GuardNet: An Architecture Based on NIST v2.0 for Confidential Data Protection in Higher Education Institutions in Peru

Brian Linan-Acosta
Information Systems Engineering Department, Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Peru
u202017814@upc.edu.pe

Oscar Bazalar-Gonzales
Information Systems Engineering Department, Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Peru
u201816491@upc.edu.pe

Jose Santisteban
Information Systems Engineering Department, Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Peru
PCSILSAN@upc.edu.pe (corresponding author)

Received: 27 June 2025 | Revised: 3 August 2025 and 22 August 2025 | Accepted: 2 September 2025

 DOI: https://doi.org/10.48084/etasr.12978

ABSTRACT

In recent years, educational institutions have been frequent targets of cyberattacks that compromise the integrity, confidentiality, and availability of their digital assets. Despite the growing threat, many of these institutions lack effective prevention mechanisms. In this study, we designed an architecture called GuardNet, which is based on the National Institute of Standards and Technology (NIST) v2.0 framework and inspired by a comprehensive review of existing cybersecurity frameworks to enhance the protection of confidential data in higher education institutions. The architecture includes a virtual firewall, an Intrusion Prevention System (IPS), and an anomaly-based detection method to identify malicious traffic or data within the network. Following this implementation, the architecture was assessed based on expert opinions and feedback from the IT staff of a Peruvian higher education institution. The results indicated a satisfactory score of 4.5 from the experts and a score of 70 on the System Usability Scale (SUS) questionnaire administered to the IT staff. Both assessments used a Likert scale, demonstrating the feasibility and usability of the proposed solution. The findings highlight that the GuardNet architecture, designed to protect confidential data, has strong potential for addressing the cybersecurity vulnerabilities of higher education institutions in Latin America. However, its implementation may face challenges related to resource availability and technical expertise.

Keywords-cyberattack; cybersecurity; architecture; institution; education

I. INTRODUCTION

As various sectors continue to digitize, cyberattacks have become a persistent threat, increasing at an alarming rate due to the inherent vulnerabilities in Internet infrastructure. The digitization of academic, administrative, and research processes has led to an increase in the amount of sensitive data being stored and processed, including personal information of users. This situation became more critical during the COVID-19 pandemic, as employees and students were required to work and study remotely from home, often without adequate security measures in place. As a result, sensitive information and data stored on local devices and across the network were exposed to various cyber threats [1].

Following the rise in cyberattacks, information storage in computing environments requires a rigorous cybersecurity approach. To ensure an adequate level of protection, various methods, techniques, and security mechanisms have been developed and implemented. Numerous studies have proposed multiple algorithms, procedures, and strategies to enhance security and reduce the risks associated with cloud computing [2]. One of the most used strategies for improving cybersecurity in network environments is the implementation

of Intrusion Prevention Systems (IPSs). These systems continuously monitor and supervise network traffic in real-time, conducting in-depth analyses to detect and identify potential threats before they can compromise the system's integrity [3].

The absence of advanced security infrastructure, including Network-based Intrusion Prevention Systems (NIPSs), presents a serious threat to the protection of confidential data. This risk is amplified by the fact that around 40% of organizations in Peru do not have sufficiently strong digital defense mechanisms, making them more susceptible to cyberattacks [4]. In 2022, Peru saw a concerning rise in the number of cyberattacks, with over 5,000 security incidents reported, primarily targeting educational institutions and government entities [5]. Many of these attacks on higher education institutions were primarily aimed at obtaining unauthorized credentials and tricking institution staff into performing insecure actions that could be exploited by cybercriminals.

The IPS specializes in identifying unusual or malicious patterns in network traffic. When it detects a potential threat, the system generates security alerts and takes automated actions to block or reduce the impact of the attack in real-time. This process significantly enhances the proactive protection of IT infrastructure [6]. According to authors in [4], about 70% of the companies in Latin America have implemented an IPS as a fundamental element of their security infrastructure. The most adopted providers in the region include Cisco, Fortinet, and Palo Alto Networks, known for the effectiveness and reliability of their solutions in real-time threat detection and mitigation. IPS technologies not only focus on identifying threats but also take proactive measures to prevent potential damage from malicious traffic. This helps ensure the integrity and availability of network resources [7]. The effectiveness of IPSs depends on their capability to identify potential threats through continuous real-time monitoring of network traffic. These systems analyze network behavior and utilize anomaly detection techniques to recognize suspicious activities, allowing for early risk mitigation [8].

The main objective of this study is to design an IPS-based architecture, called GuardNet, based on the National Institute of Standards and Technology (NIST) framework v2.0 and specifically adapted for higher education institutions in Peru. This study makes several key contributions: (a) it introduces GuardNet as an IPS-based architecture to improve cybersecurity in educational institutions across Latin America; (b) it is one of the first studies aimed at supporting the educational sector in the area of cybersecurity; and (c) it summarizes five main Cybersecurity Frameworks (CSFs) to emphasize the importance of this component in today's world. GuardNet features an IPS with functions and specifications tailored to institutional needs and integrates a virtual firewall to manage network traffic and identify anomalous or corrupted activities, thereby preventing potential cyberattacks. By incorporating NIST security standards, the architecture enhances the protection of confidential data and secures private networks.

A. National Institute of Standards and Technology Cybersecurity Framework

The NIST CSF provides guidelines and standards to enhance cybersecurity risk management in organizations. The framework consists of three components, core, implementation tiers, and profiles, each containing functions, categories, and subcategories that guide specific actions [9]. The NIST CSF outlines a process for addressing cyber threats, beginning with the identification of an organization's strategic objectives, critical systems, assets, regulatory requirements, and risk management approach, followed by a detailed analysis of potential threats [10].

B. Health Information Trust Alliance Cybersecurity Framework

Created by the non-profit organization Health Information Trust Alliance (HITRUST), HITRUST CSF is a comprehensive model designed to protect sensitive information in healthcare settings by combining regulatory requirements with industry standards [11]. Initially focused on healthcare information risk management, the HITRUST CSF has evolved into a universally applicable security model, integrating tools, controls, and best practices for regulatory compliance and asset safeguarding [12].

C. Control Objectives for Information and Related Technologies Cybersecurity Framework

Control Objectives for Information and Related Technologies (COBIT), developed by the Information Systems Audit and Control Association (ISACA), enhances IT governance and management by aligning business objectives with technological capabilities. It promotes effective control, identifies gaps and vulnerabilities, and supports cyber risk prevention [13]. The COBIT framework ensures that IT-related needs across the enterprise are addressed, optimizes resource utilization, and aligns corporate IT operations with stakeholder expectations, providing comprehensive and effective governance solutions [14].

D. Cyber Essentials Cybersecurity Framework

Cyber Essentials is a CSF endorsed by the UK government and overseen by the National Cyber Security Centre (NCSC), aimed at enhancing organizations' defenses against common cyber threats [15]. The scheme offers two levels: Cyber Essentials, which includes an online self-assessment, one-year certification, and official badge, and Cyber Essentials Plus, which provides a more thorough assessment and specialized technical support. The main goal of this framework is to encourage the adoption of current information security practices, ensuring that organizations implement effective, accessible, and easy-to-manage protection mechanisms against common cyber threats [16].

E. MITRE ATT&CK Cybersecurity Framework

Developed by the MITRE Corporation, a non-profit organization, the MITRE ATT&CK framework provides a comprehensive model for understanding adversary behavior across the cyberattack lifecycle, from reconnaissance to execution and exploitation [17]. It categorizes tactics, techniques, and procedures used by malicious actors and is

continuously updated through global expert collaboration. The framework includes enterprise and mobile components, addressing threats in IT, cloud, and mobile environments, and can be integrated with advanced security solutions such as User and Entity Behavior Analytics (UEBA) and Extended Detection and Response (XDR) [18].

F. Alternative Cybersecurity Frameworks

Table I presents nine alternative CSFs identified through academic literature, institutional reports, and international standards. Although these frameworks are less globally adopted compared to the most widely recognized models, they still provide valuable guidance for organizations seeking to strengthen specific aspects of information security, including cloud services, software assurance, and regulatory compliance [19]. Despite their relevance, the Peruvian government has noted that the majority of these proposals are associated with high implementation costs, extensive technical requirements, and a primary focus on large private organizations. Consequently, they are often less practical or sustainable for smaller institutions, particularly within the education sector, where limited budgets, resource constraints, and lower cybersecurity maturity levels require more adaptable and cost-effective solutions.

TABLE I. ALTERNATIVE CSFS FOR ORGANIZATIONAL DATA PROTECTION

ID	Name	Description	Domain/sector	Results	Source
1	ISO/IEC 15408	Security certification for IT products	Technology, defense, software	Over 1,645 products certified globally since 2010	[20]
2	OWASP SAMM	Maturity model for security in software development	Software development	Average maturity score of 1.44–3.0 across assessed organizations	[21]
3	NIS Directive (EU)	EU directive on network and information systems security for essential service operators	Public and private sector (Europe)	28% improvement in detection and response capabilities since 2020	[22]
4	CSA CCM	Control matrix for cloud environments developed by the Cloud Security Alliance (CSA)	Cloud computing	45% of companies improved visibility and control over cloud data	[23]
5	IT-Grundschutz	German framework for IT security management	Public sector (Europe)	22% decrease in critical incidents in German public entities	[24]
6	ISO/IEC 27032	Guidelines for cybersecurity collaboration across sectors	Multisectoral	18% reduction in data breaches among certified organizations	[25]
7	FAIR	Quantitative model for evaluating cybersecurity risk	Auditing, risk management, corporate	20–30% reduction in financial impact from cyberattacks after implementation	[26]
8	CIS Controls	Prioritized set of cybersecurity best practices to prevent common attacks	Cross-sector	Organizations implementing CIS Controls show 46% reduction in security incidents within the first year	[27]
9	SOC 2	Framework for evaluating security, availability, processing integrity, confidentiality, and privacy of systems	Cloud services, SaaS	Certified companies report a 30–50% improvement in client trust and data handling transparency	[28]

II. GUARDNET ARCHITECTURE

An architecture based on an IPS was developed to reduce cyberattacks on a higher education institution. This architecture includes three main components (Figure 1): (a) the IPS for network security, (b) a virtual firewall, and (c) a threat detection method. The architectural components were chosen based on NIST security standards, specifically regarding the protection of personal and private data, and allow the institution to adapt the functions of each component to address future threats.

The entities that interact with the institution's network include users, internal staff, and external actors such as hackers operating over the Internet. The IT personnel are responsible for ensuring that all components of the architecture function correctly. They also generate reports on any incidents or failures that occur during system operation and report any issues that may interfere with other tasks or functions. In this architecture, personnel can interact with and configure the IPS to meet the institution's specific needs or customize its functions to enhance performance in critical tasks. Additionally, the architecture features a virtual firewall that blocks access to malicious data from the Internet, acting as the first line of defense against cyberattacks targeting the institution. The systems team monitors both the firewall and IPS in coordination with the security manager, ensuring compliance with cybersecurity best practices and policies. This enables proper handling of any incidents that may arise.

The proposed architecture outlines how the IPS will function once implemented in the educational institution. It will operate as follows: (a) the IPS will monitor network traffic over the Internet to detect any anomalies; (b) when suspicious data are identified, the virtual firewall will block this malicious traffic from entering the institution's intranet; and (c) at the same time, the IPS will issue an alert, leading to restricted access to the institution's servers and the initiation of preventive measures against a potential cyberattack. The architecture consists of components, as described below.

A. Intrusion Prevention System

The IPS is a network security tool that allows for real-time detection and response to potential threats or suspicious activities originating from the Internet [29]. When the system identifies a potentially harmful traffic pattern, it promptly issues alerts and activates preventive measures to safeguard the organization's internal network (intranet). The IPS operates in

close coordination with the virtual firewall and the router, both of which are directly connected to the organization's central servers. For the current architecture, the Cisco Stealthwatch IPS was selected because of its cost-effectiveness, scalability, and user-friendly design. These characteristics make it a practical solution for educational institutions, even in environments where personnel may not have advanced knowledge of intrusion prevention or network security.

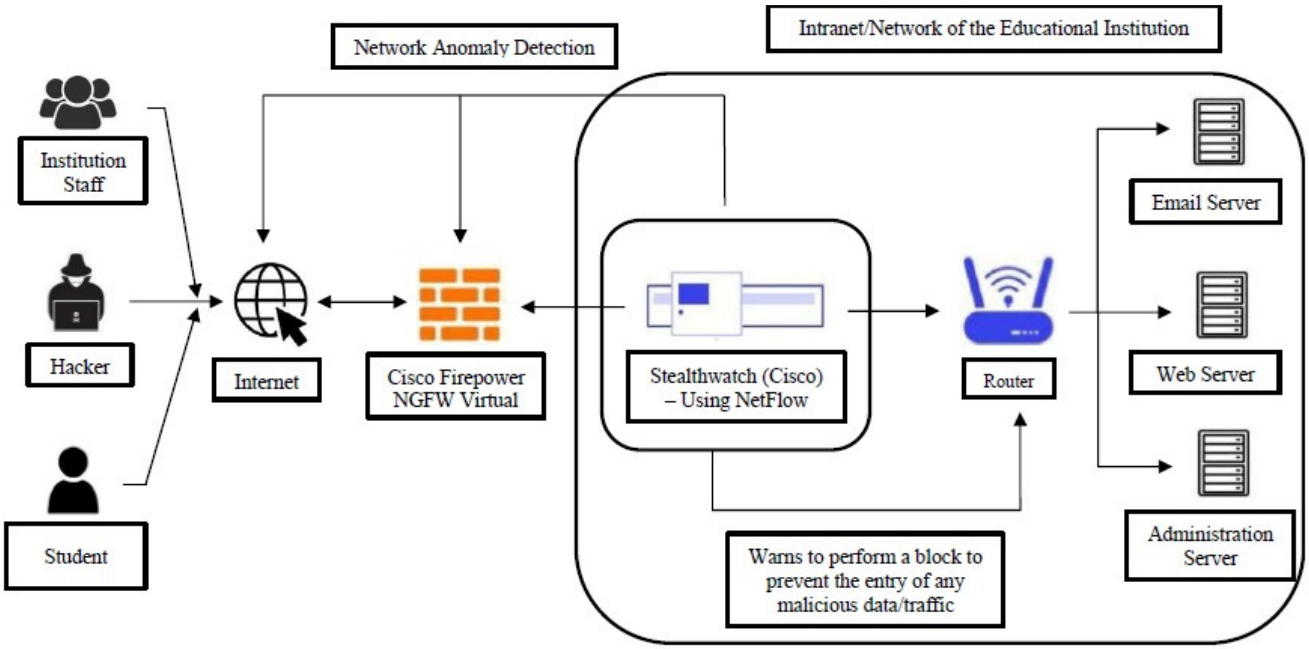

Fig. 1. GuardNet architecture integrating an IPS, virtual firewall, and threat detection for institutional data protection.

Likewise, the IPS can be integrated with Intrusion Detection Systems (IDSs) to strengthen network traffic monitoring and control, thereby creating a more resilient environment against cyber threats. This combination allows the IDS to leverage its ability to efficiently identify malicious behavior. Furthermore, IDS performance can be significantly improved through the incorporation of advanced technologies such as neural networks, deep learning, and machine learning, which improve accuracy in detecting anomalous patterns and sophisticated cyberattacks [30].

B. Virtual Firewall

The Virtual firewall is a software-based security solution designed to protect virtualized infrastructures, including web servers, databases, and cloud platforms. Often referred to as a "cloud firewall," this component is compatible with cloud environments and is responsible for monitoring and managing network traffic from the Internet. It allows or blocks access to specific internal segments based on established security policies [31]. Similar to IPS, its primary function is to filter data flows in real time to prevent unauthorized access. The Cisco Virtual Firewall was chosen for its high compatibility with the Cisco Stealthwatch (the selected IPS) and its ability to provide excellent performance in web traffic inspection. This capability is particularly valuable for educational institutions that prioritize efficiency and speed in critical environments.

C. Method of Detection

The threat detection method refers to the strategy used by an IPS to identify malicious behavior or suspicious traffic flows within a network. The selection of a detection strategy is influenced by several factors, including adaptability to the environment, response speed, scalability in managing large volumes of data, and its ability to integrate with other security systems. In the proposed architecture, we selected an anomaly-based detection method. This approach allows us to identify unusual deviations in network traffic behavior, interpreting these variations as potential threats or early indicators of cyberattacks [32]. This technique was chosen for its high adaptability, enabling it to function effectively across various types of infrastructure. Additionally, its scalability ensures consistent performance, even under high-demand conditions, without compromising system effectiveness.

III. EXPERIMENTS AND RESULTS

To evaluate the proposed framework, we assessed its usability, user satisfaction, and adoption through two questionnaires that utilized the System Usability Scale (SUS).

A. Population

The study included 32 participants from a Peruvian educational institution, divided into 7 experts and 25 individuals from the IT department. As shown in Table II, the expert participants ranged in age from 40 to 55 years old, were all male, and the majority worked in the systems area. In contrast, as shown in Table III, the IT staff participants were younger, aged between 20 and 30 years, with 24% identifying as female. Over 65% of them were employed in the security or systems departments. Additionally, a specialist reviewed and validated the participants' responses to the questionnaires.

TABLE II. PROFILES OF EXPERT PARTICIPANTS

ID	Age	Years of experience	Sex	Specialty
E01	46	8	Male	Security
E02	50	10	Male	IT services
E03	53	9	Male	Data science
E04	40	7	Male	Database management
E05	44	8	Male	IT services
E06	46	8	Male	Database management
E07	47	7	Male	Data science

TABLE III. PROFILES OF IT STAFF PARTICIPANTS

ID	Age	Sex	Specialty
P01	25	Male	Security
P02	22	Male	Data analysis
P03	28	Male	Technical support
P04	27	Female	Security
P05	29	Male	Systems analyst
P06	26	Male	Systems analyst
P07	25	Female	Technical support
P08	27	Female	Security
P09	22	Male	Data analysis
P10	29	Male	Security
P11	30	Male	Data analysis
P12	25	Male	Technical support
P13	27	Male	Security
P14	28	Female	Systems analyst
P15	28	Male	Data analysis
P16	26	Male	Systems analyst
P17	30	Male	Security
P18	25	Male	Security
P19	24	Male	Technical support
P20	29	Male	Technical support
P21	26	Female	Data analysis
P22	25	Male	Security
P23	23	Male	Technical support
P24	27	Female	Data analysis
P25	29	Male	Systems analyst

B. Evaluation Instruments

Two questionnaires were utilized: one targeted at experts and the other at IT staff. Each questionnaire included questions with five possible responses, based on the Likert psychometric scale: 1 (none), 2 (low), 3 (moderate), 4 (high), and 5 (very high).

- The questionnaire used to evaluate the experts, shown in Table IV, included questions on critical judgment (JC1–JC4), adaptability (JC5–JC8), and adoption (JC9–JC12).
- The questionnaire used to evaluate the IT staff, shown in Table V, included questions on usefulness (U1–U3), content (U4–U6), follow-up (U7, U8), and satisfaction (U9, U10).

C. Results

The findings from the questionnaire regarding the architecture, as assessed by the institution's experts, are presented in Table VI, whereas the usability results from the IT staff's perspective are shown in Table VII.

The Likert scale uses integer values. Since the mean results can be fractional, the following interpretation scheme was applied: [1, 1.8): None, [1.8, 2.6): Low, [2.6, 3.4]: Moderate, (3.4, 4.2]: High, (4.2, 5]: Very High. This scheme has been utilized in various studies, including [33].

TABLE IV. EXPERTS' EVALUATION QUESTIONNAIRE

ID	Question
JC1	Does the proposed architecture meet the minimum requirements for the protection of the Institute's confidential data?
JC2	Is the proposed architecture easy to implement for technical staff?
JC3	Does the respondent fully understand the functionality of the presented architecture?
JC4	Does the architecture ensure an appropriate balance between security and system performance?
JC5	Is the proposed architecture scalable to accommodate the Institute's future growth?
JC6	Does the architecture include detection and protection against new and known threats?
JC7	Does the architecture allow for easy integration with the Institute's existing systems?
JC8	Is the proposed architecture adequately adapted to the Institute's current technological environment?
JC9	Does the architecture presented create a positive impression, motivating people to consider it?
JC10	Does the respondent think that the presented architecture could bring a long-term benefit?
JC11	Will the proposed architecture address the Institute's web vulnerabilities?
JC12	Will the proposed architecture improve the protection of the Institute's confidential data?

TABLE V. IT STAFF'S USABILITY QUESTIONNAIRE

ID	Question
U1	I believe that the proposed architecture would be useful to improve the protection of confidential data at the Institute.
U2	I perceive that the architecture provided is unnecessarily complex.
U3	The proposed architecture is clear and easy to understand.
U4	I believe that you would need advanced technical knowledge to fully understand this architecture.
U5	I perceive that the components of the architecture are well integrated to fulfill their purpose.
U6	I think there is too much inconsistency or contradictions in the structure of the architecture.
U7	I imagine that the technical staff at the Institute could understand and implement this architecture with relative ease.
U8	I perceive that the architecture would be difficult to implement.
U9	I trust the architecture proposal to achieve the protection of confidential data.
U10	I believe that extensive training would be necessary before being able to implement this architecture.

1) Experts' Questionnaire

Table VI presents the results from the questionnaire administered to the experts. Each CJ value represents the response given by each expert (E01–E07) to the respective question. The rightmost column shows the mean response for each question, calculated by summing the scores in each row. The results indicate high scores across all evaluated dimensions, reflecting a generally positive perception among the experts. Questions JC1–JC4 demonstrate agreement that the architecture meets the minimum requirements for data security and network protection. High scores for JC5–JC8 highlight the adaptability of the architecture to the institution's technological environment and existing systems. Finally, questions JC9–JC12 show strong confidence in the institution's potential for adoption, addressing network vulnerabilities effectively.

TABLE VI. EXPERTS' EVALUATION RESULTS

Dimension	ID	E01	E02	E03	E04	E05	E06	E07	Average	
Critical judgment	JC1	5	5	4	5	5	5	5	4.9	4.1
	JC2	5	4	3	4	3	4	4	3.9	
	JC3	3	4	4	3	4	3	3	3.4	
	JC4	5	5	4	4	4	4	5	4.4	
Adaptability	JC5	5	4	4	4	4	4	4	4.1	4.5
	JC6	5	5	4	4	4	4	4	4.3	
	JC7	5	4	5	5	5	4	5	4.7	
	JC8	5	5	5	5	4	5	5	4.9	
Adoption	JC9	5	5	4	5	5	5	5	4.9	4.8
	JC10	5	5	5	5	5	5	4	4.9	
	JC11	5	5	4	5	4	5	5	4.7	
	JC12	5	5	4	5	4	4	5	4.6	

2) IT Staff Questionnaire and System Usability Scale Assessment

The IT staff's usability results are presented in Table VII. Each integer value (1–5) represents the response given by each participant (P01–P25) for each question (U1–U10).

TABLE VII. IT STAFF USABILITY RESULTS

Participant	Utility			Content			Follow-up		Satisfaction	
	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10
P01	5	3	4	3	4	2	4	3	4	4
P02	5	3	5	3	5	3	5	3	5	4
P03	5	2	5	4	4	2	4	4	5	4
P04	5	3	3	3	4	3	5	3	5	4
P05	5	2	4	3	5	2	4	3	5	4
P06	5	3	3	2	5	2	4	2	4	4
P07	5	2	5	5	5	3	5	2	5	3
P08	5	2	5	3	5	1	4	4	5	3
P09	5	3	5	3	5	3	5	3	4	5
P10	5	3	4	2	5	3	4	3	5	5
P11	4	3	3	3	3	3	4	3	3	4
P12	5	3	3	3	4	2	4	3	5	3
P13	5	2	5	2	5	2	5	2	5	3
P14	4	3	5	3	5	2	5	2	5	4
P15	5	3	5	4	5	3	4	4	5	3
P16	5	3	5	5	5	2	5	3	5	5
P17	4	2	5	2	4	2	5	3	5	5
P18	5	3	4	3	4	3	5	2	4	3
P19	4	3	4	4	5	3	3	3	5	3
P20	5	2	5	3	5	2	4	2	5	5
P21	5	2	5	2	5	2	5	2	5	4
P22	4	3	4	4	4	2	5	4	4	4
P23	5	3	4	3	4	3	5	2	4	4
P24	4	2	5	4	4	3	3	3	5	3
P25	5	2	5	2	5	2	5	3	5	4
Average	4.8	2.6	4.4	3.1	4.6	2.4	4.4	2.84	4.68	3.88
	3.92			3.36			3.64		4.28	

To assess usability, the SUS was applied, and the results are presented in Table VIII. The SUS score was computed as follows:

- Odd-numbered questions: sum the total points of the odd-numbered questions and then subtract 5.
- Even-numbered questions: for each even-numbered question, subtract 5 from its score, then sum the results.
- SUS score: sum the above two values and multiply by 2.5.

TABLE VIII. IT STAFF SUS SCORES

Participant	Sum (odd questions)	Sum (even questions)	Total sum	SUS
P01	16	10	26	65
P02	20	9	29	72.5
P03	18	9	27	67.5
P04	17	9	26	65
P05	18	11	29	72.5
P06	16	12	28	70
P07	20	10	30	75
P08	19	12	31	77.5
P09	19	8	27	67.5
P10	18	9	27	67.5
P11	12	9	21	52.5
P12	16	11	27	67.5
P13	20	14	34	85
P14	19	11	30	75
P15	19	8	27	67.5
P16	20	7	27	67.5
P17	18	11	29	72.5
P18	17	11	28	70
P19	16	9	25	62.5
P20	19	11	30	75
P21	20	13	33	82.5
P22	16	8	24	60
P23	17	10	27	67.5
P24	16	10	26	65
P25	20	12	32	80
Average	17.84	10.16	28	70

According to Table VIII and Figure 2, the proposed architecture achieved an acceptable usability level, with a mean SUS score of 70 as perceived by the IT staff. Similar approaches have been used in previous studies, such as in [34], to evaluate the perceived usability of automated cybersecurity frameworks. By employing this standardized questionnaire, the authors confirmed the effectiveness of their proposal, emphasizing the tool's reliability in measuring user-perceived acceptance and ease of use. Recent studies in the Peruvian higher education context further highlight the importance of integrating the NIST CSF with institutional policies to strengthen cybersecurity programs and protect sensitive data [35-37].

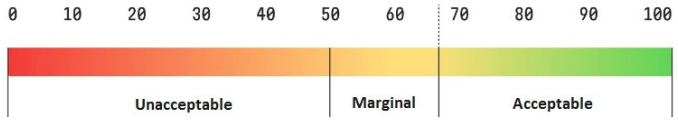

Fig. 2. SUS's usability range.

These results indicate a moderate to high level of perception among the IT staff, particularly regarding the architecture's ability to address cybersecurity challenges, ease of understanding, and accessibility for users with limited technical knowledge. This underscores the importance of making the architecture and its functionalities understandable, even for less experienced personnel, in preparation for future implementation. Additionally, the high scores related to the willingness to implement and develop the architecture, as well as confidence in its capabilities and training mechanisms (questions U9 and U10) demonstrate the IT staff's readiness to adopt the proposed solution. Overall, the findings emphasize the need to offer

solutions that align with the institution's current needs while remaining adaptable to future technological developments.

IV. DISCUSSION

GuardNet exhibits conceptual similarities to several international CSFs, as illustrated by both the five primary frameworks analyzed and the secondary frameworks identified in the literature review (see Table I). In the study conducted by authors in [19], it is concluded that organizations should adopt at least one CSF to effectively protect their data's integrity and confidentiality from potential threats. This proposal adheres to this recommendation by incorporating the NIST v2.0 framework as its primary reference, enhancing its alignment with international best practices in information security risk management. Unlike other frameworks that are more rigid or resource-intensive, NIST v2.0 offers a flexible structure that can be tailored to institutions with varying levels of cybersecurity maturity. This is particularly relevant for the Peruvian educational sector, where many organizations operate with limited technical capabilities and lack formal cybersecurity policies. Additionally, a study conducted by authors in [34] reported a SUS score exceeding 70, demonstrating a positive user perception of the ease of use of their proposed system. In comparison, the proposed architecture received a score of 70 on the same scale, which is considered acceptable. This result confirms the feasibility of the proposed solution and indicates that users perceive its usability as suitable for implementation within the institutional context.

In the study conducted by authors in [29], key vulnerabilities that can threaten both systems and applications are identified. The study also proposes various defensive technologies as effective countermeasures, including firewalls, IDSs, IPSs, and traffic filtering methods. Although that study addresses these technologies individually, highlighting their specific advantages, the architecture presented in this work goes a step further by integrating a virtual firewall with an IPS, complemented by an anomaly-based detection method. This combination significantly enhances the institution's ability to protect against cyber threats, ensuring more robust safeguarding of the confidential information stored on its servers. In the study conducted by authors in [2], the AOD-CSHEI technique is introduced to efficiently detect intrusions and cyberattacks in higher education institutions. This approach is an effective tool in the academic setting. When comparing this method to the current proposal, it was found that GuardNet achieved a usability score of 70 points, indicating a similar level of effectiveness in tackling ongoing cybersecurity challenges within the education sector. This underscores its potential as a practical and functional solution against emerging threats.

Authors in [31] demonstrated the effectiveness of integrating a next-generation firewall (pfSense) with an IPS (Suricata) to mitigate threats from internal networks toward the main data center network. The proposed approach has a notable advantage: it utilizes solutions from the same provider (Cisco) for both the firewall and the IPS. This consistency in technology ensures smoother and more precise integration between components. It also enhances operational coordination in threat detection and mitigation, thereby strengthening the institution's ability to protect its infrastructure against cyberattacks. The study by authors in [8] introduces intelligent rule-based algorithms for collecting and classifying attributes, specifically designed to enhance IPS efficiency by significantly reducing response times to malicious events. Although the proposed architecture does not include automated classification algorithms in the IPS, a thorough evaluation of available detection methods was performed. Based on this assessment, an anomaly-based detection approach was selected, providing effective response times with an estimated detection range of 1–10 s. This ensures that the architecture remains a responsive and practical solution for the assessed institutional environment.

V. CONCLUSIONS

This study presents an architecture designed to enhance cybersecurity awareness within educational institutions in Latin America. It is notable as the first prevention-focused Intrusion Prevention System (IPS) designed to encourage increased attention to the protection of confidential data about personnel in the educational sector.

The architecture was built using Cisco Stealthwatch IPS, which employs an anomaly-based detection method to identify malicious data on the Internet. Additionally, a virtual firewall provides further protection for the educational institution's internal network, also known as its intranet. The chosen solution was the Cisco Virtual Firewall, a software tool from Cisco. The proposed architecture was then evaluated by seven experts and twenty-five IT staff members from an educational institution.

The results were collected via questionnaires designed to assess the usability of the architecture. The survey, conducted among IT staff, strongly endorsed the proposal's effectiveness. Respondents highlighted that the selected components were suitable, user-friendly, and expressed interest in the proposal's implementation within the institution.

Our proposal is distinguished by being the first security framework focused on an IPS for Latin American educational institutions. This is due to the limited governmental focus on cybersecurity in the education sector in Peru, and the fact that several existing proposals focus on Intrusion Detection Systems (IDSs) without considering early detection of cyberattack indicators to enable preventive measures.

One limitation of this study is its short duration, which restricted the collection of additional responses or feedback from experts and personnel with advanced knowledge in computer science or cybersecurity. Furthermore, each institution has unique software components that may not seamlessly integrate with the proposed architecture, potentially requiring specific modifications to tailor the system to each institution's needs.

Future research should focus on the full implementation of the proposed architecture in an institution that has expressed interest in the project. The installation of both the IPS and the virtual firewall should be conducted in collaboration with the institution's IT team to ensure compatibility with existing software. Additionally, a dedicated tester should verify that all functions operate correctly without interfering with other network services within the institution.

ACKNOWLEDGMENT

The authors express their gratitude to the Dirección de Investigación de la Universidad Peruana de Ciencias Aplicadas (UPC) for their support during this study.

REFERENCES

[1] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021, https://doi.org/10.1109/ACCESS.2021.3073408.

[2] A. S. A. AL-Ghamdi, M. Ragab, M. F. S. Sabir, A. Elhassanein, and A. A. Gouda, "Optimized Artificial Neural Network Techniques to Improve Cybersecurity of Higher Education Institution," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 3385–3399, Mar. 2022, https://doi.org/10.32604/cmc.2022.026477.

[3] A. Kumar, K. Abhishek, M. R. Ghalib, A. Shankar, and X. Cheng, "Intrusion detection and prevention system for an IoT environment," *Digital Communications and Networks*, vol. 8, no. 4, pp. 540–551, Aug. 2022, https://doi.org/10.1016/j.dcan.2022.05.027.

[4] "Magic Quadrant for Intrusion Detection and Prevention Systems – Practech." Practech. https://practech.vn/tin-tuc-su-kien/magic-quadrant-for-intrusion-detection-and-prevention-systems.

[5] M. Reyna and V. Hugo, "Cybersecurity model to improve information technology management in a public Higher Technological Institute, Lima - 2021," M.S. thesis, Faculty of Engineering, Cesar Vallejo University, Lima, Peru, 2022.

[6] R. Bocu and M. Iavich, "Real-Time Intrusion Detection and Prevention System for 5G and beyond Software-Defined Networks," *Symmetry*, vol. 15, no. 1, Jan. 2023, Art. no. 110, https://doi.org/10.3390/sym15010110.

[7] M. Pedrera Suen, "Intrusion Prevention System for Nova Servers 7," B.S. thesis, University of Computer Sciences, Havana, Cuba, 2020.

[8] D. Selva, B. Nagaraj, D. Pelusi, R. Arunkumar, and A. Nair, "Intelligent Network Intrusion Prevention Feature Collection and Classification Algorithms," *Algorithms*, vol. 14, no. 8, Aug. 2021, Art. no. 224, https://doi.org/10.3390/a14080224.

[9] M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," *Network*, vol. 3, no. 3, pp. 422–450, Sep. 2023, https://doi.org/10.3390/network3030018.

[10] A. Mahn, J. Marron, S. Quinn, and D. Topper, "Getting started with the NIST Cybersecurity Framework : a quick start guide," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, USA, NIST SP 1271, Aug. 2021. https://doi.org/10.6028/NIST.SP.1271.

[11] A. Cooper, "Mind the Security Gap : Evaluating the Effectiveness of the UK Cyber Essentials Scheme and its Suitability for Large Enterprises," M.S. thesis, Department of Computing and Information Sciences, University of Strathclyde, Glasgow, UK, 2023.

[12] K. Renaud and J. Ophoff, "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs," *Organizational Cybersecurity Journal: Practice, Process & People*, vol. 1, no. 1, pp. 24–46, Jul. 2021, https://doi.org/10.1108/OCJ-03-2021-0004.

[13] H. M. Melaku, "A Dynamic and Adaptive Cybersecurity Governance Framework," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 327–350, Sep. 2023, https://doi.org/10.3390/jcp3030017.

[14] A. Efe, "A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT," *Journal of Auditing and Assurance Services*, vol. 3, no. 2, pp. 185–205, Jul. 2023.

[15] A. Y. Abohatem, F. M. M. Ba-Alwi, and A. A. Al-Khulaidi, "Suggestion Cybersecurity Framework (CSF) for Reducing Cyber-Attacks on Information Systems," *Sana'a University Journal of Applied Sciences and Technology*, vol. 1, no. 3, pp. 234–252, Sep. 2023, https://doi.org/10.59628/jast.v1i3.248.

[16] P. Alzuri, F. Cabral Berenfus, S. Paz, A. Nowersztern, and P. Libedinsky, "Protecting Digital Healthcare - A Cybersecurity Guide for the Healthcare Sector," *IDB Publications*, Oct. 2021, https://doi.org/10.18235/0003741.

[17] G. Ahn, K. Kim, W. Park, and D. Shin, "Malicious File Detection Method Using Machine Learning and Interworking with MITRE ATT&CK Framework," *Applied Sciences*, vol. 12, no. 21, Nov. 2022, Art. no. 10761, https://doi.org/10.3390/app122110761.

[18] Y. Jo, O. Choi, J. You, Y. Cha, and D. H. Lee, "Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework," *Sensors*, vol. 22, no. 5, Mar. 2022, Art. no. 1860, https://doi.org/10.3390/s22051860.

[19] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics*, vol. 11, no. 14, Jul. 2022, Art. no. 2181, https://doi.org/10.3390/electronics11142181.

[20] N. Sun *et al.*, "Defining Security Requirements With the Common Criteria: Applications, Adoptions, and Challenges," *IEEE Access*, vol. 10, pp. 44756–44777, 2022, https://doi.org/10.1109/ACCESS.2022.3168716.

[21] D. Fucci, E. Alégroth, M. Felderer, and C. Johannesson, "Evaluating software security maturity using OWASP SAMM: Different approaches and stakeholders perceptions," *Journal of Systems and Software*, vol. 214, Aug. 2024, Art. no. 112062, https://doi.org/10.1016/j.jss.2024.112062.

[22] E. Seid, O. Popov, and F. Blix, "Security Attack Behavioural Pattern Analysis for Critical Service Providers," *Journal of Cybersecurity and Privacy*, vol. 4, no. 1, pp. 55–75, Mar. 2024, https://doi.org/10.3390/jcp4010004.

[23] T. Hegde, J. Gangl, S. Babenko, and J. Coffman, "Cloud Security Frameworks: A Comparison to Evaluate Cloud Control Standards," in *Proceedings of the IEEE/ACM 16th International Conference on Utility and Cloud Computing*, Taormina, Italy, 2023, pp. 1–6, https://doi.org/10.1145/3603166.3632553.

[24] A. Alexei, "Implementing Design Science Research Method to Develop a Cyber Security Framework for HEIs in Moldova," in *The 11th International Conference on Electronics, Communications and Computing*, Chisinau, Moldova, 2021, pp. 228–231, https://doi.org/10.52326/ic-ecco.2021/NWC.02.

[25] X. Hu, D. Cheng, J. Chen, X. Jin, and B. Wu, "Multiontology Construction and Application of Threat Model Based on Adversarial Attack and Defense Under ISO/IEC 27032," *IEEE Access*, vol. 10, pp. 117955–117972, 2022, https://doi.org/10.1109/ACCESS.2022.3220637.

[26] V. Shypovskyi, "Enhancing the factor analysis of information risk methodology for assessing cyberresilience in critical infrastructure information systems," *Political Science and Security Studies Journal*, vol. 4, no. 1, pp. 25–33, Mar. 2023, https://doi.org/10.5281/zenodo.7876556.

[27] R. Sasidharan, "A Case Study to Implement Windows System Hardening using CIS Controls," *International Journal of Computer Trends and Technology - IJCTT*, vol. 70, no. 7, pp. 1–7, Jul. 2022, https://doi.org/10.14445/22312803/IJCTT-V70I7P101.

[28] A. K. Makhija, "SOC for Cybersecurity & SOC 2® for Service Organizations – An empirical study on industry's perspective," *Journal of Accounting, Finance, Economics, and Social Sciences*, vol. 6, no. 2, pp. 19–29, Dec. 2021, https://doi.org/10.62458/jafess.160224.6(2)19-29.

[29] L. Ramírez Quevedo, "Defense Technologies Against Threat Intelligence and Cyberattacks," *InnDev*, vol. 3, no. 1, pp. 127–141, Apr. 2024, https://doi.org/10.69583/inndev.v3n1.2024.94.

[30] S. W. Nourildean, W. Mefteh, and A. M. Frihida, "DTXG-RF-based Intrusion Detection System for Artificial IoT Cyber Attacks," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19610–19614, Feb. 2025, https://doi.org/10.48084/etasr.9464.

[31] A. J. Alhasan and N. Surantha, "Evaluation of Data Center Network Security based on Next-Generation Firewall," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 9, pp. 518–525, Sep. 2021, https://doi.org/10.14569/IJACSA.2021.0120958.

[32] S. H. Abbas, W. A. K. Naser, and A. A. Kadhim, "Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)," *Global Journal of Engineering and Technology Advances*, vol. 14, no. 2, pp. 155–158, Feb. 2023, https://doi.org/10.30574/gjeta.2023.14.2.0031.

[33] W. Yeoh, M. Liu, M. Shore, and F. Jiang, "Zero trust cybersecurity: Critical success factors and A maturity assessment framework," *Computers & Security*, vol. 133, Oct. 2023, Art. no. 103412, https://doi.org/10.1016/j.cose.2023.103412.

[34] R. Alnafrani and D. Wijesekera, "An Automated Framework for Generating Attack Graphs Using Known Security Threats," in *2022 10th International Symposium on Digital Forensics and Security*, Istanbul, Turkey, 2022, pp. 1–6, https://doi.org/10.1109/ISDFS55398.2022.9800833.

[35] A. Rivera Camaqui and E. F. Paniura Valencia, "Proposal for a Cybersecurity Program based on the integration of the NIST CSF 1.0 framework and the ISO 27001 Standard for the Higher Education Sector," M.S. thesis, Peruvian University of Applied Sciences, Lima, Peru, 2025.

[36] R. Egusquiza and H. Natividad, "Design of a Cybersecurity Program based on the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), using ISO/IEC 27001:2013 for electric distribution companies in Peru," B.S. thesis, Faculty of Engineering, Peruvian University of Applied Sciences, Lima, Peru, 2023.

[37] C. R. Q. Lezama, "Cyberdefense and cybersecurity in Peru: reality and challenges surrounding the Armed Forces' capacity to neutralize cyberattacks that threaten national security," *Revista de Ciencia e Investigación en Defensa*, vol. 4, no. 1, pp. 55–76, Feb. 2023, https://doi.org/10.58211/recide.v4i1.99.