficazes de conscientização e capacitação no ambiente acadêmico.

Outro aspecto importante, que é bastante complicado de lidar, diz respeito às ações que são tomadas quando acontece algum problema de segurança, tanto em tentativas de ataques quanto em ataques que realmente acontecem. Se não houver planos claros para lidar com essas situações, o tempo que as instituições ficam expostas aos ataques pode aumentar, o que pode agravar os problemas e atrapalhar as atividades da escola ou da administração.

Além de parar os ataques, recuperar dados que foram vazados ou comprometidos é um desafio grande para as instituições de ensino, especialmente com ameaças como ransomware e acessos não autorizados a informações sensíveis. O sucesso na recuperação desses dados depende de ter políticas de backup que sejam seguras, realizações de testes regulares para ver se a restauração funciona e integração com sistemas automáticos de resposta, de acordo com orientações de organizações como o NIST e práticas atuais de segurança cibernética.

O trabalho segue estruturado da seguinte forma:

- **Capítulo 1** – Introdução: desafios crescentes em relação à segurança cibernética, desafios aos ataques em relação à grande quantidade de metadados armazenados em seus bancos de dados institucionais.
- **Capítulo 2** – Revisão Bibliográfica: apresenta os conceitos teóricos relacionados a cibersegurança em instituições de ensino superior.
- **Capítulo 3** – Metodologia: descreve os procedimentos utilizados no desenvolvimento, da análise sistemática com o auxílio do método TEMAC.
- **Capítulo 4** – Resultados: da analisa sistemática com base em dados quantitativos e qualitativos.
- **Capítulo 5** – Conclusão: descrever os resultados e o que poderá ser realizado para mitigar os riscos de intrusão de cibercriminosos.

2 – REVISÃO BIBLIOGRÁFICA

2.1 PHISHING E A ENGENHARIA SOCIAL

O malware de *phishing* é uma técnica de engenharia social reversa que se fundamenta na manipulação do usuário para levá-lo a tomar decisões prejudiciais à sua própria segurança digital. Por meio de abordagens enganosas, o atacante busca conquistar a confiança da vítima, fazendo com que ela acredite estar diante de uma comunicação legítima.

Esses ataques costumam ocorrer por e-mails, mensagens instantâneas ou páginas falsas que simulam serviços conhecidos. Ao interagir com esse conteúdo, a vítima pode fornecer informações confidenciais, como senhas e dados pessoais, sem perceber que está sendo induzida ao erro.

Em muitos casos, o simples ato de clicar em um link suspeito já é suficiente para iniciar o comprometimento do dispositivo. A partir desse clique, podem ser instalados programas maliciosos que atuam como hospedeiros, permitindo o acesso indevido a dados armazenados ou ao próprio sistema operacional. (Neves, 2022)

Os softwares mal-intencionados operam de forma discreta, dificultando a percepção do usuário quanto à violação em curso. Com isso, os atacantes conseguem manter o controle por períodos prolongados, ampliando os danos causados à vítima e, em situações mais graves, a redes corporativas inteiras.

De acordo com Neves (2022), o *phishing* destaca-se por ser um método simples, porém extremamente eficaz. Sua facilidade de aplicação e o baixo custo operacional contribuem para que seja amplamente empregado em ataques em larga escala, alcançando um número significativo de pessoas simultaneamente.

Durante a pandemia de COVID-19, essa prática tornou-se ainda mais recorrente. Os criminosos passaram a utilizar temas relacionados à crise sanitária, benefícios sociais e alertas de saúde, explorando a incerteza e o medo vivenciados pela população naquele período.

A vulnerabilidade emocional e o aumento da dependência de meios digitais criaram um ambiente favorável à expansão dessas fraudes. Nesse contexto, a atenção do usuário estava voltada à busca por informações rápidas, o que reduzia a capacidade crítica diante de mensagens suspeitas. (Neves, 2022)

Dessa forma, percebe-se que o *phishing* permanece como uma ameaça recorrente no cenário da segurança da informação. Mesmo com avanços tecnológicos e maior conscientização dos usuários, a exploração de aspectos psicológicos continua sendo eficaz, o que demonstra que as técnicas de engenharia social, baseadas no comportamento humano, nunca saem de moda.

No artigo Nguyet Q. *et al,* (2022), ele e seus coautores descrevem a preocupação em relação ao malware phishing, que se consolidou como uma ameaça recorrente no ambiente digital, despertando a atenção tanto de usuários comuns quanto de profissionais especializados em segurança da informação. À medida que os serviços on-line se expandem, cresce também a superfície de ataque explorada por agentes mal-intencionados (Cybercriminosos), tornando esse tipo de fraude cada vez mais presente no cotidiano digital.

Apesar dos avanços obtidos ao longo dos anos, as técnicas tradicionais de detecção de phishing ainda apresentam limitações relevantes. Muitos mecanismos existentes enfrentam dificuldades relacionadas à precisão dos resultados, além de não conseguirem identificar, de forma eficaz, ataques inéditos ou variantes recentemente desenvolvidas.

Esse cenário evidencia que, mesmo após décadas de pesquisas e aprimoramentos, os métodos convencionais não acompanham plenamente a evolução das estratégias adotadas pelos atacantes. A constante adaptação das campanhas de phishing desafia soluções baseadas apenas em regras fixas ou listas previamente conhecidas. (Nguyet, Q. *et al*, 2022)

Diante dessas limitações, pesquisadores da área de segurança cibernética passaram a buscar abordagens mais robustas e adaptativas. Nesse contexto, técnicas fundamentadas em aprendizado de máquina ganharam destaque por sua capacidade de analisar grandes volumes de dados e identificar padrões complexos associados a comportamentos maliciosos.

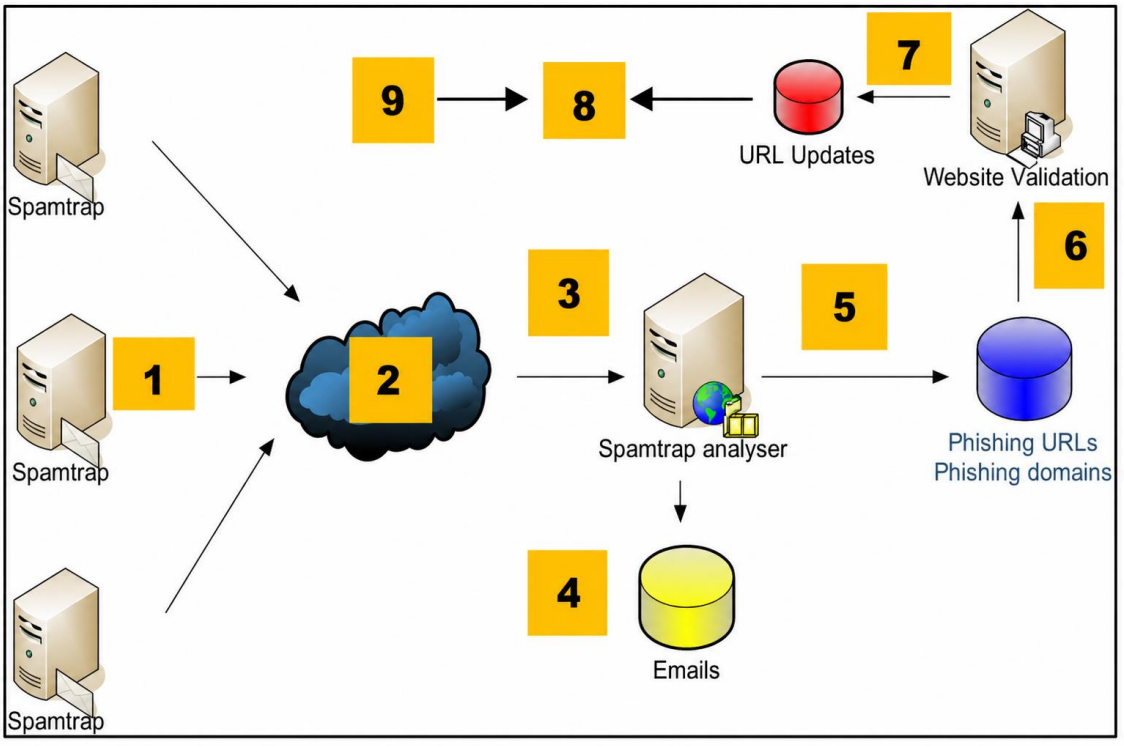
O aprendizado profundo, como uma vertente mais avançada do aprendizado de máquina, passou a ocupar papel central nas pesquisas recentes. Sua habilidade de extrair características relevantes de forma automática tornou-se especialmente útil na identificação de estruturas e comportamentos típicos de ataques de phishing. (Nguyet, Q. *et al*, 2022)

Nos últimos anos, estudos indicam que modelos baseados em aprendizado profundo apresentam desempenho superior quando comparados às técnicas tradicionais, sobretudo na detecção de ataques desconhecidos. Essa capacidade adaptativa contribui para reduzir falsos negativos e ampliar a efetividade das defesas digitais.

Assim, embora o ataque por malware de *phishing* possa aparentar ser simples, frágil ou até insignificante à primeira vista, ele continua sendo considerado por especialistas uma das

técnicas mais eficientes no cenário das ameaças cibernéticas. Sua persistência e capacidade de adaptação reforçam que, mesmo diante de soluções tecnológicas avançadas, o fator humano segue como um dos principais alvos explorados pelos atacantes. (Nguyet, Q. *et al*, 2022) Na Figura 2.1 segue um exemplo de um sistema de proteção contra-ataques de *phishing:*

Figura 2.1: Ataque de Phishing



Fonte: Pillay e Sharma (2023) adaptado.

A abaixo segue o fluxo lógico traduzido do sistema acima (Pillay e Sharma, 2023):

1º. Central de Spam – representam os inúmeros pontos de origem das mensagens maliciosas (E-mails fraudulentos), normalmente distribuídos em larga escala pelos atacantes;

2º. Rede de Internet (Nuvem) – representa os diversos pontos de origem e o percurso das mensagens suspeitas até o servidor de análise, constituindo o canal de comunicação pelo qual os e-mails trafegam antes de serem inspecionados;

3º. Servidor Analisador de Spamtranps – atua como um núcleo do sistema, recebendo os e-mails coletados e realizando:

a) Inspeção do conteúdo da mensagem;

b) Análise de cabeçalhos (headers);

c) Identificação de padrões típicos de phishing (links suspeitos, linguagem fraudulenta e domínios falsos.

4º. Base de Dados de E-mails – Armazena as mensagens analisadas, permitindo:

a) Auditoria e rastreabilidade;
b) Treinamento de mecanismos de detecção (regras de inteligência artificial);

c) Correlação com incidentes anteriores.

5º. Extração e classificação de URL's – Durante a análise, os links contidos nos e-mails os dados são extraídos para verificação específica, pois normalmente o link direciona para uma página falsa.

6º. Validação de Websites (Websites Validation) – As URL's são acessadas em ambiente controlado para verificar:

a) Autenticidade do Site;

b) Presença de formulários Fraudulentos;

c) Tentativa de coleta indevida de credencias.

7º. Atualização de URL's (URL's Updates) – URL's confirmadas como maliciosa são registradas continuamente em listas de bloqueio (blacklist).

8º. Base de Dados de URL's de Phishing e Domínios Maliciosos – Consolida os endereços identificados como phishing, permitindo:

a) Bloqueio preventivo de acessos futuros;

b) Compartilhamento de informações com outros sistemas de segurança;

c) Redução do risco de reincidência do ataque.

9º. **Resultado Final do Sistema** – O conjunto de processos permite detectar, classificar, registrar e bloquear ataques de phishing de forma proativa proporcionada proteção ao usuário de roubo de credencias, fraudes financeiras e comprometimento do sistema.

Entretanto nessas situações, o invasor realiza um estudo prévio detalhado sobre o comportamento da vítima. Ele analisa padrões de comunicação, hábitos profissionais, redes de contato e informações públicas divulgadas em sites institucionais ou redes sociais. (Pillay e Sharma, 2023).

Após a coleta dos metadados, os criminosos cibernéticos estruturam abordagens altamente personalizadas, capazes de proporcionar e transmitir a vítima credibilidade e confiança, aumentando significativamente o percentual de intrusão aqueles dados almejados. (Ulven e Wanger, 2021)

Em vez de enviar mensagens genéricas para um grande número de pessoas, o criminoso concentra seus esforços em poucos alvos estratégicos, desenvolvendo mensagens sofisticadas e bem elaboradas. Essa personalização torna a ameaça particularmente perigosa, pois dificulta a detecção por filtros de segurança e aumenta a probabilidade de que a vítima interaja com o conteúdo malicioso. (Neves, 2022)

Em situações mais elaboradas de phishing, o invasor não atua de forma aleatória, mas realiza um levantamento prévio minucioso sobre o perfil da vítima. Esse estudo envolve a observação de comportamentos recorrentes, formas de comunicação, rotinas profissionais e vínculos institucionais, além da análise de informações disponíveis publicamente em sites oficiais e redes sociais, conforme apontam Pillay e Sharma (2023).

A partir desse mapeamento inicial, o criminoso passa a compreender melhor o contexto em que a vítima está inserida, identificando oportunidades para tornar o ataque mais convincente. Dados aparentemente inofensivos, quando analisados em conjunto, fornecem subsídios suficientes para a construção de estratégias direcionadas e eficazes.

Com os metadados coletados, os cibercriminosos estruturam abordagens personalizadas, cuidadosamente elaboradas para transmitir legitimidade e confiança. Segundo Ulven e Wanger (2021), essa personalização aumenta de forma significativa a taxa de sucesso das tentativas de intrusão, uma vez que reduz a desconfiança inicial da vítima.

Diferentemente de campanhas massivas e genéricas, esse tipo de ataque concentra-se em um número restrito de alvos considerados estratégicos. As mensagens são formuladas com maior nível de sofisticação, o que dificulta sua identificação por mecanismos automáticos de segurança e eleva a probabilidade de interação com o conteúdo malicioso, conforme destaca Neves (2022).

Em síntese, embora o ataque por malware de *phishing* possa, à primeira vista, parecer trivial ou de baixo impacto, ele permanece classificado por especialistas como uma das estratégias mais eficazes no contexto da segurança cibernética. A constante adaptação dos métodos utilizados e a exploração direta do comportamento humano contribuem para a permanência e a efetividade dessa ameaça, que segue relevante mesmo diante da evolução das tecnologias de proteção. (Ulven e Wanger, 2021)

Por fim, torna-se fundamental investir em ações voltadas ao combate e à mitigação dos ataques de phishing. Medidas como a conscientização dos usuários, o fortalecimento de políticas de segurança, a adoção de tecnologias de detecção avançadas e a atualização contínua

dos sistemas são essenciais para reduzir riscos, minimizar impactos e impedir que esse tipo de malware comprometa informações sensíveis e infraestruturas críticas da instituição.

2.2 RANSOMWARE E SEUS IMPACTOS

Outro tipo de malware que vem causando grande preocupação em escolas, institutos e universidades é o avanço dos ataques de ransomware. Essa ameaça digital atua de forma invasiva, acessando os sistemas institucionais e identificando arquivos sensíveis, como registros acadêmicos, dados administrativos e resultados de pesquisas científicas.

Após localizar essas informações, o ransomware bloqueia o acesso aos dados por meio de técnicas de criptografia, impedindo seu uso pelos responsáveis legítimos. A partir desse momento, os invasores passam a exigir o pagamento de um resgate como condição para a liberação dos arquivos sequestrados, caracterizando um grave cenário de extorsão digital.

Instituições de ensino superior tornaram-se alvos frequentes desse tipo de ataque devido ao alto valor das informações que armazenam. Além de grandes volumes de dados pessoais, essas organizações lidam com pesquisas estratégicas, projetos financiados e informações institucionais críticas, o que aumenta o interesse de grupos criminosos. (Cheng e Wang, 2022)

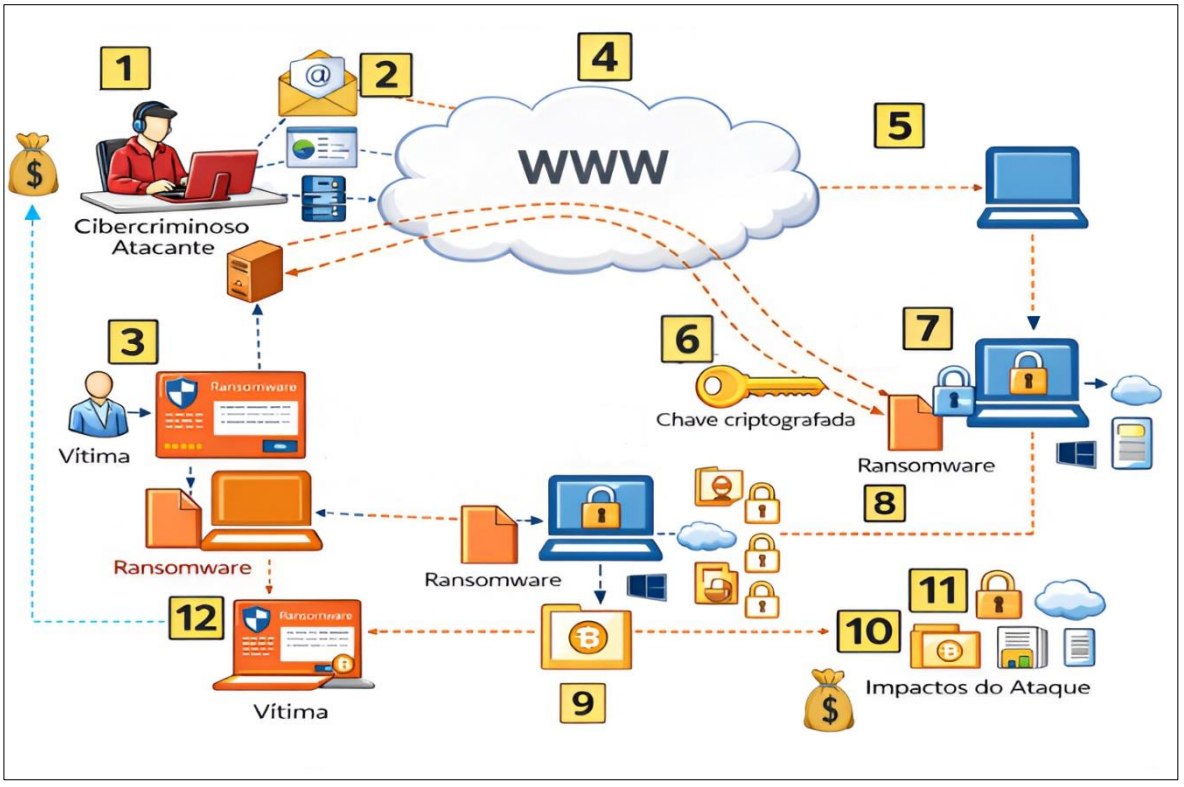
As consequências de um ataque de ransomware vão muito além da exigência financeira. Conforme destacam Cheng e Wang (2022), o comprometimento dos sistemas pode afetar diretamente o funcionamento da universidade, tornando indisponíveis plataformas essenciais para ensino, gestão acadêmica, administração e controle financeiro.

A interrupção prolongada desses serviços pode resultar na suspensão de aulas, atrasos em processos administrativos e dificuldades na execução de atividades científicas. Em situações mais graves, o calendário acadêmico é impactado, prejudicando estudantes, docentes e pesquisadores, além de comprometer prazos estabelecidos por agências de fomento (Lachi, 2021).

Outro efeito relevante é a possibilidade de perda definitiva de dados ou a exposição indevida de informações confidenciais. Quando arquivos são corrompidos ou divulgados, os prejuízos podem ser irreversíveis, afetando tanto a produção científica quanto a integridade institucional. Além dos danos operacionais, há impactos significativos sobre a imagem e a credibilidade da instituição. A divulgação de incidentes dessa natureza tende a abalar a confiança de alunos, servidores, parceiros e da sociedade em geral, dificultando futuras colaborações e investimentos. (Lallie, H. Singh. *et al*,2021)

Diante desse conjunto de fatores, o ataque de ransomware é considerado extremamente grave no contexto prevencionista e técnico. Seus efeitos abrangem aspectos financeiros, operacionais e acadêmicos reforçando a necessidade de estratégias robustas de prevenção e resposta para mitigar riscos e proteger o patrimônio informacional das instituições de ensino. (Lallie, H. Singh. *et al*,2021) Na Figura 2.2 segue um exemplo de um sistema de como o ransomware funciona:

Figura 2.2: Como Funciona o Ransomware



Fonte: Pillay e Sharma (2023) Adaptado.

Para uma compreensão mais clara desse contexto, modelos explicativos que descrevem o funcionamento do ransomware contribuem para visualizar as etapas do ataque. Esses modelos apresentam o ciclo completo da ameaça, que se inicia, em geral, por meio de mensagens de phishing ou pela exploração de falhas de segurança ainda não corrigidas nos sistemas.

Após a infecção inicial, o malware atua de forma discreta, promovendo a criptografia dos dados sem chamar a atenção imediata dos usuários ou administradores. Somente ao final desse processo o invasor revela sua presença, exibindo a mensagem de resgate e condicionando a liberação dos arquivos ao pagamento exigido. (Pillay e Sharma, 2023)

O conhecimento detalhado dessas fases é essencial para o fortalecimento das estratégias de segurança no ambiente acadêmico. Conforme destacam Pillay e Sharma (2023), esse entendimento subsidia a definição de políticas de prevenção, respostas mais ágeis a incidentes

e o aumento da resiliência cibernética das instituições de ensino. A abaixo segue o fluxo lógico traduzido do sistema acima (Pillay e Sharma, 2023):

1º. Atacante (Hacker / Grupo Criminoso) – É conceituado como agente malicioso que desenvolve ou utiliza o malware e define qual vetor de ataque será lançado (e-mail, site fraudulento etc.);

2º. Vetor de Infecção Inicial – O ataque geralmente começa por:

a) E-mail de phishing com anexo ou link malicioso;

b) Download de software infectado;

c) Exploração de vulnerabilidades em sistemas ou serviços à internet;

3º. Infecção da Vítima Inicial – O usuário executa o arquivo ou acessa o link, permitindo que o ransomware seja instalado no computador ou servidor;

4º. Conexão com a Internet (WWW) – Após a infecção, o malware se comunica com servidores externos controlados pelo atacante, normalmente para:

a) Enviar informações do sistema infectado;

b) Obter instruções adicionais;

c) Receber chaves ou parâmetros de criptografia.

5º. Geração/ Recebimento da Chave de Criptografia – O malware ransomware utiliza algoritmos criptográficos (simétricos ou assimétricos) para gerar ou receber a chave que será utilizada para lesar a vítima;

6º. Criptografia dos Arquivos – Os dados do sistema infectado (documentos, imagens, bancos de dados entre outros) são criptografados pelo atacante tornando-os inacessíveis ao usuário legítimo;

7º. Propagação na Rede Interna – Em ambientes corporativos, o ransomware pode espalhar para outros computadores com o objetivo de explorar:

a) Credencias compartilhadas;

b) Pastas de rede;

c) Vulnerabilidades não mitigadas.

8º. Infecção de Outras Máquinas – Após alguns ataques efetivados e bem-sucedidos outros dispositivos passam a sofre com o mesmo processo de criptografia, ampliando assim a

proporção e os impactos dos ataques;

9º. Mensagem de Resgate – Após o sucesso com a criptografia ao sistema infectado o atacante lança uma mensagem a vítima informando que:

a) Seus arquivos pessoas foram bloqueados e capturados;
b) Os valores das informações sequestradas devem ser pagos por criptomoedas;

c) As instruções para pagamento e contato com o atacante.

10º. Exigências de Pagamento – O Criminoso Cibernético condiciona a vítima a chave de descriptografia condicionado ao pagamento de um resgate, mas não garante a reocupação dos dados sequestrados.

11º. Impactos dos Ataques – A intrusão de um sistema pode proporcionar a vítima indisponibilidade das informações, prejuízos financeiros, risco a sua reputação a depender de qual conteúdo poderá ser divulgado e perda definitiva de seus dados.

12º. Conclusão do Ciclo – O ataque é considerado completo quando a vítima:

a) Paga o resgate (com ou sem a recuperação dos dados), ou

b) Restaura os sistemas a partir de backups e medidas de resposta a incidentes

Em virtude dos fatos apresentados, o malware do tipo ransomware revela-se extremamente agressivo, pois transfere o controle da situação para o atacante e impõe à vítima as regras de seu jogo criminoso. Ao definir prazos, valores e condições para o suposto resgate, o invasor determina a dinâmica do ataque e limita as possibilidades de reação, forçando decisões rápidas em um cenário de alta pressão.

Além do impacto técnico, esse tipo de ataque atua diretamente no aspecto psicológico do alvo, utilizando estratégias de intimidação e chantagem emocional. A ameaça de perda definitiva de dados, a divulgação de informações sensíveis e o comprometimento das atividades institucionais são explorados para gerar medo e urgência, aumentando a probabilidade de submissão às exigências impostas pelos criminosos.

2.3 ATAQUES DE NEGAÇÃO DE SERVIÇOS DISTRIBUÍDOS (DDOS)

Os ataques distribuídos de negação de serviço, conhecidos como DDoS, são classificados como técnicas de ataque cibernético e não como códigos maliciosos propriamente ditos, uma vez que não envolvem a instalação direta de malware nos sistemas-alvo. Essa modalidade de ataque baseia-se na sobrecarga intencional da infraestrutura de rede, por meio do envio massivo

de tráfego malicioso.

O objetivo principal dessa prática é esgotar os recursos disponíveis da rede atacada, resultando em lentidão significativa ou na completa indisponibilidade de serviços. Em ambientes universitários, esse tipo de ataque pode comprometer o funcionamento de sistemas essenciais, como correio eletrônico, portais institucionais, plataformas acadêmicas e demais serviços on-line, além de provocar congestionamentos na rede interna. (Ma Haque, Md. *et al*., 2023)

Segundo Dolliver *et al.* (2021), os ataques DDoS podem ser executados por diferentes metodologias. Uma das mais comuns envolve a criação de uma rede distribuída de dispositivos comprometidos, conhecidos como bots, zumbis ou hosts de intrusão, controlados remotamente pelo atacante.

Essa rede distribuída permite que o tráfego malicioso seja gerado simultaneamente a partir de múltiplas origens, dificultando a identificação da fonte do ataque. Como consequência, os mecanismos tradicionais de defesa tornam-se menos eficazes diante do volume e da dispersão das requisições. Os danos provocados por ataques DDoS não se limitam à interrupção momentânea dos serviços. Em muitos casos, os efeitos se estendem para além do período do ataque, exigindo esforços técnicos prolongados para a restauração completa dos sistemas afetados. (Ma Haque, Md. *et al*., 2023)

No contexto do ensino superior, esse cenário torna-se ainda mais preocupante. De acordo com Lachi e Anatolie (2022), universidades e institutos de pesquisa passaram a atrair maior atenção de ciberespiões devido ao valor estratégico das informações que produzem e armazenam. Os autores apontam um aumento expressivo de aproximadamente 350% nos registros de intrusões por meio de ataques DoS e DDoS. Esses ataques têm sido direcionados, principalmente, a ambientes de ensino a distância, cuja dependência de conectividade contínua é elevada.

A paralisação de sistemas críticos pode gerar prejuízos financeiros significativos para as instituições. Além disso, atrasos em projetos acadêmicos e científicos tornam-se frequentes, comprometendo cronogramas previamente estabelecidos. Quando serviços administrativos e científicos são afetados, os impactos se ampliam para toda a comunidade acadêmica. Processos internos, atividades de pesquisa e rotinas institucionais passam a enfrentar obstáculos operacionais relevantes.

Outro aspecto crítico é o uso de ataques DDoS como estratégia complementar a outras ações

maliciosas. Conforme destacam Fan *et al.* (2021), esses ataques podem funcionar como uma cortina de fumaça, desviando a atenção das equipes técnicas enquanto outras intrusões são realizadas. Durante esse período de instabilidade, invasores podem tentar acessar dados sensíveis, extrair informações confidenciais ou instalar malwares adicionais nos sistemas comprometidos. Isso amplia significativamente o nível de risco para a universidade e seus usuários.

De forma geral, observa-se que as instituições de ensino superior enfrentam um conjunto diversificado de ameaças cibernéticas. Entre as mais recorrentes destacam-se o phishing, as ameaças internas, os ataques DDoS, as violações de dados e o ransomware.

Conforme a explanação de Naagas *et al.* (2018) e autores, eles ressaltam que esses ataques podem ter origem tanto externa quanto interna. Enquanto os hackers representam uma fonte clássica de ameaças externas, falhas associadas à Zona Desmilitarizada (DMZ), integrada à rede local, configuram riscos internos relevantes.

Em razão destes ataques, torna-se evidente a necessidade de fortalecer a segurança digital nas universidades. A adoção de soluções mais avançadas, especialmente aquelas baseadas em inteligência artificial, é fundamental para identificar padrões anômalos, antecipar comportamentos suspeitos e mitigar ataques antes que provoquem danos significativos às instituições acadêmicas.

2.4 MALWARE EXPLORANDO AS VULNERABILIDADES DOS SISTEMAS

O termo malware, abreviação de software malicioso, refere-se a programas desenvolvidos com a finalidade de acessar sistemas computacionais de forma não autorizada. Esses códigos têm como objetivo principal subtrair, capturar, alterar ou destruir informações sensíveis, muitas vezes de caráter pessoal ou restrito, comprometendo a integridade e a confidencialidade dos dados.

Os softwares maliciosos podem assumir diferentes formas e empregar variados mecanismos de intrusão. Entre os mais conhecidos podemos destacar: os vírus, *worms* e *trojans* outras técnicas que exploram vulnerabilidades de sistemas e redes para se propagar e atingir finalidades ilícitas. (Ferreira *et al*., 2023) Conceituando-os os mais conhecimos pode-se observa que:

a) ***Vírus*** – é uma forma de *malware* que depende de um arquivo hospedeiro — como programas, documentos ou executáveis — para se disseminar. Sua ativação ocorre quando o usuário abre ou executa o arquivo contaminado, momento em que o código malicioso passa a agir no sistema. A partir disso, pode comprometer a integridade dos

dados, modificar o funcionamento do sistema e se replicar, infectando outros arquivos e ampliando sua propagação.

b) ***Worms*** **–** também conhecidos como vermes, são tipos de malware capazes de se disseminar de forma autônoma por redes de computadores, sem depender da ação direta do usuário. Eles exploram vulnerabilidades existentes em sistemas e serviços para se replicar rapidamente, alcançando múltiplos dispositivos em pouco tempo. Como consequência, podem degradar o desempenho das redes, consumir recursos excessivos e comprometer a estabilidade dos sistemas afetados.

c) ***Trojans*** **–** é um tipo de malware que se apresenta como um programa legítimo ou confiável, induzindo o usuário à sua instalação. Uma vez executado, o código malicioso atua de forma oculta, podendo criar acessos não autorizados ao sistema, viabilizar o roubo de dados sensíveis ou permitir o controle remoto do dispositivo por terceiros.

A disseminação desses códigos ocorre, em grande parte, por meio de vetores comuns do cotidiano digital como e-mails fraudulentas, sites suspeitos, mídias removíveis contaminadas e anexos aparentemente legítimos, figuram entre os principais meios utilizados para introduzir o malware nos dispositivos das vítimas.

Ao serem executados, esses arquivos ativam rotinas ocultas que liberam códigos nocivos, capazes de comprometer o funcionamento do sistema, coletar informações sigilosas ou permitir o controle remoto do equipamento atacado. (Rajput *et al*., 2021) Com o passar do tempo os programas maliciosos passaram por um processo significativo de evolução. O que antes era relativamente simples tornou-se progressivamente mais sofisticado, dificultando sua identificação e contenção por mecanismos tradicionais de defesa.

Atualmente, técnicas como ofuscação de código, polimorfismo e variação dinâmica de comportamento permitem que o malware altere suas características durante a execução. Essas estratégias reduzem a eficácia de antivírus baseados exclusivamente em assinaturas conhecidas.

Além disso, o uso de recursos de inteligência artificial tem ampliado a capacidade de adaptação desses códigos, possibilitando que eles aprendam padrões de detecção e ajustem seu comportamento para evitar bloqueios automáticos, conforme apontam Ferreira *et al*. (2023).

Em escala global, as intrusões realizadas por meio de malwares podem gerar consequências severas. Entre os impactos mais recorrentes estão a interrupção de serviços essenciais, o vazamento de dados sensíveis, prejuízos financeiros expressivos e danos à imagem institucional.

Instituições de ensino superior, órgãos governamentais e empresas privadas figuram entre os alvos mais frequentes desses ataques. O grande volume de dados armazenados e o uso intensivo de redes compartilhadas aumentam a superfície de ataque, especialmente na ausência de políticas adequadas de proteção digital. (Ma Haque *et al*., 2023)

Em virtude desse contexto, a prevenção contra programas maliciosos exige uma abordagem integrada. Não se trata apenas de tecnologia, mas também de processos bem definidos e, sobretudo, da conscientização e do comportamento dos usuários.

Medidas como autenticação forte, realização periódica de backups, atualização constante de sistemas, uso de ferramentas de análise comportamental e capacitação contínua dos usuários são essenciais para reduzir a exposição a riscos. Assim, investir em segurança digital deixa de ser uma escolha e passa a ser uma exigência fundamental em qualquer ambiente conectado.

2.5 NORMATIVOS E BOAS PRÁTICAS DE SEGURANÇA CIBERNÉTICAS

A adoção de sistemas automatizados que tratam de dados sensíveis exige cuidados rigorosos quanto à segurança da informação. Esses sistemas precisam operar de acordo com padrões reconhecidos internacionalmente, de modo a garantir a confidencialidade, a integridade e a disponibilidade das informações processadas.

Em virtude dessa premissa inicial, normas como a norma (ISO/IEC) 27001 assumem papel central, pois estabelecem requisitos para a implementação de um Sistema de Gestão da Segurança da Informação. Essa norma orienta organizações na identificação de riscos, na definição de controles e na melhoria contínua dos processos de segurança. (ISO/IEC 27001,2022)

Além da norma (ISO/IEC) 27001, as diretrizes publicadas pelo *National Institute of Standards and Technology* (NIST) são amplamente utilizadas como referência técnica. Esses documentos fornecem orientações práticas para o fortalecimento dos controles de segurança, especialmente em ambientes que dependem intensamente de tecnologias digitais.

No cenário brasileiro, a conformidade com normas internacionais deve ser acompanhada da observância aos instrumentos normativos nacionais. O arcabouço regulatório interno busca alinhar as boas práticas globais às especificidades legais e administrativas do país. Entre esses instrumentos, destaca-se o Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria SGD/MGI nº 852/2023. O programa estabelece diretrizes voltadas à governança de dados e à proteção da informação no âmbito da administração pública federal. (BRASIL, 2023)

O PPSI atua de forma complementar à Lei Geral de Proteção de Dados Pessoais, prevista na Lei nº 13.709/2018. Enquanto a LGPD define princípios, direitos e deveres relacionados ao tratamento de dados pessoais, o programa fornece orientações operacionais para a sua efetiva implementação. (BRASIL, 2018)

Esse conjunto normativo contribui para a consolidação de um framework de governança digital, promovendo a adoção de boas práticas de segurança da informação. Tal abordagem é particularmente relevante em instituições públicas que lidam com grandes volumes de dados sensíveis. (Maranhão, JPA. *et al*, 2021)

Outro ponto enfatizado pelas diretrizes do NIST é a importância do registro e da manutenção de logs de auditoria. Esses mecanismos permitem o rastreamento de eventos, facilitando a detecção de incidentes e a responsabilização em caso de uso indevido das informações.

Em ambientes educacionais, a aplicação desses princípios assume relevância ainda maior. A segurança dos sistemas impacta diretamente a confiabilidade de registros acadêmicos, processos avaliativos e emissão de certificados. A autenticidade das informações digitais é fundamental para assegurar a validade acadêmica de cursos, diplomas e certificações. Falhas nesse aspecto podem comprometer a credibilidade institucional e gerar questionamentos legais e administrativos. (Rajput, P. *et al*. 2021)

Dessa forma, a implementação de sistemas automatizados em conformidade com normas internacionais e nacionais não deve ser vista apenas como uma exigência regulatória, mas sim como parâmetro de proteção. Trata-se de uma estratégia essencial para garantir a proteção dos dados, a confiança dos usuários e a sustentabilidade das operações em ambientes cada vez mais digitalizados.

A adoção de padrões reconhecidos contribui para a padronização de processos, a identificação antecipada de riscos e a definição de controles adequados. Com isso, as organizações passam a atuar de forma preventiva, diminuindo a probabilidade de incidentes que possam comprometer informações sensíveis ou a disponibilidade de sistemas críticos. (de Neira,A.*et al*, 2023)

Quando essas normas não são seguidas, os impactos de um ataque mal-intencionado tendem a ser mais severos. Vazamentos de dados, interrupções prolongadas de serviços, prejuízos financeiros e danos à reputação institucional são consequências frequentes de falhas na governança da segurança da informação.

Além dos prejuízos imediatos, incidentes dessa natureza podem gerar efeitos duradouros e,

em alguns casos, irreversíveis. A perda de confiança por parte de usuários, parceiros e da sociedade compromete a credibilidade da instituição e dificulta sua recuperação no médio e longo prazo. (Ma Haque, Md. *et al*. 2023)

Dessa forma, seguir rigorosamente as normas e boas práticas de segurança da informação representa uma medida essencial para evitar inconvenientes operacionais e mitigar danos significativos. Trata-se de um investimento necessário para garantir a proteção dos ativos digitais, a confiabilidade dos serviços e a sustentabilidade das organizações diante de um cenário de ameaças cibernéticas em constante evolução.

2.6 SÍNTESE DA REVISÃO SISTEMÁTICA

A segurança cibernética tornou-se elemento estratégico para as instituições de ensino superior, que vêm enfrentando desafios cada vez mais complexos no ambiente digital. O crescimento de ataques como *phishing, ransomware* e DDoS evidencia a vulnerabilidade desses espaços, marcados pelo grande volume de dados acadêmicos, administrativos e científicos. A interconectividade dos sistemas e o uso intensivo de plataformas on-line ampliam a superfície de exposição.

Além dos impactos técnicos, incidentes de segurança podem gerar prejuízos financeiros, interrupções operacionais e danos à reputação acadêmica. A adoção de políticas consistentes, aliada ao uso de tecnologias adequadas e à capacitação dos usuários, torna-se indispensável para mitigar riscos. Investir em prevenção e monitoramento contínuo fortalece a resiliência institucional diante de ameaças emergentes.

O trabalho científico nesse contexto apresenta uma revisão bibliográfica sistemática em relação as ameaças oriundas de softwares maliciosos e propõe artifícios técnicos para mitigar os riscos e minimizar os danos sofridos. Para consolidar os resultados da revisão foi utilizada a Teoria do Enfoque Meta-Analítico (TEMAC), ferramenta aplicada na revisão de literatura.

A análise de metadados associada às palavras-chave phishing, ransomware, ataques DDoS, malware, instituições de ensino superior e detecção, realizada nas bases *Web of Science* e *IEEE Xplore*, no período de 2021 a 2025, resultou na identificação de 755 publicações científicas. Esse levantamento permitiu mapear a produção acadêmica recente relacionada às principais ameaças cibernéticas no contexto educacional.

Após a consolidação e eliminação de registros duplicados do escopo da pesquisa, obteve-se um conjunto final de 706 documentos considerados relevantes para análise. Esse quantitativo representou o dado efetivo utilizado no estudo, assegurando maior consistência e alinhamento

temático aos objetivos propostos.

Entre as ameaças mais recorrentes está o ransomware, que bloqueia arquivos e sistemas mediante criptografia, exigindo pagamento para sua liberação. Esse tipo de ataque compromete rotinas administrativas, atividades acadêmicas e pesquisas em andamento. A paralisação de serviços essenciais pode gerar prejuízos financeiros e institucionais de difícil reparação.

Outro vetor explorado é a injeção de SQL, técnica que busca vulnerabilidades em aplicações web para obter acesso indevido a bancos de dados. Quando bem-sucedida, permite a extração ou manipulação de informações sensíveis. Pillay e Sharma (2023) apontam que falhas de configuração e ausência de validação adequada de entradas são fatores que favorecem esse tipo de invasão.

Neves (2022) observa que muitos incidentes têm origem na engenharia social, prática que explora confiança e desatenção dos usuários. Durante a pandemia de COVID-19, houve aumento significativo de golpes baseados em mensagens falsas e comunicações fraudulentas. A personalização das abordagens, após coleta prévia de dados, eleva as chances de sucesso da fraude.

Ulven e Wangen (2021) ressaltam que, após o acesso inicial, os atacantes ampliam sua presença na rede institucional, buscando privilégios elevados. No caso do ransomware, a criptografia dos dados é seguida por exigências financeiras acompanhadas de ameaças de divulgação de informações. Cheng e Wang (2022), apontam que esse cenário afeta diretamente a continuidade acadêmica.

As consequências de um ataque não se limitam ao pagamento de resgates. Sistemas de matrícula, plataformas virtuais e serviços administrativos podem ficar indisponíveis por dias ou semanas. Tal interrupção compromete o calendário acadêmico e a confiança da comunidade universitária.

Os ataques distribuídos de negação de serviço (DDoS) também figuram entre as principais ocorrências. Essa técnica consiste em sobrecarregar servidores e redes com tráfego excessivo, tornando serviços inacessíveis. Portais institucionais, ambientes de aprendizagem e sistemas de e-mail estão entre os alvos mais comuns.

Dolliver *et al*. (2021) explicam que ataques DDoS costumam ser realizados por meio de redes de dispositivos comprometidos, ampliando o alcance da ofensiva. Lachi e Anatolie (2022) registraram crescimento dessas ações em instituições que adotaram ensino remoto. Em muitos casos, o ataque serve como distração para outras invasões simultâneas.

Fan et al. (2021) indicam que o uso combinado de técnicas aumenta a complexidade da resposta institucional. Enquanto a equipe técnica lida com a sobrecarga da rede, pode ocorrer estratificação de dados ou instalação de códigos maliciosos. Essa sobreposição de eventos amplia o impacto do incidente.

No campo das defesas, soluções baseadas em análise de comportamento e aprendizado de máquina têm sido empregadas para identificar padrões anômalos. Naagas *et al*. (2018) defendem que mecanismos automatizados contribuem para respostas mais rápidas. Ainda assim, a tecnologia deve ser acompanhada de políticas internas consistentes.

O termo malware abrange programas desenvolvidos para infiltrar, monitorar ou danificar sistemas. Ferreira *et al*. (2023) mencionam vírus, worms e trojans como exemplos recorrentes. A disseminação ocorre, em muitos casos, por meio de e-mails fraudulentos ou downloads inseguros.

Rajput *et al*. (2021) destacam que a combinação de redes abertas, dispositivos pessoais e múltiplos perfis de acesso amplia os riscos nas universidades. Instituições públicas e privadas enfrentam desafios semelhantes, sobretudo pela grande circulação de dados estratégicos. Ma Haque *et al*. (2023) reforçam que o volume informacional atrai grupos especializados.

Para compreender o avanço dessas ameaças, estudos bibliométricos têm sido utilizados na organização do conhecimento científico. O modelo TEMAC, apresentado por Mariano e Rocha (2017), auxilia na identificação de tendências e lacunas de pesquisa. Essa abordagem permite visualizar a evolução dos debates sobre segurança no ensino superior.

Pesquisas recentes exploram técnicas de classificação automática de tráfego malicioso (Zhang *et al*., 2024), mitigação de DDoS em redes 5G com switches programáveis (Xiang *et al*., 2023), detecção de phishing por aprendizado profundo (Nguyet Quant *et al*., 2022), análises sobre a evolução do ransomware (Kamil *et al*., 2022) e modelos preditivos para ataques distribuídos. (de Neira *et al*., 2023)

Com base no Gil (2002), é comum classificar a pesquisa a partir de seus objetivos gerais, os quais, neste caso, estão orientados à realização de uma análise sistemática das publicações, utilizando a Teoria do Enfoque Meta-Analítico Consolidado (TEMAC).

Segundo Gil (2019), a pesquisa aplicada em uma revisão sistemática da literatura proporciona maior familiaridade com o problema proposto. Nesse caso específico, o estudo é caracterizado como exploratório, uma vez que envolve levantamento bibliográfico e análises que favorecem uma compreensão mais aprofundada do tema investigado.

Essas pesquisas demonstram que a proteção dos ambientes digitais demanda revisão contínua de processos, ferramentas e políticas internas. A rápida evolução das ameaças impõe a necessidade de aperfeiçoamento técnico permanente. Ao mesmo tempo, é indispensável alinhar soluções tecnológicas às práticas de gestão e governança. A segurança não pode ser tratada de forma isolada, mas integrada à estratégia institucional.

2.6.1 Preucupação das IES em ações Criminosas

Ulven e Wangen (2021) destacam que as instituições de ensino superior concentram grande volume de dados pessoais, acadêmicos e científicos, o que as torna alvos frequentes de ações criminosas no ambiente digital. A circulação intensa de informações e a diversidade de usuários ampliam a superfície de ataque. Nesse contexto, a proteção desses ativos passa a ser questão estratégica, e não apenas técnica.

As Instituições de Ensino Superior (IES) enfrentam um conjunto amplo de vulnerabilidades que, embora por vezes pareçam pontuais, mas podem comprometer de forma profunda e destrutiva toda a sua cadeia de informação da instituição.

Entre os principais fatores, destaca-se a presença de infraestrutura tecnológica obsoleta, com servidores e equipamentos sem suporte adequado, o que impede a aplicação de atualizações de segurança que favorecem as falhas e ataques. Somado a isso, a ausência de políticas robustas de segurança da informação, ou sua aplicação inconsistente, criando um ambiente despadronizado, no qual práticas inseguras se disseminam entre os diferentes setores institucionais.

Outro aspecto crítico é a falta de segmentação de rede, que permite a rápida propagação de incidentes entre áreas acadêmicas e administrativas, ampliando significativamente o impacto dos ataques. Os controles de acesso inadequados são problemas que afetam de forma expressiva uma IES, pois privilégios excessivos e ausência de revisões periódicas, aumentam o risco de ações indevidas e vazamentos de dados sensíveis.

O problema é potencializado com o baixo nível de conscientização dos usuários, tornando a comunidade acadêmica especialmente vulnerável a ataques como phishing, nos quais o fator humano é explorado como principal vetor de invasão.

A fragilidade também se evidencia na inexistência ou ineficácia de planos de resposta a incidentes e de continuidade de negócios, o que compromete a capacidade de reação diante de ataques e prolonga o tempo de indisponibilidade dos sistemas da instituição.

Paralelamente, a ausência de backups confiáveis, atualizados e testados regularmente

dificulta — ou até inviabiliza — a recuperação de dados após incidentes graves, como ataques de *ransomware*. O uso de softwares não licenciados ou desatualizados intensifica ainda mais esse quadro, pois expõe a instituição a vulnerabilidades e, em alguns casos, a códigos maliciosos incorporados sem perceber.

A integração insegura entre sistemas acadêmicos, administrativos e plataformas externas também constitui um ponto sensível, uma vez que falhas nessas conexões podem permitir acessos indevidos e vazamentos de informações críticas. A falta de auditorias e de monitoramento contínuo agrava a situação, pois impede a detecção precoce de ameaças, permitindo que ataques se desenvolvam de forma silenciosa e prolongada. Ademais, o crescimento desordenado de dispositivos conectados amplia a superfície de ataque e dificulta o controle e a gestão da segurança.

Outro fator relevante é a exposição de dados sensíveis de alunos, professores e pesquisas decorrente de falhas de configuração, o que pode gerar impactos legais, financeiros e reputacionais significativos. A dependência de fornecedores externos sem a devida avaliação de segurança também introduz riscos adicionais, uma vez que vulnerabilidades em terceiros podem comprometer diretamente os sistemas institucionais.

Por fim, a ausência de uma cultura organizacional voltada à segurança da informação fragiliza todas as demais medidas, pois reduz o engajamento e a responsabilidade dos usuários e gestores. Cabe ressaltar que tais vulnerabilidades, quando não tratadas de maneira integrada e estratégica, podem desencadear incidentes de grande magnitude, dificultando a recuperação dos sistemas e comprometendo, de forma abrangente, a continuidade das atividades acadêmicas, administrativas e científicas das Instituições de Ensino Superior.

2.7 Publicações Realizadas.

Em relação as publicações acadêmicas, atuei como autor e coautor, em assuntos que se concentram no eixo da segurança cibernética aplicada às instituições de ensino superior e aos seus usuários. Os trabalhos desenvolvidos buscam analisar vulnerabilidades, propor melhorias ao sistema, melhores técnicas e reforçar a importância da proteção de dados no ambiente acadêmico.

A primeira publicação da qual participei foi intitulada “A Importância da Usabilidade e a Colaboração Positivista Aplicada à Segurança Cibernética: Um Estudo de Caso do Aplicativo Sougov”. (Reis *et al*., 2025)

O estudo abordou a relação entre o desenvolvedor da solução tecnológica e o usuário final,

destacando como aspectos de usabilidade influenciam diretamente a adoção segura das ferramentas digitais.

Nesse trabalho, a análise concentrou-se na interação entre quem projeta o software e quem o utiliza, evidenciando que falhas de comunicação ou de design podem comprometer a segurança. A pesquisa demonstrou que a integração entre tecnologia e experiência do usuário é elemento essencial para fortalecer a proteção digital.

Já no segundo artigo, intitulado como “Aumentando a Segurança do Gerenciamento de Usuários do Moodle Usando Bancos de Dados de Terceiros” teve como foco a plataforma Moodle da Universidade de Brasília. A proposta consistiu em aprimorar o gerenciamento de usuários e tornar o processamento acadêmico mais eficiente, sem comprometer a segurança. (Nascimento *et al*., 2025)

No estudo realizado, foram analisados mecanismos de autenticação e integração com bases de dados externas, visando reduzir riscos de acesso indevido e mitigar possíveis ataques. O objetivo principal foi assegurar um ambiente virtual mais protegido para estudantes, docentes e demais usuários da plataforma.

Por fim, o trabalho científico de minha autoria, foi proposta uma revisão intitulada como “Detecção de Malware em Instituições de Ensino Superior: Uma Revisão das Ameaças De Phishing, Ransomware e DDos”. (Silva *et al*., 2026)

O trabalho evidenciou o crescente interesse dos cibercriminosos a instituição de ensino superior, motivado pelo grande volume de dados estratégicos armazenados, além de reforçar a necessidade de conscientização de usuários internos e externos quanto aos vetores de ataque e às medidas preventivas.

3 – METODOLOGIA

A Teoria do Enfoque Meta-Analítico (TEMAC) é reconhecida como um método organizado para condução de revisões bibliográficas. Sua proposta central consiste em reunir, sistematizar e interpretar grandes volumes de metadados científicos. Ao estruturar esse processo, o modelo contribui para maior clareza na análise da produção acadêmica. Conforme apontado por Ferreira *et al*. (2023), a metodologia favorece a integração de informações dispersas. Dessa forma, amplia a compreensão sobre determinado campo de estudo.

O estudo contou com apoio o das ferramentas de IA generativa como o ChatGPT e COPILOT, ferramentas utilizadas de forma complementar para aprimorar a redação e a estrutura textual deste trabalho, sem qualquer substituição da autoria intelectual, mantendo- se a responsabilidade integral do autor sobre o conteúdo descrito e apresentado.

Com base em Gil (2002), é comum classificar a pesquisa a partir de seus objetivos gerais, os quais, neste caso, estão direcionados à realização de uma análise sistemática das publicações científicas. Essa abordagem metodológica permite organizar o conhecimento existente de forma estruturada, favorecendo a identificação de padrões, lacunas e tendências no campo investigado.

A aplicação da TEMAC contribui para a sistematização das informações coletadas, permitindo integrar diferentes estudos em uma perspectiva analítica mais ampla. Esse método possibilita não apenas a consolidação dos dados, mas também a construção de uma visão crítica sobre a produção científica, ampliando a compreensão do fenômeno estudado. Dessa forma, a pesquisa ganha maior rigor metodológico e confiabilidade nos resultados obtidos. (Ferreira, L. et al. 2023)

Um dos pilares do modelo é o uso de indicadores bibliométricos. Essas métricas possibilitam examinar quantitativamente a produção científica. Entre os aspectos analisados estão frequência de publicações, redes de coautoria e impacto dos estudos. Com base nesses dados, é possível reconhecer tendências consolidadas. Também se tornam evidentes áreas que demandam maior aprofundamento. (Mariano e Rocha, 2017)

Ao mapear o estado atual do conhecimento, o TEMAC auxilia na identificação de padrões relevantes. O método evidencia quais abordagens teóricas predominam e quais métodos são mais empregados. Essa análise contribui para orientar novas pesquisas. Mariano e Rocha (2017) ressaltam que a técnica favorece a organização do panorama científico. Com isso, fortalece a

base conceitual de investigações futuras.

A versatilidade do modelo permite sua aplicação em diferentes áreas do saber. Seja nas ciências sociais, tecnológicas ou da saúde, o método adapta-se às especificidades de cada campo. Essa flexibilidade amplia seu alcance e utilidade.

O pesquisador pode ajustar critérios conforme o objetivo do estudo. Ainda assim, mantém-se a estrutura lógica proposta pela metodologia. (Mariano e Rocha, 2017)

Para estudiosos que iniciam a exploração de um tema, o TEMAC oferece suporte relevante e facilita a sistematização e compreensão do contexto teórico e metodológico existente. Em vez de analisar publicações de forma isolada, o pesquisador passa a observar o conjunto. Isso contribui para delimitar problemas de pesquisa com maior precisão. Também auxilia na definição de estratégias metodológicas adequadas.

Em síntese, o TEMAC consolida-se como instrumento eficiente para organizar e interpretar conhecimento científico. Ao combinar rigor metodológico e análise bibliométrica, o modelo proporciona visão estruturada da literatura. Essa abordagem fortalece a qualidade das revisões acadêmicas. Além disso, favorece decisões fundamentadas na escolha de referenciais teóricos. Trata-se de ferramenta relevante para o avanço sistemático da pesquisa.

3.1 Fundamentação Teórica e Abordagens Metodológicas

Segundo Gil (2019), a revisão sistemática da literatura é um procedimento que proporciona maior familiaridade com o problema de pesquisa, uma vez que envolve a análise detalhada de estudos previamente publicados. Esse tipo de investigação permite aprofundar o conhecimento sobre o tema, identificar abordagens teóricas e metodológicas adotadas por outros pesquisadores e compreender a evolução das discussões acadêmicas ao longo do tempo.

Nesse contexto, a pesquisa é caracterizada como exploratória, pois envolve levantamento bibliográfico e análises que visam ampliar a compreensão do tema investigado. Esse tipo de estudo é especialmente adequado quando se busca desenvolver maior entendimento sobre um fenômeno ainda pouco consolidado, contribuindo para a construção de novas perspectivas e para o avanço do conhecimento científico na área.

Tal perspectiva prioriza a mensuração e a análise objetiva de dados e conceitos relacionados ao tema proposto. O foco recai sobre a organização sistemática das informações coletadas que garante maior precisão na interpretação dos resultados.

A investigação concentrou-se em publicações dos últimos cinco anos, abrangendo o período de 2021 a 2025. O recorte temporal foi definido para assegurar atualidade do assunto. Dessa forma, buscou-se refletir o cenário recente da produção científica. A delimitação também favoreceu maior coerência na análise comparativa.

As bases de dados utilizadas foram Web of Science e IEEE Xplore. Ambas reconhecidas pela relevância e rigor na indexação de trabalhos acadêmicos. A escolha dessas plataformas ampliou a confiabilidade do material examinado. Além disso, permitiu acesso a estudos de alcance internacional.

O conjunto de documentos selecionados contemplou apenas publicações de acesso aberto, assegurando transparência e verificabilidade das informações analisadas. A disponibilidade integral dos textos contribuiu para aprofundamento da leitura. Assim, garantiu-se consistência ao desenvolvimento da pesquisa.

O método adotado caracteriza-se como descritivo de natureza quantitativa. Essa abordagem permite examinar dados amostrais com base em critérios objetivos. A análise concentra-se na identificação de padrões e frequências. O tratamento estatístico favorece maior clareza na exposição dos achados. (Creswell, 2010)

Segundo o autor Creswell (2010), o método quantitativo possibilita compreender fenômenos complexos por meio de dados organizados e mensuráveis. A ênfase recai na objetividade e na sistematização das informações. Tal perspectiva reduz interferências subjetivas na interpretação e com isso, amplia-se a robustez das conclusões.

Em síntese, a combinação entre fundamentação teórica consistente e método quantitativo estruturado fortalece a credibilidade do estudo. A definição clara de bases, período e critérios de seleção assegura rigor metodológico. O enfoque descritivo contribui para interpretação precisa dos dados. Dessa forma, o trabalho apresenta resultados alinhados aos objetivos propostos. (Mariano e Rocha, 2017)

A revisão da literatura pode assumir diferentes formatos, destacando-se a narrativa e a sistemática. A revisão narrativa caracteriza-se por maior flexibilidade na escolha das fontes. Em geral, baseia-se na conveniência do pesquisador e não adota critérios rígidos de seleção. Embora contribua para contextualização teórica, apresenta maior risco de vieses.

A revisão sistemática, por outro lado, fundamenta-se em procedimentos metodológicos definidos. As buscas são realizadas com critérios claros e previamente estabelecidos. Frequentemente utilizam-se indicadores bibliométricos e, em alguns casos, análises

estatísticas. Essa estrutura fortalece a confiabilidade dos resultados obtidos. (Mariano e Rocha, 2017)

Um dos principais objetivos da revisão sistemática é reduzir erros na seleção dos estudos. Para isso, adota parâmetros explícitos de inclusão e exclusão de registros. Tal rigor amplia a transparência do processo investigativo. Mariano e Rocha (2017) ressaltam que essa abordagem favorece maior precisão na organização do conhecimento.

A revisão narrativa, por exemplo, oferece uma abordagem mais ampla e descritiva, enquanto a revisão sistemática segue critérios rigorosos de seleção e análise das fontes. Há ainda a revisão integrativa, a revisão bibliométrica e o estado da arte, cada qual com métodos específicos de organização e interpretação do conhecimento produzido.

Além dessas classificações, a revisão bibliográfica pode ser organizada em cinco modalidades distintas, conforme apresentado no Quadro 3.1. Cada tipo apresenta características próprias quanto aos procedimentos metodológicos, à profundidade da análise e à finalidade científica. (Mariano e Rocha, 2017)

Quadro 3.1 Tipos de revisão da Literatura

Tipo	Revisão qualitativa	Revisão Integrativa	Revisão Sistemática	Meta-análises	Enfoque meta analítico
Definição	Tipo de revisão que sintetiza os achados de estudos qualitativos. É uma recriação do metaanalises aplicado a dados qualitativos.	É criação de estudos integradores de conceitos, métodos e opiniões para categorizar, objetivar e lançar novas perspectivas sobre um tema. Neste método, ter uma sistemática ajuda no processo.	É a pesquisa Planejada por meio de ações que permitem diminuir o viés da pesquisa combinando os estudos mais relevantes, por isso, possui alta rigorosidade.	Integra vários estudos primários por meio de técnicas estatísticas, melhorando a validade da pesquisa através do efeito total e magnitude do efeito	Utiliza abordagens da revisão qualitativa, integrativa e sistemática, podendo em análises mais profundas utilizar o metaanálises como uma análise final.
Propósito	Informar pesquisas ou práticas pela sumarização (resumo) de processos ou experiências	Revisar métodos, teorias, e/ou estudos empíricos sobre um tópico particular	Sumariar (resumir) evidência concernente a um problema específico	Estimar o efeito de intervenções ou de relacionamentos	Mapear a literatura sobre um tema oferecendo
Tipo	Revisão qualitativa	Revisão Integrativa	Revisão Sistemática	Meta-análises	Enfoque meta analítico

Escopo	Limitado ou amplo	Limitado ou amplo	Limitado	Limitado	Limitado ou amplo
Amostra	Pesquisa qualitativa	Pesquisa quantitativa ou qualitativa; literatura teórica; literatura metodológica	Pesquisa quantitativa de metodologia similar	Pesquisa quantitativa de metodologia similar	Pesquisa qualitativa e quantitativa
Análise	Narrativa	Narrativa	Narrativa ou estatística	Estatística	Narrativa e estatística

Fonte: Mariano e Rocha, 2017.

Ao iniciar uma revisão de literatura, é essencial que o pesquisador defina com clareza o objetivo e o alcance pretendido. Essa reflexão orienta a escolha do tipo de revisão e dos critérios de seleção das fontes. Embora nem sempre seja parte obrigatória de um artigo, a revisão tem sido cada vez mais demandada. Abramo e D'Angelo (2011), destacam sua importância para fundamentar decisões em estudos e projetos.

A adoção de critérios bem estabelecidos contribui para maior objetividade na análise do material selecionado. A definição prévia de bases de dados, palavras-chave e recortes temporais fortalece a consistência do trabalho. Esse cuidado metodológico amplia a credibilidade dos resultados. Além disso, favorece a transparência do processo investigativo.

Nesse cenário, o enfoque meta-analítico tem conquistado maior espaço entre pesquisadores. A possibilidade de apresentar dados quantitativos da produção científica amplia seu alcance. O uso de indicadores estatísticos permite mapear padrões e tendências. Tal abordagem agrega maior rigor à revisão bibliográfica. (Abramo e D'Angelo, 2011)

Entretanto, a presença de estatísticas na análise pode gerar dúvidas conceituais. Em alguns casos, há confusão entre enfoque meta-analítico e meta-análise. Embora possuam pontos de contato, tratam-se de procedimentos distintos. A delimitação clara de cada método é fundamental para evitar interpretações equivocadas. (Mariano e Rocha, 2017)

3.2 Teoria de Enfoque Meta-analítico Consolidado (TEMAC)

A Teoria do Enfoque Meta-Analítico (TEMAC) configura-se como um método estruturado de revisão bibliográfica sistemática e integradora. Sua base está apoiada em princípios e leis da bibliometria, o que confere rigor à análise da produção científica. A proposta central consiste em organizar e interpretar grandes volumes de publicações. Assim, promove uma visão ampla e fundamentada do campo investigado. (Mariano e Rocha, 2017)

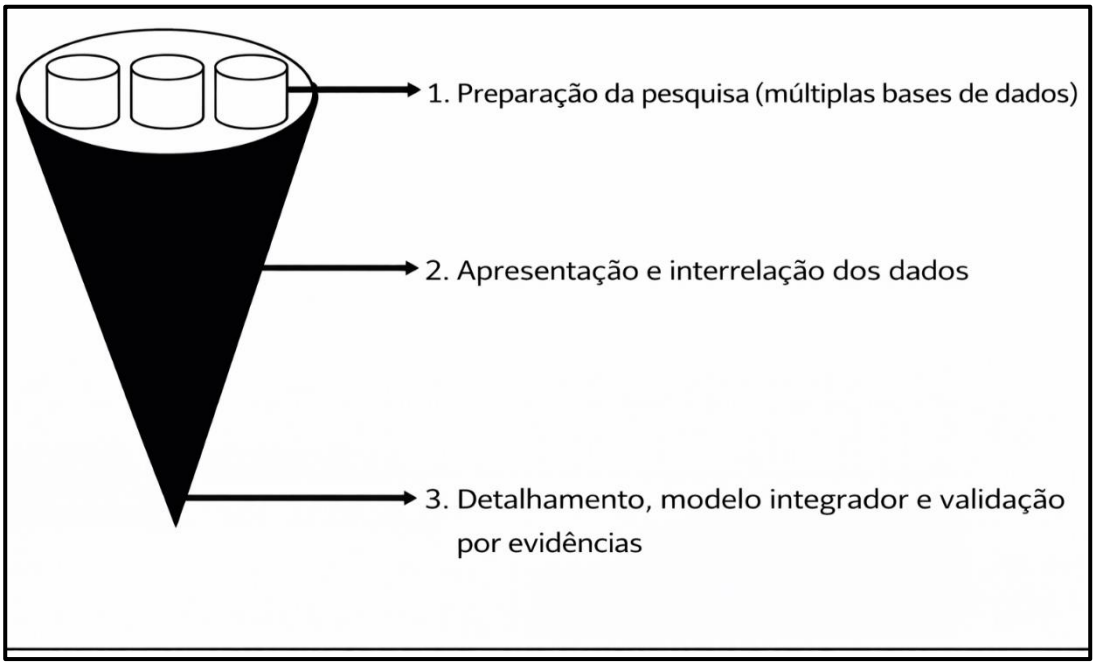
O modelo pode ser empregado em distintas áreas do conhecimento. Mostra-se especialmente útil para pesquisadores em fase inicial de estudo de determinado tema. Ao oferecer um panorama estruturado da literatura, facilita a compreensão do contexto teórico e metodológico. Mariano e Rocha (2017) destacam sua aplicabilidade em pesquisas exploratórias.

Ao oferecer um panorama estruturado da literatura, o modelo também fortalece a fundamentação teórica e amplia a capacidade crítica do pesquisador diante das diferentes correntes interpretativas.

Conforme ressaltam Mariano e Rocha (2017), sua aplicabilidade é especialmente significativa em pesquisas exploratórias, nas quais a compreensão inicial do fenômeno investigado é determinante para o desenvolvimento subsequente da investigação. Nesse contexto, o método auxilia na consolidação do referencial teórico, orienta escolhas metodológicas e contribui para a construção de um estudo cientificamente fundamentado.

O método é composto por três etapas principais sendo a primeira que envolve a preparação da pesquisa, com definição de critérios e bases de dados. Em seguida, ocorre a apresentação e a inter-relação das informações coletadas. Por fim, realiza-se o detalhamento dos achados, a construção de um modelo integrador e a validação por evidências. (Ferreira, L *et al*., 2023) Na Figura 3.1 é apresentado o modelo TEMAC.

Figura 3.1: Modelo TEMAC



Fonte: Mariano e Rocha, 2017

Entre suas contribuições está a identificação de tendências em determinado tema. A análise

do volume de publicações e citações permite avaliar o grau de relevância dos assuntos ao longo do tempo. Com isso, torna-se possível verificar quais áreas estão em expansão. Também se evidenciam campos que apresentam retração ou menor produção científica.

O TEMAC ainda possibilita reconhecer lacunas no conhecimento disponível. Ao mapear tópicos pouco explorados, o método orienta novas agendas de pesquisa. Essa identificação de déficits contribui para direcionar esforços acadêmicos. Dessa forma, fortalece o desenvolvimento sistemático do campo estudado.

Outro aspecto relevante é a análise do impacto de eventos contemporâneos na produção científica. A correlação entre publicações e fatos do cotidiano permite compreender mudanças de foco nas pesquisas. Esse acompanhamento temporal revela a dinâmica do debate acadêmico. Assim, amplia-se a interpretação do contexto em que os estudos são produzidos. (Ferreira, L *et al*., 2023)

O modelo também possibilita a comparação entre pesquisas desenvolvidas em diferentes países. Essa análise comparativa amplia a compreensão das abordagens adotadas em distintos contextos acadêmicos.

Ao evidenciar convergências e particularidades, favorece a construção de referenciais mais sólidos. Assim, o TEMAC contribui para a organização e o fortalecimento do conhecimento científico.

Outra contribuição relevante está na capacidade de acompanhar a evolução da produção ao longo do tempo. O método permite identificar temas em ascensão, áreas em retração e tópicos que ainda demandam maior aprofundamento. Essa leitura temporal oferece panorama estruturado do campo investigado. Conforme Ferreira *et al*. (2023), tal recurso orienta decisões mais fundamentadas.

A identificação de lacunas no conhecimento permite ampliar a compreensão sobre aspectos ainda pouco explorados pela literatura. Esse diagnóstico contribui para evidenciar temas que demandam maior aprofundamento científico. Ao reconhecer essas ausências, o pesquisador passa a ter maior clareza sobre as oportunidades investigativas existentes. Esse processo favorece escolhas mais estratégicas e alinhadas às necessidades acadêmicas. Dessa forma, o modelo fortalece a construção de pesquisas com maior relevância e impacto.

Esse panorama estruturado também orienta a definição de objetos de estudo mais consistentes e fundamentados. O mapeamento sistemático da produção científica contribui para organizar o campo do conhecimento de forma clara e objetiva. Com isso, torna-se possível

identificar tendências, concentrações temáticas e áreas emergentes. Essa organização contribui diretamente para o planejamento de novas investigações. Como resultado, a definição de prioridades passa a ocorrer com base em critérios técnicos e evidências concretas.

Adicionalmente, a análise estruturada das informações disponíveis favorece o uso mais eficiente dos recursos acadêmicos. O pesquisador consegue direcionar seus esforços para temas com maior potencial de contribuição científica. Essa abordagem reduz redundâncias e amplia a efetividade das pesquisas desenvolvidas. O processo contribui para maior rigor metodológico e melhor qualidade dos resultados obtidos. Assim, o desenvolvimento científico ocorre de forma mais organizada e consistente.

Nesse contexto, o modelo TEMAC consolida-se como ferramenta relevante para o fortalecimento da pesquisa científica. Sua aplicação contribui para qualificar o processo de revisão e análise da literatura existente. Ao fornecer base estruturada para a tomada de decisão, favorece maior precisão na condução dos estudos. Essa metodologia amplia a confiabilidade e a coerência das investigações acadêmicas. Conforme destacado por Mariano e Rocha (2017), sua utilização representa importante suporte ao avanço

3.3 Gerenciamento de Riscos

A gestão de riscos nas Instituições de Ensino Superior públicas consolidou-se como uma prática indispensável para assegurar a organização administrativa, a transparência dos processos e a proteção de recursos essenciais. Contudo, na prática, observa-se que essa gestão ainda é conduzida de forma básica e, em muitos casos, apresenta fragilidades significativas.

Em um cenário marcado pela intensa transformação digital, os riscos, especialmente aqueles relacionados à segurança da informação, tornaram-se mais frequentes e evidentes, exigindo abordagens mais estruturadas, integradas e eficazes por parte das IES. (Gonçalves, E. *et al*., 2023)

Informações acadêmicas, dados pessoais e plataformas institucionais demandam medidas de proteção eficazes contra os cibercriminosos. Cabe ressaltar que o tratamento sistemático dos riscos se torna parte integrante de uma estrutura organizacional. Essa abordagem está diretamente vinculada à responsabilidade institucional e ao fortalecimento da governança. (Gonçalves, E. *et al*., 2023)

O avanço tecnológico ampliou a dependência de sistemas informatizados para ensino, pesquisa e gestão. Com isso, aumentaram também as vulnerabilidades associadas à privacidade

e à segurança da informação. A adoção de mecanismos formais de identificação e tratamento de riscos contribui para reduzir impactos negativos. Além disso, fortalece a capacidade de resposta diante de incidentes. O gerenciamento de riscos passa, assim, a integrar a estratégia organizacional. (Araújo, A.,2019)

Conforme apontado por Gonçalves, E. *et al. (*2025), a aplicação dessa abordagem vai além do cumprimento de exigências normativas. Envolve a proteção de ativos críticos e a continuidade das atividades acadêmicas e administrativas. A prevenção de falhas e interrupções depende de avaliação constante das ameaças. Essa prática favorece decisões mais fundamentadas. Também amplia a cultura institucional voltada à prevenção.

A gestão de riscos pressupõe etapas estruturadas de identificação, análise e mitigação de ameaças. O objetivo é reduzir a probabilidade de ocorrência e os impactos associados. No ambiente universitário, isso inclui proteção de dados sensíveis e manutenção da integridade dos sistemas. A adoção de controles adequados contribui para estabilidade operacional. Dessa forma, preserva-se a missão social da instituição. (Araújo, A.,2019)

Apesar dos benefícios, a implementação enfrenta desafios internos. Barreiras culturais e limitações operacionais dificultam a consolidação de práticas sistemáticas. Muitas instituições ainda apresentam níveis distintos de maturidade em governança de riscos. A superação dessas limitações requer políticas claras e capacitação contínua. A integração do tema aos processos institucionais é medida necessária. (Cunha e Loose, 2024)

No âmbito normativo, as universidades públicas vinculam-se às diretrizes do Poder Executivo federal. A Instrução Normativa MP/CGU nº 01/2016 e o Decreto nº 9.203/2017 orientam a incorporação do gerenciamento de riscos à estratégia institucional. Esses instrumentos estabelecem parâmetros para fortalecer a governança pública. A conformidade com tais normas contribui para maior transparência. Também reforça a responsabilidade administrativa. (Cunha e Loose, 2024)

Complementarmente, o Programa de Proteção e Segurança da Informação estabelece controles voltados à salvaguarda de dados no âmbito do Executivo. São previstos diversos mecanismos de proteção que dialogam com a gestão de riscos. Contudo, sua efetiva aplicação nas universidades demanda adaptação à realidade local.

O fortalecimento de políticas estruturadas é condição para implementação eficiente. Assim, consolida-se uma gestão mais resiliente e alinhada às exigências contemporâneas. (Gonçalves, E. *et al*., 2023)

Conforme artigo científico de Gonçalves, E. *et al*., (2023), a base conceitual do PPSI apoia-se em referenciais reconhecidos na área de segurança e privacidade da informação. Sua estrutura dialoga com os controles do CIS, com o núcleo do *Privacy Framework do NIST* e com normas ISO/IEC e ABNT NBR. Essa combinação confere consistência técnica ao programa. O alinhamento a padrões consolidados amplia a confiabilidade de sua aplicação. Assim, o modelo adota práticas reconhecidas internacionalmente

O PPSI configura-se como um framework voltado ao fortalecimento da privacidade e da segurança da informação. Seu foco principal está na adequação à Lei Geral de Proteção de Dados e à Política Nacional de Segurança da Informação. Para isso, organiza controles específicos de cibersegurança e proteção de dados. Esses controles são distribuídos em grupos de implementação. Também estão harmonizados com orientações do GSI e da ANPD. (Gonçalves, E. *et al*., 2023)

A estrutura do programa distribui os controles em grupos de implementação, permitindo aplicação gradual e alinhada à realidade institucional. Essa organização favorece planejamento estratégico e priorização de medidas conforme o nível de risco identificado.

Além disso, mantém compatibilidade com orientações emanadas por órgãos reguladores e instâncias governamentais responsáveis pela temática. Tal alinhamento reforça a consistência normativa do programa. (Gonçalves, E. *et al*., 2023)

O programa propõe uma metodologia baseada em ciclos de execução internos e externos, além de favorecer a dinâmica e o acompanhamento contínuo das ações implementadas. Além disso, prevê avaliação do nível de maturidade por meio de indicadores definidos. Tal mecanismo permite mensurar avanços e identificar pontos de melhoria. Dessa forma, o PPSI contribui para evolução gradual e estruturada da governança em segurança da informação.

Segundo Gonçalves, E. *et al* (2023), outro aspecto relevante é a previsão de mensuração do nível de maturidade por meio de indicadores previamente definidos. Esse mecanismo possibilita verificar avanços, identificar fragilidades e direcionar melhorias com base em evidências. A avaliação contínua fortalece a cultura de segurança institucional e contribui para tomada de decisões fundamentadas. Assim, o PPSI favorece evolução progressiva e organizada da governança em segurança da informação.

3.4 Lista de Riscos e Impacto nas Vulnerabilidades nas IES

A detecção de malware em Instituições de Ensino Superior (IES) exige compreensão detalhada dos riscos que incidem sobre o ambiente acadêmico. Universidades concentram

grande volume de dados pessoais, científicos e administrativos, tornando-se alvos estratégicos de ataques digitais.

Conforme demonstrado por Caminha e Susuki (2024), a implementação de sistemas de monitoramento em universidades públicas evidenciou a alta incidência de eventos de segurança relacionados a tentativas de intrusão. Esse cenário reforça a necessidade de mapeamento estruturado de vulnerabilidades. A ausência dessa análise compromete a capacidade preventiva institucional.

O *phishing* permanece entre as ameaças mais recorrentes no ambiente universitário. Trata-se de técnica que explora engenharia social para obtenção de credenciais institucionais. A partir do comprometimento inicial de contas, o invasor pode escalar privilégios e acessar sistemas críticos. A Lei nº 13.709/2018 estabelece dever de proteção de dados pessoais, impondo responsabilidade à instituição em caso de exposição indevida. Assim, falhas de conscientização dos usuários configuram vulnerabilidade relevante.

O *ransomware* representa risco de elevado impacto operacional. Ao criptografar dados acadêmicos e administrativos, compromete matrículas, sistemas financeiros e pesquisas em andamento. Segundo estudos recentes sobre ataques direcionados ao setor público, o pagamento de resgates não garante integral recuperação das informações. Além do prejuízo financeiro, há danos à reputação institucional. A indisponibilidade prolongada compromete a missão acadêmica. (Cheng e Wang, 2022)

Os ataques DDoS afetam diretamente a disponibilidade de serviços digitais. Plataformas de ensino remoto, bibliotecas virtuais e portais institucionais tornam-se inacessíveis diante da sobrecarga de tráfego malicioso. Conforme abordagens técnicas discutidas em pesquisas sobre arquitetura de rede e proteção avançada, a indisponibilidade impacta não apenas a operação interna, mas também a imagem pública da universidade. A continuidade dos serviços depende de infraestrutura resiliente. (Fan, C. et al, 2021)

Falhas de configuração e ausência de atualização de sistemas ampliam a superfície de ataque. Sistemas legados, comuns em universidades públicas, podem conter vulnerabilidades exploráveis. A falta de inventário atualizado de ativos dificulta a gestão de riscos. Cunha e Loose (2024), destacam que a maturidade da gestão de riscos nas universidades brasileiras ainda apresenta variações significativas. Isso evidencia a necessidade de padronização de práticas. O uso de dispositivos pessoais em redes institucionais amplia vetores de ameaça. A política de acesso remoto deve considerar autenticação forte e segmentação de rede. A

arquitetura de Zero Trust, conforme proposta por Rose *et al.* (2020), recomenda verificação contínua de identidade e contexto antes de conceder acesso. Esse modelo reduz o risco de movimentação lateral do invasor. A adoção dessa abordagem fortalece a detecção de comportamentos anômalos.

Riscos internos também merecem análise, pois acessos indevidos realizados por colaboradores, falhas de segregação de funções e ausência de monitoramento ampliam vulnerabilidades e o risco de intrusão maliciosa. A Instrução Normativa MP/CGU nº 01/2016 e o Decreto nº 9.203/2017 reforçam a necessidade de integrar gestão de riscos à estratégia institucional. A prevenção deve abranger ameaças internas e externas. O controle contínuo é essencial. (CGU,2017)

A dependência de fornecedores terceirizados também amplia exposição. Contratos que não estabelecem requisitos claros de proteção de dados criam lacunas. A responsabilidade institucional permanece mesmo quando o serviço é prestado por terceiros. A avaliação prévia de riscos deve integrar processos licitatórios. A governança contratual torna-se componente da segurança.

A ausência de monitoramento centralizado dificulta a detecção precoce de malware. Sistemas de gerenciamento de eventos de segurança permitem correlação de logs e identificação de padrões suspeitos. Caminha e Susuki (2024) demonstram que a implementação de soluções integradas reduz tempo de resposta a incidentes. A detecção rápida minimiza impactos. A centralização fortalece a visão estratégica. A coleta excessiva de dados pessoais amplia responsabilidade institucional. A LGPD determina que o tratamento deve observar finalidade específica e necessidade. Quanto maior o volume de dados armazenados, maior o risco em caso de violação. A gestão adequada do ciclo de vida da informação reduz exposição Brasil (2018).

Em síntese, a detecção de malware nas IES depende do reconhecimento estruturado de riscos. *Phishing, Ransomware* e DDoS configuram ameaças centrais no ambiente acadêmico. A vulnerabilidade decorre tanto de fatores técnicos quanto humanos. A integração entre gestão de riscos e monitoramento contínuo fortalece a proteção institucional. O enfrentamento dessas ameaças exige abordagem sistêmica. (CGU,2017)

3.4.1 Matriz de Riscos Probabilidade X Impacto

A matriz de risco, também conhecida como matriz de probabilidade e impacto, representa um instrumento essencial para a gestão de riscos em segurança cibernética. Sua aplicação permite estruturar e classificar ameaças de acordo com a probabilidade de ocorrência e o

impacto gerado, oferecendo uma visão clara e estratégica do ambiente digital. Com isso, torna-se possível priorizar ações e direcionar recursos para os pontos mais críticos da infraestrutura tecnológica. (Frons, 2020)

No campo da segurança cibernética, a utilização dessa matriz contribui diretamente para a identificação de vulnerabilidades e ameaças importantes, como ataques de malware, phishing e negação de serviço. A partir dessa classificação, as organizações conseguem estabelecer níveis de criticidade, o que facilita a tomada de decisão e a implementação de medidas preventivas mais eficazes. (Frons, 2020)

A visualização proporcionada pela matriz favorece a compreensão rápida dos riscos, permitindo que gestores e equipes técnicas interpretem as informações de forma objetiva. Esse aspecto é fundamental em ambientes corporativos, nos quais a agilidade na resposta a incidentes pode reduzir significativamente os danos causados por ataques cibernéticos.

Outro ponto importante refere-se à priorização de investimentos em segurança da informação. Ao identificar quais riscos apresentam maior probabilidade e impacto, a organização consegue alocar recursos de forma mais eficiente, concentrando esforços em controles que realmente contribuem para a mitigação de ameaças críticas. (Frons, 2020)

A matriz também desempenha papel importante na governança de segurança, pois auxilia na comunicação entre áreas técnicas e estratégicas. Por meio de uma representação visual simplificada, executivos e gestores conseguem compreender o nível de exposição ao risco, o que fortalece o alinhamento entre decisões de negócio e práticas de segurança cibernética. Abaixo a Figura 3.2 mostra a matrix de probabilidade e impacto.

Figura 3.2: Matriz de Probabilidade e Impacto

Probabilidade / Impacto	Sem Impacto	Leve	Médio	Grave	Gravíssimo
Quase certo	Risco Elevado	Risco Elevado	Risco Extremo	Risco Extremo	Risco Extremo
Alta	Risco Moderado	Risco Elevado	Risco Elevado	Risco Extremo	Risco Extremo
Média	Risco Baixo	Risco Moderado	Risco Elevado	Risco Extremo	Risco Extremo
Baixa	Risco Baixo	Risco Baixo	Risco Moderado	Risco Elevado	Risco Extremo
Raro	Risco Baixo	Risco Baixo	Risco Moderado	Risco Elevado	Risco Elevado

Fonte: Frons, 2020

Sob a ótica da prevenção, a ferramenta permite antecipar cenários adversos e estruturar planos de resposta a incidentes. Essa capacidade de antecipação contribui para reduzir o tempo de reação diante de ataques, aumentando a resiliência organizacional e a continuidade dos serviços digitais. (Frons, 2020)

Outro benefício importante está relacionado à conformidade com normas e boas práticas, como frameworks de segurança da informação. A utilização da matriz de risco evidencia a adoção de processos estruturados de análise e tratamento de riscos, o que pode ser determinante em auditorias e certificações.

A aplicação contínua da matriz possibilita o monitoramento da evolução dos riscos ao longo do tempo. Com isso, a organização consegue acompanhar mudanças no cenário de ameaças, ajustando suas estratégias de defesa de acordo com novas vulnerabilidades e tendências do ambiente cibernético. (Frons, 2020)

Em síntese, a matriz de probabilidade e impacto configura-se como uma ferramenta indispensável para a segurança cibernética, pois permite compreender, priorizar e tratar riscos de forma estruturada. Sua utilização fortalece a capacidade de prevenção, resposta e adaptação das organizações diante de um cenário cada vez mais dinâmico e desafiador.

3.4.2 Listagem dos Riscos e Impacto nas Vulnerabilidades de uma IES

A articulação entre gestão de riscos e mecanismos eficazes de detecção constitui fator determinante para a mitigação de impactos em ambientes institucionais complexos. A adoção de monitoramento contínuo possibilita identificar padrões atípicos de comportamento antes que evoluam para incidentes de maior gravidade. A análise correlacionada de eventos e registros de auditoria amplia a capacidade de resposta e favorece decisões baseadas em evidências.

Com isso, reduz-se o tempo de exposição a ameaças e limita-se a extensão de danos operacionais, financeiros e reputacionais. O nível de maturidade em segurança está diretamente associado à integração equilibrada entre tecnologia, processos bem definidos e práticas consolidadas de governança. (Gonçalves, *et al*, 2024)

No contexto das instituições de ensino superior, a diversidade de usuários, sistemas e fluxos informacionais amplia a superfície de ataque e exige abordagem estruturada para identificação de riscos e vulnerabilidades. A ausência de políticas consistentes de controle de acesso, atualização tecnológica e capacitação contínua favorece a exploração de fragilidades técnicas e humanas. (Gonçalves, *et al*, 2024)

Ataques como phishing, ransomware, acessos internos indevidos e indisponibilidade de serviços evidenciam a necessidade de medidas preventivas articuladas. A análise sistemática dos riscos e de seus impactos permite priorizar investimentos, fortalecer controles internos e assegurar maior resiliência institucional diante de ameaças digitais. Abaixo segue a listagem dos riscos, vulnerabilidades e impactos.

1. Phishing

- **Risco:** Obtenção fraudulenta de credenciais institucionais.
- **Vulnerabilidade associada:** Baixo nível de conscientização dos usuários e ausência de autenticação multifator.
- **Impacto:** Acesso indevido a sistemas acadêmicos, vazamento de dados pessoais e possível escalonamento de privilégios.

2. Ransomware

- **Risco:** Criptografia maliciosa de bases de dados institucionais.
- **Vulnerabilidade associada:** Falhas em políticas de backup e ausência de segmentação de rede.
- **Impacto:** Paralisação de serviços, prejuízos financeiros e comprometimento da continuidade acadêmica.

3. Ataques DDoS

- **Risco:** Sobrecarga intencional de servidores e serviços online.
- **Vulnerabilidade associada:** Infraestrutura de rede limitada e ausência de mecanismos de mitigação.
- **Impacto:** Indisponibilidade de plataformas acadêmicas e administrativas.

4. Vazamento de Dados Pessoais

- **Risco:** Exposição indevida de informações sensíveis.
- **Vulnerabilidade associada:** Falhas de controle de acesso e ausência de classificação da informação.
- **Impacto:** Responsabilidade legal, danos a reputação e perda de confiança social.

5. Acessos Internos Indevidos

- **Risco:** Uso inadequado de permissões institucionais.
- **Vulnerabilidade associada:** Falta de segregação de funções e auditoria contínua.
- **Impacto:** Manipulação de dados, fraudes internas e comprometimento da integridade informacional.

6. Sistemas Desatualizados

- **Risco:** Exploração de falhas conhecidas em softwares obsoletos difíceis de atualizar.

- **Vulnerabilidade associada:** Ausência de política de atualização e inventário tecnológico incompleto.
- **Impacto:** Ampliação da superfície de ataque e aumento da probabilidade de intrusão e sequestros de informações sensíveis.

Quadro 3.2 Relação entre Risco, Vulnerabilidade e Impactos nas IES

Nº	Ameaça / Evento de Risco	Descrição do Risco	Vulnerabilidades Associadas	Impactos Institucionais	Nível de Severidade*
1	Phishing	Obtenção fraudulenta de credenciais institucionais por meio de engenharia social.	Baixo nível de conscientização dos usuários; ausência de autenticação multifator; filtros de e-mail insuficientes.	Acesso indevido a sistemas acadêmicos; vazamento de dados pessoais; escalonamento de privilégios e comprometimento da rede interna.	Alto
2	Ransomware	Criptografia maliciosa de bases de dados institucionais com exigência de resgate.	Falhas em políticas de backup; ausência de segmentação de rede; monitoramento ineficiente.	Paralisação de serviços acadêmicos e administrativos; prejuízos financeiros; comprometimento da continuidade institucional.	Crítico
3	Ataques DDoS	Sobrecarga intencional de servidores e serviços online para causar indisponibilidade.	Infraestrutura de rede limitada; ausência de mecanismos de mitigação e balanceamento de carga.	Interrupção de plataformas acadêmicas; impacto em processos seletivos e avaliações; prejuízo à imagem institucional.	Alto
4	Vazamento de Dados Pessoais	Exposição indevida de informações sensíveis de estudantes e servidores.	Falhas de controle de acesso; ausência de classificação da informação; criptografia inadequada.	Responsabilidade legal; danos a reputação à instituição; perda de confiança da comunidade acadêmica.	Alto
5	Acessos Internos Indevidos	Uso inadequado ou excessivo de permissões institucionais por colaboradores.	Falta de segregação de funções; ausência de auditoria contínua; revisão insuficiente de perfis de acesso.	Manipulação ou exclusão de dados; fraudes internas; comprometimento da integridade informacional.	Médio a Alto
6	Sistemas Desatualizados	Exploração de vulnerabilidades conhecidas em softwares legados.	Ausência de política de atualização; inventário tecnológico incompleto; dependência de sistemas antigos.	Ampliação da superfície de ataque; aumento da probabilidade de intrusão e propagação de malware.	Alto

Elaborado pelo Autor (2026).

O quadro apresentado monstra que grande parte das ameaças não ocorre de forma isolada, mas representa a resultante da interação entre fragilidades técnicas e fatores humanos. Sistemas desatualizados, controles insuficientes e falhas de conscientização tendem a se sobrepor, ampliando a probabilidade de incidentes.

Essa dependência mútua, evidencia que a proteção institucional exige abordagem integrada, capaz de tratar simultaneamente infraestrutura, processos e comportamento dos usuários.

A análise conjunta desses elementos permite compreender como pequenas vulnerabilidades podem evoluir para eventos de maior gravidade.

É observado que os riscos classificados como elevados ou críticos costumam comprometer mais de um dos pilares da segurança da informação. Incidentes dessa natureza afetam não apenas a confidencialidade dos dados, mas também sua integridade e disponibilidade. Quando esses três fundamentos são atingidos de forma concomitante (simultânea), os impactos operacionais e reputacionais tornam-se significativamente mais severos. (NIST,2024)

Por essa razão, a gestão de riscos deve concentrar esforços na implementação de controles que assegurem o equilíbrio entre confidencialidade, integridade e disponibilidade, garantindo proteção sistêmica e contínua. Embora segurança da informação e privacidade possuam fundamentos conceituais próprios e escopos distintos, há pontos de convergência relevantes, especialmente quando se trata da proteção de dados pessoais e da mitigação de incidentes.

Em diversas situações, medidas voltadas à segurança técnica também contribuem para a preservação da privacidade, assim como práticas de governança de dados reforçam a postura de segurança institucional. Essa inter-relação evidencia que a atuação coordenada entre ambas as disciplinas é indispensável para assegurar conformidade normativa, reduzir vulnerabilidades e fortalecer a resiliência organizacional (NIST,2024). Apesar do Risco a Segurança e Privacidade sejam disciplinas independentes seus objetivos se sobrepõem em determinadas circunstância de acordo com a Figura 3.3 ilustrada abaixo:

Figura 3.3: Relação entre Segurança Cibernética e Risco de Privacidade

Fonte: NIST, 2024.

A inclusão de uma coluna no Quadro 3 referindo a vinculação normativa à Lei Geral de Proteção de Dados Pessoais (LGPD) e ao Programa de Privacidade e Segurança da Informação (PPCI), esta análise dos riscos ao estabelecer correspondência direta entre ameaças identificadas e obrigações regulatórias aplicáveis fortalece o entendimento do sistema. Esse alinhamento evidencia que a gestão de vulnerabilidades não se limita ao campo técnico, mas também envolve responsabilidade jurídica e conformidade institucional. (MGI,2024)

A avaliação dos riscos deverá ser conduzida por equipes técnicas multidisciplinares, compostas por profissionais com conhecimento especializado e experiência no contexto analisado. Essa abordagem assegura maior confiabilidade e consistência na identificação dos eventos de risco, bem como na modelagem dos critérios de probabilidade de ocorrência e do nível de impacto associado, considerando aspectos operacionais, técnicos, financeiros, legais e organizacionais. (CGU,2017)

Entretanto a utilização de escalas padronizadas de probabilidade e impacto é de suma relevância e possibilita a uniformização das análises. Além de reduzir a subjetividade inerente ao processo avaliativo e contribui sistematicamente para a construção de matrizes de risco mais precisas e eficazes. Dessa forma, torna-se possível estabelecer prioridades de tratamento, orientar a alocação de recursos e fortalecer os mecanismos de controle e mitigação. (CGU,2017)

Os Quadros 3.3 e 3.4 apresentam, respectivamente, a Escala de Probabilidade e a Escala de Impacto, as quais servem como referência metodológica para a classificação e mensuração dos riscos identificados no presente estudo.

Quadro 3.3 Escala de Probabilidade

Probabilidade	**Descrição da probabilidade, desconsiderando os controles**	**Peso**
Muito Baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

Fonte: CGU, 2017

O Quadro 3.4 apresenta a Escala de Impacto, a qual estabelece critérios técnicos para mensurar a severidade das consequências decorrentes da materialização de um evento de intrusão. Essa escala permite avaliar os efeitos adversos sobre a confidencialidade, integridade e disponibilidade das informações e dos ativos organizacionais. Além disso, fornece subsídios para classificar o nível de criticidade do incidente, considerando possíveis prejuízos operacionais, financeiros, legais e reputacionais.

A partir dessa classificação, torna-se possível definir respostas proporcionais e adequadas, incluindo ações de contenção, mitigação e recuperação. Dessa forma, a Escala de Impacto constitui um instrumento fundamental para orientar a tomada de decisão e fortalecer a capacidade de resposta frente a incidentes de segurança.

Quadro 3.4. Escala de Impacto

Probabilidade	**Descrição da probabilidade, desconsiderando os controles**	**Peso**
Muito Baixa	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/ divulgação ou de conformidade).	1
Baixa	Pequeno impacto nos objetivos.	2
Média	Moderado impacto nos objetivos, porém recuperável.	5
Alta	Significativo impacto nos objetivos, reversão difícil.	8
Muito alta	Catastrófico impacto nos objetivos, reversão forma irreversível.	10

Fonte: CGU, 2017

De acordo com a CGU (2017), o nível do risco inerente é determinado a partir da combinação entre a probabilidade de ocorrência do evento e a magnitude do impacto associado. Esse cálculo, geralmente realizado por meio da multiplicação desses dois fatores, permite estimar a criticidade do risco em seu estado bruto.

Nessa condição, não são considerados os mecanismos de controle existentes ou potenciais que possam mitigar ou reduzir seus efeitos. Dessa forma, o risco inerente representa a exposição original da organização diante de uma ameaça específica. Essa mensuração é fundamental para subsidiar a priorização de riscos e orientar a definição de estratégias adequadas no tratamento e controle. (CGU, 2017)

Segue a formula dos Níveis de Riscos e Probabilidades:

RI = NP x NI

Em que:

RI = nível do risco inerente

NP = nível de probabilidade do risco

NI = nível de impacto do risco

Após a determinação do nível de risco, obtido pela combinação entre os valores atribuídos à probabilidade de ocorrência e ao impacto do evento, torna-se possível estabelecer sua classificação quanto ao grau de criticidade. Essa classificação é realizada com base em faixas de referência previamente definidas, que permitem categorizar o risco em diferentes níveis, como baixo, médio, alto ou crítico.

Tal categorização possibilita uma análise estruturada e padronizada, favorecendo a priorização dos riscos que demandam maior atenção e resposta imediata. Além disso, contribui para o direcionamento eficiente dos recursos e das estratégias de mitigação. Nesse contexto, o Quadro 3.5 apresenta as faixas de classificação utilizadas como parâmetro para o enquadramento do nível de risco identificado.

Quadro 3.5 Classificação do Risco

Classificação	Faixa
Risco Baixo - RB	0 – 9,99
Risco Médio - RM	10 – 39,99
Risco Alto - RA	40 – 79,99
Risco Extremo - RE	80 – 100

Fonte: CGU, 2017

Ao relacionar cada risco aos dispositivos legais e aos controles previstos no programa, amplia-se a clareza quanto às medidas exigidas e às consequências do descumprimento. Tal representação facilita a compreensão sistêmica do risco e orienta a priorização de controles preventivos e corretivos. (Gonçalves, *et al*, 2024) Abaixo segue o Quadro 3.6:

Quadro 3.6. Relação entre Risco, Vulnerabilidade e Impactos e Vinculação Normativa nas IES

Nº	Ameaça / Evento de Risco	Vulnerabilidades Associadas	Impactos Institucionais	Dispositivos LGPD Relacionados	Controle do PPSI Relacionadas
1	Phishing	Baixo nível de conscientização; ausência de autenticação multifator	Acesso indevido; vazamento de dados; escalonamento de privilégios	Art. 6º (princípio da prevenção); Art. 46 (medidas de segurança)	Controle de gestão de identidades; autenticação forte; capacitação contínua

2	Ransomware	Falhas em backup; ausência de segmentação de rede	Paralisação de serviços; prejuízo financeiro; indisponibilidade de dados	Art. 46 (segurança); Art. 48 (comunicação de incidente)	Plano de resposta a incidentes; política de backup e recuperação
3	Ataques DDoS	Infraestrutura limitada; ausência de mitigação	Indisponibilidade de plataformas acadêmicas	Art. 6º (prevenção); Art. 46 (proteção contra acessos não autorizados)	Monitoramento contínuo; gestão de continuidade de serviços
4	Vazamento de Dados Pessoais	Falhas de controle de acesso; ausência de classificação da informação	Responsabilidade legal; danos reputacionais	Art. 6º (necessidade e finalidade); Art. 42 (responsabilização)	Classificação da informação; controle de acesso baseado em risco
5	Acessos Internos Indevidos	Falta de segregação de funções; auditoria insuficiente	Fraudes internas; manipulação de dados	Art. 6º (responsabilização); Art. 46 (proteção administrativa)	Segregação de funções; auditorias periódicas; revisão de perfis
6	Sistemas Desatualizados	Ausência de política de atualização; inventário incompleto	Ampliação da superfície de ataque; maior probabilidade de intrusão	Art. 46 (medidas técnicas adequadas)	Gestão de ativos; atualização e gestão de vulnerabilidades

Elaborado pelo Autor (2026).

A LGPD estabelece o dever de prevenir danos e adotar medidas capazes de resguardar informações pessoais contra acessos indevidos e situações acidentais. Além disso, prevê responsabilização em caso de falhas na proteção. Esse comando normativo impõe postura ativa das instituições no tratamento dos riscos digitais. A prevenção deixa de ser faculdade administrativa e assume caráter obrigatório e técnico. Assim, a proteção de dados passa a compor a agenda estratégica da governança (Brasil,2018).

Já o PPSI, por sua vez, traduz essas exigências em controles organizados e mecanismos de acompanhamento contínuo. Sua estrutura contempla diretrizes voltadas à mitigação de ameaças e à avaliação periódica do nível de maturidade institucional. Ao operacionalizar os deveres legais, o programa fornece instrumentos concretos para implementação das medidas necessárias. Isso permite que a conformidade seja monitorada de forma sistemática. A integração entre norma e prática fortalece a efetividade das ações. (Brasil,2023)

O artigo 46 da legislação de proteção de dados assume posição central nesse contexto ao determinar a adoção de medidas técnicas e administrativas aptas a proteger dados pessoais. Tal dispositivo consolida o princípio da prevenção como fundamento da segurança informacional.

Sua aplicação exige controles proporcionais aos riscos identificados. Dessa maneira, a análise de vulnerabilidades deve ser contínua e documentada. O cumprimento desse artigo representa base jurídica da política de segurança. (Brasil,2018)

No âmbito operacional, o programa detalha instrumentos como controle de acessos, monitoramento de eventos, gestão de ativos e procedimentos de resposta a incidentes. Esses mecanismos estruturam a atuação preventiva e corretiva diante de ameaças digitais.

A definição clara de responsabilidades e fluxos de atuação contribui para maior eficiência na contenção de danos. A mensuração de maturidade permite identificar fragilidades e promover melhorias graduais ao processo tornando-o, assim, dinâmico e orientativo. (Brasil,2023)

A articulação entre os dispositivos legais e os programas institucionais estabelece uma base sólida para a prevenção e a identificação de incidentes de segurança nas instituições de ensino superior. Esse alinhamento promove a integração entre diretrizes normativas e práticas operacionais, fortalecendo os mecanismos de proteção digital. Nesse cenário, o enfrentamento de ameaças como malware passa a ocorrer de forma estruturada e contínua. As ações deixam de ser pontuais e passam a integrar o planejamento estratégico institucional. Como resultado, a proteção informacional torna-se parte essencial da gestão da IES.

A segurança da informação deixa de ser atribuição exclusiva das equipes técnicas e passa a envolver diferentes níveis organizacionais. Esse processo amplia a responsabilidade institucional e favorece a adoção de práticas coordenadas entre setores acadêmicos e administrativos.

A participação da alta administração torna-se indispensável para garantir recursos e direcionamento adequado. Essa atuação contribui para consolidar políticas e procedimentos alinhados às exigências normativas. Dessa forma, a segurança passa a ser compreendida como responsabilidade compartilhada. (Gonçalves, et al, 2024)

Esse alinhamento também contribui para o fortalecimento da cultura organizacional voltada à proteção da informação. A adoção de diretrizes formais promove maior conscientização sobre riscos e responsabilidades associadas ao uso de sistemas institucionais. Esse movimento favorece a prevenção de incidentes e reduz a exposição a ameaças digitais.

A governança informacional passa a exercer papel estruturante na condução das atividades institucionais. Como consequência, a tomada de decisão torna-se mais segura e fundamentada.

Esse processo fortalece a continuidade dos serviços acadêmicos e administrativos. Além disso,amplia a confiabilidade das informações sob sua responsabilidade. Conforme destacado por Gonçalves *et al.* (2024), esse alinhamento promove o fortalecimento organizacional.

3.5 Boas Práticas Privacidade e Segurança PPSI em uma IES

As boas práticas de segurança da informação nas Instituições de Ensino Superior públicas exigem alinhamento simultâneo às normas nacionais e aos referenciais internacionais. Crescentes incidências de ataques como *phishing, ransomware* e DDoS evidencia que medidas isoladas não são suficientes para garantir proteção adequada dos ativos digitais de uma organização.

Os instrumentos normativos como a LGPD, a ISO/IEC 27701 e o PPSI estabelecem diretrizes estruturantes para governança e conformidade. A integração dessas referencias fortalece a capacidade institucional de prevenir, detectar e responder a incidentes cibernéticos. A maturidade em segurança depende da internalização sistemática dessas práticas.

A Lei Geral de Proteção de Dados Pessoais estabelece princípios como finalidade, necessidade, prevenção e responsabilização, que orientam o tratamento adequado de dados pessoais. Para as universidades públicas, isso implica implementar controles técnicos e administrativos capazes de reduzir riscos de vazamento e acesso indevido (Brasil,2018).

Ela exige adoção de medidas aptas a proteger informações contra incidentes de segurança, o que inclui mecanismos de detecção de malwares e monitoramento contínuo das redes. A conformidade normativa não se limita ao aspecto jurídico, mas envolve reorganização de processos internos. Dessa forma, a proteção de dados passa a integrar a estratégia institucional.

No âmbito internacional, a ISO/IEC 27701 amplia o sistema de gestão de segurança ao incorporar requisitos específicos de privacidade. Essa norma complementa estruturas tradicionais de segurança ao definir controles voltados ao gerenciamento de informações pessoais. (ISO/IEC 27701,2025)

Sua adoção contribui para padronização de procedimentos, definição clara de papéis e avaliação periódica de riscos. Para as IES, o alinhamento a esse padrão fortalece a governança e demonstra comprometimento com boas práticas reconhecidas globalmente. A certificação ou adoção parcial de seus controles eleva o nível de confiança institucional.

No setor público federal, o Programa de Privacidade e Segurança da Informação estrutura

diretrizes específicas para órgãos e entidades da administração pública. O programa organiza controles em grupos de implementação e estabelece metodologia de avaliação de maturidade. Essa abordagem permite identificar lacunas e priorizar ações corretivas conforme o nível de risco. Para as universidades públicas, o PPSI funciona como guia operacional para consolidação de políticas internas. A padronização promovida pelo programa fortalece a integração entre tecnologia e gestão. (BRASIL, 2023)

Entre as boas práticas recomendadas destaca-se a classificação da informação. A identificação de níveis de sensibilidade permite aplicar controles proporcionais ao grau de risco associado a cada tipo de dado. Informações acadêmicas estratégicas e dados pessoais sensíveis exigem proteção reforçada. Ao realizar a classificação adequada do sistema, esta contribui para definição de políticas de retenção e descarte seguro. Esse procedimento reduz exposição desnecessária e fortalece a prevenção. (CGU,2107)

A autenticação multifator é medida essencial para mitigar riscos de *phishing.* O controle de acessos baseado no princípio do menor privilégio limita impactos. A revisão periódica de permissões evita excessos. A implementação de arquitetura Zero Trust, conforme Rose et al. (2020) e Santos Jr. et al. (2024), reforça verificação contínua. Essa abordagem fortalece a segurança em ambientes distribuídos.

A gestão de identidades e acessos constitui outra prática essencial. A aplicação do princípio do menor privilégio limita a concessão de permissões apenas ao necessário para execução das funções institucionais. A autenticação reduz significativamente o risco de comprometimento de credenciais por *phishing.* A revisão periódica de perfis evita acúmulo indevido de acessos ao longo do tempo. Esse controle é determinante para mitigar ataques que exploram falhas humanas. (Ulver e Wanger, 2021)

A implementação de monitoramento contínuo e centralizado amplia a capacidade de detecção de *malware*. Sistemas de gerenciamento de eventos de segurança permitem correlacionar registros e identificar padrões anômalos. A análise preventiva possibilita resposta rápida antes que o incidente cause danos extensivos. Essa prática está alinhada ao princípio da prevenção previsto na legislação nacional. A detecção tempestiva reduz impactos operacionais e reputacionais. (Caminha e Suzuki, 2024)

A manutenção de políticas estruturadas de backup e recuperação de desastres representa medida crítica contra *ransomware.* Cópias de segurança periódicas e armazenadas de forma

segregada garantem possibilidade de restauração sem pagamento de resgates. Testes regulares de recuperação asseguram efetividade do plano de contingência. A ausência desses procedimentos amplia vulnerabilidade institucional. A continuidade dos serviços acadêmicos depende dessa preparação. (Cheng e Wang, 2022)

A capacitação permanente de servidores e estudantes complementa as medidas técnicas. A conscientização reduz a probabilidade de sucesso de ataques baseados em engenharia social. Programas educativos fortalecem cultura organizacional voltada à segurança. A dimensão humana deve ser tratada como elemento estratégico da defesa digital. A integração entre tecnologia e comportamento institucional é indispensável. (Cunha e Loose, 2024)

A realização de avaliações periódicas de risco consolida o ciclo de melhoria contínua. Auditorias internas verificam aderência às normas e identificam oportunidades de aperfeiçoamento. Indicadores de maturidade permitem mensurar evolução institucional ao longo do tempo. O alinhamento entre planejamento estratégico e segurança da informação fortalece governança digital. A atualização constante das práticas assegura resiliência diante de novas ameaças. (Gonçalves, E. *et al*., 2023)

Em suma, a incorporação das diretrizes da Lei Geral de Proteção de Dados Pessoais, da ISO/IEC 27701 e do Programa de Privacidade e Segurança da Informação fornece base normativa consistente para o fortalecimento da segurança nas Instituições de Ensino Superior públicas. A adoção integrada dessas referências promove proteção de dados, aprimora governança e amplia capacidade de detecção de malware. A consolidação dessas boas práticas contribui para sustentabilidade institucional e conformidade legal.A segurança da informação, nesse contexto, assume caráter estruturante e estratégico.

Quadro 3.7. Comparação entre LGPD x ISSO/IEC 27701 x PPCI em uma IES

Critério de Análise	**LGPD**	**ISO/IEC 27701**	**PPSI**
Natureza Jurídica	Lei federal brasileira de aplicação obrigatória a órgãos públicos e privados.	Norma internacional voluntária, passível de certificação.	Programa normativo obrigatório no âmbito do Poder Executivo Federal.
Finalidade Principal	Proteger direitos fundamentais de liberdade e privacidade,	Estabelecer sistema de gestão de informações de privacidade	Estruturar diretrizes e controles para proteção de dados e
	disciplinando o tratamento de dados pessoais.	integrado à segurança da informação.	segurança no setor público federal.

Abrangência Institucional	Todas as organizações que tratam dados pessoais no Brasil.	Organizações que desejam implementar sistema formal de gestão de privacidade.	Órgãos e entidades da administração pública federal direta, autárquica e fundacional.
Foco na Gestão de Riscos	Determina adoção de medidas técnicas e administrativas aptas a proteger dados pessoais.	Estrutura avaliação sistemática de riscos à privacidade e à segurança da informação.	Prevê metodologia de implementação com avaliação de maturidade e priorização de riscos.
Tratamento de Incidentes	Exige comunicação à autoridade competente e aos titulares quando houver risco relevante.	Define procedimentos documentados de resposta e registro de incidentes.	Estabelece diretrizes para gestão e resposta a incidentes no setor público.
Responsabilização e Governança	Prevê responsabilização administrativa, civil e sanções.	Define papéis e responsabilidades no sistema de gestão.	Estrutura governança institucional com definição de responsabilidades formais.
Controles Técnicos	Não detalha tecnicamente os controles, mas exige proteção adequada.	Especifica controles organizacionais e técnicos alinhados à gestão da informação.	Detalha controles organizados em grupos de implementação e níveis de maturidade.
Certificação / Conformidade	Não há certificação formal, mas pode haver comprovação de conformidade.	Permite certificação por organismo acreditado.	Não prevê certificação, mas avaliação interna de maturidade institucional.
Aplicação à Detecção de Malware	Fundamenta juridicamente a necessidade de monitoramento e prevenção.	Estrutura controles formais de monitoramento e gestão de incidentes.	Orienta implementação prática de mecanismos de detecção e resposta no setor público.
Impacto Estratégico nas IES	Impõe dever legal de proteção e responsabilização institucional.	Eleva padrão de governança e credibilidade internacional.	Padroniza práticas e fortalece alinhamento à política nacional de segurança.

Elaborado pelo Autor (2026).

A comparação expressa no quadro acima, demonstra que a LGPD estabelece a base jurídica obrigatória, impondo dever de proteção de dados pessoais e responsabilização em caso de falhas. Contudo, a lei não detalha tecnicamente como implementar os controles, exigindo que as instituições adotem referenciais complementares. Nesse ponto, a ISO/IEC 27701 fornece estrutura metodológica robusta para organização dos processos de privacidade, permitindo padronização e melhoria contínua.

O PPSI, por sua vez, atua como instrumento de operacionalização no âmbito da administração pública federal. Ele traduz princípios legais e boas práticas internacionais em controle e práticas adaptadas ao contexto governamental brasileiro. Para as Instituições de Ensino Superior públicas federais, o PPSI funciona como elo entre exigência legal e aplicação técnica concreta.

Dessa forma, as três referências não competem entre si, mas se complementam. A LGPD estabelece a obrigação jurídica, a ISO/IEC 27701 oferece a arquitetura gerencial e o PPSI adapta e operacionaliza no setor público federal. A integração dessas três dimensões fortalece a governança digital nas universidades e amplia a capacidade de prevenção, detecção e resposta a ataques cibernéticos.

3.5.1Maturidade Normativa e Desafios de Implementação nas IES

A consolidação da segurança da informação nas universidades públicas brasileiras revela um cenário de avanço normativo acompanhado por desafios operacionais significativos. A existência de marcos regulatórios como a Lei Geral de Proteção de Dados Pessoais, a ISO/IEC 27701 e o Programa de Privacidade e Segurança da Informação demonstra que o arcabouço jurídico e técnico encontra-se relativamente consolidado.

Entretanto, a maturidade normativa não implica, automaticamente, maturidade operacional. A distância entre prescrição normativa e prática institucional constitui um dos principais obstáculos à efetiva proteção contra ameaças como *phishing, ransomware* e DDoS. Essa dissociação evidencia necessidade de integração mais profunda entre governança e execução técnica. **(**Bilal, H. *et al*. 2021)

Sob a perspectiva normativa, a LGPD impõe dever legal inequívoco de adoção de medidas técnicas e administrativas aptas a proteger dados pessoais. No entanto, muitas universidades ainda enfrentam limitações estruturais relacionadas a orçamento, pessoal qualificado e infraestrutura tecnológica. A exigência legal de prevenção e mitigação de incidentes demanda investimentos contínuos em monitoramento, controle de acessos e resposta a incidentes. (BRASIL,2018)

Em instituições caracterizadas por autonomia acadêmica e descentralização administrativa, a uniformização de políticas torna-se complexa. Assim, a conformidade formal nem sempre se traduz em proteção efetiva.

A adoção da ISO/IEC 27701 representa avanço metodológico ao estruturar sistema de gestão integrado à privacidade. Contudo, sua implementação requer cultura organizacional orientada a processos, documentação e auditorias periódicas. Muitas universidades públicas brasileiras operam com sistemas legados e estruturas fragmentadas, dificultando padronização de procedimentos. (ISO/IEC 27701,2025)

A ausência de inventário completo de ativos e fluxos de dados compromete avaliação precisa

de riscos. Dessa forma, o desafio não reside apenas na adoção do referencial, mas na internalização de sua lógica de gestão contínua. A rotatividade de estudantes e colaboradores amplia necessidade de treinamento permanente. Sem cultura consolidada de segurança, os controles técnicos tornam-se insuficientes.

O PPSI, por sua vez, apresenta abordagem adaptada ao setor público federal, com diretrizes claras e metodologia de avaliação de maturidade. Ainda assim, sua aplicação depende de engajamento da alta administração e de comitês de governança digital efetivamente atuantes. Em algumas instituições, a segurança da informação permanece concentrada em setores técnicos, sem integração plena ao planejamento estratégico. (BRASIL,2023)

Essa fragmentação limita capacidade de resposta coordenada a incidentes complexos. A maturidade institucional exige liderança comprometida e visão sistêmica. Outro desafio relevante refere-se à dimensão humana da segurança. Ataques de engenharia social exploram vulnerabilidades comportamentais, que não são solucionadas apenas com normativos e tecnologias. Programas de capacitação contínua ainda são incipientes em parte das universidades públicas. (CGU,2017)

Adicionalmente, a limitação orçamentária imposta às instituições públicas impacta diretamente a capacidade de modernização tecnológica. A implementação de sistemas avançados de monitoramento, segmentação de redes e análise comportamental demanda recursos financeiros significativos. Em muitos casos, prioridades acadêmicas competem com investimentos em segurança digital. Essa tensão estrutural influencia o ritmo de evolução da maturidade institucional. (BRASIL,2024)

A governança digital também enfrenta desafios decorrentes da descentralização universitária. Campi distribuídos geograficamente e unidades acadêmicas autônomas adotam práticas heterogêneas de tecnologia da informação. Essa diversidade dificulta padronização de políticas e controles. A consolidação de diretrizes institucionais exige articulação entre reitoria, pró-reitorias e setores técnicos. A coordenação intersetorial torna-se fator crítico de sucesso.

Além dessas limitações, observa-se que a gestão de riscos nas IES ainda evolui de forma tímida e insuficiente, sem avanços consistentes em sua plena institucionalização. Embora iniciativas como a designação de encarregados de dados, a criação de comitês de segurança e a formalização de políticas indiquem um movimento de adequação normativa, tais medidas ainda não se traduzem, de maneira efetiva, em práticas consolidadas.

A incorporação de métricas de maturidade e indicadores de desempenho, quando presente, ocorre de forma incipiente, limitando o monitoramento contínuo. Nesse contexto, apesar da tendência de integração entre conformidade legal e práticas técnicas, o amadurecimento institucional permanece lento e aquém das demandas atuais. (BRASIL, 2024)

No contexto da detecção de *malware*, a maturidade normativa fornece base indispensável, mas sua eficácia depende de implementação concreta. A proteção contra *phishing* exige autenticação robusta e educação digital. A mitigação de *ransomware* depende de políticas estruturadas de backup e segmentação de rede. A prevenção de DDoS demanda infraestrutura resiliente e monitoramento ativo. A norma orienta, mas a execução determina resultados. (Zhang, X. *et al* 2024)

Em síntese, as universidades públicas brasileiras encontram-se em processo de transição entre conformidade formal e maturidade operacional plena. O arcabouço normativo está estabelecido, porém sua efetividade depende de investimentos, capacitação e integração estratégica.

A consolidação da governança de Tecnologia da Informação requer compromisso institucional permanente. A superação dos desafios identificados fortalecerá a capacidade de prevenção, detecção e resposta a incidentes cibernéticos. A maturidade normativa somente se concretiza quando traduzida em prática organizacional consistente. (BRASIL,2023)

3.6 Governança: Conceito e Interpretação a Detecção de Malware

A governança digital pode ser compreendida como estrutura de direção e controle voltada ao uso estratégico da tecnologia no setor público. Seu objetivo é alinhar recursos tecnológicos às finalidades institucionais. No contexto das IES, envolve proteção de dados acadêmicos e administrativos. A Estratégia Nacional de Governo Digital (2024) reforça essa diretriz. A segurança integra essa estrutura.

A Lei nº 13.709/2018 estabelece bases para proteção de dados pessoais. A governança digital deve incorporar seus princípios. Transparência, responsabilidade e prevenção tornam-se pilares. A conformidade fortalece legitimidade institucional. A gestão adequada da informação sustenta confiança social. Uma boa gestão de riscos constitui elemento central da governança digital.

Segundo Cunha e Loose (2024) destacam desafios na maturidade das universidades públicas brasileiras. A integração entre planejamento estratégico e segurança fortalece prevenção. A análise sistemática de ameaças orienta decisões. A governança depende de visão integrada.

A arquitetura Zero Trust, conforme Rose et al. (2020), reforça conceito de verificação contínua. Essa abordagem redefine modelo tradicional de confiança em redes internas. A segmentação e autenticação constante reduzem riscos. A governança digital deve incorporar tais princípios. A inovação deve estar alinhada à proteção.

Com implementação de sistemas de gerenciamento de eventos fortalece governança operacional. Caminha e Susuki (2024) demonstram benefícios na centralização de logs. A visibilidade ampliada facilita detecção de malware. O monitoramento contínuo integra estratégia institucional. A prevenção torna-se proativa.

Entretanto a governança digital requer a definição clara de responsabilidades, com a alta administração assumindo papel central na liderança das políticas de segurança institucional. A atuação de comitês especializados fortalece a coordenação, qualifica as discussões e contribui para decisões mais consistentes e estratégicas. A padronização de processos reduz custos operacionais, minimiza inconsistências e aumenta a eficiência organizacional.

Em suma, governança digital representa estrutura estratégica que integra segurança, conformidade e inovação. No contexto da detecção de malware em IES, sua aplicação fortalece prevenção e resposta a incidentes. A articulação entre normas, tecnologia e gestão reduz vulnerabilidades. O alinhamento às referências legais e técnicas sustenta proteção duradoura. A consolidação dessa estrutura é requisito para resiliência institucional.

4 – RESULTADOS E DISCUSSÕES

4.1 Fonte de Dados Utilizado no Trabalho

Inicialmente, foram estabelecidos os critérios metodológicos que orientaram o processo de identificação das publicações pertinentes ao tema investigado. Para isso, selecionaram-se bases de dados consolidadas e amplamente reconhecidas no meio acadêmico internacional. Essas plataformas foram escolhidas em razão da qualidade dos periódicos indexados e do rigor dos processos editoriais. O acesso a estudos possibilita maior confiabilidade e consistência ao conjunto bibliográfico adotado, o que reforça a robustez e a credibilidade dos resultados obtidos na pesquisa.

Nesse sentido, optou-se pela utilização das bases Web of Science, em sua coleção principal, e IEEE Xplore, ambas reconhecidas pela consistência e relevância científica. Essas bases reúnem publicações oriundas de periódicos e eventos acadêmicos de elevado impacto. Adicionalmente, oferecem recursos avançados de refinamento e organização dos resultados. Nesse sentido, sua escolha contribuiu diretamente para a qualidade da amostra selecionada, resultando em maior precisão na identificação dos estudos mais relevantes.

Em seguida, realizou-se a etapa de coleta e mineração dos dados disponíveis nessas plataformas, respeitando critérios previamente definidos. Esse procedimento ocorreu entre os dias 07 de outubro de 2025 e 12 de janeiro de 2026, período destinado à consolidação das informações. Para viabilizar esse processo, foram aplicadas estratégias estruturadas de busca, com o uso de operadores lógicos e descritores técnicos específicos. Com isso, foi possível delimitar os resultados de acordo com o escopo da pesquisa. Desse modo, assegurou-se maior aderência entre os estudos selecionados e os objetivos do trabalho.

Posteriormente, foi conduzida a análise quantitativa dos registros obtidos em cada uma das bases consultadas. A base Web of Science apresentou um total de 400 publicações relacionadas ao tema investigado, enquanto a IEEE Xplore retornou 355 registros dentro dos critérios estabelecidos. Esse quantitativo evidencia a expressiva produção científica voltada à segurança digital, bem como o crescente interesse da comunidade acadêmica nessa área do conhecimento.

Ao término dessa etapa, os dados coletados constituíram uma base consistente para o desenvolvimento da revisão sistemática proposta. Esse conjunto de publicações permitiu identificar tendências, lacunas e contribuições significativas no campo investigado. Ademais,

possibilitou a construção de uma análise fundamentada em evidências científicas consolidadas.

4.2 ETAPA I: Planejamento da Pesquisa

A etapa inicial da revisão bibliográfica consiste na definição adequada das palavras-chave que irão orientar a busca científica. Essa escolha é determinante, pois influencia diretamente a quantidade e a qualidade dos resultados obtidos.

Quando os termos são mal definidos, há risco de recuperar registros irrelevantes ou de não identificar estudos importantes. Nessa perspectiva, a seleção criteriosa dos descritores configura-se como um fator essencial para a consistência metodológica, contribuindo diretamente para a precisão e a confiabilidade da pesquisa.

As bases de dados disponibilizam operadores lógicos que permitem refinar e combinar os termos de busca. Os operadores “AND” e “OR” são amplamente utilizados para ampliar ou restringir os resultados conforme o objetivo do pesquisador.

O operador “AND” reduz os resultados ao exigir que ambos os termos estejam presentes. (Mariano e Rocha, 2017) Em contrapartida, o operador “OR” amplia o alcance ao incluir registros que contenham qualquer um dos termos definidos, o que torna a estratégia de busca mais eficiente.

De forma equivalente, o uso de aspas em expressões compostas é recomendado para garantir maior precisão, pois assegura que a base de dados identifique a expressão completa, e não apenas palavras isoladas. (Mariano e Rocha, 2017)

Em decorrência disso, os resultados tendem a apresentar maior aderência ao tema investigado. Tal procedimento mostra-se particularmente relevante em áreas técnicas, nas quais termos compostos possuem significado específico. Nesse sentido, o uso adequado desse recurso contribui para maior exatidão na recuperação dos registros.

Ademais, algumas áreas do conhecimento dispõem de plataformas específicas para padronização de descritores científicos. Essas ferramentas auxiliam na identificação de termos reconhecidos e amplamente utilizados na literatura. A título de exemplo, determinadas bases oferecem vocabulários estruturados que favorecem a uniformidade das buscas. Esse processo reduz ambiguidades e aprimora a qualidade dos resultados obtidos, fortalecendo, assim, a consistência da revisão. (Mariano e Rocha, 2017)

Outra estratégia pertinente consiste na análise prévia de artigos diretamente relacionados ao

tema estudado. A partir dessa leitura, o pesquisador pode identificar palavras-chave empregadas por outros autores, permitindo alinhar a busca à terminologia adotada na literatura científica. Adicionalmente, tal procedimento amplia a abrangência da pesquisa e reduz o risco de omissões significativas. Desse modo, a análise de estudos anteriores favorece a construção de uma base mais consistente. (Mariano e Rocha, 2017)

O recorte temporal também representa um elemento fundamental no processo de busca bibliográfica. A definição do período possibilita delimitar a análise e priorizar estudos mais recentes e pertinentes. Bases de dados distintas apresentam coberturas temporais variadas, o que exige atenção do pesquisador. Em razão disso, torna-se necessário manter o mesmo intervalo cronológico em todas as plataformas utilizadas, assegurando maior uniformidade e comparabilidade dos resultados obtidos.

Atualmente, observa-se que grande parte das revisões científicas prioriza publicações dos últimos cinco a dez anos. Essa prática busca contemplar avanços recentes e acompanhar a evolução do conhecimento na área, bem como identificar tendências emergentes e novas abordagens metodológicas. Tal recorte contribui para manter a atualidade e a pertinência da análise, reforçando a qualidade da revisão bibliográfica. (Mariano e Rocha, 2017)

Outro aspecto importante refere-se à seleção das bases de dados a serem utilizadas no estudo. Cada plataforma possui características específicas e maior aderência a determinadas áreas do conhecimento. Nesse contexto, é fundamental que o pesquisador justifique a escolha com base na temática investigada, uma vez que essa decisão influencia diretamente a abrangência e a qualidade dos registros recuperados. Assim sendo, a seleção criteriosa das bases contribui para maior robustez metodológica. (Mariano e Rocha, 2017)

Entre as principais bases utilizadas em pesquisas científicas destacam-se a Web of Science, a IEEE Xplore e a Scopus. Essas plataformas são reconhecidas internacionalmente pela qualidade e consistência de seus registros, além de reunirem publicações revisadas por pares e indexadas em periódicos de alto impacto. Tal característica eleva a confiabilidade das informações coletadas e fortalece a consistência e a credibilidade da revisão.

No presente estudo, foram aplicados critérios adicionais de refinamento com o objetivo de aprimorar os resultados de forma sistemática. Inicialmente, delimitou-se o período de publicação entre os anos de 2021 e 2025, priorizando estudos atualizados e alinhados às demandas contemporâneas da segurança digital. Foram empregados filtros relacionados ao número de citações e à aderência temática, o que possibilitou reduzir a inclusão de registros

pouco significativos.

Para chegar no resultado, foram utilizadas palavras-chave diretamente relacionadas ao escopo da pesquisa.

Tabela 4.1 Termos para pesquisa avançada

Base de Dados	Termos da Pesquisa	Resultados
Web of Science	("phishing" OR "ransomware" OR "DDoS" OR "malware") AND ("higher OR "universities" OR "higher education institutions" OR "instituições de ensino superior" OR "TEMAc	400
IEEE Xplore	("phishing" OR "ransomware" OR "DDoS" OR "malware") AND ("higher OR "universities" OR "higher education institutions" OR "instituições de ensino superior" OR "TEMAc	355

Fonte: Banco de Dados WoS e IEEE (2021 a 2025)

No *Web of Science*, destacaram-se termos como *Malware Detection, Intrusion Detection e Cyber Defense.* Esses descritores estão associados à identificação e à prevenção de ameaças digitais. Tal procedimento possibilitou recuperar estudos alinhados ao contexto da segurança da informação. Nessa perspectiva, a seleção adequada dos termos contribuiu para maior precisão na busca.

De forma equivalente, na base IEEE Xplore foram empregados descritores específicos relacionados à segurança cibernética. Entre eles, destacam-se *Malware, Distributed Denial of Service, Intrusion Detection e Ransomware.* Esses termos representam ameaças expressivas no contexto das instituições de ensino superior.

Com isso, a busca tornou-se mais direcionada e eficiente, possibilitando a identificação de estudos diretamente relacionados ao tema investigado. Acima foi apresentada a Tabela 4.1 referente aos termos utilizados na pesquisa. Ao término dessa etapa, a combinação de operadores lógicos, palavras-chave e critérios de refinamento permitiu consolidar uma base bibliográfica consistente.

Esse conjunto de procedimentos garantiu maior precisão e rigor na seleção dos estudos analisados, bem como contribuiu para a redução de inconsistências e para o aprimoramento da qualidade da revisão. Em decorrência disso, a fundamentação teórica tornou-se mais sólida e

confiável, estabelecendo uma base adequada para o desenvolvimento da revisão sistemática.

4.3 ETAPA II: Apresentação e Correlação de Dados

Nesta fase da pesquisa, foi conduzido o processo de verificação e tratamento dos registros obtidos nas bases de dados selecionadas. Essa etapa teve como objetivo assegurar a consistência e a integridade das amostras utilizadas na revisão bibliográfica. Inicialmente, os documentos pesquisados foram reunidos em um único conjunto para análise comparativa, o que permitiu identificar registros repetidos provenientes das diferentes bases. Com isso, foi possível iniciar o processo de mineração dos dados coletados.

Em seguida, realizou-se a consolidação dos resultados provenientes dos bancos de dados das bases Web of Science e IEEE Xplore. A soma inicial dos registros resultou em um total de 755 artigos relacionados ao tema investigado.

Esse volume expressivo evidencia o interesse crescente da comunidade científica na área de segurança cibernética em Instituições de Ensino Superior (IES), bem como demonstra a importância do tema no contexto acadêmico contemporâneo. Desse modo, essa base inicial representou o ponto de partida para a mineração das amostras coletadas.

Contudo, observou-se que parte desses registros estava duplicada, uma vez que determinados artigos estavam indexados em ambas as plataformas. Essa condição é comum em revisões que utilizam múltiplas bases de dados.

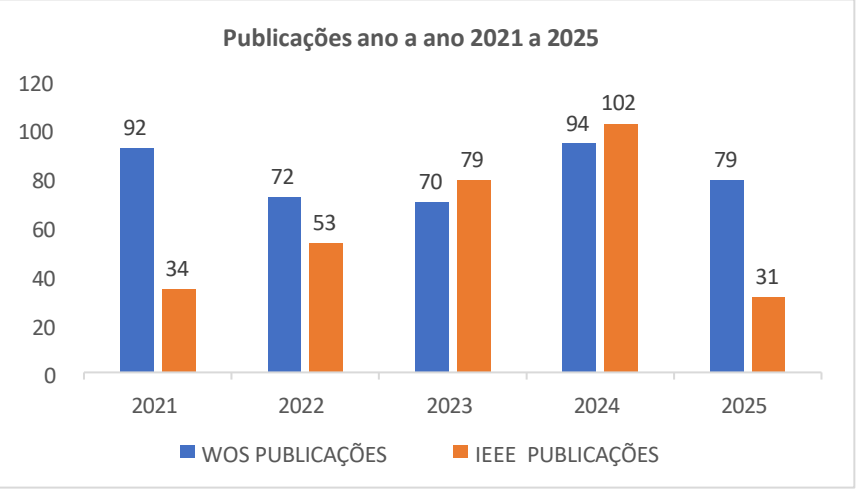
Em virtude disso, tornou-se necessário aplicar critérios de identificação e exclusão de duplicatas, procedimento que evita distorções e garante maior precisão na análise dos resultados, assegurando que cada estudo seja considerado apenas uma vez.

Posteriormente, foi realizada a exclusão sistemática dos registros repetidos identificados durante o processo de verificação. Ao todo, foram removidos 49 documentos duplicados do conjunto inicial. Essa etapa contribuiu para a qualificação da base de dados utilizada na pesquisa, bem como possibilitou a eliminação de redundâncias que poderiam comprometer a análise estatística. Assim sendo, o conjunto final passou a representar de forma mais fidedigna o universo investigado.

Após esse processo de depuração, a amostra consolidada passou a contar com 706 registros válidos. Esse quantitativo corresponde ao conjunto definitivo de estudos considerados na revisão bibliográfica, os quais atendem aos critérios de seleção previamente estabelecidos e constituem a base científica que sustenta as análises e discussões desenvolvidas no estudo. Nessa perspectiva, essa amostra confere maior confiabilidade aos resultados obtidos.

Ao término dessa etapa, os dados consolidados foram organizados de forma a permitir melhor visualização e interpretação dos resultados. A Figura 4.1, apresentada posteriormente, ilustra a distribuição das publicações entre as bases analisadas. Essa representação gráfica facilita a compreensão da origem dos registros selecionados, além de contribuir para maior transparência no processo metodológico adotado. Dessa forma, reforça-se a clareza e a rastreabilidade das etapas da pesquisa.

Figura 4.1: Publicação ano a ano 2021 a 2025



Fonte: Elaborado pelo Autor (2026).

Durante o cruzamento dos registros provenientes das bases Web of Science e IEEE Xplore, foi possível identificar os estudos com maior impacto acadêmico. Essa análise considerou o número de citações como indicador de relevância científica. Nessa perspectiva, foram destacados os artigos que apresentaram maior reconhecimento na literatura, contribuindo para a identificação de referências consolidadas na área.

Inicialmente, verificou-se que o estudo desenvolvido por Zili, L. et al. (2024) apresentou o maior número de citações, totalizando 258 referências. Esse resultado evidencia a ampla aceitação e utilização desse trabalho por outros pesquisadores, bem como demonstra sua contribuição significativa para o avanço do conhecimento. Desse modo, esse estudo configura-se como uma referência expressiva no campo investigado.

Na sequência, observou-se que o trabalho de Bilal, H. et al. (2021) alcançou 253 citações, posicionando-se entre os mais influentes. Esse quantitativo reforça a importância do estudo no contexto da segurança cibernética. De forma análoga, o artigo publicado por Nguyet, Q. et al. (2022) registrou 240 citações, confirmando a consistência e o reconhecimento dessas pesquisas no cenário acadêmico.

Adicionalmente, o estudo de Yitong, R. et al. (2023) apresentou 194 citações, evidenciando

sua importância recente. Paralelamente, o trabalho desenvolvido por Kai, P. et al. (2021) contabilizou 149 citações, consolidando sua presença na literatura científica. Esses dados demonstram a continuidade das contribuições significativas ao longo dos últimos anos, indicando uma evolução progressiva das pesquisas na área.

Cabe destacar que os quantitativos de citações foram obtidos por meio da consulta direta aos títulos dos artigos na plataforma Google Scholar. Essa ferramenta permite mensurar o alcance e a influência das publicações científicas, além de fornecer dados atualizados sobre o impacto acadêmico dos estudos, o que confere maior confiabilidade à análise realizada.

Ao término dessa etapa, os resultados obtidos foram organizados de forma a facilitar sua visualização e interpretação. A Figura 4.2, apresentada posteriormente, ilustra a distribuição das citações identificadas nas bases analisadas. Essa representação contribui para melhor compreensão da importância dos estudos selecionados, reforçando a fundamentação teórica da revisão bibliográfica conduzida.

Figura 4.2: Publicação Citações ano a ano 2021 a 2025

Fonte: Elaborado pelo Autor (2026).

A partir da integração dos registros provenientes das bases Web of Science e IEEE Xplore, foi possível identificar os estudos com maior impacto acadêmico. Esse procedimento considerou o número de citações como indicador de relevância científica. Nessa perspectiva, destacaram-se os artigos que apresentaram maior influência na literatura especializada, contribuindo para o fortalecimento da base teórica da pesquisa.

Entretanto, verificou-se que o estudo conduzido por Zili, L. et al. (2024) apresentou o maior número de citações, totalizando 258 referências. Esse resultado evidencia sua ampla aceitação pela comunidade científica, bem como demonstra sua contribuição significativa para

o avanço do conhecimento. Trabalhos com elevado número de citações tendem a influenciar pesquisas posteriores, consolidando-se como referências importantes na literatura especializada.

Na sequência, observou-se que o artigo de Bilal, H. et al. (2021) registrou 253 citações, posicionando-se entre os mais influentes. Esse número confirma a importância do estudo no contexto da detecção de ameaças digitais. De forma análoga, o trabalho publicado por Nguyet, Q. et al. (2022) alcançou 240 citações, indicando que ambos os estudos apresentam forte reconhecimento acadêmico.

Adicionalmente, o artigo elaborado por Yitong, R. et al. (2023) apresentou um total de 194 citações, evidenciando sua importância recente. Paralelamente, o estudo conduzido por Kai, P. et al. (2021) contabilizou 149 citações, consolidando sua presença na literatura científica. Esses resultados evidenciam a continuidade das contribuições significativas na área, indicando o fortalecimento progressivo do conhecimento técnico.

Cabe destacar que os quantitativos mencionados foram obtidos por meio da consulta direta aos títulos dos artigos na plataforma Google Scholar. Essa ferramenta permite mensurar o alcance e a influência das publicações, bem como fornece indicadores amplamente utilizados na avaliação científica, o que confere maior confiabilidade à análise dos dados.

A análise das bases de dados selecionadas permitiu identificar a distribuição geográfica das publicações científicas relacionadas ao tema nos últimos cinco anos. Observou- se que 54 países contribuíram com estudos relevantes, demonstrando ampla participação internacional. Esse resultado evidencia que a temática possui interesse global crescente. Além disso, reforça sua importância no contexto da segurança digital e da detecção de ameaças.

Nesse sentido, a Tabela 4.2 apresenta a relação dos dez países com maior número de publicações no período analisado. Essa classificação permite compreender a concentração da produção científica em determinadas regiões. Ademais, possibilita identificar os centros mais ativos no desenvolvimento de pesquisas. Essa distribuição contribui para avaliar o nível de maturidade científica entre os países. Portanto, a análise fortalece a compreensão do cenário acadêmico internacional.

No contexto dessa distribuição, o Brasil ocupa a oitava posição, empatado com os Emirados Árabes Unidos, ambos com 13 publicações. Esse quantitativo corresponde a aproximadamente 1,8% do total de artigos identificados. Embora não esteja entre os primeiros colocados, o resultado demonstra participação relevante.

Tabela 1Tabela 4.2 – Número de Publicações por País

Países	**Publicações**	**%**
China	238	33,7 %
India	107	15,0 %
USA	99	14,0 %
Italy	26	3,7 %
Saudi Arabia	24	3,4 %
France	23	3,3 %
Japan	15	2,1 %
Brazil	13	1,8 %
United Arab Emirates	13	1,8 %
Spain	11	1,6 %
Outros	137	19,4 %
Total	**706**	**100 %**

Fonte: Banco de Dados WoS e IEEE (2021 a 2025).

Verificou-se que diversos países apresentaram participação inferior a 1,6% do total de publicações analisadas, o que corresponde a menos de 11 estudos por país no período considerado. Em razão dessa baixa expressividade individual, esses registros foram agrupados na categoria denominada “outros”. Tal estratégia permitiu organizar os dados de forma mais estruturada, possibilitando a priorização dos países com maior representatividade científica.

A consolidação dessas informações possibilitou compreender com maior precisão a distribuição global da produção acadêmica. Embora haja contribuição de diferentes nações, observa-se concentração significativa em poucos países. Esse cenário indica a existência de centros mais consolidados na pesquisa em segurança digital, refletindo níveis distintos de investimento e desenvolvimento tecnológico entre as nações.

No caso do Brasil, foram identificadas treze publicações acadêmicas relacionadas ao tema investigado, evidenciando a participação nacional nesse campo de pesquisa. Embora esse quantitativo seja inferior ao de países com maior tradição científica, sua contribuição mostra-se significativa. Ademais, parte desses estudos apresenta impacto expressivo na literatura especializada. Nesse contexto, o país mantém presença consistente no desenvolvimento do conhecimento na área.

Entre as publicações brasileiras, destacam-se cinco estudos que apresentaram maior número de citações, demonstrando elevado reconhecimento acadêmico. O trabalho desenvolvido por de Neira et al. (2023), voltado à previsão de ataques distribuídos de negação de serviço, registrou 61 citações, evidenciando sua relevância científica e ampla repercussão. Dessa forma, esse estudo consolidou-se como referência importante no contexto analisado.

De maneira análoga, o estudo conduzido por Ceschin et al. (2023), que abordou a detecção

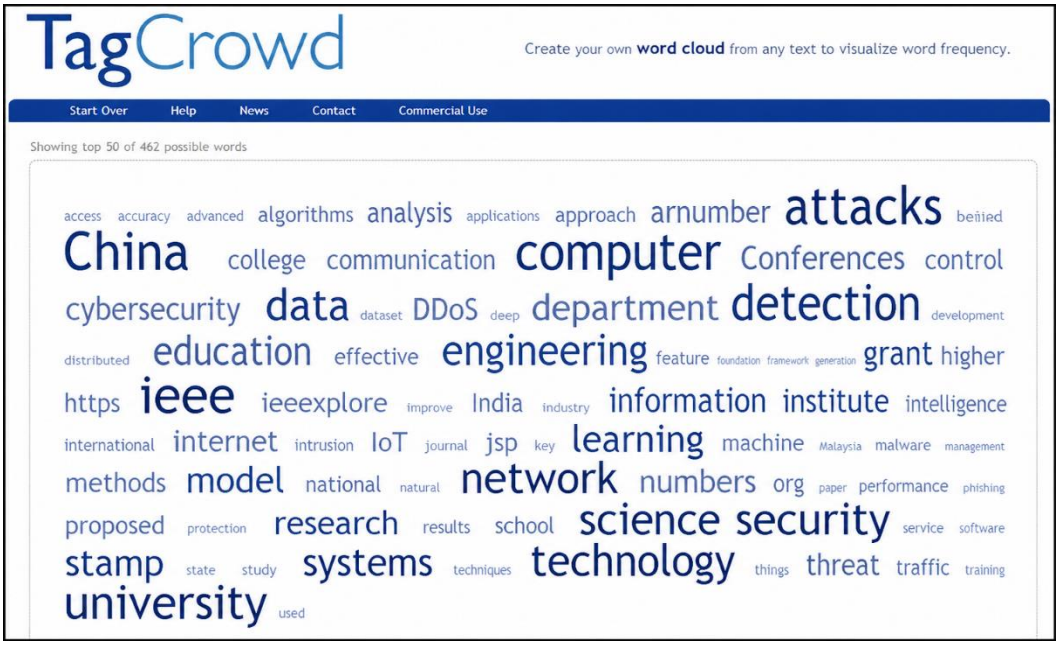
de malware em fluxos de dados dinâmicos, alcançou 32 citações, demonstrando significativa aceitação na comunidade científica. Adicionalmente, sua abordagem contribuiu para ampliar a compreensão sobre técnicas de detecção em ambientes complexos, favorecendo o avanço metodológico na área de segurança digital.

Complementarmente, a pesquisa realizada por Maranhão et al. (2021), baseada em análise estruturada por tensores, apresentou 15 citações, reforçando sua importância científica. Em paralelo, outro estudo de de Neira et al. (2023), voltado à previsão de ataques com base em sinais antecipados, registrou 11 citações. Por sua vez, a abordagem baseada em engenharia de recursos não supervisionada apresentou três citações.

Ao término, no que se refere à análise das palavras-chave, realizou-se a consolidação dos termos extraídos das bases Web of Science e IEEE Xplore. Para esse propósito, utilizou-se a ferramenta TagCrowd, responsável pela geração da nuvem de palavras.

Tal recurso permite identificar os termos mais recorrentes nos estudos analisados, contribuindo para a compreensão dos principais temas e tendências presentes na literatura especializada. Na Figura 4.3, apresenta-se a nuvem de palavras gerada a partir dos dados compilados.

Figura 4.3: Palavras-chave vinculadas aos temas por frequência



Fonte: (TagCrowd, 2022).

4.4 ETAPA III: Aprofundamento, Modelo de Integração e Validação

Na etapa III, foi conduzida a inter-relação dos metadados obtidos, com o objetivo de

aprofundar o processo de integração e validação das informações com base em evidências consistentes. Esse procedimento permitiu ampliar a confiabilidade dos dados analisados e favoreceu a identificação de padrões relevantes na produção científica, o que possibilitou alcançar resultados mais precisos e fundamentados.

Para atingir esse resultado, realizou-se o mapeamento científico com o apoio do software *VOSviewer* (2022). Esse recurso permite a organização e a visualização das relações existentes entre os estudos selecionados, além de contribuir para a análise estrutural das conexões entre autores e temas. Com isso, o uso da ferramenta fortaleceu a análise bibliométrica desenvolvida.

O mapeamento foi estruturado a partir dos metadados extraídos das bases *Web of Science e IEEE*, previamente consolidados em um único conjunto. Essa integração ampliou o escopo da análise e reduziu possíveis lacunas informacionais, favorecendo uma visão mais abrangente das relações acadêmicas existentes. Consequentemente, a consolidação dos dados resultou em maior robustez analítica.

A proposta do mapa de densidade consiste em representar visualmente a intensidade das relações entre os trabalhos científicos. Esse tipo de visualização permite compreender como os estudos se conectam entre si e identificar áreas com maior concentração de produção científica, o que possibilita interpretar a estrutura do conhecimento no campo analisado.

Nos mapas gerados, utilizam-se cores mais intensas e elementos visuais destacados para representar os itens com maior frequência de associação. Esse destaque facilita a identificação dos principais núcleos de colaboração e produção científica. Por sua vez, elementos com menor frequência são representados com cores mais suaves, refletindo a intensidade das conexões existentes.

O uso de diferentes tamanhos de fonte também contribui para evidenciar a relevância dos elementos presentes no mapa. Itens com maior ocorrência ou associação são apresentados com maior destaque visual, enquanto aqueles com menor incidência aparecem com menor evidência gráfica, tornando a interpretação dos dados mais intuitiva e objetiva.

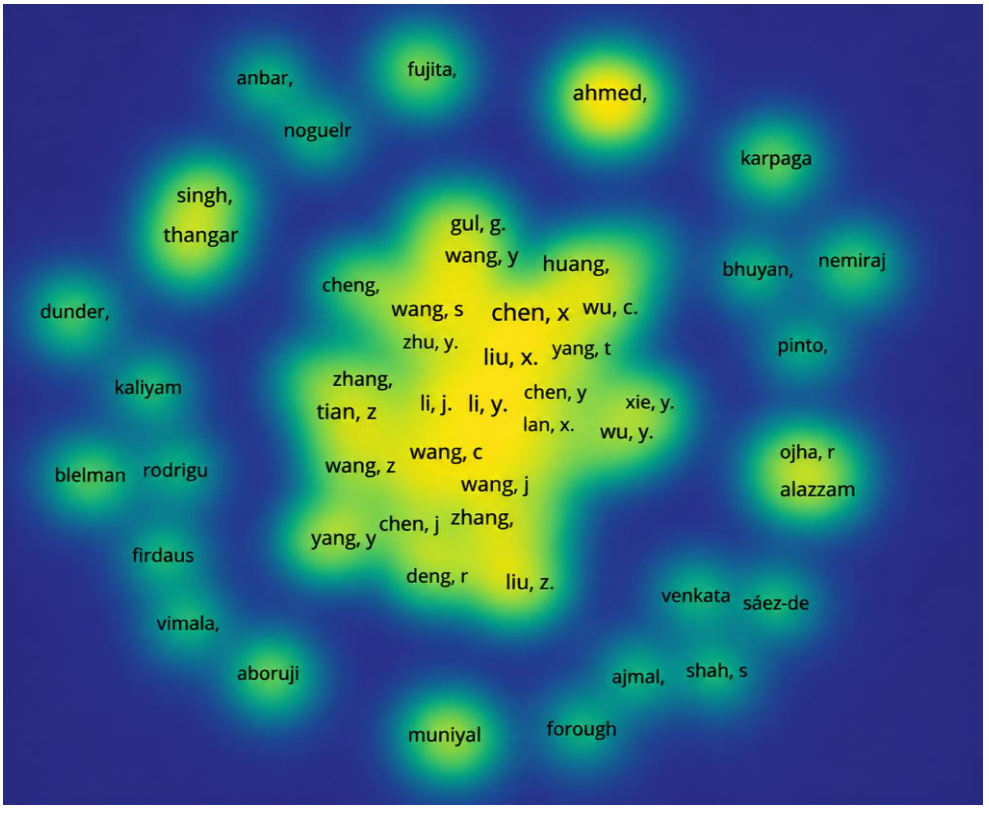
Na sequência da análise, foi examinado o mapa de densidade relacionado à coautoria entre pesquisadores. Esse tipo de abordagem permite identificar padrões de colaboração científica entre autores e compreender como as redes acadêmicas estão estruturadas, contribuindo para avaliar o nível de interação entre os pesquisadores.

Para garantir maior consistência, foram considerados apenas os autores que possuíam pelo menos duas publicações científicas no conjunto analisado. Esse critério permitiu selecionar

pesquisadores com participação mais consolidada e evitou distorções causadas por ocorrências isoladas, direcionando a análise para relações mais representativas.

O resultado desse procedimento é apresentado por meio do mapa de densidade ilustrado na Figura 4.4, gerado com o auxílio do *VOSviewer* (2022). Essa representação permite visualizar de forma clara as conexões entre os autores selecionados e facilita a identificação de grupos de colaboração científica, contribuindo para a compreensão da estrutura relacional da produção acadêmica analisada.

Figura 4.4: Mapa de Densidade de co-autoria



VosViewer (2022).

A amostra examinada indicou que o software identificou um total de 138 autores associados ao conjunto de publicações analisadas. Esse resultado demonstra a dimensão da rede científica vinculada ao tema investigado e evidencia a participação de diversos pesquisadores atuando de forma colaborativa. Com isso, observa-se uma estrutura acadêmica composta por múltiplas conexões, revelando uma rede consistente de produção científica.

Ao observar a Figura 4.5, verifica-se a existência de diversos núcleos de coautoria distribuídos no mapa de densidade. Esses agrupamentos representam autores que desenvolveram pesquisas em colaboração direta, indicando a formação de parcerias científicas consolidadas. Nessa perspectiva, o mapa permite visualizar a organização das relações

acadêmicas, possibilitando compreender a dinâmica de cooperação entre os pesquisadores.

Entre os núcleos identificados, destaca-se a forte conexão entre os autores Xiang Chen e Xuan Liu. Essa associação apresenta elevada densidade visual, o que indica proximidade científica relevante. O tamanho do agrupamento reforça sua representatividade no conjunto analisado, evidenciando a contribuição significativa de ambos. Desse modo, essa dupla configura um dos principais núcleos de colaboração identificados.

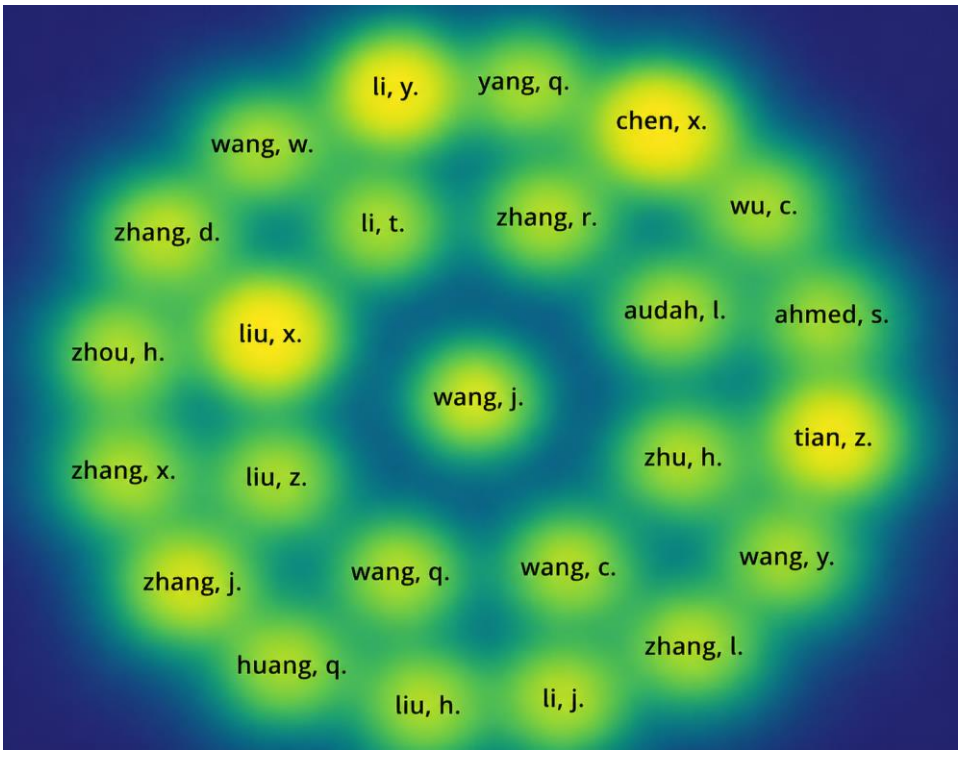
Os referidos autores participaram da publicação do estudo intitulado “Fortalecendo a segurança de rede com switches programáveis: uma pesquisa abrangente.” (Xiang et al., 2023) Esse trabalho aborda aspectos relevantes relacionados à segurança em infraestruturas de rede programáveis e apresenta contribuições que ampliam o entendimento sobre mecanismos de proteção digital. Nesse quadro, o estudo assume relevância científica expressiva, o que reforça sua influência acadêmica no mapa analisado.

Outro agrupamento relevante envolve os autores Xixi Zhang, Guan Guiu e Yu Wang, que também apresentaram forte interligação no mapa de coautoria. Esse núcleo é composto por um autor principal e colaboradores diretamente associados à publicação, com intensidade de conexão que demonstra cooperação científica consolidada. Sob essa ótica, esse grupo representa um polo importante de produção acadêmica, contribuindo para o avanço do campo estudado.

Esses autores participaram do artigo intitulado “Um método automático e eficiente de classificação de tráfego de malware para uma Internet das Coisas segura.” (Zhang et al., 2024) O estudo apresenta contribuições voltadas à identificação de tráfego malicioso em ambientes conectados e aborda soluções relevantes para o fortalecimento da segurança digital. Nessa linha, o trabalho apresenta impacto científico significativo, evidenciando sua relevância no conjunto analisado.

Em complemento à análise, a Figura 4.5 apresenta o mapa de densidade de citação entre os autores identificados. Esse tipo de representação permite observar a intensidade das relações acadêmicas estabelecidas e demonstra o nível de associação entre os pesquisadores com base nas citações compartilhadas. A partir disso, torna-se possível identificar padrões de influência científica, contribuindo para a compreensão da estrutura do campo investigado.

Figura 4.5: Mapa de Densidade de Citação de Autores



Fonte:VosViewer (2022).

A intensidade das conexões é determinada pela frequência com que determinados autores são citados em conjunto. Quanto maior o número de citações compartilhadas, maior será a densidade visual no mapa. Os destaques gráficos, por sua vez, indicam maior relevância científica, enquanto conexões menos intensas refletem menor frequência de associação. Desse modo, o mapa permite identificar diferentes níveis de influência acadêmica.

Para assegurar maior confiabilidade aos resultados, foram considerados apenas os autores que atingiram no mínimo 25 citações. Esse critério direcionou a análise para pesquisadores com maior impacto científico e reduziu interferências associadas à baixa representatividade. Nessa perspectiva, a filtragem contribuiu para fortalecer a consistência analítica, permitindo que os resultados representem com maior precisão a estrutura científica existente.

Esse tipo de abordagem possibilita compreender quais autores exercem maior influência no campo investigado e identificar os principais núcleos responsáveis pela produção científica relevante. Com isso, torna-se viável reconhecer os pesquisadores que apresentam contribuição significativa, favorecendo o entendimento da organização acadêmica e evidenciando a dinâmica da produção científica.

As regiões com maior densidade de citações indicam áreas mais consolidadas e amplamente reconhecidas, refletindo temas com maior maturidade científica e maior aceitação pela comunidade acadêmica. Sob essa ótica, tais áreas representam o núcleo central do

conhecimento desenvolvido, sendo fundamentais para a compreensão do processo de consolidação do campo.

Em outra perspectiva, áreas com menor densidade de citações podem estar associadas a temas emergentes ou em expansão, caracterizando novas linhas de investigação ainda em desenvolvimento. Esses núcleos sinalizam oportunidades para avanços científicos futuros, permitindo que o mapa apresentado na Figura 4.5 evidencie tantas áreas consolidadas quanto emergentes, o que contribui para a compreensão da evolução e das tendências da pesquisa científica.

4.5 Resultado Final da Pesquisa

Após a realização da análise sistemática da literatura, verificou-se que o tema investigado apresenta elevada relevância científica, sustentada por um volume significativo de publicações qualificadas e amplamente reconhecidas. A consistência das evidências encontradas reforça a importância do aprofundamento contínuo das pesquisas nessa área.

Observa-se, ainda, que o interesse acadêmico pelo tema tem crescido de forma consistente, de modo que a literatura confirma sua pertinência no contexto científico atual.

a) An Automatic and Efficient Malware Traffic Classification Method for Secure Internet of Things (Zhang, X. et al, 2024);

b) Empowering Network Security With Programmable Switches: A Comprehensive Survey (Xiang, C. et al, 2023);

c) The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges (Nguyet Qaunt, D. et al. 2022);

d) The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges (Kamil, S. et al, 2022);

e) Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network (de Neira,A.et al, 2023);

f) An Intelligent System for DDoS Attack Prediction Based on Early Warning Signals (de Neira,A.et al, 2023);

g) Unsupervised Feature Engineering Approach to Predict DDoS Attacks (de Neira,A.et al, 2023).

A mitigação das ameaças cibernéticas exige a adoção de métodos avançados capazes de

identificar e classificar comportamentos maliciosos em ambientes digitais. Nesse contexto, destaca-se o método automático de classificação de tráfego de malware voltado à segurança da Internet das Coisas.

Essa abordagem busca aprimorar a identificação de padrões suspeitos em redes complexas. Além disso, contribui para fortalecer os mecanismos de proteção preventiva. Dessa forma, torna-se possível reduzir riscos operacionais e melhorar a confiabilidade dos sistemas.

Segundo Zhang *et al.* (2024), a classificação de malware representa um elemento essencial para a manutenção da segurança cibernética. Entretanto, os autores ressaltam que esse processo apresenta elevada complexidade, especialmente em ambientes com grande volume de dados. Além disso, a diversidade de comportamentos maliciosos dificulta a detecção precisa. Portanto, torna-se necessário o uso de soluções automatizadas e inteligentes. Nesse sentido, técnicas baseadas em aprendizado computacional apresentam resultados promissores.

O sistema proposto pelos autores utiliza uma arquitetura neural estruturada para classificar tráfegos maliciosos de forma eficiente. Essa arquitetura permite identificar padrões que poderiam passar despercebidos por métodos tradicionais. Além disso, o modelo apresenta maior capacidade de adaptação a novos tipos de ameaças. Dessa maneira, amplia-se a capacidade de resposta frente a ataques emergentes. Consequentemente, a rede torna-se mais resiliente e segura.

Adicionalmente, os resultados demonstraram que o método MTC, aliado ao mecanismo NASP, alcançou desempenho elevado na análise do tráfego de rede. Esse desempenho contribuiu significativamente para o gerenciamento seguro de ambientes de Internet das Coisas. Além disso, a solução apresentou níveis satisfatórios de precisão e confiabilidade. Dessa forma, reforça-se a viabilidade da aplicação prática desse modelo. Portanto, essa abordagem constitui uma alternativa relevante para proteção digital.

Outro estudo relevante aborda o fortalecimento da segurança de rede por meio do uso de switches programáveis. Conforme Xiang et al. (2023), o avanço das redes 5G ampliou as possibilidades de conectividade e desempenho. Entretanto, esse crescimento também contribuiu para o aumento das superfícies de ataque. Além disso, novas tecnologias passaram a ser exploradas por agentes maliciosos. Assim, torna-se necessário adotar mecanismos mais robustos de proteção.

Nesse contexto, os ataques de negação de serviço distribuídos passaram a ocorrer com maior

frequência e intensidade. Esses ataques comprometem a disponibilidade dos serviços e afetam a continuidade operacional. Além disso, exploram limitações estruturais das redes tradicionais. Portanto, soluções inovadoras tornam-se fundamentais para enfrentar essas ameaças. Nesse sentido, os switches programáveis apresentam vantagens significativas.

Os autores destacam que os switches programáveis permitem maior controle sobre o tráfego de rede. Essa capacidade facilita a identificação de comportamentos suspeitos em tempo real. Além disso, possibilita a implementação de políticas dinâmicas de segurança. Dessa forma, amplia-se a capacidade de resposta frente a incidentes. Consequentemente, fortalece-se a proteção da infraestrutura digital.

Outro aspecto relevante refere-se à detecção de ataques de phishing, que continuam representando uma ameaça significativa. Conforme Nguyet Quant *et al.* (2022), essas ameaças exploram vulnerabilidades humanas e técnicas. Além disso, utilizam estratégias sofisticadas para enganar usuários e sistemas. Portanto, torna-se essencial o desenvolvimento de métodos mais eficientes de detecção. Nesse sentido, o aprendizado profundo apresenta grande potencial.

Os autores propuseram uma taxonomia baseada em algoritmos de aprendizado profundo, fundamentada em revisão sistemática da literatura. Essa estrutura contribui para organizar o conhecimento existente na área. Além disso, facilita a compreensão das técnicas mais eficazes. Dessa maneira, possibilita o aprimoramento dos mecanismos de detecção. Consequentemente, fortalece-se a segurança dos sistemas digitais.

No que se refere ao ransomware, observa-se que essa modalidade de ataque representa uma das principais ameaças atuais. Segundo Kamil *et al.* (2022), esse tipo de invasão compromete o acesso às informações das vítimas. Além disso, gera impactos operacionais e financeiros relevantes. Portanto, torna-se um desafio significativo para organizações públicas e privadas. Nesse contexto, medidas preventivas são indispensáveis.

Os autores destacam que, mesmo com avanços tecnológicos, os ataques de ransomware continuam sendo eficazes. Isso ocorre porque exploram vulnerabilidades técnicas e falhas humanas. Além disso, utilizam técnicas de criptografia avançadas. Dessa forma, dificultam a recuperação dos dados comprometidos. Consequentemente, reforça-se a necessidade de estratégias preventivas e preditivas.

Além disso, o estudo conduzido por de Neira *et al.* (2023) destaca a relevância da previsão de ataques distribuídos de negação de serviço. Esses ataques comprometem a disponibilidade de sistemas críticos. Ademais, exploram limitações estruturais da rede. Portanto, sua

antecipação constitui um fator estratégico. Dessa forma, torna-se possível minimizar seus impactos.

Nesse sentido, os autores propuseram o sistema cooperativo COOPRED DDoS, voltado à previsão antecipada de ataques. Os resultados demonstraram elevada taxa de precisão na identificação de ameaças. Além disso, o sistema apresentou capacidade de prever ataques com antecedência significativa. Dessa maneira, contribui para a implementação de medidas preventivas. Consequentemente, fortalece-se a segurança das redes.

Por fim, destaca-se a abordagem baseada em engenharia de recursos não supervisionada para previsão de ataques. Conforme de Neira *et al.* (2023), essa técnica permite identificar padrões ocultos no tráfego de rede. Além disso, possibilita antecipar ataques com elevada precisão. Dessa forma, amplia-se a capacidade de resposta preventiva. Portanto, essa abordagem representa uma contribuição relevante para a segurança cibernética. O Quadro 3.8 mostra algumas informações descritas pelos autores.

Quadro 3.8 – Estimativa de Frequência de Ataques em IES

Tipo de Ataque	Percentual	Fundamentação na Literatura
Phishing	**40%**	Alta recorrência em estudos sobre engenharia social e vetor inicial de ataques. Lallie, H. S. et al 2022)
Ransomware	**35%**	Crescimento significativo e alto impacto em universidades Kamil, S. et al.2022 e Dolliver, D., S. et al. 2021)
DDoS	**25%**	Frequente em infraestruturas acadêmicas abertas e distribuídas Bilal, H. et al. 2020, De Neira 2023, Fan, C. et al. 2021)

Fonte: Autor, 2025

Em síntese, os estudos analisados evidenciam que o uso de métodos automatizados, preditivos e programáveis contribui significativamente para a proteção dos sistemas digitais. Além disso, essas soluções fortalecem a capacidade de identificação e resposta a ameaças. Dessa maneira, promovem maior segurança e confiabilidade operacional.

5 – CONCLUSÕES E TRABALHOS FUTUROS

A análise sistemática da literatura permite concluir que a detecção de ataques em Instituições de Ensino Superior configura-se como um componente estratégico essencial para a proteção dos ativos informacionais e para a continuidade das atividades acadêmicas. Essas instituições concentram um volume expressivo de dados científicos, administrativos e pessoais, o que as torna alvos recorrentes de ataques cibernéticos.

As ameaças de phishing, ransomware e ataques distribuídos de negação de serviço apresentam elevado vetor de impacto e reforçam a necessidade de mecanismos e ferramentas modernas além de monitoramento e resposta rápida.

Além disso, os incidentes podem comprometer a confidencialidade, a integridade e a disponibilidade das informações. Portanto, torna-se indispensável adotar medidas estruturadas de prevenção e detecção.

Nesse sentido, a implementação de redes automatizadas de monitoramento representa uma abordagem que fortalece a segurança institucional. Esses mecanismos permitem a identificação precoce de comportamentos anômalos e padrões suspeitos, possibilitando respostas mais rápidas e precisas.

A automação do sistema também contribui para reduzir a dependência exclusiva de intervenções manuais, aumentando a eficiência operacional. Consequentemente, a capacidade de detecção e contenção de ameaças é ampliada de forma significativa. Dessa forma, o monitoramento contínuo passa a integrar a estratégia permanente de proteção digital.

Adicionalmente, a conscientização dos usuários internos e externos constitui um fator importante para a redução de incidentes de segurança. Muitos ataques exploram falhas humanas, especialmente por meio de técnicas de engenharia social, como o *phishing*. Por essa razão, programas de capacitação e orientação devem ser adotados de forma contínua. Além disso, a disseminação de boas práticas fortalece a cultura institucional de segurança da informação. Assim, os usuários tornam-se agentes ativos na proteção do ambiente digital.

Por fim, conclui-se que a proteção dos dados sensíveis das Instituições de Ensino Superior depende da integração entre tecnologia, governança e conscientização dos usuários. Atualizações frequentes corrigem falhas que poderiam ser exploradas por agentes maliciosos para obter acesso não autorizado. Além disso, sistemas desatualizados aumentam a superfície de ataque e elevam o risco institucional. Portanto, políticas de gestão de atualizações devem ser

implementadas de maneira rigorosa e contínua. Dessa maneira, a infraestrutura tecnológica permaneceria mais resiliente frente às ameaças emergentes.

5.1 Contribuição da pesquisa utilizando o TEMAC

A presente pesquisa foi desenvolvida com base na Teoria do Enfoque Metaanalítico Consolidado (TEMAC), aplicada ao período compreendido entre os anos de 2021 e 2025. Inicialmente, esse modelo metodológico permitiu organizar, analisar e interpretar, de forma estruturada, os dados científicos disponíveis. Ademais, possibilitou identificar padrões, tendências e lacunas relevantes na literatura especializada. Dessa forma, o estudo foi conduzido com rigor metodológico e fundamentação consistente, assegurando, portanto, maior confiabilidade aos resultados obtidos.

Nesse sentido, a utilização do TEMAC contribuiu para consolidar uma base bibliográfica robusta e alinhada ao tema investigado. Por conseguinte, o método favoreceu a seleção criteriosa dos estudos mais relevantes, considerando critérios de impacto e pertinência científica. Igualmente, permitiu estabelecer relações entre os principais autores e suas contribuições. Consequentemente, tornou-se possível compreender o estágio atual do conhecimento na área, o que fortaleceu a qualidade analítica da pesquisa.

Adicionalmente, o estudo foi sustentado por autores reconhecidos na área de segurança cibernética e detecção de ameaças digitais. Nesse contexto, esses pesquisadores contribuíram com modelos, técnicas e análises que fundamentaram a compreensão dos riscos existentes. Outrossim, suas publicações forneceram evidências relevantes para a construção da discussão científica. Dessa maneira, a pesquisa foi estruturada com base em referências importantes, proporcionando uma coerência teórica e de qualidade a acadêmica.

Posteriormente, a análise quantitativa revelou que cinco estudos apresentaram maior número de citações no período analisado. Entre eles, destaca-se o trabalho de Zili *et al.* (2024), que alcançou expressivo reconhecimento científico. De modo semelhante, os estudos de Bilal et al. (2021), Nguyet *et al.* (2022), Yitong *et al.* (2023) e Kai *et al.* (2021) também demonstraram elevado impacto. Esses resultados, portanto, evidenciam a relevância dessas pesquisas para o avanço da área, configurando-se como referências fundamentais no campo investigado.

Além disso, o elevado número de citações indica que essas publicações contribuíram significativamente para o desenvolvimento de novas abordagens de detecção e prevenção, uma vez que esse reconhecimento reflete a consistência metodológica e a aplicabilidade prática das soluções propostas. Dessa forma, essas pesquisas influenciam diretamente a evolução das

estratégias de segurança digital, tornando-se essenciais para orientar estudos futuros. Assim, consolidam-se como pilares do conhecimento científico na área.

Observou-se, ainda, que grande parte das pesquisas se concentra na identificação e mitigação de malwares em ambientes institucionais. Esse cenário, por sua vez, evidencia a crescente preocupação com a proteção de sistemas acadêmicos e administrativos. Adicionalmente, reforça a importância da segurança da informação no contexto das instituições de ensino superior. Dessa maneira, a literatura demonstra alinhamento com as demandas atuais de proteção digital, evidenciando a elevada relevância científica e institucional do tema.

Entre as ameaças analisadas, destacam-se os ataques de phishing, ransomware e DDoS como os mais recorrentes e impactantes, visto que exploram vulnerabilidades técnicas e comportamentais, ampliando os riscos institucionais. Ademais, podem comprometer o funcionamento de serviços essenciais e a proteção de dados sensíveis, configurando-se como desafios críticos para a gestão universitária. Assim, reforça-se a necessidade de estratégias eficazes de detecção e prevenção.

Nesse contexto, a literatura analisada apresentou contribuições voltadas ao tema descrito em relação à mitigação dos riscos. Por exemplo, estudos recentes propuseram soluções baseadas em inteligência artificial e aprendizado de máquina. Essas abordagens, por sua vez, permitem identificar padrões suspeitos com maior precisão e rapidez. Além disso, favorecem a automação dos processos de detecção, ampliando a capacidade institucional de resposta a incidentes.

Entre as soluções identificadas, destaca-se o uso de técnicas de classificação automatizada de tráfego de malware. Essas ferramentas, portanto, permitem distinguir comportamentos legítimos de atividades maliciosas em redes digitais. Adicionalmente, contribuem para o fortalecimento da segurança em ambientes conectados, como a Internet das Coisas. Consequentemente, reduzem o risco de intrusões e acessos indevidos, promovendo maior controle sobre o ambiente tecnológico.

Da mesma forma, o uso de switches programáveis foi apontado como uma solução eficaz para fortalecer a segurança das redes institucionais, uma vez que esses dispositivos permitem maior flexibilidade no controle e monitoramento do tráfego de dados. Além disso, facilitam a implementação de mecanismos avançados de proteção, contribuindo para reduzir a vulnerabilidade a ataques distribuídos. Portanto, representam uma alternativa relevante para a proteção digital.

No mesmo sentido, técnicas baseadas em aprendizado profundo demonstraram elevada eficiência na detecção de ataques de phishing. Esses modelos, por sua vez, permitem analisar grandes volumes de dados e identificar padrões complexos, aumentando a precisão na Identificação de ameaças. Dessa forma, fortalecem a capacidade preventiva das instituições, contribuindo para reduzir os riscos associados a ataques baseados em engenharia social.

Adicionalmente, estudos voltados à detecção e previsão de ataques de ransomware e DDoS apresentaram resultados promissores, considerando que esses trabalhos demonstraram ser possível antecipar ataques por meio da análise de sinais e comportamentos suspeitos. Ademais, sistemas inteligentes podem emitir alertas precoces, permitindo ações preventivas e reduzindo o impacto potencial dos ataques. Portanto, essas soluções representam avanços significativos na área.

Diante disso, os resultados obtidos evidenciam que a adoção de tecnologias avançadas pode fortalecer significativamente a segurança das instituições de ensino superior. Do mesmo modo, demonstram que a integração entre monitoramento, análise e resposta é essencial para a proteção digital. Dessa forma, as instituições tornam-se mais resilientes frente às ameaças cibernéticas, assegurando maior proteção aos dados institucionais e promovendo estabilidade operacional.

Como contribuição científica, esta pesquisa consolida o conhecimento existente sobre detecção de malware no contexto acadêmico. Adicionalmente, apresenta uma análise estruturada das principais ameaças e das soluções propostas na literatura recente. Dessa maneira, fornece subsídios teóricos e práticos para pesquisadores e gestores institucionais, contribuindo diretamente para o avanço do conhecimento científico e o desenvolvimento de novas estratégias de segurança.

Por fim, o estudo amplia a compreensão sobre os desafios e as oportunidades relacionados à segurança cibernética nas instituições de ensino superior. Ademais, oferece uma base consistente para o desenvolvimento de futuras pesquisas e políticas institucionais. Dessa forma, contribui para o fortalecimento da governança em segurança da informação, promovendo maior proteção aos ativos digitais e científicos e consolidando-se como uma referência importante no campo da segurança digital acadêmica.

5.2 Trabalhos Futuros e Perspectivas de Pesquisa

A análise sistemática da literatura evidenciou que a segurança cibernética em Instituições de Ensino Superior constitui um campo de elevada relevância científica, sobretudo em razão do crescimento contínuo do volume de dados acadêmicos e administrativos armazenados. Diante desse cenário, a proteção dessas informações configura-se como um requisito essencial para assegurar a continuidade das atividades institucionais.

Entretanto, a diversidade de dispositivos conectados amplia a complexidade do gerenciamento da segurança. Dessa maneira, torna-se necessário adotar abordagens inovadoras e tecnicamente robustas. A literatura apresenta diferentes soluções voltadas à prevenção e mitigação de ameaças digitais.

Entre as principais propostas identificadas na literatura, destacam-se as seguintes abordagens:

a) **An Automatic and Efficient Malware Traffic Classification Method for Secure Internet of Things** – Conforme apresentado por (Zhang *et al.*,2024), esse método utiliza arquiteturas neurais avançadas para identificar padrões associados a atividades maliciosas. Dessa forma, contribui para o aprimoramento do controle e da gestão do tráfego de rede. A automação reduz falhas humanas e amplia a eficiência operacional. Consequentemente, fortalece a segurança em ambientes conectados.

b) **Empowering Network Security With Programmable Switches: A Comprehensive Survey** – Estudos do (Xiang, C *et al.*, 2023), indicam que esses dispositivos permitem maior controle sobre o fluxo de dados e facilitam a implementação de políticas de segurança mais eficazes. Nesse sentido, proporcionam maior visibilidade do tráfego de rede. Além disso, contribuem para a rápida identificação de atividades suspeitas. Portanto, representam uma solução relevante para o fortalecimento da infraestrutura digital.

c) **Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions** – Pesquisas recentes do (Ngut. Q, D *et al.*,2022) demonstram que modelos baseados em aprendizado profundo apresentam elevada precisão na identificação de tentativas de fraude. Dessa maneira, possibilitam detectar padrões complexos que métodos convencionais não identificariam. Além disso, aumentam a capacidade preventiva das instituições. Assim, contribuem significativamente para

a proteção dos usuários e dos sistemas.

d) **The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges** – Os estudos analisados por (Kamil, S *et al.*,2022) destacam que o ransomware continua sendo uma das principais ameaças à integridade dos dados institucionais. Nesse contexto, a compreensão de seus mecanismos de funcionamento torna-se essencial para o desenvolvimento de medidas de proteção eficazes. Além disso, técnicas de detecção precoce contribuem para reduzir danos operacionais. Consequentemente, fortalecem a continuidade dos serviços institucionais.

e) **Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network** – As pesquisas de (Bilal, H *et al.* ,2021) demonstram que o uso de sistemas inteligentes permite identificar sinais antecipados de ataques. Dessa forma, possibilita a adoção de medidas preventivas antes da interrupção dos serviços. Além disso, melhora a capacidade de resposta institucional. Portanto, contribui diretamente para a estabilidade da infraestrutura tecnológica.

f) **An Intelligent System for DDoS Attack Prediction Based on Early Warning Signals** – Essas soluções de acordo (de Neira, A *et al*., 2023) utilizam análise contínua do tráfego para detectar comportamentos anômalos em tempo real. Nesse sentido, favorecem a implementação de estratégias preventivas. Além disso, reduzem o tempo de resposta frente às ameaças. Assim, ampliam a eficiência das ações de defesa cibernética.

g) **Unsupervised Feature Engineering Approach to Predict DDoS Attacks.** – Essa abordagem da (de Neira, A *et al*., 2023) permite identificar padrões ocultos nos dados de rede, mesmo na ausência de informações previamente classificadas. Dessa maneira, amplia a capacidade de detecção de novas ameaças. Além disso, contribui para o desenvolvimento de sistemas mais adaptáveis. Consequentemente, fortalece a segurança em ambientes complexos.

Como perspectiva de trabalhos futuros, evidencia-se a necessidade de desenvolver modelos mais precisos e adaptáveis às constantes transformações no cenário das ameaças digitais. Nesse contexto, recomenda-se o aprimoramento de sistemas automatizados voltados ao monitoramento contínuo.

Ademais, torna-se essencial a integração entre diferentes tecnologias de proteção, a fim de potencializar a eficiência dos mecanismos de defesa. É extremamente possível, ampliar a capacidade institucional de prevenção e resposta a incidentes. As pesquisas futuras poderão contribuir de maneira significativa para o fortalecimento da segurança digital no ambiente acadêmico.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRAMO, G., & D'ANGELO, C. A. Evaluating research: from informed peer review to bibliometrics 2011**.** Scientometrics, 87(3), 499-514.

ADRIAANSE, L.S.; RENSLEIGH, C. A Content Comprehensiveness Comparison. Web of Science, Scopus and Google Scholar 2011. Disponível em: <https: // www .researchgate .net/publication/259258650_Web_of_Science_Scopus_and _Google_Scholar_A_contente _ com prehensiveness _comparison> . Acesso em: 14 nov. 2025.

ARAÚJO, A. A. Gestão de risco no setor público: percepção do gerenciamento de riscos nas universidades federais. MSc Dissertation, Universidade Federal Rural de Pernambuco, Recife, 229 pages 2019 . Disponível em:< https://www.lareferencia.info/vufind /Record/ BR _ b32 e 98cdd64995cf3fdf11d6c4b69935>. Acesso em: 14 fev. 2025.

BILAL, H. *et al*. Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network. IEEE. 2020. Disponível em:<https://ieeexplore.ieee.org/abstract /document /9716113 >Acesso em: 21 nov. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 852, de 28 de março de 2023. Institui o Programa de Privacidade e Segurança da Informação (PPSI). Diário Oficial da União: seção 1, Brasília, DF, 29 mar. 2023.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Estratégia Nacional de Governo Digital (ENGD).Brasília: Governo Federal,2024. Disponível em <https: //www. Gov .br/governodigital/pt-br/estrategias-e-governanca-digital /estrategiana cional>. Acesso em: 08 jan. 2026.

BRASIL. Presidência da República Secretaria Geral. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. 2017. Disponível em:< https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm> Acesso em: 08 jan. 2026.

CAMINHA, Jean; **SUSUKI**, Renan Heiji. Implantação de um sistema de gerenciamento de eventos e informações de segurança em uma universidade pública. 2024. Disponível em: <https://sol.sbc.org.br/index.php/eri-mt/article/view/31189> Acesso em: 19 jan. 2025.

CESCHIN, F. *et al*. Fast & Furious: On the modelling of malware detection as an evolving data stream. Elsevier Scopus 2022. Disponível em: < https: // www . sciencedirect .com/science/ article/abs/pii/S0957417422016463 >Acesso em: 25 nov. 2025.

CHENG, C. K. E.;, WANG, T. Institutional Strategies for Cybersecurity in Higher Education Institutions. MDPI: Information 9 versões 2022. Disponível em: <https://www.mdpi .com/2078-2489/13/4/192>. Acesso em: 12 nov. 2025.

CGU. Ministério da Transparência e Controladoria – Geral da União. Metodologia de Gestão de Riscos. 2017. Disponível em:< https://www.gov.br/cgu/pt-br/acesso-a-informacao /gover nanca gestao-de-riscos> Acesso em: 27 jan. 2025.

CRESWELL, John. W. Projeto de Pesquisa: Métodos Qualitativos, Quantitativo e Misto. 3ed. – Porto Alegre: Artmed, 2010. 296 p.

CUNHA, M. B and **LOOSE**, C. E. "Gestão de riscos nas universidades públicas no Brasil", (2024). IOSR Journal of Humanities and Social Science, vol. 29, pp. 40–46 . Disponível em:< https://ri.unir.br/jspui/handle/123456789/5358>. Acesso em: 14 fev. 2025.

DE NEIRA, A. B. *et al*. An Intelligent System for DDoS Attack Prediction Based on Early Warning Signals. IEEE 2023. Disponível em: <https:// ieeexplore .ieee . org /abstract/document/ 10261168?signout=success>.Acesso em: 09 nov. 2025.

DE NEIRA, A. B. *et al*. Distributed denial of service attack prediction: Challenges, open issues and opportunities ELSEVIER 2023. Disponível em: <https:/ /www.sciencedirect. com/science/article/abs/pii/S1389128622005874 >Acesso em: 16 nov. 2025.

DE NEIRA, A. B.*et al*. Unsupervised Feature Engineering Approach to Predict DDoS Attacks. 2023. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10437029> Acesso em: 14 nov. 2025.

DOLLIVER, D., S. *et al*. Building a robust cyberthreat profile for institutions of higher education: An empirical analysis of external cyberattacks against a large university's computer network. Elsevier Scopus. 2 versões 2021. Disponível em:< https://www .science dir ect.com/science/article/abs/pii/S175606162100029X >. Acesso em: 16 nov. 2025.

FAN, C. *et al*. Detection Of Ddos Attacks In Software Defined Networking Using Entropy. MDPI. 7 versões 2021. Disponível em: <https://doi.org/10.3390/app12010370>. Acesso em: 16 nov. 2025.

FERREIRA, L. V. A. *et al*. Uso de honeypots na detecção de rootkits de malware: proposta de uma agenda de pesquisa. RISTI. 3 versões 2023. Disponível em: <https://www. researchgate

.net/publication /373439857 _Uso_de _honeypots _na _d eteccao _de _rootkits _de _malware_proposta_de_uma_agenda_de_pesquisa >. Acesso em: 02 out. 2025.

FRONS. Matriz de Probabilidade e Impacto. 2020. 1 ilustração. Disponível em: https://frons.com.br/blog/processos/matriz-probabilidade-impacto/. Acesso em: 25 abr. 2026.

GIL, Antônio Carlos. Como Elaborar Projetos de Pesquisa. 6. ed. São Paulo: Atlas, 2019. → Obra clássica, apresenta os tipos de pesquisa (exploratória, descritiva, explicativa, aplicada) e orienta sobre estrutura metodológica.

Gil, Antônio Carlos. Como Elaborar Projetos de Pesquisa. 4ª ed. São Paulo: Atlas, 2002. → Obra clássica que apresenta os tipos de pesquisa (exploratória, descritiva, explicativa, aplicada) e orienta sobre estrutura metodológica.

GONÇALVES, E. *et al*. Universidades sob ataque hacker: riscos de negócio para segurança cibernética em universidades brasileiras. 2025. Disponível em: < https://ppee.unb.br/wp-content/uploads/2025/04/Artigo_ataque_hacker_IES_UnB.pdf> Acesso em: 02 fev. 2026.

ISO/IEC 27701:2025. Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

KAI, P. *et al*. Security challenges and opportunities for smart contracts in Internet of Things: A survey. IEEE 2022 Disponível em:<https://ieeexplore.ieee. org/abstract/document /9409120>. Acesso em: 21 nov. 2025.

KAMIL, S. *et al*. The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges. 2022. Disponível em: <https://ieeexplore .ieee .org/abstract / docu ment / 9 7 59000> Acesso em: 10 nov. 2025.

LACHI, A.A.; ANATOLIE, A.. Cybersecurity Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. Instrumentaul Bibliometric Nacional.p. 128-133, 2022. 6 versões. Disponível em: <https://ibn.idsi.md/vizualizare _ articol /16 3773>Acesso em: 16 nov. 2025.

LACHI, A. A. Network Security Threats to Higher Education Institutions. Instrumentaul Bibliometric Nacional. p. 323-333. 2021 7 versões 2022. Disponível em: < https://ibn. idsi.md / vizualizare_articol/132828 >. Acesso em: 15 nov. 2025.

LALLIE, H. S.. *et al*. Understanding Cyber Threats Against the Universities, Colleges, and Schools. Cornell University 3versões. 2021. Disponível em : <https://arxiv.org/abs/2307.07755>

Acesso em: 15 nov. 2025.

MA HAQUE, Md. *et al*. Cybersecurity In Universities: An Evaluation Model. SN Computer Science. 4 versões 2023. Disponível em: <https:// link .springer .com / article / 10.1007/s42979-023-01984-x >Acesso em: 16 nov. 2025.

MACHADO, Jeferson Barboza. Automação de tarefas de segurança e melhorias na resposta a incidentes cibernéticos: como a automação impacta a eficácia da resposta a incidentes cibernéticos em termos de tempo e precisão? 2024. Trabalho de Conclusão de Curso. https://repositorio.esg.br/handle/123456789/1967

MARANHÃO, J. P.A. *et al*. Tensor based framework for Distributed Denial of Service attack detection. Elsevier Scopus 2021. Disponível em:<https://www.sciencedirect.com /Science/article/abs/pii/S1084804520303556> . Acesso em: 16 out. 2025.

MARIANO, A. M ; ROCHA, M. S. Revisão da Literatura: Apresentação de uma Abordagem Integradora." XXVI Congresso Internacional de la Academia Europea de Dirección y Economía de la Empresa (AEDEM), 2 versões p. 427–443, n. Setembro 2017.

MGI - Ministério de Gestão e Inovação . Guia Framework do Programa de Privacidade e Segurança da Informação (PPSI) (2024). Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos> Acesso em: 11 fev. 2026.

NAAGAS, M.A. *et al*. Defense-Through-Deception Network Security Model: Securing University Campus Network From Dos/Ddos Attack. Bulletin of Electrical Engineering and Informatics (BEEI). p.593-600, 14 versões 2018. Disponível em:<https://beei. Org /index .php /EEI/article/view/1349 > Acesso em: 16 nov. 2025.

NASCIMENTO, L. M. M. *et al*. Aumentando a Segurança do Gerenciamento de Usuários do Moodle Usando Banco de Dados de Terceiros. 2025. Revista de Engenharia e Tecnologia. Disponível em: <https://revistas.uepg.br/index.php/ret/article/view/25201>. Acesso em: 28 dez. 2025.

NBR ISO/IEC 27001:2022. Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos.

NEVES, R.A.C. Vitimação Por Phishing: Um Estudo Empírico. Proquest 2022. Disponível em:<https://www.proquest.com/openview/0b3450e6e7eebbe6ece34ad794b54ce8/1?pq-origsite =gscholar&cbl=2026366&diss=y>Acesso em: 08 nov. 2025.

NGUYET, Q. D., *et al*. Deep Learning for Phishing Detection: Taxonomy, Current Challenges and

Future Directions IEEE 2022. Disponível em: < https://ieeexplore .ieee.org/ abstract/document/9716113 >Acesso em: 16 nov. 2025.

NIST. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. 2024. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 16 jan. 2026.

PILLAY, A.; SHARMA, N. A. Applicable cyber security commendations to prevent cyber attacks in Universities. IEEE.2023. Disponível em: <https://ieeexplore.ieee.org /abstract/ document/10089360 > Acesso em: 09 nov. 2025.

RAJPUT, P. H. N.*et al*. Remote Non-Intrusive Malware Detection for PLCs based on Chain of Trust Rooted in Hardware. IEEE European Symposium on Security and Privacy (EuroS&P),p.369-384.5versões-2021.Disponívelem:<https://ieeexplore.ieee.Org document /9581272>. Acesso em: 15 nov. 2025.

REIS, J. G. B.; *et al*.. A Importância Da Usabilidade E A Colaboração Positivista Aplicada À Segurança Cibernética: Um Estudo De Caso Do Aplicativo Sougov. Revista FT, v. 29, n. 148, pag 17-18, 2025.

SANTOS JR., *et al***.** Implementação De Segurança Zero-Trust Para Redes Industriais. Sociedade Brasileira de Automática (SBA) XXV Congresso Brasileiro de Automática - CBA 2024, 15 a 18 de outubro de 2024. Disponível em:< https://www.sba.org.br / open _ jornal_ systems/index.php/cba/article/view/4237/3721> Acesso em: 10 fev. 2026.

SILVA, C. E. C , *et al*. Detecção de malware em instituições de ensino superior: uma revisão das ameaças de phishing, ransomware e DDoS. Revista DELOS, v.19, n.76, p. 01-26, 2026. Disponível em**:** https://ojs.revistadelos.com/ojs/index.php/delos/article/view/ 8468.

ROSE, S. *et al.* Zero Trust Architecture. NIST special publication, 800, 207 - 2020. Disponível em: https://csrc.nist.gov/pubs/sp/800/207/final. Acesso em: 10 fev. 2026.

STEINBOCK, D. D. (2022). TagCrowd. Disponível em: https://tagcrowd.com/. Acesso em: 08 nov. 2025.

ULVEN, Joachim Bjørge, WANGEN, Gaute. A Systematic Review of Cybersecurity Risks in Higher Education. MDPI: Future Internet . 7 versões. 2021. Disponível em: <https:/ /www .mdpi .com/1999-5903/13/2/39> .Acesso em: 11 nov. 2025.

UNIVERSIDADE DE BRASÍLIA. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR). Portal da ETIR. Brasília, DF, 2026. Disponível em: https://etir.unb.br.

Acesso em: 8 jan. 2026.

WANG, J *et al*. Visualizing the Landscape of Home IoT Research: A Bibliometric Analysis UsingVOSviewer,MDPI.2023.Disponívelem:https://www.mdpi.com/1424-8220/23/6/ 3086 > Acesso em: 08 nov. 2025.

XIANG, C. *et al*. Empowering Network Security With Programmable Switches: A Comprehensive Survey. IEEE 2023. Disponível em: <https://ieeexplore.ieee.org/abstract /document/10098550 > Acesso em: 21 nov. 2025.

YITONG, R. L *et al*. CSKG4APT: A Cybersecurity Knowledge Graph for Advanced Persistent Threat Organization Attribution.2022. Disponível em: <https://www .ijesat .com / ijesat/files/V23I107_1696484982.pdf >. Acesso em: 21 nov. 2025.

ZHANG, X. *et al*. An Automatic and Efficient Malware Traffic Classification Method for Secure Internet of Things. 2023. Disponível em: <https://ieeexplore .ieee. org/ abstract / docu ment/10261168?signout=success>. Acesso em: 09 nov. 2025.

ZILI, L. *et al*. Federated Learning With Non-IID Data: A Survey. IEEE 2024. Disponível em: < https://ieeexplore.ieee.org/abstract/document/10468591 >. Acesso em: 21 nov. 2025.