Universidades sob ataque hacker: riscos de negócio para segurança cibernética em universidades brasileiras

Emílio Gonçalves, Ígor Ramos Bezerra da Silva, Carlos Eduardo Miranda Zottmann, João Souza Neto, Rafael Rabelo Nunes

Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil - CEP 70910-900.

emiliogoncalves@gmail.com, igorbramos1@unb.br, carlos.zottmann@gmail.com, sznetoj@gmail.com, rafaelrabelo@unb.br

Abstract*: Digitalization has enhanced efficiency and accessibility in educational institutions and increased privacy and security risks. This study aims to identify the business risks faced by universities, where the causes stem from the absence or failure of cybersecurity controls. Through interviews with IT teams, faculty, academic secretaries, and managers, and by employing the Bow Tie technique, nine main business risks were identified, along with their 43 causes and 17 consequences. The findings underscore the relationship between organizational and cyber risks, emphasizing the need for adequate controls, robust security policies, and continuous training to strengthen risk management.*

Resumo: *A digitalização tem potencializado a eficiência e a acessibilidade em instituições de ensino, mas também ampliado os riscos de privacidade e segurança. Este estudo tem como objetivo identificar os riscos de negócio de universidades cujas causas são a ausência ou falha de controles de segurança cibernética. Por meio de entrevistas com equipes de TI, docentes, secretários acadêmicos e gestores, e da análise com a técnica bow tie, foram identificados 9 principais riscos de negócio, suas 43 causas e 17 consequências. Os resultados evidenciam a relação entre riscos organizacionais e cibernéticos, destacando a necessidade de implementar controles eficazes, políticas de segurança robustas e capacitação contínua para fortalecer a gestão de riscos.*

1. Introdução

A gestão de riscos em Instituições de Ensino Superior (IES) públicas tem se consolidado como prática essencial para garantir a eficiência, transparência e proteção dos ativos críticos, principalmente frente aos desafios de privacidade e segurança da informação. Com o aumento da digitalização e a necessidade de governança voltada para a eficiência, transparência e a segurança da informação, o gerenciamento de riscos surge como instrumento para mitigar as ameaças que podem afetar o desempenho institucional e o cumprimento de suas funções sociais [Araújo; Callado, 2022].

A aplicação da gestão de riscos nessas instituições vai além da conformidade regulatória, abrangendo a proteção de ativos, a continuidade dos serviços e o fortalecimento de práticas preventivas. Nesse sentido, a gestão de riscos busca identificar, avaliar e mitigar ameaças potenciais a dados e sistemas essenciais para o funcionamento acadêmico

e administrativo, incluindo a proteção da privacidade de dados pessoais e institucionais [Barbosa; Cunha; Loose, 2024].

Em termos de normativos, a gestão de riscos no Poder Executivo, ao qual as universidades públicas brasileiras são subordinadas, é regulamentada pela Instrução Normativa MP/CGU Nº 01/2016 e pelo Decreto nº 9.203/2017, que estabelecem orientações para integrar o gerenciamento de riscos à estratégia institucional. Por outro lado, o Programa de Proteção e Segurança da Informação (PPSI) é uma iniciativa que busca proteger as informações sensíveis no âmbito do poder executivo, prescrevendo pouco mais de 300 controles de privacidade e segurança da informação que atuam nesses riscos. No entanto, a aplicação prática em universidades ainda enfrenta barreiras culturais e operacionais, demonstrando níveis variados de maturidade e a necessidade de políticas estruturadas que apoiem a implementação eficiente dessa prática [Barbosa; Cunha; Loose, 2024].

Apesar dos desafios, as IES podem melhorar sua governança e capacidade de prevenção e resposta a incidentes ao implementar estruturas de gestão de riscos adaptadas às suas necessidades específicas. A integração dessas práticas aos processos institucionais favorece uma gestão mais transparente e resiliente, capaz de mitigar os efeitos adversos de riscos internos e externos sobre os objetivos acadêmicos e administrativos [Araújo; Callado, 2022], [Barbosa; Cunha; Loose, 2024].

Nesse sentido, levanta-se a questão central desta pesquisa: quais são os riscos de negócio que impactam os objetivos das universidades e cujas causas são violações de privacidade e segurança da informação? Se há lacunas nesse entendimento, se os incidentes decorrentes desses riscos podem acarretar não apenas perdas operacionais e reputacionais, mas também comprometer o próprio desempenho da gestão acadêmica e administrativa. Portanto, compreender o grau de conhecimento e a preparação das IES frente a possíveis riscos torna-se fundamental para orientar estratégias de mitigação e melhorar a governança institucional [Araújo; Callado, 2022], [Barbosa; Cunha; Loose, 2024].

Este trabalho, assim, tem como objetivo identificar os riscos de negócio de IES cujas causas são a ausência ou falha de controles de segurança cibernética. Ao final, espera-se contribuições que sirvam de subsídio para o fortalecimento das políticas de segurança e a conscientização dos agentes envolvidos, consolidando uma cultura institucional orientada pela privacidade e segurança, pela proteção de dados e pela resiliência operacional. Esse trabalho segue a estrutura tradicional de um artigo científico, ou seja, além dessa introdução, será apresentado o referencial teórico na seção 2, os métodos empregados para se atingir o objetivo de se identificar os riscos de negócio na seção 3, os resultados obtidos com as discussões na seção 4, e por fim, as conclusões na seção 5.

2. Referencial Teórico

A tecnologia, embora ofereça inúmeras vantagens, também traz desafios, riscos e ameaças, introduzindo complexidades adicionais e potenciais vulnerabilidades que exigem uma gestão cuidadosa [Moreira et al., 2021].

No que se refere à segurança da informação, esta é definida como a proteção de dados e sistemas contra acessos não autorizados, uso indevido, divulgação, interrupção, modificação ou destruição, preservando confidencialidade, integridade e disponibilidade [Alves; Queiroz; Nunes, 2024]. Já a segurança cibernética, uma vertente da segurança da

informação, concentra-se especificamente na proteção de informações no meio digital [Alves; Georg; Nunes, 2023].

Em âmbito organizacional, as incertezas ocorrem a todo momento. Uma incerteza se refere a situações em que não há informações suficientes para entendimento do cenário ou conhecimento quanto às consequências de determinado evento [Bermejo et al., 2018]. Conceitua-se risco o efeito da incerteza no atingimento dos objetivos organizacionais [ABNT, 2018].

O gerenciamento de riscos é uma estrutura que inclui diversos processos com o fim de gerar o controle sobre esses [Araújo; Gomes, 2021]. Trata-se de uma adição relativamente nova ao conceito mais amplo de governança corporativa e que inclui processos e sistemas estabelecidos pela administração para garantir que a filosofia de risco seja agregada às atividades diárias da organização [Coetzee; Lubbe, 2011].

Conforme Pardini (2019), a governança corporativa só é efetiva quando acompanhada de boa consciência e gestão de riscos. Esse instrumento contribui para melhorar o desempenho por meio da identificação de oportunidades e a redução da probabilidade e impacto dos riscos, além de apoiar os esforços de garantia da conformidade dos agentes aos princípios éticos e às normas legais [Vieira; Barreto, 2019].

Frameworks como o COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) são amplamente utilizados como referência na gestão de riscos, fornecendo diretrizes essenciais para a identificação, avaliação e mitigação de ameaças organizacionais [Giestosa et al., 2023], [Menezes et al., 2019].

Padrões internacionais como a ISO 31000 fornecem diretrizes para a implementação de processos sistemáticos e eficazes de gestão de riscos [Giestosa et al., 2023], [Menezes et al., 2019]. No Brasil, a Instrução Normativa Conjunta nº 1/2016, da CGU e do Ministério do Planejamento, estabeleceu a Política de Gestão de Integridade, Riscos e Controles Internos na administração pública federal, reforçando a importância da governança e da gestão de riscos no poder executivo [Araújo; Gomes, 2021].

Além disso, a Portaria SGD/MGI nº 852, de 28 de março de 2023, instituiu o Programa de Privacidade e Segurança da Informação (PPSI), uma iniciativa do governo federal voltada para orientar os órgãos e entidades do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) na implementação de práticas robustas de privacidade e segurança da informação. O programa tem como objetivo elevar a resiliência e a maturidade institucional, garantindo maior proteção aos dados e sistemas da administração pública.

A fundamentação do PPSI é inspirada na abordagem de controles e implementação do CIS (CIS, 2021), estrutura do núcleo do *Privacy Framework* (NIST, 2020) e normas ISO/IEC e ABNT NBR. O PPSI é um framework para aprimorar a privacidade e segurança da informação, com foco no atendimento à Lei Geral de Proteção de Dados Pessoais (LGPD) e à Política Nacional de Segurança da Informação (PNSI). O PPSI detalha controles de cibersegurança e privacidade, estruturados em grupos de implementação e alinhados a normativos do Gabinete de Segurança Institucional (GSI) e da Autoridade Nacional de Proteção de Dados (ANPD). Ele propõe uma metodologia de implementação em ciclos interno e externo, além de um sistema de avaliação de maturidade por meio de indicadores.

A implementação da gestão de riscos no setor público, incluindo as universidades, enfrenta desafios significativos relacionados à cultura de conformidade, que frequentemente dificulta a internalização de uma abordagem proativa e eficaz de gestão de riscos [Araújo; Callado, 2022]. Segundo os autores essa prática, quando percebida apenas como um requisito formal, tende a resultar em uma adoção superficial, centrada na documentação de conformidade em vez de promover a efetiva mitigação de riscos. Nesse sentido, Ahmeti e Vladi, (2017) destacam que a gestão de riscos em ambientes públicos demanda esforços substanciais para superar a cultura de conformidade prevalente, que frequentemente prioriza o cumprimento normativo em detrimento de uma perspectiva estratégica e integrada.

A gestão de riscos em IES é um tema de crescente relevância, impulsionado pela necessidade de transparência, prestação de contas e melhoria na qualidade dos serviços oferecidos [Barbosa; Cunha; Loose, 2024]. A complexidade do ambiente universitário, com sua diversidade de atividades, atores e novos desafios e ameaças cada vez mais sofisticadas na área de tecnologia da informação exige uma abordagem sistemática e integrada para identificar, avaliar e tratar os riscos [Araújo; Callado, 2022] [Dioubate; Wan Daud, 2022].

Apenas em 2022, conforme levantamento da Fortinet, 103 bilhões de tentativas de ataques cibernéticos foram registradas no Brasil. Em maio de 2021 seis instituições sofreram ciberataque, entre elas, a Universidade Federal do Rio de Janeiro (UFRJ), a Universidade Federal de Alagoas (UFAL), Universidade Federal do Tocantins (UFT), Universidade Federal de Minas Gerais (UFMG), Universidade Federal da Grande Dourados (UFGD) e a Universidade Federal da Bahia (UFBA) [Polícia Federal, 2022]. Em setembro de 2023, a Universidade Federal de Mato Grosso do Sul (UFMS) também sofreu ataque cibernético [*Security Leaders*, 2022].

A adoção da gestão de riscos pelas Instituições de Ensino Superior (IES) representa uma estratégia fundamental para a mitigação de impactos que comprometem seus ambientes acadêmicos. A identificação e a análise da probabilidade e do impacto dos riscos permitem aos gestores acadêmicos agirem de forma mais ágil e eficaz diante de adversidades [Ramos et al., 2018]. Este processo é essencial, pois viabiliza a antecipação de ameaças que envolvem aspectos como finanças, infraestrutura, tecnologia, manutenção e pesquisa científica, os quais influenciam diretamente a reputação e a sustentabilidade da educação superior [Wang et al., 2018].

Nesse cenário, torna-se imprescindível avaliar o desempenho das IES públicas, uma vez que essas informações subsidiam a tomada de decisões e promovem uma gestão mais eficiente e orientada a resultados [Moreira; Benedicto; Carvalho, 2019]. Considerando as especificidades que caracterizam essas instituições, a adoção de práticas robustas de controle e governança torna-se ainda mais relevante diante das exigências do contexto educacional contemporâneo [Sedrez; Fernandes, 2011].

A capacitação do capital humano, incluindo gestores e servidores, é fundamental para o sucesso da implementação da gestão de riscos [Araújo; Callado, 2022]. O envolvimento ativo da alta administração também é essencial para garantir que a gestão de riscos seja priorizada e integrada em todas as áreas da instituição [Araújo; Callado, 2022]. A disseminação da estratégia institucional e a comunicação transparente são elementos-chave para fortalecer a gestão de riscos, garantindo que todos compreendam as suas responsabilidades e os riscos envolvidos.

No contexto das IES, os riscos podem variar desde evasão escolar e dificuldades financeiras até falhas de segurança da informação e ameaças à imagem institucional [Barbosa; Cunha; Loose, 2024] e [Araújo, 2019]. Esses riscos devem ser analisados considerando tanto fatores internos quanto externos [Araújo; Callado, 2022]. A ausência de controles internos eficazes, aliada ao descumprimento de leis e normas, pode amplificar esses riscos e comprometer a sustentabilidade institucional [Barbosa; Cunha; Loose, 2024].

A gestão de riscos em ambientes de pesquisa não se limita à proteção de dados, mas também resguarda o conhecimento produzido, incluindo segredos industriais e propriedade intelectual [Junior; Santos; Albuquerque, 2014]. As universidades precisam garantir que os dados estejam sempre protegidos contra corrupção, destruição ou roubo em potencial [Ismail et al., 2022]. Estas instituições gerenciam, segundo Bittencourt et al. (2024), grandes quantidades de pesquisas valiosas e dados sensíveis, o que as torna alvos atrativos para criminosos cibernéticos, espionagem e *hackers* em geral.

Dessa maneira, estão cada vez mais expostas a riscos cibernéticos em função da crescente conectividade e transposição de suas atividades para o meio digital. O aumento significativo no número e na gravidade dos ataques cibernéticos recentemente ressaltam a necessidade crítica de uma gestão eficiente de segurança cibernética [Krumay et al., 2018].

3. Metodologia

Este artigo apresenta uma pesquisa de natureza aplicada. Adotou-se abordagem qualitativa que não requer utilização de métodos e técnicas estatísticas, tendo como focos principais o processo e seu significado. A partir desta perspectiva busca-se interpretar e atribuir significado a um fenômeno do mundo real caracterizado por sua subjetividade e que nem sempre pode ser representado numericamente [Silva e Menezes, 2005]. Essa abordagem é apropriada para compreensão de temas pouco compreendidos, oferecendo análise aprofundada acerca de fatores subjetivos e contextuais. Para a coleta de dados, foram utilizadas entrevistas semiestruturadas e grupo focal, possibilitando reunir informações relevantes, com o intuito de capturar diferentes percepções e experiências dos participantes.

O estudo tem um caráter exploratório, pois busca investigar um problema ou tema ainda pouco estudado. Essa abordagem é amplamente utilizada quando há escassez de informações disponíveis, permitindo uma análise flexível, adaptável e não rígida. Segundo Gil (2017), pesquisas acadêmicas costumam assumir um viés exploratório em seus estágios iniciais, uma vez que, nesse momento, o pesquisador pode ainda não ter delimitado com clareza o objeto de investigação. De acordo com Selltiz (1967), esse tipo de pesquisa frequentemente inclui revisões de literatura, estudos de caso e entrevistas com indivíduos que possuem experiência relacionada ao problema em análise, possibilitando uma compreensão mais ampla do fenômeno estudado.

Além disso, este estudo contou com o emprego de ferramentas de IA generativa, como o ChatGPT e o NotebookLM, para aprimorar a tradução de trechos textuais, a revisão ortográfica e gramatical, bem como a consolidação dos dados obtidos nas entrevistas.

Os eventos que pudessem gerar consequências legais, estratégicas, financeiras, operacionais e de imagem para as atividades finalísticas da organização, foram

classificados como riscos de negócio. Para sua definição, foram empregadas ferramentas amplamente utilizadas nas etapas de identificação e análise de riscos, incluindo análise preliminar de perigos, entrevistas semiestruturadas e a técnica Bow Tie, garantindo uma abordagem estruturada e abrangente. Optou-se por adotar neste estudo a mesma abordagem metodológica utilizada no trabalho desenvolvido por Alves et al. (2023). Essa escolha contribui nos procedimentos de coleta, sistematização dos dados e análise dos resultados.

A técnica *Bow Tie* foi escolhida por sua capacidade de expressar visualmente, de maneira estruturada, a relação entre um risco, suas possíveis causas e as consequências associadas. Essa abordagem é amplamente empregada na gestão de riscos, pois permite representar cenários complexos de forma clara e acessível. Segundo a ABNT (2019), a técnica é particularmente útil quando um mesmo evento pode ser desencadeado por múltiplas causas e gerar diversas consequências, como ocorre no contexto das IES.

Para identificar e compreender os riscos, a pesquisa seguiu um processo estruturado em sete etapas interligadas (Figura 1), garantindo uma análise abrangente e contextualizada. Essas etapas incluíram a definição do escopo da pesquisa, a coleta e análise de dados e a validação dos resultados.

Figura 1 - Etapas da pesquisa

Foram selecionados nove participantes de três Instituições de Ensino Superior, representando diferentes áreas dessas organizações. Entre os participantes, estavam dois professores, com média superior a onze anos de atuação, três secretários acadêmicos, dois técnicos de TI e dois gestores (um da área técnica de TI e outro da área administrativa), com média de sete anos de experiência no serviço público. Essa composição teve como objetivo capturar uma visão multidisciplinar sobre os riscos e suas consequências no uso e na gestão de dados acadêmicos, proporcionando uma análise mais abrangente e representativa.

Foram realizadas entrevistas semiestruturadas, nas quais cada participante respondeu individualmente a um conjunto de perguntas previamente elaboradas. O roteiro foi estruturado para estimular os entrevistados a relatarem situações de riscos vivenciadas em suas atividades na IES, analisar os cenários sob diferentes perspectivas e sugerir riscos potenciais ou já observados. Essa técnica proporciona maior flexibilidade, permitindo que a conversa explore questões emergentes e se torna particularmente útil quando não é viável reunir os participantes em uma sessão de *brainstorming* [ABNT, 2019]. Para ampliar a reflexão e incentivar os entrevistados a considerarem cenários improváveis ou inesperados, foi apresentada uma lista preliminar de riscos, destacando potenciais ameaças aos objetivos institucionais das IES. A lista preliminar de risco foi elaborada por profissionais

de IES com experiência na rotina das instituições e conhecimento dos incidentes que comumente impactam as operações.

As perguntas utilizadas foram:

1. Identificação e Impactos dos Riscos: "Na sua opinião, por que é importante identificar os riscos que podem afetar o funcionamento das instituições de ensino? Quais seriam os impactos caso esses riscos não fossem gerenciados adequadamente?"
2. Causas e Consequências: "Além de identificar os riscos, você acredita que é fundamental entender suas causas e consequências? Poderia dar um exemplo prático disso?"
3. Experiências Práticas: "Já percebeu alguma situação ou rotina na instituição que represente um risco para as atividades acadêmicas ou administrativas? Poderia nos contar mais sobre essa experiência?"
4. Avaliação dos Controles Existentes: "Na sua percepção, os controles atualmente implementados na instituição são suficientes para mitigar esses riscos? Há alguma área que você acredita estar mais vulnerável?"
5. Relevância dos Riscos Apresentados: "Ao olhar para esta lista de riscos: vazamento de dados acadêmicos; vazamento de dados pessoais; alteração de dados acadêmicos; perda de informações acadêmicas; perda de informações administrativas críticas; inadequação às legislações e regulamentações aplicáveis; falsificação ou fraude de documentos oficiais da instituição; você acredita que eles são representativos dos desafios enfrentados pela instituição? Algum desses riscos não parece tão relevante para sua realidade? Há algum outro risco que deveríamos considerar?"
6. Sugestões para Melhoria dos Controles: "Os controles existentes na sua instituição são suficientes para tratar esses riscos? Se não, que melhorias ou novos controles você sugeriria?"

Após a realização das entrevistas em duas instituições, observou-se padrões e repetições nas respostas. Para ampliar a diversidade de perspectivas, foram conduzidas novas entrevistas com participantes de uma terceira instituição. Em seguida, as respostas foram analisadas de forma criteriosa, usando o *Bow Tie* a fim de distinguir corretamente os riscos de suas causas e consequências.

Por fim, para validar os resultados, foi constituído um grupo focal composto por dois gestores de segurança da informação e um especialista em gestão de riscos, sendo um representante de cada instituição. Conforme Trad (2009), o grupo focal é uma técnica qualitativa que explora a dinâmica de grupo para coletar informações detalhadas sobre um tema específico, permitindo que os participantes, orientados por um moderador, compartilhem suas percepções, proporcionando uma compreensão mais aprofundada do assunto. Nesse sentido, apresentou-se uma proposta de classificação que inclui causas, riscos e consequências, e essa proposta foi submetida à análise dos participantes. Os dados foram, então, consolidados em tabelas, analisados e validados pelos especialistas, garantindo maior rigor e precisão aos achados da pesquisa.

4. Resultados e Discussões

A partir da análise dos dados obtidos nas entrevistas foram listados 173 possíveis riscos, que foram organizados utilizando a técnica *bow tie*, tendo sido elaborado um diagrama para cada entrevista e, posteriormente, um único diagrama com todos os dados. Após a análise, observou-se que alguns dos riscos inicialmente identificados foram confirmados efetivamente como riscos, enquanto outros revelaram-se como causas ou consequências, com ocorrências de repetições. Esse processo de verificação e categorização foi essencial para o aprimoramento e a consolidação dos resultados.

Ao final, chegou-se a nove riscos de negócio, 43 possíveis causas e 17 possíveis consequências. Após a análise das respostas, foi possível identificar nove categorias principais de riscos de negócio, conforme apresentado na Tabela 1.

Tabela 1. Riscos de negócio dos processos de registro acadêmico

[1]	Vazamento de notas, históricos escolares ou dados de desempenho acadêmico
[2]	Vazamento de CPF, endereços, números de telefone de alunos, professores ou servidores
[3]	Alteração não autorizada de notas, frequência, histórico ou diploma/certificados acadêmicos
[4]	Perda ou corrupção de registros acadêmicos como matrículas, históricos e dados de desempenho acadêmico
[5]	Indisponibilidade de sistemas acadêmicos
[6]	Perda de informações administrativas críticas (gerenciamento de turma, alocação de professor para turma).
[7]	Descumprimento de normas legais e regulatórias, como LGPD, LAI, normas do MEC e diretrizes educacionais
[8]	Falsificação de diplomas ou certificados e documentos oficiais
[9]	Processos judiciais por práticas discriminatórias, danos morais ou descumprimento de legislações vigentes

Com base na análise *bow tie*, foram identificadas diversas causas que contribuem para a materialização dos riscos mencionados. A Tabela 2 exemplifica essas causas organizadas por risco identificado, o que permite relacionar riscos técnicos com riscos de negócio.

Tabela 2. Análise Bow tie (Fontes e Riscos de Negócio)

Causas e Fontes	Riscos
Comprometimento de credenciais de acesso	
Controles de acesso físico e lógicos inadequados	
Falhas de segurança em sistemas	[1][2]
Falhas na gestão de credenciais	
Exfiltração de dados	

Ataques cibernéticos	
Falta de monitoramento e auditoria	
Sabotagem por parte de usuários e colaboradores internos	
Falta de conscientização sobre segurança da informação	
Acesso indevido a sistema acadêmicos	
Privilégios excessivos e falta de segregação dos usuários	
Sabotagem por parte de usuários ou colaboradores internos	
Vulnerabilidade em *software* ou servidor, sistema desatualizado e ausência de criptografia	[3]
Ataques cibernéticos e exploração de vulnerabilidades	
Falta de conscientização sobre segurança da informação	
Ataques cibernéticos	
Falta de padronização de procedimentos e processos	
Erros humanos e falhas operacionais	
Incompatibilidade entre sistemas e serviços legados	[4][5][6]
Falha na infraestrutura de TI	
Desastre naturais e acidentais que impactam o DataCenter	
Ausência de controle de acesso privilegiado	
Sabotagem por parte de usuários ou colaboradores internos	
Falta de conhecimento/treinamento sobre as legislações aplicáveis	
Processos de conformidade pouco claros ou inexistentes	
Concessão de permissões além do necessário	
Falta de auditoria contínua sobre processos	[7]
Normas internas desatualizadas em relação a normativos	
Falta de recursos dedicados à conformidade legal	
Desconhecimento ou interpretação confusa de leis	
Falhas na verificação de autenticidade de documentos	
Acesso indevido a sistemas de emissão de documentos	
Falta de padronização dos procedimentos e processos	[8]
Discente ou colaborador mal-intencionado	
Desmotivação por parte dos funcionários	
Falta de integração entre sistemas	

Falta de conscientização/treinamento dos usuários	
Contestações de discentes	
Inadequações a legislações aplicáveis	
Alteração/uso indevido de dados acadêmicos/pessoais sem autorização	[9]
Perda/vazamento de dados pessoais/acadêmicos	
Falsificação/fraude de documentos	

Percebe-se, na Tabela 2, que uma mesma causa ou fonte pode gerar um ou mais riscos de negócio. É fundamental compreender como uma causa comum pode se desdobrar em vários riscos diferentes e como estes podem estar interligados.

Observou-se que um único evento pode desencadear múltiplas consequências, cada qual configurando um risco distinto. Nesse sentido, os entrevistados destacaram as implicações que esses riscos podem acarretar para a universidade, reconhecendo, em alguns casos, que não possuíam plena consciência desses impactos antes da pesquisa. A Tabela 3 consolida essas consequências.

Tabela 3. Análise *Bow tie* (Consequências dos Riscos)

Riscos de Negócio	Consequências
[1][2][3][4][5][6][7][8][9]	Prejuízo à imagem e danos à reputação
[1]	Exposição de dados sensíveis
[1][4][5]	Interrupção dos serviços e atividades acadêmicos
[1][2][3][8]	Ações judiciais por violação de dados privacidade
[1][2][4][6][7]	Sanções legais, multa, indenizações e penalidades
[2][7]	Responsabilização civil, penal e administrativa
[2]	Ocorrência de fraudes e golpes contra afetados
[3][5]	Comprometimento da integridade acadêmica
[3][8]	Danos à meritocracia e à equidade
[3][8]	Ocorrência de fraude acadêmica
[4][5]	Custos de recuperação de dados e medidas corretivas

[5][6]	Comprometimento da continuidade da operação acadêmica
[6][8]	Danos financeiros à Administração Pública
[5][7]	Custo emergencial para adequação
[8]	Invalidação de documentos oficiais
[8]	Correção de processos administrativos
[8][9]	Intervenção de órgãos de controle

De modo geral, constatou-se que, embora existam políticas e normativos voltadas à proteção de dados e à segurança da informação, ainda há uma lacuna significativa no entendimento sobre as consequências de que possíveis incidentes podem causar ao negócio acadêmico. Muitos servidores, inclusive aqueles em cargo de gestão, apesar de reconhecerem a relevância de uma cultura de gestão de riscos, não possuem a exata compreensão sobre as consequências para o negócio que uma falha pode proporcionar.

Essas consequências estão alinhadas com estudos sobre impactos da segurança da informação na gestão acadêmica, destacando que vazamentos de dados podem levar a processos judiciais, sanções regulatórias e perda de credibilidade institucional [ISO/IEC 27005, 2021; ABNT NBR ISO/IEC 27701, 2020].

5. Conclusão

A crescente digitalização dos processos administrativos e acadêmicos das IES trouxe benefícios significativos, como maior acessibilidade, eficiência e transparência. No entanto, essa transformação também ampliou a superfície de exposição a riscos de segurança da informação, tornando essencial a adoção de estratégias robustas de gestão de riscos.

Os resultados da pesquisa indicam que, embora as instituições possuam diretrizes normativas relacionadas à privacidade e segurança da informação, na prática, há uma lacuna significativa na compreensão das consequências de uma violação desses princípios. A análise demonstrou que muitos gestores e servidores reconhecem a importância da segurança da informação, mas não possuem clareza sobre os impactos reais que uma falha pode acarretar, tanto em termos operacionais quanto em relação à reputação institucional.

Entre os riscos mais críticos identificados, destacam-se o vazamento de dados, acessos não autorizados e ataques direcionados a sistemas acadêmicos. As consequências potenciais dessas violações incluem interrupção das atividades acadêmicas, comprometimento da integridade dos registros institucionais, exposição de dados pessoais de alunos e servidores, além de possíveis sanções legais e perda de credibilidade perante a comunidade acadêmica e a sociedade.

Portanto, o estudo revela que o conhecimento das instituições sobre as consequências das violações dos princípios de privacidade e segurança é parcial. Embora haja preocupação com a temática, a dimensão das consequências e impactos legais, financeiros, de conformidade e reputacionais ainda não está plenamente internalizada. Apesar do

reconhecimento da necessidade de proteção de dados e conformidade regulatória, a pesquisa indica que as instituições não assimilaram completamente os impactos das violações de segurança e privacidade. Essa falta de maturidade pode comprometer a implementação de controles preventivos e a capacidade de resposta eficaz diante de incidentes.

Diante desse cenário, é possível sugerir algumas medidas para aprimorar a gestão de riscos nas universidades. O fortalecimento da governança e da cultura de segurança deve ser uma prioridade, por meio da adoção de uma abordagem proativa para a gestão de riscos. Isso envolve o engajamento da alta administração e o alinhamento estratégico das ações de segurança à missão institucional, garantindo que a proteção dos ativos de informação seja um pilar essencial para o funcionamento acadêmico e administrativo.

A implementação de programas estruturados como o PPSI tem se mostrado fundamental para o fortalecimento da resiliência das IES diante de um cenário marcado por riscos crescentes à privacidade e à segurança da informação. Ao promover a sensibilização, conscientização e capacitação dos diversos atores institucionais, o PPSI contribui para o desenvolvimento de uma cultura organizacional orientada à gestão de riscos, conforme preconizam *frameworks* como o COSO, ISO 27001 e a ISO 31000. Essa abordagem não apenas eleva o nível de maturidade em governança da informação, mas também permite que as IES respondam de forma mais eficaz a incidentes, antecipem ameaças emergentes e mantenham a continuidade de suas atividades essenciais, especialmente no que se refere à proteção dos dados acadêmicos, administrativos e científicos

Outro aspecto relevante é o monitoramento contínuo e a auditoria de sistemas, realizados com ferramentas especializadas para a detecção de ameaças e a avaliação periódica da segurança dos sistemas acadêmicos. Esses controles são recomendados pelo PPSI, o que reforça a importância de identificar vulnerabilidades e agir de forma proativa na mitigação dos riscos, contribuindo para a melhoria contínua da segurança da informação no ambiente acadêmico. Por fim, a integração da gestão de riscos à estratégia institucional é essencial para mitigar impactos financeiros, operacionais e reputacionais decorrentes de incidentes cibernéticos. Inserir a segurança da informação no planejamento estratégico das universidades assegura que a proteção dos dados seja tratada de forma transversal e alinhada às demais iniciativas institucionais.

A pesquisa reforça a necessidade de uma abordagem multidisciplinar na gestão de riscos cibernéticos, considerando não apenas aspectos tecnológicos, mas também fatores organizacionais, normativos e humanos. Ao priorizar a segurança da informação como pilar estratégico, as instituições podem fortalecer a proteção de seus ativos críticos e garantir um ambiente acadêmico seguro e confiável.

Embora promissores os resultados, é importante destacar as limitações inerentes à pesquisa. Em primeiro lugar, registra-se a dificuldade de seleção de candidatos para participação nas entrevistas. Nota-se que quanto mais elevado o posto ocupado pelo colaborador na hierarquia da sua instituição, mais difícil viabilizar as entrevistas e muitos deles demonstram relutância em discutir sobre o gerenciamento de riscos. Em segundo lugar, o tamanho da amostra pode não refletir adequadamente a diversidade e limitar a capacidade de generalizar os resultados. Por fim, percebe-se um certa estabilidade e padrão de repetição nas respostas dos entrevistados.

Como perspectiva futura, recomenda-se aprofundar análises qualitativas e quantitativas sobre a probabilidade e o impacto de cada risco, bem como expandir o número de instituições investigadas para compreender diferenças regionais e administrativas.

Dessa forma, espera-se que este trabalho contribua para o amadurecimento das estratégias de segurança e privacidade nas instituições de ensino, conduzindo a uma gestão de riscos mais eficaz e resiliente.

6. Referências

Ahmeti, R. and Vladi, B. (2017) "Risk management in public sector: A literature review", *European Journal of Multidisciplinary Studies*, vol. 2, no. 5, pp. 190–196.

Alves, R. S., Georg, M. A. C. and Nunes, R. R. (2023) "Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros", *Revista Ibérica de Sistemas e Tecnologias de Informação*, special issue E56, pp. 344–357.

Alves, R. S., Queiroz, C. E. M. and Nunes, R. R. (2024) "Os tribunais têm estrutura para gerenciar riscos de segurança da informação? Um estudo à luz das Três Linhas", *Revista CEJ*, vol. 27, no. 86.

Araújo, A. A. de (2019) *Gestão de risco no setor público: percepção do gerenciamento de riscos nas universidades federais*. MSc Dissertation, Universidade Federal Rural de Pernambuco, Recife, 229 pages.

Araújo, A. and Gomes, A. M. (2021) "Risk management in the public sector: Challenges in its adoption by Brazilian federal universities", *Revista Contabilidade e Finanças*, vol. 32, no. 86, pp. 241–254.

Araújo, A. and Gomes, A. M. (2021) "Gestão de riscos no setor público: desafios na adoção pelas universidades federais brasileiras", *Revista Contabilidade & Finanças*, vol. 32, no. 86, pp. 241–254.

Araújo, J. G. R. de and Callado, A. L. C. (2022) "Concepção e Implementação de Práticas de Gestão de Riscos: Uma Análise em uma Instituição Federal de Ensino Superior Brasileira", *Contabilidade, Gestão e Governança*, vol. 25, special issue, pp. 308–330.

Associação Brasileira de Normas Técnicas (2018) *NBR ISO 31000: Gestão de Riscos – Diretrizes*. Rio de Janeiro.

Associação Brasileira de Normas Técnicas (2021) *NBR ISO 31010: Gestão de Riscos – Diretrizes*. Rio de Janeiro.

Barbosa, M., Cunha, D. and Loose, C. E. (2024) "Gestão de riscos nas universidades públicas no Brasil", *IOSR Journal of Humanities and Social Science*, vol. 29, pp. 40–46.

Bermejo, P. H. S. et al. (2018) *ForRisco: gerenciamento de riscos em instituições públicas na prática*. Brasília, DF: Editora Evobiz.

Bittencourt, O. T., Carvalho, R. L. de, Barbosa, G. V. and Santos, G. F. do (2024) "Segurança cibernética nas universidades: uma revisão sistemática da literatura sobre a gestão de segurança da informação no ensino superior", *InterSciencePlace*, vol. 19.

Coetzee, P. and Lubbe, D. (2011) "Internal audit and risk management in South Africa: adherence to guidance", *Acta Academica*, vol. 43, no. 4, pp. 29–60.

Dioubate, B. M. and Wan Daud, W. N. (2022) “A review of cybersecurity risk management framework in Malaysia higher education institutions”, *International Journal of Academic Research in Business and Social Sciences*, vol. 12, no. 5, pp. 1081–1093.

Giestosa, J. C. et al. (2023) “Metodologias de gestão de riscos em entes públicos brasileiros: uma análise bibliográfica”, *Revista de Gestão e Secretariado (Management and Administrative Professional Review)*, vol. 14, no. 4, pp. 5889–5910.

Gil, A. C. et al. (2017) *Como elaborar projetos de pesquisa*. São Paulo: Atlas.

Ismail, W. B. W. et al. (2022) “An information security policy development process in higher education institution: a case study approach”, *Proceedings of the 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, IEEE, pp. 147–152.

Junior, A. E. de A., Santos, E. M. dos and Albuquerque, E. S. de (2014) “Segurança da Informação em um Instituto de Pesquisa: uma análise utilizando a norma ISO/IEC 27002:2005”, *Revista Formadores*, vol. 7, no. 2, p. 71.

Krumay, B., Bernroider, E. W. N. and Walser, R. (2018) “Evaluation of cybersecurity management controls and metrics of critical infrastructures: a literature review considering the NIST cybersecurity framework”, In: Gruschka, N. (Ed.) *Secure IT Systems. NordSec 2018*. Lecture Notes in Computer Science, vol. 11252. Cham: Springer.

Menezes, D. et al. (n.d.) *Manual de referência de gestão de riscos dos processos organizacionais*. [s.l.]: [s.n.].

Ministério de Gestão e Inovação (2024) *Guia Framework do Programa de Privacidade e Segurança da Informação (PPSI)*. Available at: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos (Accessed: 17 Mar. 2025).

Moreira, N. P., Benedicto, G. C. de and Carvalho, F. de M. (2019) “Discussão de alguns condicionantes da eficiência em universidades federais brasileiras a partir do Reuni”, *Revista do Serviço Público*, vol. 70, no. 3, pp. 429–457.

Pardini, E. P. (2019) *Gestão de Riscos*. 1st ed. São Paulo: Crossover Consulting & Auditing. E-book.

PF (2022) “PF deflagra operação contra ataques cibernéticos a universidades federais”, *Polícia Federal*, 20 Apr. Available at: https://www.gov.br/pf/pt-br/assuntos/noticias/2022/04/pf-deflagra-contra-ataques-ciberneticos-a-universidades-federais (Accessed: 28 Mar. 2025).

Ramos, V. G. S. et al. (2019) “Uma proposta de utilização de gestão de risco para o Planejamento Acadêmico de uma Universidade Pública”, *Revista de Gestão e Projetos*, vol. 10, no. 1, pp. 81–91.

Ruzic-Dimitrijevic, L. and Dakic, J. (2014) “The risk management in higher education institutions”, *Online Journal of Applied Knowledge Management*, vol. 2, no. 1, pp. 137–152.

Sedrez, C. and Fernandes, F. (2011) “Gestão de riscos nas universidades e centros universitários do estado de Santa Catarina”, *Gestão Universitária da América Latina*, special issue, pp. 70–93.

Silva, E. L. and Menezes, E. M. (2005) *Metodologia da Pesquisa e Elaboração de Dissertação*. Florianópolis, SC: Universidade Federal de Santa Catarina.

Trad, L. A. B. (2009) "Grupos focais: conceitos, procedimentos e reflexões baseadas em experiências com o uso da técnica em pesquisas de saúde", *Physis: Revista de Saúde Coletiva*, vol. 19, pp. 777–796.

Universidade Federal do Mato Grosso do Sul sofre ataque cibernético (2022) *Security Leaders*, 4 Aug. Available at: https://securityleaders.com.br/universidade-federal-do-mato-grosso-do-sul-sofre-ataque-cibernetico/ (Accessed: 28 Mar. 2025).

Vieira, J. B. and Barreto, R. T. S. de (2019) *Governança, gestão de riscos e integridade*. Brasília: ENAP.