REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

DESAFIOS DA SEGURANÇA DA INFORMAÇÃO EM INSTITUIÇÕES DE ENSINO SUPERIOR COM BYOD: UMA REVISÃO SISTEMÁTICA

INFORMATION SECURITY CHALLENGES IN HIGHER EDUCATION INSTITUTIONS WITH BYOD: A SYSTEMATIC REVIEW

Ciências Exatas e da Terra, Ciências Sociais Aplicadas • 25/07/2026

REGISTRO DOI: 10.70773/revistatopicos/784689850

Rafael de Oliveira Capobianco[1]

Gilson Brito Alves Lima[2]

Julio Cesar de Faria Alvim Wasserman[3]

Vanessa dos Santos Cascardo[4]

RESUMO

A rápida digitalização e a expansão tecnológica transformaram as Instituições de Ensino Superior (IES) em ecossistemas digitais complexos, tornando-as alvos preferenciais de ameaças cibernéticas. Neste cenário, o presente artigo tem o objetivo de investigar os desafios inerentes à gestão da Segurança da Informação nas Instituições de Ensino Superior, com ênfase nas vulnerabilidades introduzidas pela prática conhecida como *Bring Your Own Device* (BYOD) e avaliar como os Fatores Críticos de Sucesso podem ser estruturados para mitigar tais riscos. A metodologia adotada consistiu em uma revisão sistemática da literatura, orientada pelas diretrizes do protocolo PRISMA, englobando buscas nas bases Scopus e Google Scholar por artigos publicados predominantemente entre os anos de 2021 e 2026. A análise dos dados revela que as universidades constituem ecossistemas digitais singulares, onde a cultura enraizada de abertura, colaboração e descentralização colide com as premissas tradicionais de controle rigoroso exigidas pelas normas de segurança. A adoção de dispositivos não gerenciados intensifica exponencialmente a superfície de ataque, criando um paradoxo entre a necessidade institucional de monitoramento e o direito inalienável à privacidade do usuário. Os resultados indicam que a resolução desta problemática transcende a simples aquisição de ferramentas tecnológicas, dependendo fundamentalmente do Apoio da Alta Gestão, do Alinhamento ao Negócio e da promoção de uma Cultura de Segurança através de programas contínuos de Conscientização. Conclui-se que as instituições necessitam estabelecer modelos de governança holísticos que equilibrem o rigor técnico, a conformidade legal e a aceitação comportamental orgânica por parte da comunidade acadêmica.

Palavras-chave: Segurança da Informação; Instituições de Ensino Superior (IES); BYOD; Fatores Críticos de Sucesso (FCS).

ABSTRACT

The rapid digitalization and technological expansion have transformed Higher Education Institutions (HEIs) into complex digital ecosystems, making them prime targets for cyber threats. In this scenario, this article aims to investigate the inherent challenges of Information Security management in Higher Education Institutions, with an emphasis on the vulnerabilities introduced by the practice know as Bring Your Own Device (BYOD), and to evaluate how Critical Success Factors can be structured to mitigate such risks. The methodology adopted consisted of a systematic literature review guided by the PRISMA protocol guidelines, encompassing searches in the Scopus and Google Scholar databases for articles published predominantly between the years 2021 and 2026. Data analysis reveals that universities constitute unique digital ecosystems, where the deeply rooted culture of openness, collaboration, and decentralization clashes directly with the traditional premises of strict control required by security standards. The adoption of unmanaged devices exponentially intensifies the attack surface, creating a paradox between the institutional need for monitoring and the user's inalienable right to privacy. The results indicate that the resolution of this problem transcends the simple acquisition of technological tools, depending fundamentally on Top Management Support, Business Alignment, and the promotion of a Security Culture through continuous Awareness programs. It is concluded that institutions need to establish holistic governance models that balance technical rigor, legal compliance, and organic behavioral acceptance by the academic community.

Keywords: Information Security; Higher Education Institutions (HEI); BYOD; Critical Success Factors (CSF).

1. INTRODUÇÃO

O cenário atual é caracterizado por uma transformação digital acelerada e onipresente, redefinindo as relações sociais, produtivas e intelectuais em escala global. Neste novo paradigma, os dados transitaram da condição de meros registros operacionais para se consolidarem como os ativos mais valiosos e estratégicos das organizações. Consequentemente, a Segurança da Informação, cuja essência reside na preservação irrevogável da confidencialidade, da integridade e da disponibilidade dos dados, ascende como um dos pilares de sustentação essenciais para a continuidade de qualquer setor, especialmente frente à sofisticação exponencial e à agressividade das ameaças cibernéticas modernas (Brasil, 2021; Paiva; Gonçalves, 2025).

Quando essa premissa é transportada para o contexto das Instituições de Ensino Superior (IES), a governança digital se depara com um ecossistema peculiar e altamente desafiador. As IES operam em um formato sociocultural que difere radicalmente das corporações tradicionais do mercado financeiro ou da indústria. Historicamente fundamentadas na liberdade de cátedra, na difusão irrestrita do conhecimento e na colaboração científica, as instituições de ensino possuem uma cultura baseada em redes abertas e descentralizadas. Contudo, essas mesmas instituições atuam como guardiãs de bases de dados massivas e extremamente críticas, englobando desde registros pessoais e financeiros de milhares de discentes e servidores até o armazenamento de propriedades

intelectuais decorrentes de pesquisas científicas avançadas (Agalit *et al.*, 2023; Rohan *et al.*, 2025).

O aprofundamento dessa complexidade é diretamente catalisado pelo advento e pela proliferação do modelo conhecido como *Bring Your Own Device* (BYOD), prática que consiste na utilização de hardwares de propriedade particular dos usuários para acessar, processar e armazenar dados da rede corporativa ou institucional. Embora seja indiscutível que esta modalidade fomente a flexibilidade, a mobilidade acadêmica e reduza os custos imediatos de aquisição de equipamentos para a administração, ela insere variáveis de risco cibernético agudas nas instituições. Ao permitir que equipamentos não homologados e não gerenciados transitem pela infraestrutura interna, a instituição abdica do controle sobre o perímetro de segurança, permitindo o intercâmbio perigoso entre aplicativos de uso pessoal e dados governamentais sigilosos (Zambrano; Rafael, 2018; Safdar; Mansour, 2023).

Adicionalmente aos riscos técnicos e operacionais, a gestão da Segurança da Informação na Administração Pública Federal brasileira encontra-se estritamente vinculada a um rigoroso arcabouço legislativo e normativo. A imposição legal para a proteção dos dados dos cidadãos obriga as instituições a orquestrarem seus controles de defesa em conformidade com a Lei de Acesso à Informação (Brasil, 2011), com a Lei Geral de Proteção de Dados Pessoais (LGPD) (Brasil, 2018) e com a recém promulgada Política Nacional de Segurança da Informação (PNSI) (Brasil, 2025). Esse emaranhado jurídico exige que a implementação de políticas restritivas de segurança seja cuidadosamente balizada pelo respeito aos direitos fundamentais de privacidade dos usuários.

Para que o enfrentamento dessas vulnerabilidades não seja fundamentado no mero empirismo, as teorias da administração recomendam a adoção e a estruturação dos Fatores Críticos de Sucesso (FCS). Estes fatores delimitam as áreas vitais de atuação nas quais os resultados satisfatórios assegurarão a governança adequada da organização (Rockart, 1979). A identificação precisa destas variáveis permite que a gestão direcione seus esforços para os elementos que realmente garantem a mitigação dos riscos.

Diante da necessidade urgente de estruturar defesas coerentes com a realidade universitária, o presente artigo orienta-se pela seguinte questão de pesquisa:

Quais são os principais desafios da gestão da Segurança da Informação no ambiente acadêmico e como os Fatores Críticos de Sucesso podem ser estruturados para mitigar os riscos associados à prática de utilização de dispositivos pessoais?

A fim de responder este questionamento, o objetivo principal deste trabalho consiste em realizar uma revisão sistemática da literatura científica global para mapear as vulnerabilidades aprofundadas no contexto das Instituições de Ensino Superior, além de avaliar comparativamente os Fatores Críticos de Sucesso indispensáveis para o delineamento de uma governança madura, eficaz e legalmente amparada nestes ecossistemas. A justificativa para este estudo se baseia na constatação de que o planejamento inadequado das políticas de segurança resulta em normas ineficazes que são sumariamente rejeitadas pela comunidade acadêmica, expondo a infraestrutura nacional a vazamentos de dados com potenciais catastróficos.

2. FUNDAMENTAÇÃO TEÓRICA

A revisão de literatura desta pesquisa estrutura-se na identificação de um quadro teórico que fundamente as particularidades do objeto de estudo. A análise busca demonstrar que o problema da segurança digital nas universidades encontra sustentação nas publicações acadêmicas recentes e que a adoção de estratégias gerenciais específicas é requerida para superar tais obstáculos.

2.1. Os Desafios da Gestão da Segurança da Informação no Ambiente Acadêmico

A transposição das teorias clássicas de proteção corporativa para as Instituições de Ensino Superior esbarra em barreiras estruturais e comportamentais que tornam as universidades um dos ecossistemas mais complexos para a implantação de uma governança robusta.

Historicamente, o cerne da existência de uma instituição acadêmica fundamenta-se na disseminação do conhecimento. Segundo Rohan *et al.* (2025), esta filosofia basilar gera uma cultura de redes abertas que repudia instintivamente bloqueios lógicos ou monitoramentos que assemelhem o ambiente educacional a uma rede militarizada. Na modernidade digital, essa abertura desmesurada fragiliza substancialmente os pilares da segurança corporativa. As universidades abrigam acervos de propriedade intelectual e dados pessoais identificáveis de milhares de indivíduos que se tornam alvos preferenciais para o cibercrime (Agalit *et al.,* 2023).

A exploração maliciosa dessa abertura é atestada pelo alarmante incremento nos ataques de engenharia social voltados para a academia. O fator humano consolida-se unanimemente como a

maior superfície de exposição institucional (Metin; Özhan; Wynn, 2024). Universidades possuem uma rotatividade populacional singular, absorvendo milhares de novos discentes e pesquisadores visitantes anualmente, compondo uma base de usuários com níveis extremamente heterogêneos de letramento digital. Rastenis *et al.* (2025) sublinham que ataques de manipulação psicológica encontram um índice de credulidade altíssimo nas instituições educacionais devido à confiança implícita que os usuários depositam em comunicações originadas de domínios acadêmicos.

Durante a migração compulsória para o ensino remoto, precipitada pela pandemia de COVID19, estudos evidenciaram como as infraestruturas de dados precárias colapsaram, ocasionando interrupções sistêmicas devido a surtos de fraudes e extorsões digitais, comprovando a absoluta ineficácia da defesa reativa (Sinan *et al*., 2024).

Ademais, a infraestrutura destas organizações é rotineiramente testada por severas deficiências orçamentárias. A implementação e a manutenção de defesas cibernéticas eficazes demandam alto investimento. No entanto, diversas instituições operam com orçamentos restritos para a área de tecnologia, caracterizando uma falha gerencial profunda (Nterful *et al.,* 2024). Relatórios governamentais frequentemente revelam deficiências sistêmicas na Administração Pública Federal brasileira, apontando a falta de pessoal qualificado e a defasagem de equipamentos para a implementação de defesas estruturadas (Brasil, 2022).

A conjunção destes fatores resulta na elaboração de diretrizes normativas deficientes. Merchan-Lima *et al*. (2021) e Rios, Teixeira Filho e Rios (2017) diagnosticam que, na tentativa de cumprir meras

formalidades de auditoria, muitas instituições adotam políticas genéricas redigidas em linguajar excessivamente técnico. Tais documentos não refletem as reais operações da universidade e carecem de adesão junto aos usuários, culminando na completa ignorância ou apatia diante das normativas vigentes.

2.2. O Desafio do BYOD na Segurança da Informação

É no cenário de vulnerabilidade crônica do ambiente universitário que a prática do *Bring Your Own Device* atua como um amplificador de riscos sem precedentes. O uso de dispositivos móveis pessoais transformou-se em um padrão global de consumo de tecnologia, forçando as organizações a adaptarem seus perímetros de defesa (Ratchford *et al.*, 2022).

Em ambientes corporativos fechados, as equipes de tecnologia detêm autoridade absoluta sobre os ativos, padronizando equipamentos e bloqueando portas de comunicação. Nas instituições de ensino, a adoção de dispositivos pessoais muitas vezes não ocorre apenas pela conveniência do usuário, atuando frequentemente como um fenômeno motivado pelo subfinanciamento tecnológico estatal (De Ramos; Esponilla, 2022; Canuto, 2022). Diante da defasagem dos computadores institucionais, docentes e servidores suprem essa carência utilizando seus próprios equipamentos para a atividade laboral.

A conexão de aparelhos pessoais, muitas vezes contendo sistemas operacionais desatualizados ou oriundos de redes públicas inseguras, cria vetores para que códigos maliciosos entrem na rede institucional e burlem as proteções do firewall (Safdar; Mansour, 2023). A heterogeneidade intrínseca dos aparelhos dificulta a

aplicação de controles técnicos uniformes, pois a equipe de suporte não consegue garantir compatibilidade técnica com todas as versões de software do mercado (Zambrano; Rafael, 2018).

Neste interstício, consolida-se o maior dos desafios acadêmicos para a governança: a colisão frontal entre os controles de conformidade e o direito inalienável à privacidade. Normas internacionais e boas práticas governamentais recomendam que as organizações apliquem salvaguardas rigorosas sobre dispositivos móveis, incluindo a exigência de monitoramento de tráfego de dados e a capacidade de realizar a limpeza remota das informações em caso de perda do aparelho (ABNT, 2022; Brasil, 2024). No entanto, impor esse grau de auditoria em um bem de propriedade material e financeira do próprio servidor desencadeia forte atrito.

O medo de que a instituição acesse arquivos privados ou promova a deleção indevida dos dados pessoais do proprietário fomenta um instinto de posse corporativa que gera resistência declarada às políticas de segurança (Hovav; Putri, 2016). Os usuários resistem ativamente à norma e encontram métodos subversivos para evadir os sistemas de controle. No Brasil, esta preocupação do usuário está plenamente amparada pelo rigor da legislação de proteção de dados, que proíbe o monitoramento ostensivo e o tratamento desproporcional de dados sem a finalidade explícita e a transparência consentida (Brasil, 2018). Este paradoxo exige que a instituição adote estratégias muito além da tecnologia para garantir a cooperação dos indivíduos (Palanisamy; Norman; Mat Kiah, 2020; Palanisamy; Norman; Mat Kiah, 2021).

2.3. Os Fatores Críticos de Sucesso na Gestão da Segurança da Informação em Ambientes Acadêmicos

Para solucionar os problemas descritos e promover a transição de uma proteção focada puramente em ferramentas lógicas para uma proteção sistêmica organizacional, a academia debruça-se sobre os Fatores Críticos de Sucesso. Tais fatores consistem no número limitado de áreas nas quais os resultados, se satisfatórios, garantirão um desempenho bem-sucedido para a organização (Rockart, 1979). Os estudos de vanguarda consolidam a visão de que a segurança efetiva em cenários heterogêneos deriva invariavelmente da maturidade das decisões gerenciais (Chen; Hai, 2024).

Em uma análise combinada da literatura, o Apoio da Alta Gestão destaca-se de forma unânime. Autores como Almuqrin (2024) e Alnatheer (2015) demonstram que a influência e a postura das lideranças funcionam como predecessores causais para os demais fatores. Na ausência do compromisso institucional visível, a cibersegurança perde sua legitimidade frente à comunidade acadêmica. O envolvimento da liderança garante que a governança receba o orçamento adequado, o que permite a atração e a manutenção de pessoal qualificado (Nterful *et al.*, 2024; Metin; Özhan; Wynn, 2024).

Uma vez estabelecido o apoio político e financeiro, a formulação de uma Política de Segurança da Informação (POSIN) e de diretrizes em conformidade com o aparato legal delineiam a arquitetura normativa. As instituições devem elaborar normas que transpareçam os limites jurídicos, detalhando os deveres e as responsabilidades dos usuários de dispositivos próprios, atuando como o alicerce contratual para dirimir o conflito de privacidade (AlGhamdi; Win; Vlahu-Gjorgievska, 2020).

Contudo, como atestado nos desafios, a imposição de regras estritas não altera o comportamento humano intrínseco. É nesta lacuna que a Cultura de Segurança, a Conscientização e o Treinamento ganham protagonismo absoluto. Rohan *et al.* (2025) e Alyami *et al.* (2024) investigaram os programas de educação corporativa em cibersegurança e revelaram que disparar comunicados eletrônicos anuais possui eficácia próxima a zero. A Segurança da Informação não é uma atividade exclusiva de uma equipe, mas sim uma responsabilidade compartilhada por todos (Metin; Özhan; Wynn, 2024; Paiva; Gonçalves, 2025; Rohan *et al.,* 2025; AlGhamdi; Win; Vlahu-Gjorgievska, 2020; Alnatheer, 2015; Almuqrin, 2024). Para tornar o usuário um elo mais forte na defesa, as organizações devem adotar a personalização e a avaliação contínua das ações educativas, modelando treinamentos que respeitem o nível de letramento do servidor e desconstruindo o viés de que a segurança é uma barreira, para fixá-la como um valor acadêmico (Alyami *et al.*, 2024; Wani *et al.*, 2022).

O sucesso da normatização em dispositivos pessoais também é fortemente relacionado ao Alinhamento ao Negócio. Cheng e Wang (2022) debatem que a missão final da instituição de ensino é a pesquisa e a educação, não a segurança cibernética isolada. Logo, a equipe de governança deve mediar soluções. Em vez de exigir o controle remoto irrestrito de todo o aparelho privado do docente, o alinhamento estratégico impulsiona o uso de contêineres lógicos que proporcionam a separação das esferas de dados sem sacrificar a conveniência.

Por fim, a literatura organiza tais constatações em uma linha temporal operacional segregando os fatores de adoção em etapas prévias e posteriores à implementação. Durante as fases iniciais, as

ameaças cibernéticas, o apoio da diretoria e as pressões de leis governamentais forçam a instituição a realizar uma gestão de riscos preliminar. Durante o ciclo posterior, para que o ecossistema não atrofie, a manutenção da governança passa a exigir esforço incansável no treinamento da força de trabalho e na retroalimentação contínua de estratégias de mitigação baseada no aprendizado com incidentes anteriores (Metin; Özhan; Wynn, 2024).

3. METODOLOGIA

A presente pesquisa caracteriza-se como um estudo qualitativo de revisão sistemática da literatura. O desenho metodológico foi estruturado em conformidade estrita com as recomendações da declaração PRISMA, utilizando de forma pormenorizada os itens descritos em sua versão expandida (Page *et al.*, 2021). A adesão a este protocolo internacional visa mitigar os vieses de seleção do pesquisador, promovendo uma auditoria clara em todas as etapas da filtragem bibliográfica.

A etapa de planejamento fixou critérios de elegibilidade objetivos. Foram admitidos apenas artigos científicos originais e estudos de revisão, submetidos e aprovados sob o crivo de revisão por pares em periódicos acadêmicos. Os idiomas aceitos englobaram a língua inglesa, espanhola e portuguesa. O recorte temporal foi estrategicamente delimitado para capturar a evolução moderna das ameaças cibernéticas, com buscas automatizadas abrangendo predominantemente os anos de 2021 a 2026 para capturar o estado da arte das adaptações tecnológicas recentes. Em contrapartida, foram sumariamente excluídos artigos que possuíam caráter puramente técnico desprovidos de correlação com a governança gerencial, bem como trabalhos restritos ao uso pedagógico de

dispositivos móveis em sala de aula sem o viés da Segurança da Informação.

A busca principal foi executada na base de dados Scopus, reconhecida por sua extensa cobertura em tecnologia e ciências gerenciais. Complementarmente, realizaram-se buscas manuais na base Google Scholar e em portais governamentais para incorporar a literatura institucional brasileira de suma relevância, tais como normativas técnicas publicadas pela Associação Brasileira de Normas Técnicas, portarias, acórdãos de auditoria do Tribunal de Contas da União e leis federais que não são tradicionalmente indexadas como artigos acadêmicos.

A formulação das chaves de busca foi conduzida mediante a aplicação de operadores lógicos, cruzando informações nos campos de título, resumo e palavras-chave dos indexadores. O processo de pesquisa foi dividido em quatro fases primárias para cobrir as facetas do problema.

A primeira execução reuniu inicialmente 34 artigos. e utilizou a seguinte sintaxe:

> *(TITLE-ABS-KEY (cybersecurity)*
>
> ***OR*** *TITLE-ABS-KEY (cibersecurity)*
>
> ***OR*** *TITLE-ABS-KEY ("cyber security")*
>
> ***OR*** *TITLE-ABS-KEY ("ciber security")*
>
> ***OR*** *TITLE-ABS-KEY ("cyber safety")*
>
> ***OR*** *TITLE-ABS-KEY ("ciber safety")*
>
> ***OR*** *TITLE-ABS-KEY ("Information security")*
>
> ***OR*** *TITLE-ABS-KEY ("security polices"))*
>
> ***AND*** *(TITLE ("educational institution")*
>
> ***OR*** *TITLE ("education institution"))*
>
> ***AND*** *PUBYEAR > 2020* ***AND*** *PUBYEAR < 2027*
>
> ***AND*** *(LIMIT-TO (SRCTYPE , "j"))*
>
> ***AND*** *(LIMIT-TO (DOCTYPE , "ar"))*

Esta busca correlacionou segurança cibernética e instituições educacionais, objetivando compreender as fragilidades específicas enfrentadas pelo ensino superior. Dos 34 artigos, 2 foram prontamente descartados por não estarem disponíveis. Os 32 restantes foram então analisados sobre seus títulos e resumos.

Artigos em idiomas diferentes de inglês, espanhol ou português, artigos com foco técnico (criptografia, biometria etc.) e artigos com foco no ensino ao invés da gestão da SI, foram eliminados. Ao final desta etapa, foram selecionados **20 artigos.**

A segunda execução reuniu inicialmente 24 artigos, e utilizou a seguinte string:

> *(TITLE (BYOD OR "personal devices")*
>
> ***AND** TITLE-ABS-KEY ((security **OR** protection) **AND** policy))*
>
> ***AND** PUBYEAR > 2019 **AND** PUBYEAR < 2027*
>
> ***AND** (LIMIT-TO (SRCTYPE , "j"))*
>
> ***AND** (LIMIT-TO (DOCTYPE , "ar"))*
>
> ***AND** (LIMIT-TO (LANGUAGE , "English") **OR** LIMIT-TO (LANGUAGE , "Spanish"))*

Esta busca aprofundou o objeto de risco, isolando estudos voltados ao uso da tecnologia e combinando os termos inerentes aos dispositivos pessoais com os campos de normatização e proteção. Foram aplicados os mesmos critérios de seleção e análise utilizados na Busca 1, excluindo artigos com foco no uso do BYOD para fins educacionais, voltados estritamente a ambientes como hospitais ou bancos e aqueles com foco técnico, em detrimento à governança. Ao final, foram considerados para esta etapa um total de **12 artigos.**

A terceira execução reuniu inicialmente 17 artigos, e utilizou a seguinte string:

> *(TITLE-ABS-KEY (CSF OR "critical success factors")*
>
> ***AND*** *TITLE-ABS-KEY ("information security"))*
>
> ***AND*** *PUBYEAR > 2020 AND PUBYEAR < 2026*
>
> ***AND*** *(LIMIT-TO (SRCTYPE , "j"))*
>
> ***AND*** *(LIMIT-TO (DOCTYPE , "ar"))*

Esta busca focou nos vetores de solução propostos pela literatura, indexando a expressão exata referente aos Fatores Críticos de Sucesso em conjunto com a gestão da segurança. Foram aplicados os mesmos critérios de seleção e análise utilizados anteriormente. Ao final, foram considerados nesta etapa um total de **8 artigos.**

Dada a baixa quantidade de material relevante e com o intuito de obter um material mais voltado às políticas de segurança da informação, foi realizada uma busca complementar mais abrangente, com a seguinte string:

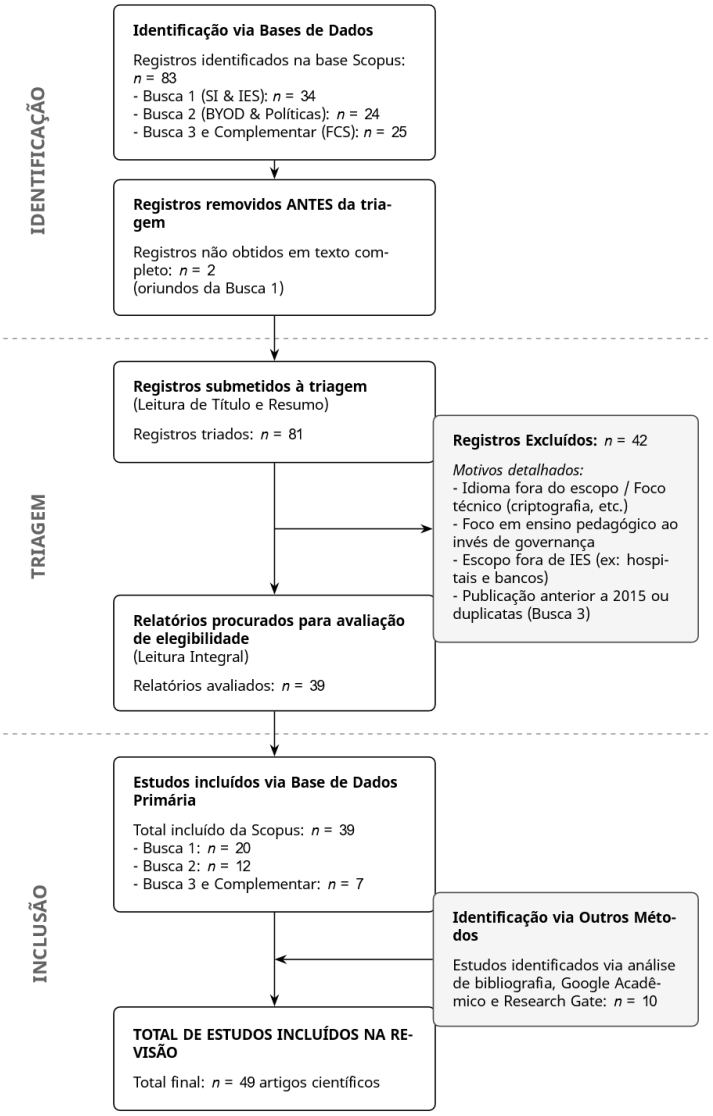
> *(TITLE (CSF OR “critical success factors”)*
>
> ***AND*** *TITLE-ABS-KEY (policy OR polices)*
>
> ***AND*** *TITLE-ABS-KEY (“information security”)*
>
> ***AND*** *PUBYEAR > 2014)*

Após a aplicação dos mesmos critérios de seleção e da remoção de duplicatas, foram selecionados mais **2 artigos.**

O processo de seleção dos estudos obedeceu ao fluxo preconizado pela diretriz PRISMA 2020, culminando no diagrama apresentado na Figura 1. Ao todo, foram obtidos 81 artigos que, após submetidos à etapa de triagem pareada por meio da leitura de títulos e resumos, resultaram em **39 artigos** elegíveis.

Complementarmente, a técnica de *snowballing* (análise das referências bibliográficas) e buscas secundárias focadas no Google Acadêmico permitiram a inclusão de 10 trabalhos e marcos regulatórios adicionais de notória relevância. Dessa forma, o referencial analítico consolidou-se em **49 estudos.**

Figura 1. Fluxograma detalhando o processo de identificação, triagem e inclusão dos estudos.



Fonte: Elaborado pelo autor com base na declaração PRISMA

Para assegurar a robustez da síntese teórica, os 49 documentos finais incluídos na revisão foram submetidos a uma avaliação de qualidade metodológica e adequação ao tema de pesquisa. A leitura crítica integral avaliou a clareza dos objetivos dos estudos selecionados, a coerência na aplicação de Fatores Críticos de Sucesso e a relevância de suas contribuições para a governança em Instituições de Ensino Superior. Trabalhos que apresentaram proposições baseadas exclusivamente em opiniões de autores sem respaldo empírico ou normativo rigoroso receberam menor peso na síntese qualitativa. Esta etapa garantiu que a consolidação dos

resultados refletisse efetivamente o estado da arte das melhores práticas gerenciais em cibersegurança e mitigasse potenciais riscos de viés na extração das recomendações para a governança de BYOD.

4. RESULTADOS E DISCUSSÕES

A análise aprofundada dos dados coletados na revisão sistemática da literatura permite responder diretamente à questão central que norteia esta pesquisa, elucidando quais são os principais desafios da gestão da Segurança da Informação (SI) no ambiente acadêmico e demonstrando como os Fatores Críticos de Sucesso (FCS) podem ser estruturados estrategicamente para mitigar os riscos associados ao uso de dispositivos pessoais (BYOD).

4.1. Os Desafios da Segurança da Informação em IES com BYOD

O primeiro eixo da questão de pesquisa busca compreender os gargalos enfrentados pelas universidades. Os resultados evidenciam que as IES constituem ecossistemas digitais singulares, cujos desafios extrapolam a dimensão tecnológica e esbarram em fatores culturais, financeiros e legais (Agalit *et al.*, 2023).

Inicialmente, observa-se que a cultura fundamental das universidades atua como um catalisador involuntário de vulnerabilidades. A promoção intrínseca do intercâmbio irrestrito de saberes e a descentralização acadêmica chocam diametralmente com os preceitos de proteção enclausurada requeridos pelos padrões internacionais de tecnologia (Rohan *et al.*, 2025). Esta abertura cultural converte o fator humano na engrenagem mais frágil e mais explorada pelas ameaças cibernéticas contemporâneas, como a engenharia social e o *phishing* (Rastenis *et al.*, 2025; Metin; Özhan; Wynn, 2024).

Quando essa abertura é combinada à adoção massiva de dispositivos pessoais (BYOD), a complexidade atinge patamares críticos. A literatura revela que a adoção desta prática, especialmente no contexto das IES públicas, resulta frequentemente da deficiência crônica de financiamento estatal (Canuto, 2022; De Ramos; Esponilla, 2022; Nterful *et al.*, 2024). O grande desafio de governança cristaliza-se quando a instituição de ensino induz o uso de equipamentos privados para manter o ensino e a administração operantes, precarizando sua infraestrutura protetiva.

A partir disso, surge a principal barreira para a gestão da SI no BYOD: o paradoxo entre o controle corporativo e a privacidade do usuário. Ao tentar aplicar os rígidos controles técnicos recomendados por normas como a ABNT NBR ISO/IEC 27002 (como o monitoramento de rede e a limpeza remota de dados) sobre o bem particular que o funcionário está custeando, gera-se um severo atrito social (ABNT, 2022). O ressentimento do usuário, impulsionado pelo medo legítimo de invasão de sua privacidade e da deleção indevida de dados pessoais, resulta em resistência ativa e na subversão das políticas de segurança institucional (Hovav; Putri, 2016; Palanisamy; Norman; Mat Kiah, 2021).

4.2. Estruturação dos Fatores Críticos de Sucesso para a Mitigação de Riscos

O segundo eixo da questão de pesquisa visa estabelecer como estruturar a governança para superar os desafios do BYOD. A análise revela que abandonar a falácia de que as vulnerabilidades serão estancadas puramente pela aquisição de modernos equipamentos de rede é o primeiro passo (Paiva; Gonçalves, 2025). A mitigação

efetiva exige uma orquestração sistêmica dos Fatores Críticos de Sucesso (FCS):

- **Apoio da Alta Gestão (AAG) e Orçamento (ORC):** o sucesso de qualquer iniciativa de segurança depende do compromisso visível e irrestrito da liderança. O Apoio da Alta Gestão (AAG) é o fator matriz que garante a alocação de recursos contínuos para a área técnica e chancela as políticas de segurança de forma documental, legitimando as ações de controle perante a comunidade acadêmica (Chen; Hai, 2024; Almuqrin, 2024; Alnatheer, 2015).

- **Alinhamento ao Negócio (ALN) e Conformidade Legal (LEG):** para solucionar o impasse da privacidade no BYOD, as políticas de segurança não podem asfixiar a usabilidade ou infringir leis (Cheng; Wang, 2022). A estruturação destes fatores exige a elaboração de normativas internas ancoradas no consentimento transparente, informando claramente os limites do monitoramento em consonância com a Lei Geral de Proteção de Dados Pessoais (Brasil, 2018). A governança deve recuar de posturas intervencionistas (como o controle total do aparelho) e adotar proteções lógicas menos invasivas, como a conteinerização (segregação de dados), que preservem a esfera pessoal do usuário (Metin; Özhan; Wynn, 2024).

- **Conscientização (CON), Treinamento (TRE) e Cultura de Segurança (CUL):** A compreensão de que a proteção de dados sensíveis depende do engajamento dos colaboradores transforma a perspectiva gerencial. Programas de capacitação genéricos possuem eficácia próxima a zero (Alyami *et al.*, 2024). A estruturação deste eixo demanda a personalização contínua

das ações educativas, modelando treinamentos que respeitem o nível de letramento digital do corpo docente e técnico (Alyami *et al.*, 2024; Rohan *et al.*, 2025). O objetivo é desconstruir o viés de que a segurança é uma "barreira burocrática", fixando-a como um "valor acadêmico" orgânico e inerente (Wani *et al.*, 2024).

Em síntese, a resposta à questão de pesquisa evidencia que os desafios do BYOD nas Instituições de Ensino Superior (IES) são, fundamentalmente, desafios estratégicos de gestão de pessoas e conformidade. Para que a prática de utilização de dispositivos pessoais ocorra de maneira segura, a governança deve estruturar seus FCS de modo a equilibrar o consentimento do indivíduo (escorado na transparência legal), o financiamento ininterrupto pelas lideranças e a capacitação humanizada. Somente através dessa integração a instituição deixará de ver seus usuários como vulnerabilidades, transformando-os na principal barreira de defesa de seu ecossistema digital e legitimando as ações operacionais de forma proporcional à magnitude da missão da pesquisa acadêmica.

5. CONSIDERAÇÕES FINAIS

Este estudo atingiu seu objetivo principal ao conduzir uma revisão sistemática e aprofundada da literatura internacional a fim de diagnosticar os desafios complexos inerentes à Segurança da Informação no ambiente acadêmico, notadamente sob a crescente adoção de dispositivos pessoais, e alinhar as estratégias mitigadoras sob a ótica dos Fatores Críticos de Sucesso.

O ecossistema das Instituições de Ensino Superior ostenta um dilema de segurança formidável, dado que a essência de sua missão

educacional figura concomitantemente como o seu vetor primário de vulnerabilidade. A adesão massiva de dispositivos de propriedade privada funde os dados institucionais protegidos por legislação governamental estrita aos interesses e comportamentos de risco dos usuários em suas esferas particulares.

A análise metodológica das dezenas de fontes qualificadas demonstra categoricamente que tentativas isoladas de resolver o risco cibernético no ambiente acadêmico através de prescrições puramente tecnológicas fracassarão perante o atrito e a rejeição cultural. As respostas a tais ameaças residem na maestria da gestão estratégica. É fundamental que os gestores aportem compromisso visível e orçamentário duradouro. Demanda-se que a área técnica formule políticas transparentes, flexíveis e alinhadas aos objetivos do negócio, assegurando que o combate ao vazamento de dados não transgrida os direitos fundamentais de privacidade civil.

Conclui-se que o verdadeiro escudo contra as interrupções de serviço não reside nas aquisições de software, mas na mentalidade daqueles que operam o ambiente digital. Investimentos exaustivos em programas perenes de conscientização e cultura de segurança firmam-se como o elemento mais imperativo, convertendo o corpo docente e os funcionários administrativos na principal barreira protetora contra o colapso dos sistemas educacionais em um mundo hiper conectado.

Como limitação inerente ao escopo estrito das revisões bibliográficas delimitadas sob a métrica do protocolo estabelecido, nota-se a potencial não captação de literaturas cinzentas acadêmicas puramente regionais e de casos documentados não indexados em bancos científicos primários de língua inglesa. Para pesquisas

futuras, recomenda-se que modelos empíricos embasados nas estratégias delineadas por este estudo sejam instrumentalizados e submetidos à validação estatística presencial em diferentes polos acadêmicos, prospectando correlações quantitativas diretas entre a evolução da cultura organizacional mensurada e a redução efetiva dos incidentes cibernéticos reportados.

REFERÊNCIAS BIBLIOGRÁFICAS

AGALIT, M.A. et al. A Review of Cybersecurity Management Standards Applied in Higher Education Institutions. **International journal of safety and security engineering,** v. 13, n. 6, p. 1109–1116, 2023. DOI: 10.18280/ijsse.130614.

ALGHAMDI, S.; WIN, K. T.; VLAHU-GJORGIEVSKA, E. Information security governance challenges and critical success factors: Systematic review. **Computers & Security,** v. 99, 102030, 2020. DOI: 10.1016/j.cose.2020.102030

ALMUQRIN, A. How About Enhancing Organizational Security: Critical Success Factors in Information Security Management Performance. Journal of Global Information Management, v. 32, n. 1, 2024.

ALNATHEER, M. A. Information Security Culture Critical Success Factors. **In: INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY - NEW GENERATIONS, 12th 2015. Proceedings [...]** 2015. DOI 10.1109/ITNG.2015.124.

ALYAMI, A. et al. Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an

empirical comparison of practitioner perspectives. **Information & Computer Security,** v. 32, n. 1, p. 53-73, 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 27002: Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação — Requisitos. 3. ed. Rio de Janeiro: ABNT, 2022.

BRASIL. Decreto nº 12.572, de 4 de agosto de 2025. Política Nacional de Segurança da Informação (PNSI). Brasília, DF, 2025.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação (LAI). Brasília, DF, 2011.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos (MGI). **Guia do Framework de Privacidade e Segurança da Informação.** Brasília, DF, 2024.

BRASIL. Portaria GSI/PR nº 93.709, de 18 de outubro de 2021. Glossário de Segurança da Informação. Brasília, DF, 2021.

BRASIL. Tribunal de Contas da União. Acórdão 1.768/2022 - Plenário. Relatório de Acompanhamento. Brasília, DF, 2022.

CANUTO, L. C. Orçamento da pesquisa científica perdeu mais de R$ 80 bilhões nos últimos sete anos. **Agência Câmara de Notícias,** Brasília, DF, 24 maio 2022. Disponível em: https://www.camara.leg.br/noticias/883070-orcamento-da-pesquisa-

cientifica-perdeu-mais-de-r-80-bilhoes-nos-ultimos-sete-anos/. Acesso em: 16 mar. 2026.

CHEN, H.; HAI, Y. Exploring the critical success factors of information security management: a mixed-method approach. **Information & Computer Security,** v. 32, n. 5, p. 545-572, 2024.

CHENG, E. C. K.; WANG, T. Institutional Strategies for Cybersecurity in Higher Education Institutions**. Information (Basel),** v. 13, n. 4, p. 192, 2022. DOI: 10.3390/info13040192.

DE RAMOS, N. M.; ESPONILLA, F. D. Cybersecurity program for Philippine higher education institutions: A multiple-case study. **International Journal of Evaluation and Research in Education,** v. 11, n. 3, p. 1198, 2022. DOI: 10.11591/ijere.v11i3.22863.

HOVAV, A.; PUTRI, F. F. This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. **Pervasive and Mobile Computing,** v. 32, p. 35–49, 2016. DOI: 10.1016/j.pmcj.2016.06.007.

MERCHAN-LIMA, J. et al. Information security management frameworks and strategies in higher education institutions: a systematic review**. Annals of Telecommunications,** v. 76, n. 3-4, p. 255-270, 2021. DOI: 10.1007/s12243-020-00783-2

METIN, B.; ÖZHAN, F. G.; WYNN, M. Digitalisation and Cybersecurity: Towards an Operational Framework. **Electronics,** v. 13, 4226, 2024. DOI: doi.org/10.3390/electronics13214226.

NTERFUL, J. et al. An assessment of critical success factors in information security implementation in organizations in Ghana.

Information & Computer Security, v. 32, n. 5, p. 573-597, 2024. DOI: 10.1108/ICS-11-2022-0174

PAGE, M. J. et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ, v. 372, n71, 2021.

PAIVA, H. W. A.; GONÇALVES, J. G. Segurança Cibernética e Resistência a Ataques em um Mundo Conectado. **Revista Aracê,** v. 7, n. 7, p. 40348–40361, 2025.

PALANISAMY, R.; NORMAN, A. A.; MAT KIAH, M. L. BYOD Policy Compliance: Risks and Strategies in Organizations. **Journal of Computer Information Systems,** v. 62, n. 1, p. 61–72, 2020. DOI: 10.1080/08874417.2019.1703225.

PALANISAMY, R.; NORMAN, A. A.; MAT KIAH, M. L. BYOD security risks and mitigation strategies: Insights from IT security experts. **Journal of organizational computing,** v. 31, n. 4, p. 320–342, 2021. DOI: 10.1080/10919392.2022.2028530.

RASTENIS, J. et al. Research on the Credulity of Spear-Phishing Attacks for Lithuanian Education Institutions' Employees. **Applied Sciences,** v. 15, 3431, 2025. DOI: 10.3390/app15073431

RATCHFORD, M. et al. BYOD security issues: a systematic literature review**. Information Security Journal: A Global Perspective,** v. 31, n. 3, p. 253-273, 2022. DOI: 10.1080/19393555.2021.1923873.

RIOS, O. K. L.; TEIXEIRA FILHO, J. G. A.; RIOS, V. P. S. Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de

segurança da informação. **Navus - Revista de Gestão e Tecnologia,** v. 7, n. 2, p. 49-65, 2017. DOI: 10.22279/navus.2017.v7n2.p49-65.482.

ROCKART, J. F. Chief executives define their own data needs. Harvard Business Review, p. 81–92, 1979.

ROHAN, R. et al. Developing a scale for measuring the information security awareness of stakeholders in higher education institutions. **Education and Information Technologies,** v. 30, n. 10, p. 13713–13777, 2025. DOI: 10.1007/s10639-024-13307-5.

SAFDAR, G. A.; MANSOUR, A. Security and Trust Issues in BYOD Networks. **IT professional,** v. 25, n. 4, p. 45-51, 2023. DOI: 10.1109/MITP.2023.3293714.

SINAN, I. I. et al. Data architectures and the prevalent cyberattacks encountered by West African higher educational institutions in the COVID-19 era. **Journal of Infrastructure, Policy and Development,** v. 8, n. 8, 3736, 2024.

WANI, T. A. et al. BYOD security behaviour and preferences among hospital clinicians: A qualitative study. **International Journal of Medical Informatics,** v. 192, 105606, 2024. DOI: 10.1016/j.ijmedinf.2024.105606

WANI, T. A. et al. BYOD usage and security behaviour of hospital clinical staff: An Australian survey. **International Journal of Medical Informatics,** v. 165, 104839, 2022. DOI: 10.1016/j.ijmedinf.2022.104839

ZAMBRANO, F. R. R.; RAFAEL, G. D. R. Bring Your Own Device (BYOD): a Survey of Threats and Security Management Models. **International**

Journal of Electronic Business, v. 14, n. 2, p. 146-170, 2018. DOI: 10.1504/IJEB.2018.094862.

---

[1] Mestrando em Sistemas de Gestão, Universidade Federal Fluminense (UFF) campus Niterói. LATTES: 5250304040547616

[2] Prof. D.Sc., Universidade Federal Fluminense (UFF) campus Niterói. LATTES: 2248567464602970

[3] Prof. D.Sc., Universidade Federal Fluminense (UFF) campus Niterói. LATTES: 4365891367994000

[4] Pós-graduada em Gestão de Projetos em TI, Fac. Int. Signorelli (FISIG). LATTES: 8674288315914082