International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

Cyber Intelligence Applied to Digital Governance in Federal Institutes: A Bibliographic Review

Brenno Barbosa de Alencar Fernandes
Federal Institute of Education, Science and Technology of Tocantins – IFTO and Faculty of Technology, University of Brasília – UnB
Palmas, Tocantins, Brazil

Georges Daniel Amvame Nze
Faculty of Technology, Department of Electrical Engineering, University of Brasília – UnB
Brasília, Federal District, Brazil

Fábio Lúcio Lopes de Mendonça
Faculty of Technology, Department of Electrical Engineering, University of Brasília – UnB
Brasília, Federal District, Brazil

João José Costa Gondim
Faculty of Technology, Department of Electrical Engineering, University of Brasília – UnB
Brasília, Federal District, Brazil

Daniel Candido de Oliveira
Federal Institute of Education, Science and Technology of Tocantins – IFTO
Palmas, Tocantins, Brazil

***Abstract* - This study investigates how Cyber Threat Intelligence (CTI) can support the strengthening of information security in Brazilian Federal Institutes (IFs), through a literature review focused on technical foundations, vulnerability mitigation approaches, and digital governance practices. In addition, by analyzing recent institution-oriented publications, including IESGO reports, the research examines the current level of cyber maturity within these institutions, as well as the progress achieved and the structural limitations related to management and incident response. The findings suggest that, although advances in governance and regulatory compliance have been observed, challenges involving workforce constraints and recurring security incidents remain significant. In this context, the integration between CTI and digital governance is identified as a relevant strategy to enhance institutional resilience and to foster a more preventive and intelligence-driven approach to cybersecurity practices.**

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

I. INTRODUCTION

A world increasingly shaped by digital technologies has become firmly consolidated in everyday life. However, this technological expansion also implies greater risks in terms of cybersecurity, requiring organizations that manage large volumes of information to adopt responses that are increasingly faster, more efficient, and adaptive [1]. Along with the growing accessibility of digital services, there has also been an increase in cyberattacks [2]. Beyond the quantitative growth, these attacks have evolved through the use of social engineering, phishing, ransomware, among other techniques [3, 4]. In line with this trend, higher education institutions have become strategic targets for malicious actors due to the significant volume of sensitive data they store [5]. Thus, this study addresses the analysis of security in the Federal Institutes (IFs), since they also store personal, financial, academic, and intellectual property data [2]. In addition, the IFs present the particularity of storing data of minors, as a consequence of their role in technical secondary education [6, 7]. Despite structural advances in information technology (IT) governance observed in part of these institutions, cyber maturity remains at an intermediate level, marked by a predominantly reactive stance towards digital threats. In this context, this study aims to investigate how Cyber Intelligence (CI) can contribute to strengthening information security in Brazilian Federal Institutes, going beyond the traditional Cyber Threat Intelligence (CTI) approach focused exclusively on threats, by incorporating a broader perspective that integrates technical intelligence, risk management, and institutional governance into the analysis of digital security in the IFs.

Specifically, this work seeks to: (i) map the state of the art regarding vulnerabilities and security practices in higher education institutions, with a focus on the IFs; (ii) analyze the applicability of Cyber Intelligence frameworks and methodologies within the context of these institutions; and (iii) propose a conceptual model for the integration of CI with digital governance structures. The bibliographic and documentary analysis conducted, including institutional indicators from iESGo 2024, reveals that although institutions such as the Federal Institute of Tocantins (IFTO) achieve high governance (iGovTI: 75.5%) and IT management (iGestTI: 88.5%) indices, operational challenges persist. Cases such as the Federal Institute Goiano (IF Goiano) and technical studies carried out at the Federal Institute of Rio Grande do Norte

(IFRN) highlight shortages of qualified personnel, heterogeneous infrastructures, budgetary constraints, and basic yet avoidable vulnerabilities. These findings suggest that the integration between Cyber Intelligence and digital governance represents a promising strategy to enhance institutional resilience, enabling a transition from a reactive approach to a preventive and intelligence-driven posture.

Within this scenario, it becomes essential to understand the foundations of information security and cybersecurity in the institutional context. The following section presents a synthesis of the main concepts and approaches related to vulnerabilities in information systems, contemporary analysis and mitigation methodologies, and the role of cyber intelligence as a decision-support instrument. This conceptual foundation supports the analysis of the reality of the Federal Institutes, allowing the articulation of best practices consolidated in the literature with mapped institutional experiences, as well as guiding the construction of a proposal for integration between CTI and digital governance, adapted to the characteristics and limitations of these organizations

II. FOUNDATIONS AND NATURE OF VULNERABILITIES

Information security has consolidated itself as one of the pillars of modern organizations, evolving from practices focused exclusively on the physical and logical protection of data to a multidimensional domain involving processes, people, and technology [8]. Traditionally based on the confidentiality, integrity, and availability (CIA) triad, this field has incorporated new dimensions such as authenticity and traceability, especially with the rise of interconnected environments and the use of cloud computing [9]. Furthermore, the strengthening of data protection policies, such as Law No. 13,709/2018, which establishes the Brazilian General Data Protection Law (LGPD - Lei Geral de Proteção de Dados), has reinforced the need to adopt information security standards and governance structures that ensure not only technical protection but also legal and ethical compliance.

It is important to emphasize that vulnerabilities in digital systems are not limited to technical flaws, but also involve human and institutional aspects [10]. For a clearer understanding, this work considers that a security risk exists when a threat exploits a vulnerability through attacks [1, 11]. In this sense, different types of vulnerabilities may arise, ranging from server misconfigurations and outdated applications to the human factor as a weak link, making individuals susceptible to social engineering, phishing, and related attacks [3, 12].

A. Identification and Mitigation

The various vulnerabilities in information systems can be classified according to multiple criteria, encompassing technical, human, and organizational dimensions. International frameworks facilitate this task, such as the Common Vulnerability Scoring System (CVSS), used to classify and quantify vulnerabilities and provide standardized severity scores (from 0 to 10). The Common Weakness Enumeration (CWE) lists the most common software weaknesses, thus facilitating the identification of recurring patterns [12, 13]. In the context of web applications, the OWASP Top 10 highlights the most critical and widespread vulnerabilities, serving as an essential reference for developers and security teams [14]. Furthermore, governance and management frameworks, such as the NIST Cybersecurity Framework (CSF) and the ISO/IEC 27001 and 27002 standards, establish comprehensive guidelines for identifying, protecting, detecting, responding to, and recovering from incidents, integrating information security into organizational governance [9]. Overall, this systematic classification aims to provide organizations with a structured basis for allocating their efforts and ensuring service continuity.

The identification and mitigation of vulnerabilities require well-defined methodologies and the use of specific tools. In this context, penetration testing, especially black-box approaches, enables the mapping of vulnerabilities without prior knowledge of the infrastructure, simulating real-world attack scenarios. To support this process, tools such as Nmap and Nessus are commonly used to detect open ports, active services, and classify identified vulnerabilities [12]. In addition, security parameters defined by the OWASP project guide essential secure development practices, highlighting recurrent flaws in web applications [14]. Case studies, such as the one conducted at the Centro de Inovações Tecnológicas do Rio Grande do Norte (CINTE-RN), show that most critical vulnerabilities could be avoided through basic security measures, such as patch application, library updates, and server configuration adjustments [12].

B. Cyber Intelligence

In this scenario of increasing complexity in digital ecosystems, Cyber Intelligence (CI) emerges as a strategic approach that goes beyond the simple detection and analysis of digital threats, constituting an integrated ecosystem that transforms raw data from multiple sources — such as system logs, intelligence feeds, user behavioral analysis, and governance metrics — into actionable knowledge for different decision-making levels. While Cyber Threat Intelligence (CTI) specifically focuses on the identification, analysis, and mitigation of cyber threats through technical indicators, such as Indicators of Compromise (IoCs) and Indicators of Attack (IoAs), CI integrates threat intelligence, vulnerability analysis, risk management, and governance practices. It provides technical insights at the operational level, guides the prioritization of investments and resource allocation at the tactical level, and supports institutional policy definition and cyber maturity assessment at the strategic level [1, 15].

1) Cyber Threat Intelligence

In this context of increasing complexity of digital ecosystems, CTI is presented as a relevant strategy to anticipate, detect, and respond to incidents more efficiently. CTI is characterized by the use of Artificial Intelligence (AI) and Machine Learning (ML) techniques, enabling the analysis of large volumes of data with near real-time feedback and allowing the identification of attack patterns [1]. This approach goes beyond simple threat detection by incorporating predictive analyses that allow organizations to anticipate potential attack vectors before they materialize [15]. In this process, Indicators of Attack (IoAs) and Indicators of Compromise (IoCs) play a central role in guiding defensive measures, providing contextualized information about the tactics, techniques, and procedures (TTPs) used by malicious actors [11].

Furthermore, frameworks such as the Cyber Kill Chain enable the understanding of the stages of an intrusion, from initial reconnaissance to data exfiltration, thereby strengthening preventive and proactive responses at each phase of the attack [11,15]. The integration of CTI with reference models such as MITRE ATT&CK enhances the capability to map adversarial behaviors, allowing security teams to develop more robust defense strategies aligned with the institutional context [15].

2) Application of Computer Science in Educational Institutions

For educational institutions such as the Federal Institutes (IFs), the adoption of Cyber Intelligence implies transcending a reactive incident response posture and developing capabilities for anticipation, prevention, and continuous learning. This process involves not only the implementation of technical CTI tools, but also the construction of a data-driven organizational culture, the development of analytical skills within teams, and systemic integration between the areas of Information Technology (IT), information security, and institutional governance [16].

In the educational context, especially in institutions with limited resources such as the IFs, the adoption of CI solutions based on open-source tools and collaborative intelligence sharing among campuses can represent a strategic advantage for increasing cyber maturity without significantly compromising the budget [2,16]. Figure 1 illustrates the hierarchical relationship between the components of Cyber Intelligence and their integration with institutional digital governance.

Within this scenario, understanding the fundamentals of information security and cybersecurity in the institutional context becomes essential. The following section presents a synthesis of the main concepts and approaches related to vulnerabilities in information systems, contemporary methodologies for analysis and mitigation, and the role of cyber intelligence as a decision-support instrument. This conceptual basis supports the analysis of the reality of the Federal Institutes, enabling the articulation of best practices consolidated in the literature with mapped institutional experiences, as well as guiding the construction of a proposal for integration between CTI and digital governance, adjusted to the characteristics and limitations of these organizations. In this way, the elements presented in Fig. 1 consolidate the conceptual foundation necessary to understand the insertion of Cyber Intelligence into the digital governance of the IFs.

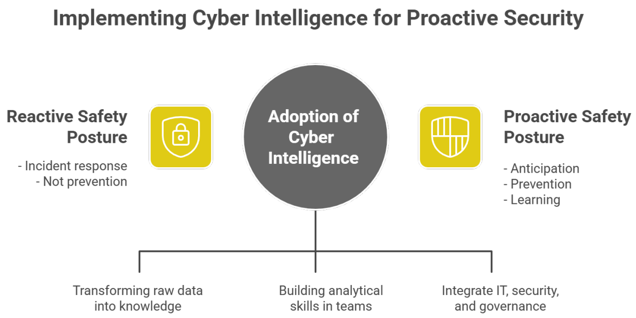
Implementing Cyber Intelligence for Proactive Security
Reactive Safety Posture
- Incident response
- Not prevention
Adoption of Cyber Intelligence
Proactive Safety Posture
- Anticipation
- Prevention
- Learning
Transforming raw data into knowledge
Building analytical skills in teams
Integrate IT, security, and governance

Fig. 1. Components of Cyber Intelligence and its Integration with Digital Governance

C. *Integration between Cyber Intelligence and Digital Governance*

The growing complexity of digital ecosystems in educational institutions requires that information security no longer be treated merely as a technical function, but rather integrated into the core of institutional governance. In the Federal Institutes (IFs), marked by heterogeneous infrastructures, multiple campuses, and a large volume of sensitive data, Digital Governance plays a central role in articulating technology, processes, and strategic objectives [5, 17, 18]. The TCU's iESGo 2024 report highlights important advances in IT management and governance in institutions such as IFTO, but indicates that security maturity is still at an intermediate level, which demands more integrated and continuous actions in the field of cybersecurity.

In this context, Cyber Intelligence emerges as a strategic element capable of connecting the technical, tactical, and managerial levels of digital protection. Unlike a CTI approach restricted solely to threat analysis, Cyber Intelligence, as argued by Conti et al. [1] and Sánchez del Monte and Hernández-Álvarez [18], involves the integration of technical intelligence, risk analysis, decision-support processes, and organizational culture. Studies on higher education institutions indicate that the lack of such articulation contributes to the persistence of reactive postures in response to incidents [2, 4, 19]. Thus, by aligning CTI practices with digital governance policies, the IFs can evolve toward a more preventive and evidence-based security model, integrated with iESGo institutional indicators [17] and capable of strengthening organizational resilience in the face of the growing cybersecurity threat landscape [9, 16, 18]. Fig. 2 visually synthesizes this integration between Cyber Intelligence and Digital Governance in the institutional context.

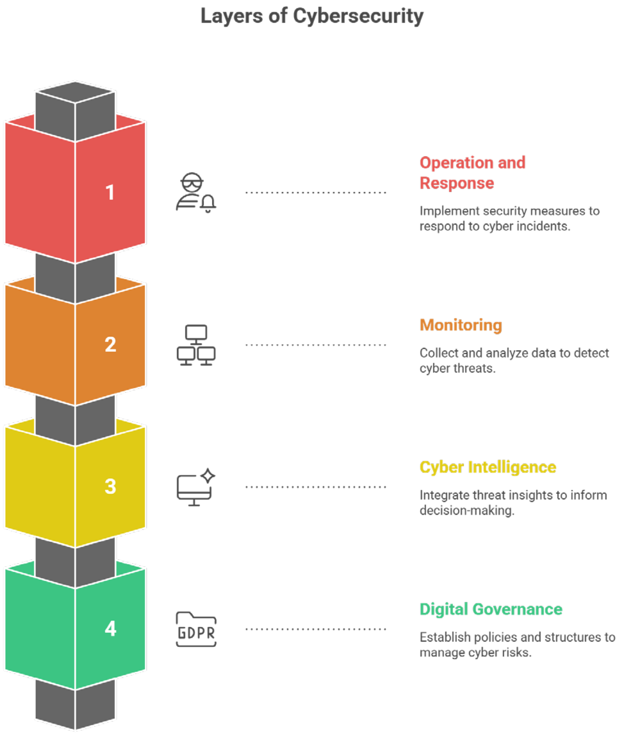
Layers of Cybersecurity
1
Operation and Response
Implement security measures to respond to cyber incidents.
2
Monitoring
Collect and analyze data to detect cyber threats.
3
Cyber Intelligence
Integrate threat insights to inform decision-making.
4
GDPR
Digital Governance
Establish policies and structures to manage cyber risks.

Fig. 2. Layers of integration between Cyber Intelligence and Digital Governance

III. METHODOLOGY

According to Cervo and Bervian [20], research is fundamentally a process aimed at problem solving through the use of scientific methods. Thus, it starts from a question or uncertainty and, through the scientific method, seeks to arrive at an answer or solution. In this sense, the central question of the present study is to understand how the application of Cyber Threat Intelligence (CTI) can contribute to strengthening information security and digital governance in the Federal Institutes (IFs).

The methodology adopted for this research is based on conducting a literature review, structured through the collection and analysis of specialized theoretical references that allow for outlining an overview of the state of the art regarding vulnerability levels and information security practices in the IFs' systems from a CTI perspective. In this way, the objective is to identify existing academic and institutional contributions, as well as gaps that highlight the need to further deepen the topic within the context of the IFs. In addition to the theoretical references, studies based on institutional indicators were considered, especially the iESGo 2024 reports [17], which present the level of IT governance and management maturity and Information Security at IFTO, thus building a comparative basis for the analysis of results. This approach makes it possible to understand international proposals on information security and cyber intelligence, as well as to contextualize the experience of the IFs in relation to these practices. This strengthens and supports the analysis of the results, while also contributing to the debate on digital governance and cyber maturity in the context of public educational institutions.

The searches were conducted using Google Scholar, prioritizing publications between 2020 and 2025, with a high number of citations and published in journals recognized in the field of information technology security and cyber intelligence. The analysis of the collected material enabled the establishment of a dialogue between the theoretical frameworks and the empirical data drawn from studies based on institutional indicators, thus allowing the comparison between the state of the art and the reality of the IFs. Finally, the study sought to meet its proposed objectives, as well as its initial research problem, thereby providing support for future academic and strategic reflections.

IV. DISCUSSION

The findings from the literature reviewed in this study indicate that the Federal Institutes (IFs) have advanced in the structural aspects of IT administration and management, while their cyber capability remains at an intermediate stage, being more reactive than predictive. This finding is consistent with the national scenario described in [18], which shows that the digital transformation of the IFs does not depend solely on the consolidation of information security policies and incident response capacity. The incorporation of Cyber Threat Intelligence (CTI), through an expected evolution of digital governance, enables the use of monitoring data and behavioral analysis to anticipate actions and reduce dependence on manual and emergency responses.

It was observed, particularly in the case of the Federal Institute Goiano (IF Goiano), that the most recent challenges are concentrated on the shortage of technical personnel, organizational constraints, and the overload of IT teams [19]. These factors, which are also present in other educational contexts [15], limit the implementation of more effective security controls. In this sense, the governmental structure and the accumulation of direct regulations, such as the General Data Protection Law (LGPD), indicate that the foundations for strengthening a security culture are already established. Therefore, the challenge lies in integrating data analysis and applied intelligence into these existing structures, making security part of a continuous ecosystem of learning and response.

However, it is important to highlight that the integration between CTI and digital governance implies a paradigm shift, moving from isolated protection measures to continuous, evidence-based monitoring. This perspective, already implemented in international models such as the NIST Cybersecurity Framework (NIST CSF) and MITRE ATT&CK, expands the institutional capacity to detect attack patterns before they cause significant negative impact. In the context of the IFs, this integration can be enabled through the sharing of threat indicators among campuses, the use of open-source event correlation solutions, and the strengthening of security teams through continuous training and interinstitutional cooperation.

Defining this scenario not only allows for a better understanding of risks, but also supports the proposal of solutions adapted to institutional needs, thus contributing to the strengthening of security policies and the reduction of exposure to incidents [16]. Furthermore, considering the Brazilian context, this study aims to contribute to the application of the CTI concept within the IFs, strengthening the integration of technology, governance, and organizational culture as a means to promote effective protection [9].

V. RESULTS

In Brazil, the Federal Institutes (IFs) face the challenge of strategically aligning high academic demand with digital security requirements. A recent study on digital governance in IFs [18] demonstrated that maturity in IT and information security is a critical factor for consolidating digital transformation and, consequently, for mitigating institutional vulnerabilities. The education sector is among the most targeted by cyberattacks in Brazil. Educational institutions are constantly victims of ransomware and phishing attacks, reflecting the growing interest of malicious actors in this sector. Estimates indicate that around 80% of these institutions have already suffered some type of attack, resulting in significant losses, both financially and in terms of business continuity [18].

Overall, the cyber maturity of these institutions is moderate, as observed in the case of IF Goiano, highlighting the need for continuous progress in policies and training [19]. Research conducted at this institution identified strengths in technological infrastructure and the adoption of IT management policies. However, significant gaps were also noted in staff training and in the standardization of security practices across its multiple campuses. Furthermore, the need for greater compliance with the General Data Protection Law (LGPD) and with international standards such as ISO/IEC 27001 was emphasized.

Although some institutions present high scores in IT management and information security, such as the Federal Institute of Tocantins (IFTO), with 75.5% in iGovTI and 88.5% in iGestTI, demonstrating the existence of well-defined governance structures and operational processes [17], there is still room for the implementation of Cyber Threat Intelligence (CTI) techniques. In addition, budgetary constraints, heterogeneous infrastructures, and workforce allocation represent challenges that hinder the uniform implementation of preventive measures throughout the network. According to Silva et al. (2025) [19], the unequal distribution of resources among campuses is one of the main factors that weakens institutional security.

In this context, conducting vulnerability analyses of IF systems from a CTI perspective becomes relevant. Even in a moderate scenario, with good governance and management indicators, it is necessary to verify whether security practices are effectively consolidated through concrete actions such as patch application, secure coding, and access control [17]. Moreover, a study carried out at CINTE-RN showed that, even in environments with structured policies, basic vulnerabilities still persist [12]. The use of tools such as Nmap and Nessus revealed 216 flaws, indicating that simple actions such as patch application and configuration adjustments can significantly reduce risks. By relating these findings to the results from IFTO and IF Goiano, it is possible to verify that, despite advances in governance and management, continuous integration between strategic management and technical execution remains necessary, as presented in Table 1.

TABLE I. SYNTHESIS OF RESULTS: GOVERNANCE, CHALLENGES AND CTI INTEGRATION

Progress Achieved (Governance and Security)	**Remaining Challenges**	**Suggestion for Integration with CTI**
Consolidated governance structures (high iGovTI and iGestTI scores)	Shortage of qualified technical personnel	Automating threat analysis with AI/ML
Formalized information security policies	Heterogeneous infrastructure across campuses	Sharing of indicators of commitment (IoCs)
Partial compliance with LGPD and ISO standards	Budgetary constraints	Use of open-source CTI tools
Capability to respond to developing incidents	Basic vulnerabilities still exist	Implementation of frameworks such as Cyber Kill Chain and MITRE ATT&CK

VI. CONCLUSION

Thus, the integration between Cyber Intelligence and Digital Governance indicates a promising path towards strengthening cyber maturity in the Federal Institutes (IFs), enabling the transition from a largely reactive posture to a preventive and strategic approach in dealing with digital threats [18, 19].

Finally, the results indicate that the adoption of a CTI-based approach is not merely a technical procedure, but also a strategic and cultural one. By transforming operational data into exploitable knowledge, CTI can support management in administrative decision-making, optimize resource allocation, and enhance the resilience of incident response systems.

However, it is acknowledged that this study was limited to a bibliographic and documentary analysis and does not cover the practical application of the proposed measures. Nevertheless, it is expected that this work may motivate future research, enabling its use in case studies to explore practical situations in controlled institutional environments, allowing real tests and evaluations of cyber maturity and incident response capabilities.

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.