ISSN 2007-9737

SCERA: Model for the Management of Social Cybersecurity in Private Universities

Elton Rodriguez*, José Santisteban

Universidad Nacional Mayor de San Marcos,
Facultad de Ingeniería de Sistemas e Informática,
Peru

{elton.rodriguez1, jsantistebanp1}@unmsm.edu.pe

Abstract. Educational institutions in Peru have faced significant challenges in terms of data security. This is largely due to the predominance of cyberattacks using social techniques, reflecting a lack of implementation of controls and practices in cyber management. In this context, it is crucial to develop a model that improves the collective management of cyberattacks, with the aim of strengthening resilience and promoting continuous improvement in private higher education institutions. This study proposes a model based on six constructs identified within social security. To validate the seven resulting relationships between the constructs, this research was carried out that included the participation of 30 technology managers from various institutions, using the partial least squares technique (PLS-SEM). The results obtained showed that six of the relationships were successfully validated, while one relationship suggests a possible area for future research. Notably, the relationship between "cybersecurity awareness" and "cybersecurity regulations" stood out as the most validated, underscoring its potential use within the proposed model to improve regulatory practices and comprehensive security in the educational field.

Keywords. Model, cybersecurity, social cybersecurity, data privacy, education.

1 Introduction

Educational institutions have rapidly transformed through digital adoption, enhancing collaboration and connectivity among students, teachers, and administrative staff. As the reliance on digital assets increases, educating about cybersecurity and ethics in cyberspace becomes essential [34]. According to the International Telecommunication Union (ITU) in its 2024 Global Cybersecurity Index report, there is a widespread deficiency in developing effective strategies for raising awareness and adopting cybersecurity practices. Peru shows only a fundamental commitment to cybersecurity [26], which presents ongoing challenges -particularly in the social context, where the behavior of university users plays a crucial role in preventing and mitigating cyber incidents.

Furthermore, the growing reliance on technology in universities has raised significant concerns about the awareness, apprehension, and prior knowledge regarding cybersecurity among university staff and students, often emphasizing the risk of victimization [7]. In this context, the emerging concept of "social cybersecurity" refers to strategies and policies aimed at reducing cyber risks through the awareness and proper behavior of university internal users [9]. This presents a challenge for private universities to create a model that incorporates these factors into their cybersecurity practices, especially in Peru, where the regulatory and technological landscapes are still evolving.

The Presidency of the Council of Ministers (PCM) has announced that Supreme Decree No. 085-2023-PCM, which approves the National Digital Transformation Policy for 2030, highlights that Peru is facing challenges related to the limited advancement of digital security and the lack of trust in digital systems within society [42]. Supreme Decree No. 029-2021-PCM establishes a digital security framework, defining the principles and

components of the digital security model [43]. In February 2024, public universities, due to the lack of a digital security incident response team [44], are classified as critical infrastructures. Despite attempts to enhance cybersecurity culture, they still lack a comprehensive approach that addresses the social aspects of cybersecurity. According to the National Center for Strategic Planning (CEPLAN) [10], the country anticipates that cyber threats will increase alongside technological advancements, potentially reaching up to 67% by 2030. It is also highlighted that the shortage of resources allocated to cybersecurity training will not only create technological barriers but could also lead to physical harm to users.

Eshetu's study [16], found that Ethiopian universities are vulnerable to cyber infringements in their web systems, highlighting the insufficient involvement of internal university users. Technological innovations necessitate that users possess greater knowledge and skills to promote cybersecurity awareness for everyone throughout their lives. For this reason, Madrigal [31] emphasizes the importance of comprehensive preparation in cybersecurity and cyber defense topics within university settings. This preparation should not only concentrate on technical aspects like network protection and information systems but also take into account the broader context of digital culture.

An analysis of the social dimensions of cybersecurity in private universities has not yet been corroborated, despite ongoing efforts. These studies have highlighted existing technical threats but have not examined the social factors that influence cybersecurity in private universities. The proposed models mainly emphasize the technical infrastructure while neglecting critical aspects such as user behavior and the culture surrounding digital security. There is a gap in the existing literature that highlights the need for a model incorporating social dimensions vital for effective cybersecurity in universities. Additionally, the absence of studies that integrate these factors into a framework for managing social cybersecurity underscores the importance of addressing this issue.

The study aims to create a model for managing social cybersecurity in private universities, called SCERA, based on six key variables identified through a literature review. This model offers private universities a practical tool to enhance their security by managing these variables.

The proposed model will adopt an interdisciplinary approach, integrating aspects of organizational culture, information security, and regulatory management. Its goal is to enhance security practices against cyber threats by involving all stakeholders within private universities more actively.

The remainder of this study is structured as follows: Section 2 provides a review of the literature on social cybersecurity. Section 3 introduces a proposed model for managing social cybersecurity in private universities. Sections 4 and 5 present the validation and results of the study, respectively. Finally, Section 6 summarizes the conclusions.

2 Literature Review

This section is divided into three subsections that discuss related works: a) the first subsection examines studies that analyze how human behavior affects cybersecurity in higher education institutions; b) the second focuses on research exploring specific contexts, such as social engineering and cybersecurity awareness; and c) the third describes existing models that propose solutions for managing cybersecurity in higher education institutions, taking into account both technical and social aspects.

2.1 Human Factors and Behavior

Cybersecurity is considered a sociotechnical phenomenon that emphasizes not just the technology used for defense, but also the interactions between people, environments, and systems. McAlaney [32] notes that to create more effective strategies for preventing and mitigating risks, it is essential to focus not only on attackers and defenders but also on the users who engage with technological systems.

Wu [63] examined the ongoing balance that individuals maintain between sharing personal information—whether consciously or not—and the development of social trust, both online and

offline. He describes this dynamic as leading to a "technical-social gap" in the field of cybersecurity. Additionally, Wu concludes that social groups, such as family, friends, and the wider community, can encourage positive behaviors regarding security and privacy.

Shah [54] examined the impact of human factors and the effectiveness of cybersecurity policies in two culturally distinct regions: the United States and the United Arab Emirates. In both areas, it was found that 31% of respondents reported experiencing cybercrime incidents in public spaces, workplaces, and universities. As a result, it is recommended that an effective strategy be developed that focuses on enhancing technical skills. This strategy should promote a strong cybersecurity culture supported by legal frameworks that can adapt to various sociocultural contexts.

2.2 Cybersecurity in Specific Environments

According to Nguyen [36], social engineering techniques compromise security in higher education institutions by primarily manipulating human interactions, which affects both systems and individuals. He describes the educational environment as dynamic and vulnerable, noting that the high turnover of staff and students necessitates a training and awareness model. This model should be based on passive learning and consist of three phases: onboarding, awareness, and updates.

Erendor [15] examined the effectiveness of cybersecurity awareness programs in an online environment. His analysis revealed that students often lack knowledge of fundamental cybersecurity concepts and essential strategies to protect themselves against deceptive techniques such as phishing and vishing. He advocates for enhancing technical competence by educating students about the legal aspects of cybercrime. This education should involve frameworks, standards, and communication tools that help prepare students to navigate and interact securely in a digital world.

2.3 Existing Models

In the reviewed literature, various models have been developed. For instance, Rodriguez [48, 49] conducts a systematic review of social cybersecurity, highlighting factors and models.

Khader [28] proposes a Cybersecurity Awareness Framework for the Academic Sector (CAFA), which aims to enhance cybersecurity awareness. The framework emphasizes the integration of individuals within their environment, the development of relevant activities, the implementation of procedures and controls, and the assessment of cybersecurity knowledge through the university curriculum. This framework serves as a foundational guide for institutions on how to create or modify procedures and policies that align cybersecurity practices with their institutional missions.

Hijji [24] developed a Cybersecurity Awareness and Training Framework (CAT) specifically for employees working remotely. This framework aims to personalize cybersecurity education and training, addressing not only technical threats but also social manipulations that could jeopardize the security of both clients and staff. The framework is organized into three levels: awareness through basic concepts, training with technical exercises, and practice/evaluations conducted through simulations.

Finally, Ramezanian [46] developed a Framework for the Development of Cybersecurity Education (FCED) to improve educational programs by incorporating both technical and social aspects of cybersecurity. This framework consults globally recognized work frameworks such as NICE (National Initiative for Cybersecurity Education) and CSEC 2017 (Cybersecurity Curricular Guidance 2017). The process is organized into five stages. It begins with integrating competencies into the curriculum, followed by developing technological skills. The next stage involves evaluating and applying continuous improvements to ensure regular updates. After that, the focus shifts to fostering interdisciplinary collaboration among academic departments. Finally, it concludes with the implementation of labs and simulations designed to equip individuals to confront both technical and social challenges in cybersecurity.

3 Social Cybersecurity Education, Regulations, and Awareness (SCERA) Model for Private Universities

This section introduces the new Social Cybersecurity Education, Regulations, and Awareness Model, abbreviated as SCERA. It outlines the model's components and presents the research hypotheses for managing cybersecurity in higher education institutions, taking into account both technical and social aspects. Figure 1 presents a conceptual model outlining the relationships among seven dimensions that are essential for the effective management of social cybersecurity. These dimensions include a total of seven relationships, each leading to its hypothesis.

3.1 Technical Security as the Starting Point

Currently, effective technical security measures rely on robust systems that implement best practices in the digital environment. Tools like encryption and access control are vital for ensuring data integrity and protection. They help prevent data from being altered, deleted, or stolen improperly [13]. Similarly, implementing engineering practices or incorporating technical controls based on existing methodologies, alongside organizational control, can contribute to data protection. This highlights that to address data privacy, an integrated approach to privacy engineering should be considered [27].

Nejjari [35] emphasizes that attractiveness, visibility, and technical oversight are crucial factors in creating opportunities for cybercrimes. He highlights that security breaches often arise from the misuse of technical measures, which leads to data gaps and their resulting consequences. Additionally, Oyewole [41] addresses the need for regulations to be adaptable. He points out that, alongside technical security, adaptability directly impacts data privacy. Oyewole suggests that effective cybersecurity management should focus on protecting consumers or end users through data privacy, supported by strong technical tools.

As generative artificial intelligence becomes increasingly adopted across various sectors, it is essential to focus on technical security and the management of explicit consent as key sources of data assurance. This approach is necessary not only to meet legal requirements but also to build trust with users interacting with digital platforms [62]. Therefore, we can formulate the following hypothesis:

- Hypothesis 1 (H1). "Technical Security (TS)" positively influences "Data Privacy (DP)".

3.2 Ensuring Data Privacy

In today's digital world, end users play a crucial role in adopting data protection behaviors to manage their privacy amid extensive data collection and usage by various institutions and companies. This growing concern emphasizes the need for actions that protect privacy and promote the responsible use of data. These interrelated factors contribute to the development of new ethical practices in data management [45]. Furthermore, with the rise of emerging technologies such as the metaverse, artificial intelligence, and natural language processing, it is essential to ensure that data handled in digital environments is managed with integrity and transparency. This approach not only fosters user trust but also creates a more satisfactory experience based on ethical considerations [64].

Ogbuke emphasizes that organizations and institutions must take greater responsibility in managing and using data to build trust with consumers and reduce the legal or ethical risks associated with data breaches. Similarly, Anshari [4] discusses the interconnection between privacy and data accountability, highlighting that a violation of privacy involves both ethical and legal risks. This underscores the importance of responsible technology management to foster trust in the digital world.

Effectively managing confidential data can reduce risks that may cause financial losses and enhance public trust by demonstrating transparency in processes and proper data management [58]. Therefore, the following hypothesis is proposed:

- Hypothesis 2 (H2): "Data Privacy (DP)" positively influences "Data Accountability (DA)".

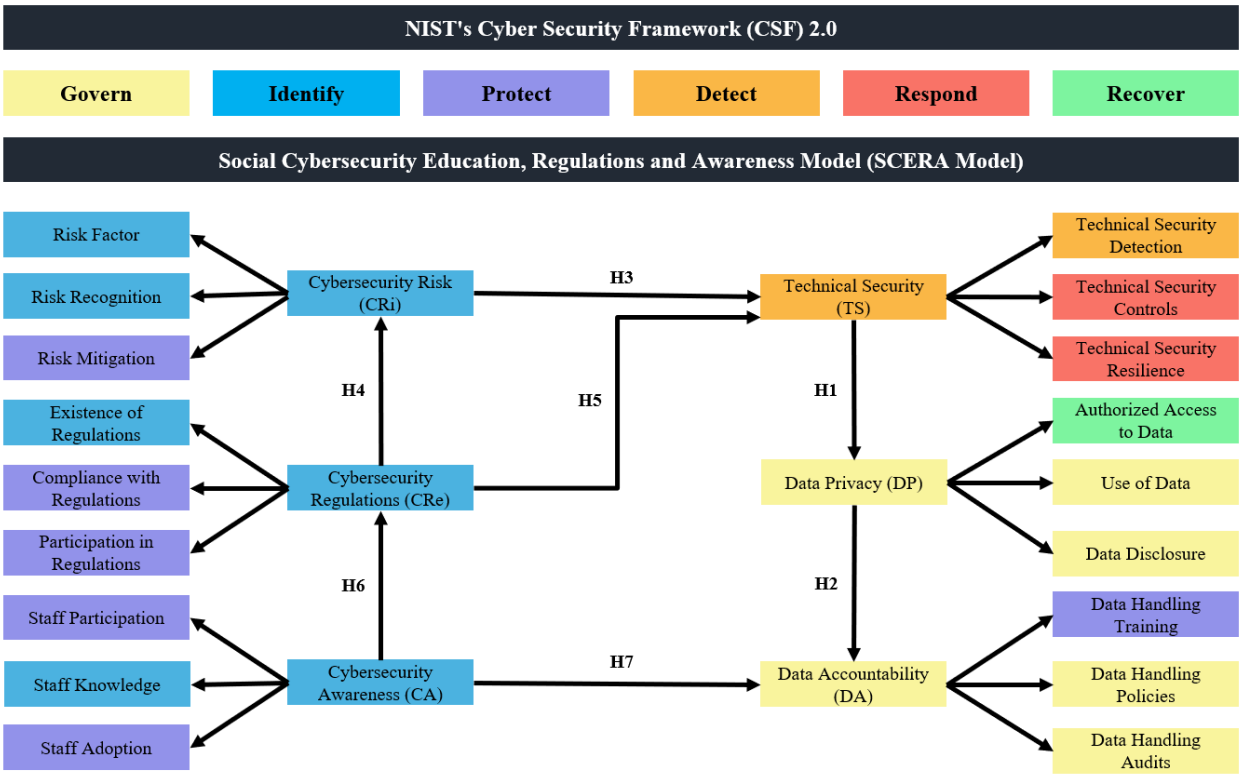

Fig. 1. SCERA Model

3.3 Recognition of Cybersecurity Risks

The adoption of technologies that enhance data privacy in small and medium-sized enterprises is driven by the growing awareness of cybersecurity risks, along with governmental regulations specific to each country.

These regulations highlight the direct relationship between technical security measures and the recognition of potential risks [21]. Additionally, in supply chains or environments with highly volatile products, technologies like blockchain have proven to be highly effective in protecting against counterfeiting and manipulation, as well as in facilitating secure digital transactions.

These technologies ensure data integrity and demonstrate that emerging latent risks can be mitigated through proper technical safeguards, provided they are effectively adopted and regulated [25].

Shaikh [55] notes that the high costs associated with cybersecurity breaches increase the attention of managers across various departments within a company or institution. This heightened awareness promotes risk assessments that not only bolster technical security but also emphasize the continuous improvement of preparedness, response, and resilience against potential future breaches. Similarly, Durst [14] indicates that effectively managing cybersecurity risks directly enhances technical security. As a result, cybersecurity managers become better equipped to tackle cyberattacks and are more resilient to the challenges posed by malicious attacks. This preparedness helps institutions and businesses avoid significant losses in trust and financial resources.

Given the high costs that cybersecurity breaches can cause, institutions and companies are encouraged to invest in adopting or contracting technical security measures to avoid potential

access violations or data breaches, which could have negative consequences if they occur. However, when prevented, these measures serve as a key catalyst for strengthening technological infrastructure [56]. Therefore, the following hypothesis is proposed:

- Hypothesis 3 (H3). "Cybersecurity Risk (CRi)" positively influences "Technical Security (TS)".

3.4 Applied Regulations

Regulations currently play a significant role in the decision-making processes of individuals, institutions, companies, and governments. These regulations are designed not only to provide best practices and guidelines but also to motivate compliance by imposing penalties for non-compliance. This focus on risk management encourages a more rigorous and conscious approach to addressing existing issues [53]. Therefore, establishing cybersecurity regulations that create models and frameworks can be an effective way to manage cybersecurity risks. These regulations enable institutions to anticipate and mitigate potential security breaches before they occur [53].

Sharma [57] emphasizes that failing to comply with regulations can result in data loss and increased cybersecurity risks. He stresses that proper management must be implemented rigorously to maintain high standards of security and data protection. Additionally, Abrahams [2] notes that standards such as ISO 27001 and the NIST Cybersecurity Framework are essential for reducing cybersecurity risks. He highlights the importance of adhering to best practices and cybersecurity regulations to safeguard sensitive information and combat cyber threats.

Regulatory changes can adversely impact organizations' cybersecurity investment strategies, particularly if they aim to minimize risks and enhance protection. This situation may lead them to adopt a passive approach to compliance with regulations [29].

Existing strategies and regulations in cybersecurity are fundamentally related to the management of cybersecurity risks. These risks create significant challenges when developing new standards based on emerging technologies in the digital market, making it difficult to achieve effective global leadership in cybersecurity [8]. Additionally, technical best practices and legislative actions from governments help establish reference models for computing security, with a strong emphasis on cyber resilience [1].

In Kryshtanovych research [30], it is discussed how state regulations enhance technical security by implementing security technologies, systematic controls, periodic audits, and cybersecurity training. These measures help establish the technical integrity necessary for managing security in businesses. Furthermore, Saeed [51] highlights that the motivation and perception of security directly influence the implementation of security policies and technical information security measures. However, it is also essential to have a legal and technological infrastructure that can ensure a trustworthy digital ecosystem for clients.

Cybersecurity regulations play a crucial role in enhancing technical security. A strong regulatory framework can improve risk management and raise technical security practices by standardizing processes, procedures, and protocols to combat cyber threats [52]. Based on this understanding, the following hypotheses are proposed:

- Hypothesis 4 (H4). "Cybersecurity Regulations (CRe)" positively influence "Cybersecurity Risk (CRi)".

- Hypothesis 5 (H5). "Cybersecurity Regulations (CRe)" positively influence "Technical Security (TS)".

3.5 Cybersecurity Awareness

In today's society, regulations play a crucial role in enhancing the capacity of supply chains to respond effectively during a crisis. By fostering awareness, individuals can learn how to strengthen their reactive capabilities in challenging situations, which promotes adherence to policies that lead to a safer and more prepared environment [61]. For this reason, implementing and complying with cybersecurity regulations—whether they are governmental or corporate—is essential, as this ensures better protection for online users [3].

Nwankpa study [38] demonstrates that increasing cybersecurity awareness, particularly

among younger individuals, leads to a better understanding of cybersecurity risks. These individuals are likely to influence existing standards and regulations in the future, making them more stringent and thereby contributing to a safer cyberspace. Additionally, Mittal [33] highlights the importance of raising cybersecurity awareness among teenagers as it is essential for developing effective strategies against cyber criminals. This awareness encourages stronger norms that focus on protecting vulnerable groups who have fallen victim to digital wrongdoing.

Educational initiatives are essential for equipping teenagers with the knowledge and skills—both social and technical—they need to navigate cyberspace safely. By doing so, they can protect their data and enhance the security of institutions or nations through the development of policies or regulatory changes [60].

Conversely, by gaining a better understanding of the risks and cyber vulnerabilities, professionals in the technology sector can develop practices that safeguard data from unauthorized access and improper manipulation. This can be achieved by fostering trust through compliance with regulations [5]. Currently, machine learning allows for the creation of models that accumulate knowledge from various security tasks, which can be readily implemented to protect organizations and institutions from emerging threats. This approach reinforces the responsibility of these entities regarding the collection, processing, and protection of data [18].

According to Sulaiman [59], raising awareness about emerging threats influences how people perceive the severity and vulnerability of cybersecurity risks. A better understanding of these vulnerabilities and the seriousness of the threats can encourage the adoption of responsible data management practices, which in turn leads to effective security behaviors. Similarly, Argyridou [6], conducted a risk-based survey that analyzed the impact of awareness on data accountability practices. The findings revealed that employees at institutions or organizations with a high level of cybersecurity knowledge are more likely to implement and adhere to practices and controls that protect the integrity and confidentiality of the data they manage.

Integrating robust cybersecurity protocols with education and ongoing training is crucial for institutions and companies. This approach enables them not only to respond to incidents effectively but also to proactively anticipate, resist, and mitigate cybersecurity risks. By doing so, they can establish a solid foundation for data protection and build trust [39]. Consequently, the following hypotheses are proposed:

- Hypothesis 6 (H6). "Cybersecurity Awareness (CA)" positively influences "Cybersecurity Regulations (CRe)".
- Hypothesis 7 (H7). "Cybersecurity Awareness (CA)" positively influences "Data Accountability (DA)".

Table 1 presents the 7 hypotheses proposed.

4 Validation

This section outlines the stages involved in statistically validating the relationships of the SCERA model (see Figure 1). The validation was conducted using Structural Equation Modeling (SEM), specifically the Partial Least Squares Structural Equation Modeling (PLS-SEM) technique. This process allows for a reliability analysis and validation of the proposed model.

4.1 Data Analysis

A research model was developed to examine the relationship between six variables, as detailed in Table 2. The multivariate statistical technique known as PLS-SEM was utilized for this analysis. This technique is commonly employed across various business research disciplines and was executed using SMARTPLS software, version 4.0, created by Ringle [47], PLS-SEM was selected because it is well-suited for analyzing the constructs of the proposed model, as demonstrated by Henseler [23]. Additionally, it effectively analyzes models with direct relationships between variables, as noted by Roldan [50].

The study focused on 30 private universities in Lima, Peru and utilized a non-probabilistic convenience sampling method. All participants

Table 1. Proposed hypotheses

ID	Description	Relationship
H1	Technical Security (TS) positively influences Data Privacy (DP)	TS - DP
H2	Data Privacy (DP) positively influences Data Accountability (DA)	DP - DA
H3	Cybersecurity Risk (CRi) positively influences Technical Security (TS)	CRi - TS
H4	Cybersecurity Regulations (CRe) positively influence Cybersecurity Risk (CRi)	CRe - CRi
H5	Cybersecurity Regulations (CRe) positively influence Technical Security (TS)	CRe - TS
H6	Cybersecurity Awareness (CA) positively influences Cybersecurity Regulations (CRe)	CA - CRe
H7	Cybersecurity Awareness (CA) positively influences Data Accountability (DA)	CA - DA

Table 2. Considered constructs

ID	Description of the construct
CRi	Cybersecurity Risk
CRe	Cybersecurity Regulations
CA	Cybersecurity Awareness
TS	Technical Security
DP	Data Privacy
DA	Data Accountability

voluntarily agreed to take part in the study, as supported by the findings of Domínguez-Lara [12]. This sampling approach was deemed appropriate given the constraints of time and resources. By using a non-probabilistic convenience sampling method, we were able to gather a diverse group of IT leaders from private universities. While this approach does not ensure that the sample is statistically representative of the entire population of private universities nationwide, it still offers valuable insights into attitudes toward cybersecurity within the university context. In terms of sociodemographic characteristics (refer to Table 3), the study revealed a higher participation rate of men (70%) compared to women (30%). Additionally, concerning the participants' age, 43% were between 35 and 44 years old, indicating that they are relatively young leaders.

The demographic analysis reveals the educational background of the participants: 40% hold a postgraduate degree, 43% have completed their undergraduate studies, and 17% have not finished their university education. Furthermore, the analysis shows that participants possess varying levels of experience in the higher education sector, with 40% having 6 to 10 years of experience, 17% having 11 to 20 years, and 10% holding 21 to 25 years of experience. This information underscores the extensive expertise of the participants in the higher education sector in Peru. Finally, it is worth mentioning that 63% of the participants in the study are not familiar with what social cybersecurity is, which is significant as it highlights that some of the responses may not accurately represent the current situation regarding social cybersecurity in the educational sector. All procedures applied in the survey were approved by the universities selected for the study, thereby giving their anonymous and informed consent.

4.2 Description of the PLS-SEM Model

Figure 2 displays the PLS-SEM model created using SMART-PLS -first, the. A CSV file containing the respondents' answers was imported. Six latent variables (unobservable variables) were generated, and the corresponding indicators (observable variables) were assigned to each latent variable. Finally, seven relationships between the latent variables were defined: CRe - CRi, CRe - TS, CRi - TS, TS - DP, DP - DA, CA - CRe, and CA - DA.

The first step in validating the model is assessing whether the latent variables or constructs used in the study accurately define and measure the intended dimensions. The following section will present the evaluation of the measurement model

4.3 Evaluation of the Measurement Model (Outer Model)

The analysis of the measurement model involves evaluating the construct and its indicators through

Table 3. Sociodemographic Profile of the Sample (n=30)

Ítem		N	%
Gender	Male	21	70
	Female	9	30
Age	18 - 24 years	2	7
	25 - 34 years	11	37
	35 - 44 years	13	43
	44 and older	4	13
Level of Education	Incomplete University	5	17
	Completed University	13	43
	Postgraduate	12	40
Experience in the Education Sector	Less than 1 year	1	3
	1 to 5 years	9	30
	6 to 10 years	12	40
	11 to 20 years	5	17
	21 to 25 years	3	10
Work Experience	1 to 5 years	5	17
	6 to 10 years	7	23
	11 to 20 years	12	40
	21 to 25 years	2	7
	26 to 30 years	3	10
	More than 30 years	1	3
Knowledge of Social Cybersecurity	Yes	11	37
	No	19	63

four stages: a) Assessing the individual reliability of the items, b) Evaluating the reliability of the constructs using Cronbach's Alpha and Composite Reliability, c) Examining convergent validity, which reflects how closely related different indicators of a construct are. This is assessed using Indicator Reliability (outer loadings) and Average Variance Extracted (AVE), and d) Evaluating discriminant validity through the Fornell-Larcker criterion and the HTMT ratio.

To assess internal consistency, we use two key indicators: Cronbach's Alpha and Composite Reliability. Both measures range from 0 to 1, with values closer to 1 indicating a higher level of reliability. Generally, values between 0.7 and 0.95 are considered acceptable. Values falling below 0.7 suggest insufficient internal consistency, while values exceeding 0.95 may indicate that all indicators are measuring the same phenomenon, making them redundant and thus not a valid measure of the construct.

To establish convergent validity, it is important to confirm the reliability of each item's indicator. The external loadings should exceed 0.708 and must be statistically significant, meaning the p-value should be less than 0.05. Additionally, AVE should be equal to or greater than 0.5. This indicates that, on average, the construct accounts for more than 50% of the variance of its indicators.

To confirm discriminant validity, which assesses how distinct different constructs are from one another, we use the Fornell-Larcker criterion. This involves comparing the square root of AVE for each construct to the correlations between the latent variables. For discriminant validity to be established, the square root of the AVE of each construct must be greater than its correlations with other constructs. Additionally, the Heterotrait-Monotrait (HTMT) ratio should be less than 0.85 and statistically significant, and the confidence intervals should not include 1. These criteria together help to determine the presence of discriminant validity.

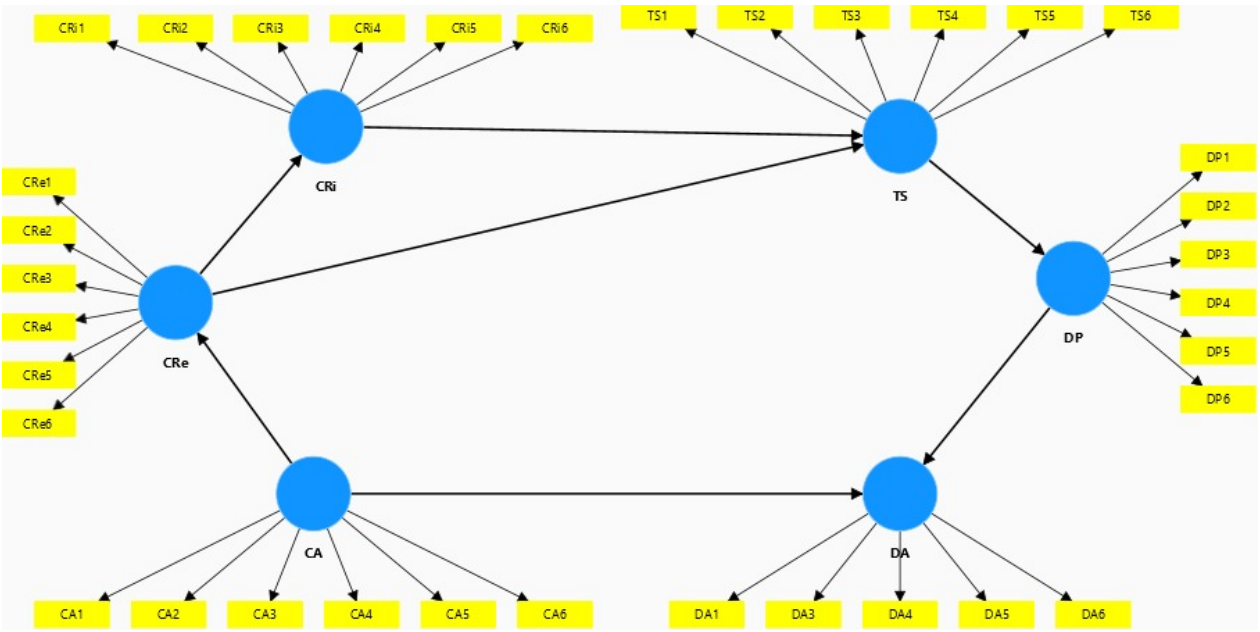

Fig. 2. Research model to be evaluated

4.3.1 Individual Item Reliability

To begin with, we assess the composite reliability of the items by examining their outer loadings, representing the relationship between each indicator and its corresponding construct. In this analysis, the factor loadings for most items exceed 0.7 and none fall below 0.4, which is the minimum threshold suggested by Hair [19]. Consequently, the proposed model retains a set of 36 items (refer to Table 4).

4.3.2 Construct Reliability

In the second step, we examine the construct reliability by utilizing Cronbach's Alpha and the Composite Reliability (CR) index. As displayed in Table 3, both Cronbach's Alpha and the Composite Reliability for all six latent variables exceed 0.7, which confirms the reliability of the constructs.

4.3.3 Convergent Validity

Convergent validity is confirmed through the Average Variance Extracted (AVE). The results indicate that the Composite Reliability (CR) values for all latent variables exceed the critical threshold of 0.8, as noted by Nunnally in his book [37]. Additionally, the AVE values are greater than 0.5, which means that each construct explains more than 50% of the variance of its indicators, as outlined by Fornell [17]. Consequently, both reliability and convergent validity are established, as shown in Table 5.

4.3.4 Discriminant Validity

The final part of the measurement model analysis involves verifying the presence of discriminant validity. To establish this validity for the constructs in the study, we first employed the Fornell and Larcker [17] criterion, which requires that the square root of the Average Variance Extracted (AVE) be greater than the correlation between the constructs. Next, we applied the Heterotrait-Monotrait ratio (HTMT - 90) method proposed by Henseler [22], where the inference tests indicated that none of the confidence intervals included the value one. This finding suggests that all the variables are empirically distinct. Both approaches confirm that our scales satisfy the

Table 4. Measurement Model of Individual and Construct Reliability

VARIABLES	CRi	CRe	CA	TS	DP	DA	Cronbach's Alpha
Cybersecurity Risk	0.927						0.927
CRi1	0.797						
CRi2	0.861						
CRi3	0.814						
CRi4	0.904						
CRi5	0.899						
CRi6	0.856						
Cybersecurity Regulations	0.921						0.921
CRe1		0.892					
CRe2		0.828					
CRe3		0.853					
CRe4		0.836					
CRe5		0.864					
CRe6		0.806					
Cybersecurity Awareness	0.925						0.925
CA1			0.865				
CA2			0.887				
CA3			0.867				
CA4			0.854				
CA5			0.770				
CA6			0.871				
Technical Security	0.911						0.911
TS1				0.871			
TS2				0.879			
TS3				0.918			
TS4				0.837			
TS5				0.707			
TS6				0.777			
Data Privacy	0.885						0.885
DP1					0.787		
DP2					0.780		
DP3					0.816		
DP4					0.766		
DP5					0.856		
DP6					0.769		
Data Accountability	0.929						0.929
DA1						0.886	
DA3						0.852	
DA4						0.901	
DA5						0.858	
DA6						0.916	

Table 5. Convergent Validity Measurement Model

Construct	CR	AVE
Cybersecurity Risk	0.927	0.733
Cybersecurity Regulations	0.921	0.717
Cybersecurity Awareness	0.925	0.728
Technical Security	0.911	0.696
Data Privacy	0.885	0.634
Data Accountability	0.929	0.780

requirements, indicating their discriminant validity, as illustrated in Table 6.

4.4 Evaluation of the Structural Model (Inner Model)

The structural model evaluates the relationships between latent variables. To determine the statistical significance of the "path" coefficients, we use the "bootstrapping" technique with 5,000 subsamples, as described in Hair's research [20]. Additionally, we present the effect size (f^2) for the relationships in our structural model, following Hair's recommendations in his book [22].

As shown in Table 7 and Figure 3, the results confirm the following research hypotheses:

— Hypothesis 1 indicates a positive relationship between Technical Security (TS) and Data Privacy (DP) (0.876***).

— In Hypothesis 2, a positive relationship is also shown between Data Privacy (DP) and Data Accountability (DA) (0.483***).

— In contrast, Hypothesis 3 (0.253) is not supported, showing that Cybersecurity Risk (CRi) is not related to Technical Security (TS).

— In Hypothesis 4, Cybersecurity Regulations (CRe) are positively related to Cybersecurity Risk (CRi) (0,912***).

— Similarly, Hypothesis 5 shows that Cybersecurity Regulations (CRe) are positively related to Technical Security (TS) (0,684***).

— Hypothesis 6 also demonstrates that Cybersecurity Awareness (CA) is positively related to Cybersecurity Regulations (CRe) (0,927***).

— Finally, Hypothesis 7 shows a moderate positive relationship between Cybersecurity Awareness (CA) and Data Accountability (DA) (0,464***).

According to Cohen [11], the effect sizes observed in the hypotheses are notable. Hypotheses H6, H4, and H1 demonstrate highly significant effects, particularly the relationship in H6, which examines the connection between Cybersecurity Awareness (CA) and Cybersecurity Regulations (CRe) with an effect size of f^2 = 6.133. Similarly, H4, which looks at the relationship between Cybersecurity Regulations (CRe) and Cybersecurity Risk (CRi), has an effect size of f^2 = 4.957. In contrast, hypotheses H5, H7, and H2 reveal medium significant effects, while H3 indicates no relationship between the two variables.

5 Results And Discussion

The objective of the study was to verify the positive relationships among six constructs (see Table 2) through seven hypotheses. This was largely achieved, except for hypothesis H3, which examined the relationship between Cybersecurity Risks and Technical Security; this relationship did not show significance. Additionally, three proposed relationships were found to be highly significant: H6 (CA - CRe), H4 (CRe - CRi), and H1 (TS - DP). Meanwhile, three relationships were deemed moderately significant: H5 (CRe - TS), H7 (CA - DA), and H2 (DP - DA).

The proposed model aims to integrate key factors that directly influence cybersecurity in private universities from a social perspective. The results indicate that technical, regulatory, and awareness elements are crucial for creating effective social cybersecurity management. Furthermore, the findings highlight the importance of an interdisciplinary approach that connects organizational culture, information security, and regulatory management.

The positive results for the first half of the year confirm that technical security is essential for maintaining data privacy. Implementing best practices directly enhances protection. This

Table 6. Discriminant Validity

Construct	CA	CRe	DP	CRi	DA	TS
Fornell and Larcker's (1981) Criterion						
Cybersecurity Awareness	0.853					
Cybersecurity Regulations	0.927	0.847				
Data Privacy	0.814	0.798	0.796			
Cybersecurity Risk	0.882	0.912	0.740	0.856		
Data Accountability	0.857	0.827	0.860	0.829	0.883	
Technical Security	0.912	0.915	0.876	0.877	0.852	0.834
Heterotrait-Monotrait Ratio (HTMT)						
Cybersecurity Awareness						
Cybersecurity Regulations	1.003					
Data Privacy	0.867	0.857				
Cybersecurity Risk	0.947	0.981	0.779			
Data Accountability	0.921	0.888	0.917	0.886		
Technical Security	0.992	0.995	0.960	0.944	0.919	

Table 7. Results of the Structural Model

Hypothesis	Path Coefficients	t-value	p-value	Cofidence Interval	Decision	f2
H1: TS - DP	0.876***	18.765	0.000	[0.769; 0.949]	Yes	3.304
H2: DP - DA	0.483***	4.709	0.000	[0.280; 0.691]	Yes	0.421
H3: CRi - TS	0.253ns	1.186	0.236	[-0.210; 0.627]	No	0.071
H4: CRe - CRi	0.912	27.122	0.000	[0.307; 1.121]	Yes	4.957
H5: CRe - TS	0.684	3.319	0.001	[0.307; 1.121]	Yes	0.517
H6: CA - CRe	0.927	30.184	0.000	[0.848; 0.967]	Yes	6.133
H7: CA - DA	0.464	4.421	0.000	[0.238; 0.658]	Yes	0.390

conclusion is supported by Nejjari [35], who shows that the misuse of technologies can lead to cybersecurity breaches, and Oyewole [41], who emphasizes that applying global legislation alongside technological best practices can more effectively address users' privacy expectations.

The support provided for H2 emphasizes the significance of data privacy in fostering data responsibility. This indicates that implementing appropriate protective measures increases end-user trust, as noted by Ogbuke [40]. Additionally, it enhances compliance with responsibilities associated with data processing through ethical and responsible practices, thereby helping to prevent privacy violations, as stated by Anshari [4]. The main takeaway is that establishing privacy management based on transparency reflects a commitment to responsible action.

The findings reveal that the influence of H3 is limited, indicating that cybersecurity risk is not linked to technical security. This suggests that organizations do not view these risks as significant factors when considering technical improvements. Shaikh [56] points out that while technical security can help mitigate risks, these risks may also arise from outdated technologies or a lack of a continuous improvement implementation plan. Similarly, Durst [14] emphasizes the importance of making enhancements in response to challenges, suggesting that there is an opportunity to investigate additional variables or constructs that, together with risks, could directly impact the management and effectiveness of resilient technical security.

Conversely, the strong relationship identified in Hypothesis 4 between cybersecurity regulations and cybersecurity risk underscores the vital role

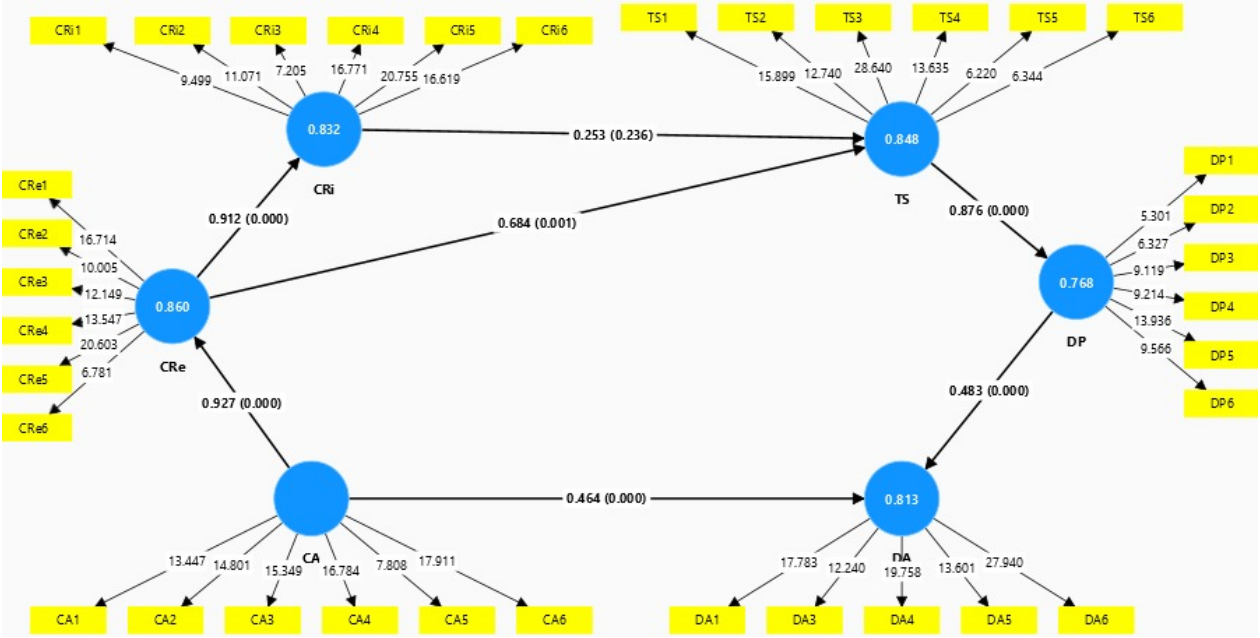

Fig. 3. Results of the Basic Model Analysis

that policies and regulations play in reducing cyber risks. This supports Sharma's [57] assertion that regulations and adherence to best practices are essential in combating cyber threats. Additionally, it illustrates that a robust framework or model, as proposed by Abrahams [2], can have a direct impact on how risks are perceived and managed.

Additionally, (in H5) cybersecurity regulations are closely linked to technical security because adopting regulatory frameworks not only supports risk management but also strengthens technological infrastructure. Authors like Kryshtanovych [30] and Saeed [51] agree that alongside technical advancements, users' perceptions of digital security have improved noticeably with these technologies. This highlights the critical need for an effective defense strategy supported by policies leveraging recent technologies to safeguard the cyber environment.

The strong connection between cybersecurity awareness and regulations (described in H6) emphasizes the importance of early education, as highlighted by Nwankpa [38], which enhances knowledge and increases awareness. Conversely, the results indicate that implementing policies and regulations stems from awareness influenced by education. This aligns with Mittal's [33] assertion that cybersecurity training efforts are crucial for establishing more stringent laws.

The results in H7 emphasize how cybersecurity awareness affects data responsibility, highlighting the importance of implementing comprehensive training in the classroom. As noted by Argyridou [6], such training can play a crucial role in the long-term development of future professionals, ensuring they act responsibly in their workplaces and society as a whole. Additionally, the impact of cybersecurity awareness on regulations was the most significant relationship in the entire model, highlighting the necessity of enhancing awareness among stakeholders to ensure proper compliance with cybersecurity standards.

Studies highlighted the importance of cybersecurity awareness, demonstrating a significant and statistically meaningful impact on both cybersecurity regulations and data responsibility (see Table 4). Private universities involved in the study should focus on this variable. Authors like Carley [9] have indicated that such variables greatly influence social cybersecurity. Additionally,

cybersecurity regulations play a crucial role in positively influencing cybersecurity risks and technical security. To mitigate the effects of social cybersecurity attacks, private universities should invest in programs that enhance cybersecurity awareness among their staff and students. Furthermore, they should establish regulations to effectively manage their cybersecurity measures. According to Wu [62] , awareness and regulations serve as tools that help minimize the risks of social cyberattacks in private higher education institutions

6 Conclusions

This study analyzed the relationships among six dimensions that influence social cybersecurity. The findings led to the development of an effective interdisciplinary model for managing social cybersecurity in universities located in metropolitan Lima. Additionally, it was confirmed that integrating various dimensions of cybersecurity effectively safeguards both computer assets and personal data. Technical security and data privacy are crucial for protecting information in educational settings. It is also important to examine the connection between cybersecurity risks and the technical solutions that can be utilized. Additionally, developing robust policies and strong regulatory frameworks is an effective way to improve the technical security of systems. Cybersecurity awareness and regulations are essential for enhancing the protection of information systems. Awareness helps staff and technology personnel understand potential risks and adopt secure practices, while regulations establish a framework for compliance and discipline, enabling effective management of these risks. This highlights the necessity of training programs and strong policies that cultivate a cybersecurity culture and ensure thorough defense against new digital threats.

To enhance clarity, the implementation of effective educational strategies must ensure that all members of the institution understand the risks associated with social cybersecurity and take proactive measures to mitigate these risks through responsible data management. Consequently, the findings of this study should inform future efforts to improve social cybersecurity practices, not only within the academic context but also across other sectors, such as business and government, which encounter similar cybersecurity challenges.

References

1. **Abdullayeva, F. (2023).** Cyber Resilience and Cyber Security Issues of Intelligent Cloud Computing Systems. Results in Control and Optimization, Vol. 12, pp. 1–16. DOI: 10.1016/j.rico.2023.100268.
2. **Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., Dawodu, S. O. (2024).** Mastering Compliance: A Comprehensive Review of Regulatory Frameworks in Accounting and Cybersecurity. Computer Science & IT Research Journal, Vol. 5, No. 1, pp. 120–140. DOI: 10.51594/csitrj.v5i1.709.
3. **AlSobeh, A. M. R., AlAzzam, I., Shatnawi, A. M. J., Khasawneh, I. (2023).** Cybersecurity Awareness Factors Among Adolescents in Jordan: Mediation Effect of Cyber Scale and Personal Factors. Online Journal of Communication and Media Technology, Vol. 13, No. 2, pp. 1–20. DOI: 10.30935/ojcmt/12942.
4. **Anshari, M., Syafrudin, M., Fitriyani, N. L., Razzaq, A. (2022).** Ethical Responsibility and Sustainability (ERS) Development in a Metaverse Business Model. Sustainability, Vol. 14, No. 23, pp. 1–14. DOI: 10.3390/su142315805.
5. **Anyanwu, A., Olorunsogo, T., Abrahams, T. O., Akindote, O. J., Reis, O. (2024).** Data Confidentiality and Integrity: A Review of Accounting and Cybersecurity Controls in Superannuation Organizations. Computer Science & IT Research Journal, Vol. 5, No. 1, pp. 1–17. DOI: 10.51594/csitrj.v5i1.735.
6. **Argyridou, E., Nifakos, S., Laoudias, C., Panda, S. (2023).** Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study. Journal of Medical Internet

Research, Vol. 25, No. 1, pp. 1–17. DOI: 10.2196/41294.

7. **Beltrán, A. (2024).** Análisis de la educación en ciberseguridad: Situación actual, estrategias y retos. Universidad de Granada. URL: https://hdl.handle.net/10481/92804.
8. **Calderaro, A., Blumfelde, S. (2022).** Artificial Intelligence and EU Security: The False Promise of Digital Sovereignty. European Security, Vol. 31, No. 3, pp. 415–434. DOI: 10.1080/09662839.2022.2101885.
9. **Carley, K. M. (2020).** Social Cybersecurity: An Emerging Science. Computational and Mathematical Organization Theory, Vol. 26, No. 4, pp. 365–381. DOI: 10.1007/s10588-020-09322-9.
10. **Centro Nacional de Planeamiento Estratégico (2025).** Actualización de las tendencias globales y regionales. Gobierno de Peru. URL: https://www.gob.pe/es/i/4985431.
11. **Cohen, J. (1988).** Statistical Power Analysis for the Behavioral Sciences. Routledge, pp. 1–567. DOI: 10.4324/9780203771587.
12. **Dominguez-Lara, S., Merino-Soto, C., Zamudio, B., Guevara-Cordero, C. (2018).** Big Five Inventory en Universitarios Peruanos: Resultados preliminares de su validación. Psykhe (Santiago), Vol. 27, No. 2, pp. 1–12. DOI: 10.7764/psykhe.27.2.1052.
13. **Duggineni, S. (2023).** Impact of Controls on Data Integrity and Information Systems. Science and Technology, Vol. 3, No. 2, pp. 29–35. DOI: 10.5923/j.scit.20231302.04.
14. **Durst, S., Hinteregger, C., Zieba, M. (2024).** The Effect of Environmental Turbulence on Cyber Security Risk Management and Organizational Resilience. Computers & Security, Vol. 137, pp. 1–10. DOI: 10.1016/j.cose.2023.103591.
15. **Erendor, M. E., Yildirim, M. (2022).** Cybersecurity Awareness in Online Education: A Case Study Analysis. IEEE Access, Vol. 10, pp. 52319–52335. DOI: 10.1109/ACCESS.2022.3171829.
16. **Eshetu, A. Y., Mohammed, E. A., Salau, A. O. (2024).** Cybersecurity Vulnerabilities and Solutions in Ethiopian University Websites. Journal of Big Data, Vol. 11, No. 118, pp. 1–35. DOI: 10.1186/s40537-024-00980-z.
17. **Fornell, C., Larcker, D. F. (1981).** Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. Journal of Marketing Research, Vol. 18, No. 3, pp. 382–388. DOI: 10.2307/3150980.
18. **George, A. S. (2024).** Emerging Trends in AI-Driven Cybersecurity: An In-Depth Analysis. PUIRP, Vol. 2, No. 4. DOI: 10.5281/zenodo.13333202.
19. **Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M. (2021).** A Primer on Partial Least Squares Structural Equation Modeling. Los Angeles, 3rd edition.
20. **Hair, J. F., Ringle, C. M., Sarstedt, M. (2011).** PLS-SEM: Indeed a Silver Bullet. Journal of Marketing Theory and Practice, Vol. 19, No. 2, pp. 139–152. DOI: 10.2753/MTP1069-6679190202.
21. **Hasani, T., Rezania, D., Levallet, N., O'Reilly, N., Mohammadi, M. (2023).** Privacy Enhancing Technology Adoption and its Impact on SMEs' Performance. International Journal of Engineering Business Management, Vol. 15, pp. 1–26. DOI: 10.1177/18479790231172874.
22. **Henseler, J. (2015).** Is the Whole More than the Sum of Its Parts? On the Interplay of Marketing and Design Research. University of Twente.
23. **Henseler, J. (2017).** Bridging Design and Behavioral Research With Variance-Based Structural Equation Modeling. Journal of Advertising, Vol. 46, No. 1, pp. 178–192. DOI: 10.1080/00913367.2017.1281780.
24. **Hijji, M., Alam, G. (2022).** Cybersecurity Awareness and Training (CAT) Framework for

Remote Working Employees. Sensors, Vol. 22, No. 22, pp. 1–23. DOI: 10.3390/s22228663.

25. **Hong, L., Hales, D. N. (2023).** How Blockchain Manages Supply Chain Risks: Evidence from Indian Manufacturing Companies. The International Journal of Logistics Management, Vol. 35, No. 5, pp. 1604–1627. DOI: 10.1108/IJLM-05-2023-0178.

26. **International Telecommunication Union (2024).** Global Cybersecurity Index. URL: https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx.

27. **Iwaya, L. H., Babar, M. A., Rashid, A. (2023).** Privacy Engineering in the Wild: Understanding the Practitioner's Mindset, Organizational Aspects, and Current Practices. IEEE Transactions on Software Engineering, Vol. 49, No. 9, pp. 4324–4348. DOI: 10.1109/TSE.2023.3290237.

28. **Khader, M., Karam, M., Fares, H. (2021).** Cybersecurity Awareness Framework for Academia. Information, Vol. 12, No. 10, pp. 1–20. DOI: 10.3390/info12100417.

29. **Kianpour, M., Raza, S. (2024).** More than Malware: Unmasking the Hidden Risk of Cybersecurity Regulations. International Cybersecurity Law Review, Vol. 5, No. 1, pp. 169–212. DOI: 10.1365/s43439-024-00111-7.

30. **Kryshtanovych, M., Panfilova, T., Khomenko, A., Dziubenko, O., Lukashuk, L. (2023).** Optimization of State Regulation in the Field of Safety and Security of Business: A Local Approach. Business: Theory and Practice, Vol. 24, No. 2, pp. 613–621. DOI: 10.3846/btp.2023.19563.

31. **Madrigal, C. A., García, M. G., Zumbado, I. M., Murillo, T. M., González, M. R., Ruiz, V. S. (2023).** Un análisis del sistema educativo costarricense: Desafío crítico para la ciberseguridad del país. Rhombus, Vol. 3, No. 2, pp. 1–19. URL: https://revistas.ulacit.ac.cr/index.php/rhombus/article/view/89.

32. **McAlaney, J., Benson, V. (2020).** Chapter 1 - Cybersecurity as a Social Phenomenon. Academic Press, pp. 1–8. DOI: 10.1016/B978-0-12-819204-7.00001-4.

33. **Mittal, C. (2024).** An Empirical Study on Cybersecurity Awareness, Cybersecurity Concern, and Vulnerability to Cyber-attacks. International Journal of Scientific Research and Management, Vol. 12, No. 04, pp. 1144–1158. DOI: 10.18535/ijsrm/v12i04.ec05.

34. **Murillo-Rosado, J. U., Rubio-García, S., Balda-Macías, M. A., Muñoz Mendoza, L. D. (2024).** Influencia de las tecnologías de la información y comunicación: Retos y potencialidades en la educación superior. Revista San Gregorio, Vol. 1, No. 57, pp. 170–185. DOI: 10.36097/rsan.v1i57.2564.

35. **Nejjari, N., Zkik, K., Hammouchi, H., Ghogho, M., Benbrahim, H. (2024).** Assessing Data Breach Factors Through Modern Crime Theory: A Structural Equation Modeling Approach. IEEE Access, Vol. 12, pp. 92198–92214. DOI: 10.1109/ACCESS.2024.3423651.

36. **Nguyen, T., Bhatia, S. (2020).** Higher Education Social Engineering Attack Scenario, Awareness & Training Model. Journal of The Colloquium for Information Systems Security Education, Vol. 8, No. 1, pp. 1–8. URL: https://cisse.info/journal/index.php/cisse/article/view/126.

37. **Nunnally, J. C., Bernstein, I. H. (1994).** Psychometric Theory. McGraw-Hill, Vol. 19, No. 3, pp. 303–305. DOI: 10.1177/01466216950190030.

38. **Nwankpa, J. K., Datta, P. M. (2023).** Remote Vigilance: The Roles of Cyber Awareness and Cybersecurity Policies Among Remote Workers. Computers & Security, Vol. 130, pp. 1–13. DOI: 10.1016/j.cose.2023.103266.

39. **Nwobodo, L. K., Nwaimo, C. S., Adegbola, A. E. (2024).** Enhancing Cybersecurity Protocols in the Era of Big Data and Advanced Analytics. GSC Advanced Research and

Reviews, Vol. 19, No. 3, pp. 1–12. DOI: 10.30574/gscarr.2024.19.3.0211.

40. **Ogbuke, N. J., Yusuf, Y. Y., Dharma, K., Mercangoz, B. A. (2022).** Big Data Supply Chain Analytics: Ethical, Privacy and Security Challenges Posed to Business, Industries and Society. Production Planning & Control, Vol. 33, No. 2-3, pp. 123–137. DOI: 10.1080/09537287.2020.1810764.

41. **Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., Bakare, S. S. (2024).** Data Privacy Laws and Their Impact on Financial Technology Companies: A Review. Computer Science & IT Research Journal, Vol. 5, No. 3, pp. 628–650. DOI: 10.51594/csitrj.v5i3.911.

42. **Presidencia del Consejo de Ministros (2023).** Decreto Supremo N.° 085-2023-PCM. Gobierno de Peru. URL: https://www.gob.pe/institucion/pcm/normas-legales/4471543-085-2023-pcm.

43. **Presidencia del Consejo de Ministros (2024).** Reglamento de la ley de gobierno digital. Gobierno de Peru. URL: https://www.gob.pe/13326-reglamento-de-la-ley-de-gobierno-digital.

44. **Presidencia del Consejo de Ministros (2024).** Reporte sobre entidades que implementaron su equipo de respuestas ante incidentes de seguridad digital. URL: https://www.gob.pe/es/i/2605569.

45. **Quach, S., Thaichon, P., Martin, K. D., Weaven, S., Palmatier, R. W. (2022).** Digital Technologies: Tensions in Privacy and Data. Journal of the Academy of Marketing Science, Vol. 50, No. 6, pp. 1299–1323. DOI: 10.1007/s11747-022-00845-y.

46. **Ramezanian, S., Niemi, V. (2024).** Cybersecurity Education in Universities: A Comprehensive Guide to Curriculum Development. IEEE Access, Vol. 12, pp. 61741–61766. DOI: 10.1109/ACCESS.2024.3392970.

47. **Ringle, C. M., Wende, S., Becker, J. M. (2024).** SmartPLS 3 - Software for PLS-SEM. URL: http://www.smartpls.com.

48. **Rodriguez, E., Santisteban, J., Morales, V., Morales, J. (2023).** Emerging Technologies that Ensure Information Resilience Against Social Engineering Attacks. Proceedings of the International Conference on Computer Science, Electronics and Industrial Engineering, Vol. 1, pp. 191–207. DOI: 10.1007/978-3-031-70981-4_14.

49. **Rodriguez, E., Santisteban, J., Morales, V., Morales, J. (2023).** Factors Influencing Frameworks for Social Cybersecurity Management. A Systematic Literature Review. Proceedings of the International Conference on Computer Science, Electronics and Industrial Engineering, Vol. 1, pp. 162–179. DOI: 10.1007/978-3-031-70981-4_12.

50. **Roldán, J. L., Sánchez-Franco, M. J. (2012).** Variance-Based Structural Equation Modeling: Guidelines for Using Partial Least Squares in Information Systems Research. In Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems. IGI Global, pp. 193–221. DOI: 10.4018/978-1-4666-0179-6.ch010.

51. **Saeed, S. (2023).** A Customer-Centric View of E-Commerce Security and Privacy. Applied Sciences, Vol. 13, No. 2. DOI: 10.3390/app13021020.

52. **Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., Alabbad, D. A. (2023).** Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, Vol. 23, No. 15, pp. 1–20. DOI: 10.3390/s23156666.

53. **Sebastian, G. (2023).** A Descriptive Study on Metaverse: Cybersecurity Risks, Controls, and Regulatory Framework. International Journal of Security and Privacy in Pervasive Computing, Vol. 15, No. 1, pp. 1–14. DOI: 10.4018/IJSPPC.315591.

54. **Shah, M. U., Iqbal, F., Rehman, U., Hung, P. C. K. (2023).** A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance. IEEE Access, Vol. 11, pp. 87970–87984. DOI: 10.1109/ACCESS.2023.3296580.

55. **Shaikh, F. A., Siponen, M. (2023).** Information Security Risk Assessments Following Cybersecurity Breaches: The Mediating Role of Top Management Attention to Cybersecurity. Computers & Security, Vol. 124, pp. 1–8. DOI: 10.1016/j.cose.2022.102974.

56. **Shaikh, F. A., Siponen, M. (2023).** Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. Information Systems Frontiers, Vol. 26, No. 3, pp. 1109–1120. DOI: 10.1007/s10796-023-10404-7.

57. **Sharma, P. (2024).** Enforcing Network Security Policies in the Context of the NIST Cybersecurity Framework and Its Legal Implications. Network Security, Vol. 2024, No. 7.

58. **Sriram, G. K. (2022).** Security challenges of big data computing. IRJMETS. URL: https://www.irjmets.com/paperdetail.php?paperId=a72c9bc7917f48291e5088df405cb17c&title=SECURITY+CHALLENGES+OF+BIG+DATA+COMPUTING&authpr=Gopala+Krishna+Sriram.

59. **Sulaiman, N. S., Fauzi, M. A., Hussain, S., Wider, W. (2022).** Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information, Vol. 13, No. 9, pp. 1–17. DOI: 10.3390/info13090413.

60. **Taherdoost, H. (2024).** A Critical Review on Cybersecurity Awareness Frameworks and Training Models. Procedia Computer Science, Vol. 235, pp. 1649–1663. DOI: 10.1016/j.procs.2024.04.156.

61. **Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., Sohal, A. (2022).** The Role of Cybersecurity and Policy Awareness in Shifting Employee Compliance Attitudes: Building Supply Chain Capabilities. International Journal of Information Management, Vol. 66, pp. 1–15. DOI: 10.1016/j.ijinfomgt.2022.102520.

62. **Wu, X., Duan, R., Ni, J. (2024).** Unveiling Security, Privacy, and Ethical Concerns of ChatGPT. Journal of Information and Intelligence, Vol. 2, No. 2, pp. 102–115. DOI: 10.1016/j.jiixd.2023.10.007.

63. **Wu, Y., Edwards, W. K., Das, S. (2022).** SoK: Social Cybersecurity. IEEE Symposium on Security and Privacy, pp. 1863–1879. DOI: 10.1109/SP46214.2022.9833757.

64. **Zhang, J., Zhang, Z.-m. (2023).** Ethics and Governance of Trustworthy Medical Artificial Intelligence. BMC Medical Informatics and Decision Making, Vol. 23, No. 7, pp. 1–15. DOI: 10.1186/s12911-023-02103-9.

Article received on 22/11/2024; accepted on 16/01/2025.
**Corresponding author is Elton Rodriguez.*