Inteligência Cibernética Aplicada à Governança Digital nos Institutos Federais: Uma Revisão Bibliográfica

Brenno Barbosa de Alencar Fernandes
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins - IFTO e Faculdade de Tecnologia, Universidade de Brasília - UnB
Palmas, Tocantins, Brasil
brenno.fernandes@ifto.edu.br

Georges Daniel Amvame Nze
Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Universidade de Brasília - UnB
Brasília, Distrito Federal, Brasil
georges.amvame@unb.br

Fábio Lúcio Lopes de Mendonça
Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Universidade de Brasília - UnB
Brasília, Distrito Federal, Brasil
fabio.mendonca@unb.br

João José Costa Gondim
Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Universidade de Brasília - UnB
Brasília, Distrito Federal, Brasil
joao.gondim@unb.br

***Resumo*— Esta pesquisa tem por objetivo investigar como a Cyber Threat Intelligence (CTI) pode contribuir para o fortalecimento da segurança da informação nos Institutos Federais Brasileiros (IFs), por meio de uma revisão bibliográfica com foco nos fundamentos técnicos, métodos de mitigação e práticas de governança digital. Ainda, com base na análise de publicações recentes e com focos institucionais, como o iESGo, buscou-se examinar o panorama atual de maturidade cibernética das instituições, os avanços, as limitações de suas estruturas de gestão e resposta a incidentes. Os resultados apontam que, devido aos avanços obtidos em governança e conformidade regulatória, desafios relacionados à evasão de recursos humanos e eventos ainda persistem. Pode-se observar que a integração entre CTI e governança digital representa uma estratégia promissora para aumentar a resiliência institucional e promover uma postura mais preventive para as atividades digitais..**

Palavras-chave*— *Inteligência Cibernética; Segurança da Informação; Institutos Federais; Governança Digita;, Cibersegurança.

***Abstract*— This research aims to investigate how Cyber Threat Intelligence (CTI) can contribute to strengthening information security in Brazilian Federal Institutes (IFs) through a literature review focusing on technical foundations, mitigation methods, and digital governance practices. Furthermore, based on the analysis of recent publications with an institutional focus, such as IESGO, we sought to examine the current cyber maturity landscape of these institutions, the advances made, and the limitations of their management and incident response structures. The results indicate that, despite advances in governance and regulatory compliance, challenges related to human resource attrition and incidents persist. It can be observed that the integration of CTI and digital governance represents a promising strategy for increasing institutional resilience and promoting a more preventive approach to digital activities.**

Keywords*— *Cyber Intelligence; Information Security; Federal Institutes; Digital Governance; Cybersecurity.

I. INTRODUÇÃO

Um mundo cada vez mais digital já se consolidou em nosso cotidiano. No entanto, essa expansão tecnológica também implica em maiores riscos no que diz respeito à cibersegurança, exigindo das organizações que administram grandes volumes de informações respostas cada vez mais rápidas, eficientes e adaptativas [1]. Com a facilidade do acesso aos serviços digitais verifica-se também o aumento de ataques cibernéticos [2]. Ainda, além do aumento quantitativo, há a evolução destes ataques com uso de engenharia social, phishing, ransomwares, entre outros [3, 4]. Acompanhando esta tendência, as instituições de ensino superior constituem alvos estratégicos para agentes maliciosos em razão do expressivo volume de dados sensíveis que estas armazenam [5]. Desta forma, este trabalho aborda a análise da segurança nos Institutos Federais (IFs), visto que estes também armazenam dados pessoais, financeiros, acadêmicos e de propriedade intelectual [2]. Além disso, os Ifs apresentam também a peculiaridade de armazenar dados de menores de idade, em consequência de sua atuação no ensino médio técnico [6, 7]. Apesar dos avanços estruturais em governança de TI observados em parte dessas instituições, a maturidade cibernética permanece em nível intermediário, marcada por uma postura ainda majoritariamente reativa frente às ameaças digitais. Neste contexto, este estudo tem como escopo investigar como a Cyber Intelligence (CI) pode contribuir para o fortalecimento da segurança da informação nos Institutos Federais Brasileiros, indo além da abordagem tradicional de Cyber Threat Intelligence (CTI) focada exclusivamente em ameaças, para incorporar uma perspectiva mais ampla que integre à análise da segurança digital nos IFs

inteligência técnica, gestão de riscos e governança institucional.

Especificamente, este trabalho busca: (i) mapear o estado da arte sobre vulnerabilidades e práticas de segurança em instituições de ensino superior, com foco nos IFs; (ii) analisar a aplicabilidade de frameworks e metodologias de Cyber Intelligence no contexto dessas instituições; e (iii) propor um modelo conceitual de integração entre CI e estruturas de governança digital. A análise bibliográfica e documental realizada, incluindo indicadores institucionais do iESGo 2024, revela que embora instituições como o IF Tocantins apresentem índices elevados de governança (iGovTI: 75,5%) e gestão de TI (iGestTI: 88,5%), desafios operacionais persistem - casos como o do IF Goiano e estudos técnicos no IFRN evidenciam escassez de pessoal qualificado, infraestruturas heterogêneas, restrições orçamentárias e vulnerabilidades básicas evitáveis. Esses achados sugerem que a integração entre Cyber Intelligence e governança digital representa uma estratégia promissora para elevar a resiliência institucional, permitindo a transição de uma abordagem reativa para uma postura preventiva e baseada em inteligência.

No cenário descrito, torna-se essencial a compreensão dos fundamentos da segurança da informação e da cibersegurança no contexto institucional. A seguir apresenta-se uma síntese dos principais conceitos e abordagens relacionados às vulnerabilidades em sistemas de informação, às metodologias contemporâneas de análise e mitigação e ao papel da inteligência cibernética como instrumento de apoio à tomada de decisão. Essa base conceitual sustenta a análise da realidade dos Institutos Federais, permitindo articular as boas práticas consolidadas na literatura com as experiências institucionais mapeadas, bem como orientar a construção de uma proposta de integração entre CTI e governança digital, ajustada às características e limitações dessas organizações.

II. FUNDAMENTOS E NATUREZA DAS VULNERABILIDADES

A segurança da informação se consolidou como um dos pilares das organizações modernas, evoluindo de práticas focadas exclusivamente na proteção física e lógica de dados para um domínio multidimensional envolvendo processos, pessoas e tecnologia [8]. Tradicionalmente baseada na tríade confiabilidade, integridade e disponibilidade (CID), essa área passou a incorporar novas dimensões, como autenticidade, rastreabilidade, entre outros, especialmente com a ascensão de ambientes interconectados e o uso de computação em nuvem [9]. Ainda, o fortalecimento de políticas de proteção de dados como a Lei nº 13.709/2018, que dispõe sobre a Lei Geral de Proteção de Dados (LGPD), reforçou a necessidade de adoção de padrões de segurança da informação e estruturas de governança que garantam não apenas a proteção técnica, mas também a conformidade legal e ética.

É importante ressaltar que as vulnerabilidades em sistemas digitais não se limitam a falhas técnicas, mas igualmente envolvem aspectos humanos e institucionais [10]. Para melhor compreensão, este trabalho entende que o risco de segurança existe quando uma ameaça explora uma vulnerabilidade por meio de ataques [1,11]. Desta forma, diversas vulnerabilidades podem se apresentar, desde erros de configuração de servidores ou aplicações desatualizadas, mas também o fator humano como um elo fraco, sendo suscetíveis a ataques de engenharia social, phishing, entre outros [3, 12].

A. Identificação e Mitigação

As diversas vulnerabilidades de sistemas de informação podem ser classificadas de acordo com múltiplos critérios, abrangendo dimensões técnicas, humanas e organizacionais. Estruturas internacionais facilitam essa tarefa, como o Common Vulnerability Scoring System (CVSS), usado para classificar e mensurar vulnerabilidades e fornecer pontuações de gravidade padronizadas (de 0 a 10). A Common Weakness Enumeration (CWE) lista as fraquezas de software mais comuns, facilitando assim a identificação de padrões recorrentes [12, 13]. No contexto de aplicações web, o OWASP Top 10 destaca as vulnerabilidades mais críticas e disseminadas, servindo como referência essencial para desenvolvedores e equipes de segurança [14]. Além disso, estruturas de governança e gestão, como o NIST Cybersecurity Framework (CSF) e as normas ISO/IEC 27001 e 27002, estabelecem diretrizes abrangentes para identificação, proteção, detecção, resposta e recuperação de incidentes, integrando a segurança da informação à governança organizacional [9]. De toda forma, essa classificação sistemática tem como objetivo oferecer meios para direcionar as organizações em como alocar seus esforços para garantir a continuidade de serviços.

A identificação e a mitigação de vulnerabilidades exigem metodologias definidas e o uso de ferramentas próprias. Nesse sentido, testes de invasão, especialmente abordagens de caixa-preta, permitem mapear vulnerabilidades sem conhecimento prévio da infraestrutura, simulando cenários de ataque da vida real. Para apoiar esse processo, ferramentas como Nmap e Nessus são comumente utilizadas para detector 2portas abertas, serviços ativos e categorizar vulnerabilidades detectadas [12]. Além disso, parâmetros de segurança, como os definidos pelo projeto OWASP, orientam práticas essenciais de desenvolvimento seguro, destacando falhas recorrentes em aplicações web [14]. Estudos de caso, como o realizado no Centro de Inovações Tecnológicas do Rio Grande do Norte (CINTE-RN), mostram que a maioria das vulnerabilidades críticas poderia ser evitada por meio de medidas básicas de segurança, como aplicação de patches, atualizações de bibliotecas e ajustes na configuração do servidor [12].

B. Inteligência Cibernética

Nesse cenário de crescente complexidade dos ecossistemas digitais, a Cyber Intelligence (CI), ou Inteligência Cibernética, emerge como uma abordagem estratégica que transcende a simples detecção e análise de ameaças digitais, constituindo um ecossistema integrado que transforma dados brutos de múltiplas fontes - logs de sistemas, feeds de inteligência, análise comportamental de usuários, métricas de governança - em conhecimento acionável para diferentes níveis decisórios. Enquanto a Cyber Threat Intelligence (CTI) concentra-se especificamente na identificação, análise e mitigação de ameaças cibernéticas por meio de indicadores técnicos (IoCs e IoAs), a CI integra inteligência de ameaças, análise de vulnerabilidades, gestão de riscos e governança, fornecendo insights técnicos no nível operacional, orientando a priorização de investimentos e alocação de recursos no nível tático, e

subsidiando a definição de políticas institucionais e avaliação de maturidade cibernética no nível estratégico [1, 15].

1) *Cyber Threat Intelligence*

Nesse cenário de crescente complexidade dos ecossistemas digitais, a CTI se apresenta como uma estratégia relevante para antecipar, detectar e responder a incidentes de forma mais eficiente. A CTI caracteriza-se pelo uso de técnicas de inteligência artificial (IA) e aprendizado de máquina (ML), possibilitando assim a análise de grandes volumes de dados com feedback quase imediato e permitindo a identificação de padrões de ataque [1]. Essa abordagem vai além da simples detecção de ameaças, incorporando análises preditivas que permitem às organizações se anteciparem a possíveis vetores de ataque antes que estes se concretizem [15]. Neste processo, os indicadores de ataque (Indicators of Attack - IoA) e os indicadores de comprometimento (Indicators of Compromise - IoC) assumem o protagonismo para orientar medidas defensivas, fornecendo informações contextualizadas sobre táticas, técnicas e procedimentos (TTPs) utilizados por agentes maliciosos [11].

Ainda, frameworks como o Cyber Kill Chain possibilitam compreender as etapas de uma intrusão, desde o reconhecimento inicial até a exfiltração de dados e, desta forma, fortalecer as respostas preventivas e proativas em cada fase do ataque [11,15]. A integração da CTI com modelos de referência como o MITRE ATT&CK amplia a capacidade de mapeamento de comportamentos adversários, permitindo que equipes de segurança desenvolvam estratégias de defesa mais robustas e adaptadas ao contexto institucional [15].

2) *Aplicação de CI em Instituições Educacionais*

Para instituições educacionais como os IFs, a adoção de Cyber Intelligence implica em transcender a postura reativa de resposta a incidentes, desenvolvendo capacidades de antecipação, prevenção e aprendizado contínuo. Isso envolve não apenas a implementação de ferramentas técnicas de CTI, mas também a construção de uma cultura organizacional orientada por dados, o desenvolvimento de competências analíticas nas equipes e a integração sistêmica entre as áreas de TI, segurança da informação e governança institucional [16].

No contexto educacional, especialmente em instituições com recursos limitados como os IFs, a adoção de soluções de CI baseadas em ferramentas open-source e compartilhamento colaborativo de inteligência entre campi pode representar um diferencial estratégico para elevar a maturidade cibernética sem comprometer significativamente o orçamento [2,16]. A Figura 1 ilustra a relação hierárquica entre os components da Cyber Intelligence e sua integração com a governança digital institucional.

No cenário descrito, torna-se essencial a compreensão dos fundamentos da segurança da informação e da cibersegurança no contexto institucional. A seguir apresenta-se uma síntese dos principais conceitos e abordagens relacionados às vulnerabilidades em sistemas de informação, às metodologias contemporâneas de análise e mitigação e ao papel da inteligência cibernética como instrumento de apoio à tomada de decisão. Essa base conceitual sustenta a análise da realidade dos Institutos Federais, permitindo articular as boas práticas consolidadas na literatura com as experiências institucionais mapeadas, bem como orientar a construção de uma proposta de integração entre CTI e governança digital, ajustada às características e limitações dessas organizações. Dessa forma, os elementos apresentados na Figura 1 consolidam a base conceitual necessária para compreender a inserção da Inteligência Cibernética na governança digital dos IFs.

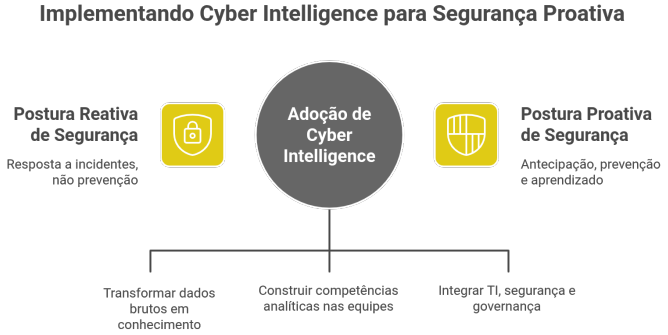

Fig. 1. Componentes da Cyber Intelligence e sua Integração com Governança Digital

C. *Integração entre Inteligência Cibernética e Governança Digital*

A complexidade crescente dos ecossistemas digitais nas instituições de ensino exige que a segurança da informação deixe de ser tratada apenas como uma função técnica e passe a integrar o núcleo da governança institucional. Nos Institutos Federais, marcados pela heterogeneidade de infraestruturas, múltiplos campi e grande volume de dados sensíveis, a Governança Digital desempenha papel central ao articular tecnologia, processos e objetivos estratégicos [5, 17, 18]. O relatório iESGo 2024 do TCU evidencia avanços importantes em gestão e governança de TI em instituições como o IFTO, mas indica que a maturidade em segurança ainda se encontra em um patamar intermediário, o que demanda ações mais integradas e contínuas no âmbito da cibersegurança.

Nesse contexto, a Inteligência Cibernética surge como elemento estratégico capaz de conectar os níveis técnico, tático e gerencial da proteção digital. Diferente de uma CTI restrita à análise de ameaças, a Cyber Intelligence, conforme defendem Conti et al. [1] e Sánchez del Monte e Hernández-Álvarez (18), envolve a integração entre inteligência técnica, análise de riscos, suporte à tomada de decisão e cultura organizacional. Estudos sobre instituições de ensino superior indicam que a ausência dessa articulação contribui para a manutenção de posturas reativas frente a incidentes [2, 4, 19]. Assim, ao alinhar práticas de CTI com políticas de governança digital, os IFs podem avançar para um modelo de segurança mais preventivo, orientado por evidências, integrado aos indicadores institucionais do iESGo [17] e capaz de fortalecer a resiliência organizacional diante do cenário crescente de ameaças cibernéticas [9, 16, 18]. A Figura 2.2 sintetiza visualmente essa integração entre Inteligência Cibernética e Governança Digital no contexto institucional.

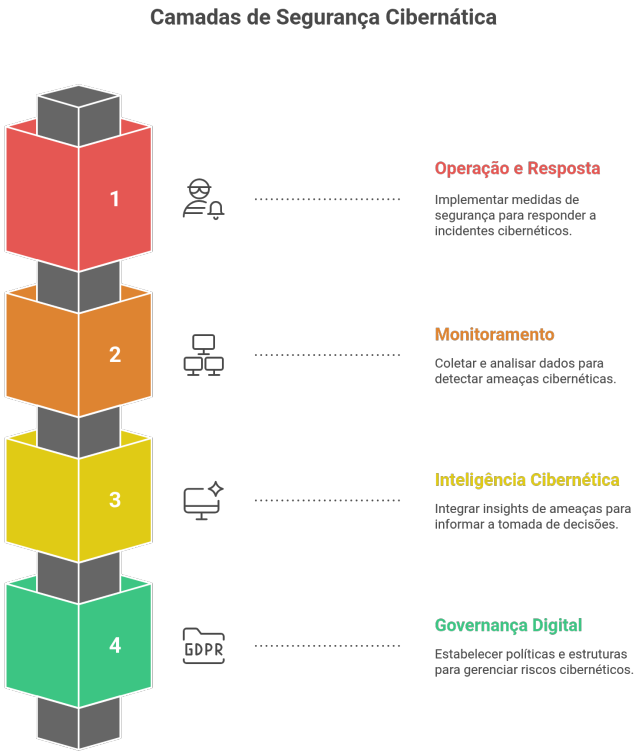

Fig. 2. Camadas de integração entre Inteligência Cibernética e Governança Digital

III. METODOLOGIA

De acordo com Cervo e Bervian [20], a pesquisa tem como base ser um processo direcionado à resolução de problemas, utilizando métodos científicos. Sendo assim, parte-se de uma questão ou incerteza e, por meio do método científico, busca-se encontrar uma resposta ou solução. Sendo assim, no presente estudo a questão central consiste em compreender como a aplicação de CTI pode contribuir para o fortalecimento da segurança da informação e da governança digital nos IFs.

A metodologia adotada para esta pesquisa tem como fundamento a realização de uma revisão de literatura, que se estrutura no levantamento e análise de referenciais teóricos especializados que permitem traçar um panorama do estado da arte acerca do nível de vulnerabilidade e as práticas de segurança da informação em sistemas dos IFs sob a perspectiva da CTI. Desta forma, o objetivo é identificar contribuições acadêmicas e institucionais já existentes, bem como lacunas que evidenciem a necessidade de aprofundar o tema no âmbito do IFs. Além dos recortes teóricos, foram levados em conta trabalhos com indicadores institucionais, especialmente os relatórios do IESGo 2024 [17], que apresentam o grau de maturidade de governança e gestão de TI e Segurança da Informação no IFTO, construindo assim uma base comparative para análise dos resultados. Esta abordagem possibilita compreender propostas internacionais de segurança da informação e inteligência cibernética, bem como um contexto para a experiência dos IFs, em relação a essas práticas. Isso fortalece e apoia a análise dos resultados, ao mesmo tempo em que fornece uma contribuição para o debate sobre governança digital e maturidade cibernética no contexto de instituições públicas de ensino.

As buscas foram realizadas no Google Scholar, priorizando publicações entre 2020 e 2025, com alto número de citações e publicadas em periódicos reconhecidos na área de segurança de tecnologia da informação e ciberinteligência. A análise de material coletado permitiu estabelecer um diálogo entre os referenciais teóricos e os dados empíricos absorvidos pelos trabalhos com indicadores institucionais, permitindo assim confrontar o estado da arte com a realidade dos IFs. Por fim, buscou-se atender aos objetivos propostos nesta pesquisa, assim como sua problemática inicial, oferecendo assim apoio para reflexões acadêmicas e estratégicas futuras

IV. DISCUSSÃO

Os achados da literatura levantados neste trabalho apontam que os IFs avançaram nos aspectos estruturais da administração e gestão de TI, bem como que a capacidade cibernética encontra-se em um estágio intermediário, mas relevante do que preditivo. Essa constatação é consistente com o cenário nacional descrito por 18, que demonstra que a transformação digital dos IFs não depende apenas da consolidação de políticas de segurança da informação e da capacidade de respostas a incidentes. A incorporação da CTI, por meio de uma evolução esperada da governança digital, permite o uso de dados de monitoramento e análise comportamental para antecipar medidas e reduzir a dependência de respostas manuais e emergenciais.

Foi observado, particularmente no caso do IF Goiano, que os desafios mais recentes se concentram na escassez de pessoal técnico, nas restrições organizacionais e na sobrecarga das equipes de TI [19]. Esses fatores, que também podem ser encontrados em outros contextos educacionais [15], limitam a implementação de controles de segurança mais eficazes. Desta forma, a estrutura governamental e o acúmulo de leis diretas, como a LGPD, indicam que as bases para o fortalecimento da cultura de segurança estão estabelecidas. Com isso, o desafio é integrar a análise de dados e inteligência aplicada a essas estruturas existentes, tornando a segurança parte de um ecossistema contínuo de aprendizagem e resposta.

No entanto, é importante ressaltar que a integração entre CTI e governança digital implica em uma mudança de paradigma, saindo da proteção pontual para a vigilância contínua e baseada em evidências. Essa perspectiva, já implementada em modelos internacionais como NIST CSF e o MITRE ATT&CK, amplia a capacidade institucional de detectar padrões de ataque antes que causem impacto negativo significativo. No contexto dos IFs, essa integração pode ser viabilizada por meio do compartilhamento de indicadores de ameaça entre campi, do uso de soluções abertas de correlação de eventos e do fortalecimento das equipes de segurança através da formação continuada e cooperação interinstitucional.

Definir esse cenário permite não apenas compreender os riscos, mas também propor soluções adaptadas às necessidades institucionais, contribuindo, assim, para o fortalecimento das políticas de segurança e a redução da exposição a incidentes [16]. Ainda, considerando o cenário brasileiro, este estudo visa contribuir para a aplicação do conceito de CTI às IFs,

fortalecendo a integração de tecnologia, governança e cultura organizacional como meio de promover a proteção efetiva [9].

V. RESULTADOS

No Brasil, os IFs enfrentam o desafio de alinhar estrategicamente a alta demanda acadêmica com as necessidades de segurança digital. Em estudo recente sobre governança digital em IFs [18], foi demonstrado que a maturidade em TI e segurança da informação é fator crítico para a consolidação da transformação digital e, consequentemente, para a mitigação de vulnerabilidades institucionais. O setor educacional está entre os alvos mais visados de ataques cibernéticos no Brasil. Instituições de ensino constantemente são vítimas de ataques de ransomware e phishing, demonstrando o crescente interesse de agentes maliciosos neste setor. Estimativas apontam que cerca de 80% dessas instituições já sofreram algum ataque, com perdas significativas, tanto financeiramente, como na continuidade do negócio [18].

No geral, a maturidade cibernética dessas instituições é moderada, como é o caso do IF Goiano, destacando a necessidade de progresso contínuo em políticas e treinamento [19]. A pesquisa nesta instituição identificou pontos fortes na infraestrutura tecnológica e na adoção de políticas de gestão de TI. No entanto, também foram notadas lacunas significativas em capacitação de pessoal e na padronização das práticas de segurança entre os diversos campi da instituição. Ainda, foi ressaltada a necessidade de maior conformidade com a LGPD e normas internacionais, como a ISO/IEC 27001.

Embora algumas instituições tenham pontuações altas em gestão de TI e segurança da informação, como o IF Tocantins, com 75,5% no iGovTI e 88,5% no iGestTI, demonstrando a existência de estruturas de governança e processos operacionais bem definidos [17], ainda há espaço para implementação de técnicas de CTI. Além disso, restrições orçamentárias, infraestruturas heterogêneas e alocação de equipes representam desafios, comprometendo a implementação uniforme de medidas preventivas em toda a rede. Conforme Silva et al. (2025) [19], a distribuição desigual de recursos entre os campi é um dos principais fatores que fragilizam a segurança institucional.

Diante disso, é relevante conduzir análises de vulnerabilidades dos sistemas dos IFs sob a perspectiva da CTI. Em um cenário moderado, mesmo com bons índices de governança e gestão, é necessário verificar se as práticas de segurança estão realmente consolidadas por meio de ações concretas, como aplicação de patches, codificação segura e controle de acesso [17]. Por outro lado, o estudo realizado no CINTE-RN, mostrou que, mesmo com políticas estruturadas, ainda existem vulnerabilidades básicas [12]. O uso de ferramentas como Nmap e Nessus revelou 216 falhas, indicando que ações simples, como aplicação de patches e ajustes de configuração, podem reduzir significativamente os riscos. Ao relacionar esses achados com os resultados do IFTO e do IF Goiano, pode-se averiguar que, apesar dos avanços em governança e gestão, é necessária uma integração contínua entre a gestão estratégica e a execução técnica, conforme apresentado na Tabela 1.

TABLE I. SÍNTESE DOS RESULTADOS: GOVERNANÇA, DESAFIOS E INTEGRAÇÃO COM CTI

Progresso Alcançado (Governança e Segurança)	**Desafios Remanescentes**	**Sugestão de Integração com CTI**
Estruturas de governança consolidadas (iGovTI e iGestTI elevados)	Escassez de pessoal técnico qualificado	Automação de análise de ameaças com IA/ML
Políticas de segurança da informação formalizadas	Infraestrutura heterogênea entre campi	Compartilhamento de indicadores de comprometimento (IoCs)
Conformidade parcial com LGPD e normas ISO	Restrições orçamentárias	Uso de ferramentas open-source de CTI
Capacidade de resposta a incidentes em desenvolvimento	Vulnerabilidades básicas ainda presentes	Implementação de frameworks como Kill Chain e MITRE ATT&CK

VI. CONCLUSÃO

Assim, a integração entre inteligência cibernética e governança digital indica um caminho promissor para o fortalecimento da maturidade cibernética nos IFs, possibilitando a transição de uma posição em grande parte reativa para uma atuação preventiva e estratégica diante das ameaças digitais [18, 19].

Por fim, os resultados indicam que a adoção de uma abordagem de CTI não é apenas uma técnica simples, mas também estratégica e cultural. Ao transformar dados operacionais em conhecimento explorável, a CTI pode fornecer um gerenciamento capaz de tomar decisões administrativas, otimizar a utilização de recursos e melhorar a resiliência dos sistemas de resposta a incidentes.

No entanto, reconhece-se que este estudo limitou-se a uma análise bibliográfica e documental e não cobre a aplicação prática das medidas propostas. Porém, espera-se que este seja motivador para pesquisas futuras, permitindo seu uso em estudos de caso, para explorar situações práticas em ambientes institucionais controlados, permitindo testes e avaliações reais sobre a maturidade cibernética e a resposta a incidentes.

REFERENCES

[1] M. Conti, T. Dargahi, and A. Dehghantanha, “Cyber threat intelligence: challenges and opportunities,” in Cyber threat intelligence. Springer, 2018, pp. 1–6.

[2] J. B. Ulven and G. Wangen, “A systematic review of cybersecurity risks in higher education,” Future Internet, vol. 13, no. 2, p. 39, 2021.

[3] F. Salahdine and N. Kaabouch, “Social engineering attacks: A survey,” Future Internet, vol. 11, no. 4, p. 89, 2019.

[4] L. A. Alexei and A. Alexei, “Cyber security threat analysis in higher education institutions as a result of distance learning,” International Journal of Scientific and Technology Research, no. 3, pp. 128–133, 2021.

[5] T. Vigneswari et al., “Enhancing cybersecurity in educational institutions: Challenges and strategies,” p. 32, 2025.

[6] S. Z. da Silva Gaudencio and C. C. Junior, “A (in) efetividade da legislação na proteção dos dados pessoais de crianças e adolescentes no

mundo virtual," Revista Universitas da FANORPI, vol. 3, no. 8, pp. 38–63, 2022.

[7] Brasil, "Lei nº 11.892, de 29 de dezembro de 2008," 2008, institui a Rede Federal de Educação Profissional, Científica e Tecnológica.

[8] N. S. Safa et al., "Information security conscious care behaviour formation in organizations," Computers & Security, vol. 53, pp. 65–78, 2015.

[9] L. Belli et al., "Cybersecurity: A systemic vision towards a proposal for a regulatory framework for a digitally sovereign brazil," 2023.

[10] M. N. Al-Nuaimi, "Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review," Global Knowledge, Memory and Communication, vol. 73, no. 1/2, pp. 1–23, 2024.

[11] E. M. Hutchins et al., "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research, vol. 1, no. 1, p. 80, 2011.

[12] G. C. Duarte et al., "Análise de vulnerabilidades sobre a aplicação web do cinte-rn: um estudo de caso," 2022.

[13] L. R. M. d. Santos et al., "Luner: um mecanismo para detecção de vulnerabilidade em serviços de rede," 2023.

[14] OWASP Foundation, "Owasp top 10 - 2021: The ten most critical web application security risks," https://owasp.org/Top10/, 2021.

[15] A. Sánchez del Monte and L. Hernández-Álvarez, "Analysis of cyber-intelligence frameworks for ai data processing," Applied Sciences, vol. 13, no. 16, p. 9328, 2023.

[16] E. C. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions,"Information, vol. 13, no. 4, p. 192, 2022.

[17] Tribunal de Contas da União, "iesgo 2024 - devolutiva ifto," 2024, acesso em: 14 jun. 2025. [Online]. Available: https://iesgo.tcu.gov.br/wp-content/uploads/sites/12/iesgo2024_devolutivas/iESGo2024-274-IFTO.pdf

[18] F. F. Cardoso, K. M. Moreira, and R. V. Parente, "Governança digital: uma estratégia para o sucesso da transformação digital na educação pública federal," Revista Sítio Novo, vol. 9, pp. e1795–e1795, 2025.

[19] A. Silva and W. H. Borba, "Análise do sistema de segurança da informação no instituto federal goiano para prevenção de ataques cibernéticos," 2025.

[20] A. L. Cervo and P. A. Bervian, Metodologia científica, 5th ed. São Paulo: Prentice Hall, 2002.