information

IMPACT FACTOR 2.9

CITESCORE 6.5

Article

Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm

Reismary Armas and Hamed Taherdoost

Special Issue

Information Security, Data Preservation and Digital Forensics

Edited by

Dr. Malinka Spasova Ivanova, Dr. Galina Bogdanova and Dr. Tomaž Klobučar

MDPI

https://doi.org/10.3390/info16050336

information

MDPI

Article

Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm

Reismary Armas [1] and Hamed Taherdoost [1,2,3,4,5,*]

[1] Department of Arts, Communications and Social Sciences, School of Arts, Science and Technology, University Canada West, Vancouver, BC V6Z 0E5, Canada; reismary.armas@gmail.com
[2] GUS Institute, Global University Systems, London EC1N 2LX, UK
[3] Q Minded | Quark Minded Technology Inc., Vancouver, BC V6E 1C9, Canada
[4] College of Technology and Engineering, Westcliff University, Irvine, CA 92614, USA
[5] Business Department, Gisma University of Applied Sciences, 10963 Berlin, Germany
* Correspondence: hamed.taherdoost@gmail.com

Abstract: Today, the world is experiencing constant technological evolution, allowing cyberattacks to manifest through different vectors and widely impacting victims, from specific users to serious damage to institutions' integrity. Research has shown that a significant percentage of recorded cyber incidents are attributed to social engineering practices or human error. In response to this growing threat, reinforcing cybersecurity awareness among users has become an urgent strategy to develop and apply. However, addressing cybersecurity awareness is a difficult challenge, specifically in the HE industry, where cybersecurity awareness should be an essential part of this type of institution due to the amount of critical data it handles. In addition to the need to strengthen the preparation of new professionals, statistics have shown a significant increase in successful security attacks in this industry. Therefore, this study proposes a conceptual Cybersecurity Awareness and Training Framework for Higher Education to facilitate the establishment of systems that improve the cybersecurity awareness of students in any academic institution, extending to all audiences that coexist in it. This framework encompasses key components intended to continually improve the development, integration, delivery, and evaluation of cybersecurity knowledge for individuals directly or indirectly related to the institution's information assets.

Keywords: cybersecurity; information security; information security framework; information security training; awareness for higher education

Academic Editors: Malinka Spasova Ivanova, Galina Bogdanova and Tomaž Klobučar

Received: 12 March 2025
Revised: 9 April 2025
Accepted: 17 April 2025
Published: 22 April 2025

Citation: Armas, R.; Taherdoost, H. Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm. *Information* **2025**, *16*, 336. https://doi.org/10.3390/info16050336

1. Introduction

Digital transformation has become a fundamental requirement for most industries worldwide, tending to be a necessity rather than an option for institutions. Companies and organizations increasingly rely on digital transformation to manage large amounts of data, provide and improve customer engagement channels, optimize their processes to remain competitive in their respective markets, and, in many cases, become dependent on digital transformation. This is supported by real data; for example, in 2021, global spending on digital transformation reached the important amount of USD 1.59 trillion, which is projected to increase to USD 3.4 trillion in 2026 [1]. This also applies to the field of cyberattacks, as also shown by the statistics registering an estimated cost of cybercrime worldwide in 2021 of USD 5.49 trillion, and with a projected cost of USD 11.36 trillion in 2026 [2].

In addition, a study revealed that, in a survey of 12,025 respondents (adults over 18 years of age) around the world, the three highest percentages pertaining to the experience of cybercrimes as of January 2023 include 41% related to viruses on computers or mobile phones, 35% through text messages to mobile phones, and 30% through phishing scams [2]. These attack vectors are related to the lack of awareness and appropriate training, targeting users that cannot identify possible threats or incidents. Additionally, when analyzing the distribution of cyberattacks worldwide, it was found that, by 2022, the industries most desired by attackers were manufacturing, with a 24.8% share; finance and insurance, with an 18.9% share; professional, business, and consumer services, with a 14.6% share; energy, with a 10.7% share; retail and wholesale, with an 8.7% share; and education, with a 7.3% share [3].

In previous research works, it has been shown that the main factor that contributes to the weakness of the HE industry is the lack of a continuous process of training and awareness specifically directed to students, professors, and administrative staff [4–8], which becomes an enormous challenge due to the constant flow of people in the industry. For example, in some universities, new students are entered every three months, and the shortest courses last from one to two years, without counting diploma courses that do not last one year. For its part, IBM, in one of its reports in 2023, indicated that the main drivers of cyberattacks in the HE industry are the phishing and theft of system access information [9]. These two factors are directly related to the handling of information by users, who, by not having the necessary training and awareness about the importance of safeguarding their information, cannot detect threats or bad intentions from emails or portals that request their data in one way or another.

On the other hand, statistics have also revealed that the HE industry has faced an increasing cybersecurity threat in recent years. An example is that, in 2022, there was a 157% increase in malware attacks globally in the HE industry compared to previous years [10]. Also, ref. [11] ranks educational organizations in first place as targets of malware attacks, recording more than 7.4 million attacks of this type in the last 30 days (this information was observed on 11 November 2023), followed by the retail and consumer goods industry, which, in contrast, saw less than 900,000 malware attacks. Also, Checkpoint recorded 75% more attacks in average weekly attacks in the education and research industry in 2021 compared to 2020 [12]. Another report showed that the industry under study ranked sixth among the industries most desired by cyber attackers in general between 2018 and 2022 [3]. This, in a way, has been the product of the rapid digital transformation and the rise of remote working without an adequate identification, classification, and control of the risk related to the information security threats present in this landscape, as well as the correct and deep preparation of users in information security issues [13]. However, it is also because HE is one of the industries that has less investment in information security in general [8].

Despite security policies, sometimes, based on the NIST Cybersecurity Framework, HE sectors need effective awareness and training programs adapted to their needs and peculiarities. An examination of multiple studies on user perception in various HE institutions shows that most users have not received proper information security training [5]. As the previous section explains, the problem that this research work seeks to solve is the need for an awareness and training framework specifically aimed at users linked to the HE industry, which are classified into professors, students, and administrative staff. Each of them has individual and specific needs according to their role and profile [4–8].

In this train of ideas, EDUCAUSE, a nonprofit association that is dedicated to supporting HE in the areas of the use of information technologies and knowledge, as well as other authors, have proposed and developed guides for the construction of information

security in HE, recommending alignment with some frameworks, such as those provided by International Organizations for Standardization (ISO), the National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT), and others [14,15]. Each of these frameworks provides information and guidance on the construction of an information security structure; some of them also guide the establishment of user awareness and training processes as part of the requirement to align the institutions to the frameworks.

However, these frameworks contain a wide range of needs for designing, implementing, and maintaining policies, standards, procedures, and guidelines that may function as institutional regulations. These must be tailored to the category, organization, information security needs, systems, infrastructure, and data type. Although these frameworks are global, they function at different levels of depth and are described generically, and they do not focus on the higher education industry or how to design, implement, and maintain a user training and awareness system that meets the needs of the HE industry.

The named frameworks are not directly aimed at HE, but the NIST produced a special publication, 800-50, in 2003 to help create an effective information technology security awareness and training program, which has the following four phases: design, development, implementation, and post-implementation [16]. In turn, this document is complimented by the publication 800-16, also from the NIST, which explains the training requirements of information technology security, and describes a model based on the roles and performance necessary for the implementation and control of the model described in NIST 800-50 [17]. Although these instruments published by the NIST are aimed at the management of mandatory information security in the United States of America, they serve as inputs, antecedents, and foundations for the secure management of information worldwide.

Other frameworks provide compliance points relating to the topic, although they are not totally focused on it. The ISO and IEC collaborated to standardize technical features in mutually relevant sectors. In the sphere of information technologies, the ISO/IEC 27001 standard provides a general and broad list of requirements for the development of an information security management system (ISMS), covering the most relevant points that can be summarized according to their applicability and which are limited to the nature of each organization [18].

In Section 7.3 of ISO/IEC 27001, there is a discussion about awareness, where it indicates that all of the people who are a part of the organization must be made aware of the company's policies, their role in contributing to information security, the benefits of this, and the implications of non-alignment to it [18]. In Annex A is control A.7.2.2, where the requirement to train and make employees aware of the security policy issues established by the organization is reinforced. Additionally, control A.12.2.1 emphasizes the importance of user awareness in detecting, preventing, and recovering from a malware attack [19].

As a complement to ISO/IEC 27001, there is ISO/IEC 27002, which is a reference to support the selection of controls. In this standard, it is mentioned that security policies at the user level must be accompanied by training and awareness, containing topics such as the use of information assets, how to take care of the information that may be exposed on desktops and screens, the transfer of information, the use of mobile devices, and the privacy and protection of identifiable data; additionally, it relists awareness and training for the detection and recognition of malware.

Another relevant framework in security construction is the Center for International Security (CIS), which, in its control 14, establishes requirements that suggest creating and maintaining a user training process for the detection and reporting of malware, social engines, erring, and other incidents, outdated information security, best practices for au-

thentication, data handling, the consequences of the unintentional exposure of information, and connecting and transmitting information in insecure networks. Also, an important piece of information provided by this framework is its recommendations for other standards toward the construction of the awareness and training process, where it lists the following: NIS SP 800-50, the National Cyber Security Center (UKUK), EDUCAUSE, the National Cyber Security Alliance (NCSA), SysAdmin, Audit, Network, and Security (SANS), CIS Controls Telework, and the Small Office Network Security Guide [20].

In this way, other frameworks, such as those provided by the NCSA and SCF, which, like the NIST, ISO, and CIS, are international standards, contain, in some of their sections, requirements to raise the level of information assurance through the training and awareness of people within an organization. However, except for NIST SP 800-50, they are not focused on the step-by-step construction of a continuous user awareness and training process, and none of them are specific to the HE industry.

It is important to highlight that a customized information security framework is key to addressing the unique needs and challenges of a particular industry, thereby further closing the chances of successful attacks. This also contributes to compliance with specific regulations for the industry. For example, the Health Insurance Portability and Accountability Act (HIPAA) addresses various aspects of healthcare, with a primary focus on protecting the privacy and security of individuals' health information [21]. As stated in the previous section, the deficiency in information security, cybersecurity knowledge, and user awareness has led to a significant rise in cyberattacks, leveling HE institutions as an emerging objective for attackers, and resulting in a rise in data breaches, malware attacks, phishing attempts, and ransomware incidents [5,9,10].

Thus, this industry needs a tailored information security awareness and training process that takes into account the diverse individuals in this field, such as students, professors, and administrative staff, the industry's dynamic information assets, and the ever-changing cybersecurity threat landscape. This personalized strategy will strengthen HE institutions' security posture and enable individuals to anticipate and mitigate possible threats through training procedures matched with information security policies. This study emphasizes the need for HE institutions and users to receive specialized awareness and training.

2. Literature Review

This section gathers the theoretical bases necessary for the understanding of the concepts related to the objective topic of this research document.

2.1. Information Security and Cybersecurity

Information security and cybersecurity have recently become a necessity, as organizations and people increasingly depend on technology and data management. To manage these two relevant topics, it is necessary to understand the concepts from a basic point of view so to easily interpret them, but, at the same time, to provide relevance to their importance and the implications that its management details.

The National Institute of Standards and Technology provides the following easy definition of information: it is any type of knowledge, data, fact, or news that can be presented in any type of format, whether physical, digital, textual, numerical, graphic, audio, or video. Therefore, information can be considered as an asset of an organization or person, since it is something that belongs to it and has value to its owner, like any other asset [22].

Concerning information security, it refers to the set of actions, processes, and controls that are applied to protect information in such a way as to avoid its misuse, access to unauthorized persons, disclosure, corruption, and/or destruction [23], which are as follows:

- Confidentiality: the prevention of unauthorized people from having access to information;
- Integrity: the prevention of information from being modified or destroyed by unauthorized individuals;
- Availability: making information available for authorized users when necessary.

As for the term cybersecurity, it follows the same principles of information security but is applied specifically to digital information. Therefore, cybersecurity is dedicated to preventing damage and protecting digital information contained in electronic communication systems, networks, databases, and digital equipment so to guarantee its availability, integrity, and confidentiality [22].

At this point, it is important to note that information security covers all types of information, while cybersecurity focuses on digital information. This is because the management of the latter faces challenges at the level of the digital plane that goes beyond the application of physical controls, such as those managed in physical information files. Figure 1 depicts this explanation, which comes from the interpretation of information security and cybersecurity concepts [22–24].

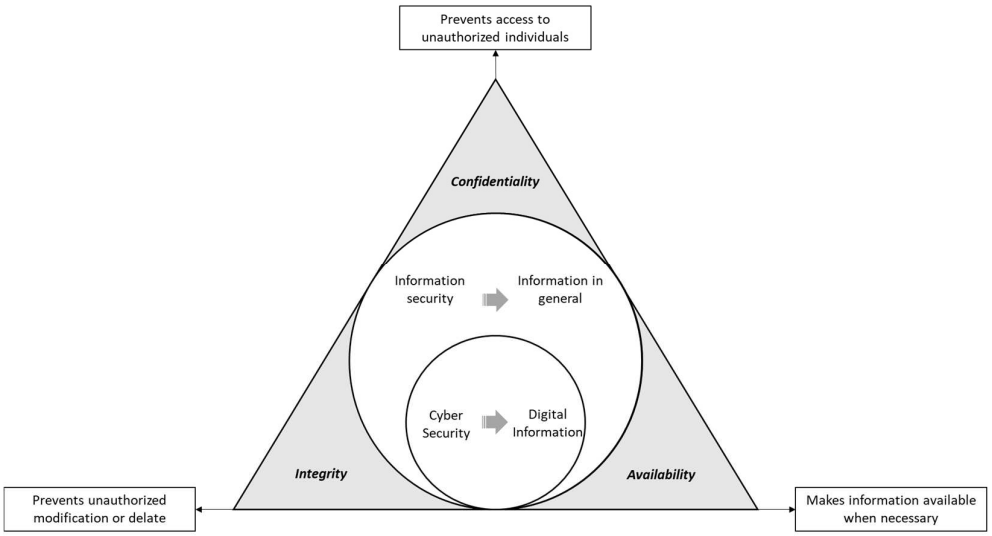

Figure 1. Information security and cybersecurity.

2.2. Importance of Information Security

Information security is essential to keeping an organization's information safe. In the case of individuals, it is crucial to keep personal identity-related information secure and confidential, as much of this information can give access to more critical information that can be used for identity theft and other assets, such as bank accounts. This can, in some cases, lead to transactions and actions that are harmful to the affected party.

On the other hand, regarding institutions, information security is related to maintaining trust in the institution, complying with regulations and privacy laws, preventing financial losses, and protecting the data of people linked to the organization. Additionally, it ensures the operational continuity and the security of critical infrastructure.

It is important to remember that many of the attacks against information security are not necessarily for monetary gain. The reason for attacks or cyberattacks can have different purposes or reasons, such as personal motivation, which can occur when an employee is dissatisfied with the company's disclosure of critical information. These causes of attacks or information leaks can also occur unintentionally but, in turn, have the same reputational

effect for the organization; other reasons may be related to cyber terrorism (hacktivism), and others to corporate espionage [25].

Another important factor to consider in this analysis is that the attacks and threats can have internal or external origins. Research and statistics indicate that an important percentage of the attacks originate internally, and the most common vector of attack is phishing or malware, where an employee or user of information is intentionally or unintentionally disclosing critical data of the organization as a product of human error [26–28].

In summary, information security is important so to cover the three key aspects of organizational and individual integrity. The first one is the protection of data and privacy, which emphasizes the safeguarding of personal and sensitive information, both for individuals and organizations, including financial security, online reputation, and privacy preservation. The second is mitigating threats, whether internal or external, through controlling data access, preventing data loss, and ensuring business continuity, trust in general, and compliance with regulations. Finally, the third aspect is applying controls to minimize internal and external threats, preventing disruptions, safeguarding intellectual property, and maintaining trust.

2.3. Who Is Information Security for?

According to the previous sections, it can be said that information security is for everyone, individuals and organizations in general, and is an issue that should be considered and addressed as an integral part of education in general, and which is the responsibility of each person regardless of the role that they fulfill.

In the beginning, computers were mainly tools for scientists and researchers, while the Internet had its roots in academic and military applications, and both were not services and tools used for the daily needs of people; with time, both became basic needs [29,30]. This process has also occurred with information security due to the advancement of the digital transformation and the simplification of daily processes, including financial transactions, profile control for access to various portals, and the generation and safeguarding of data and information in general, among others. The knowledge of information security and cybersecurity issues has become a basic need so to protect the integrity of individuals and organizations [31].

Returning to the example of computers and the Internet, as is known, over time, they began to play an important role in everyday life, extending beyond the use of experts, so that the public saw the need to manage these technologies effectively for their daily development at the educational, work, entertainment, and communication levels. In response to this growing need, educational institutions, including schools and universities, began offering elective courses designed to teach people how to use computers and the Internet; later, they became part of the mandatory courses, and, today, both are mandatory in all courses. At a global level, we all must use these tools. Relevant support for this, in addition to popular knowledge, is that, today, a total of approximately 5.3 billion Internet users are registered worldwide [32], which is a relevant number considering that the world population is close to 8 billion inhabitants according to the live census of the United States Census Bureau recorded on 10 September 2023 [33].

An important factor that has emerged during this digital transformation has been the critical need for user awareness and training in cybersecurity, which involves instructing people on how to stay safe in the digital realm, like how one learns to protect their personal belongings, but from a transversal and census language, so that everyone can understand the importance and the implications of not doing so. Aiming to equip people with the knowledge and tools to safeguard their digital assets and, in addition, to support the protection of the environments where they operate, such as the workplace, education,

and in the consumption of services and entertainment, creates the outermost layer of information security for institutions [31].

Therefore, in essence, education in information security and cybersecurity are essential components of the training of individuals and extend to organizations of all types and sizes, which must also apply other layers of security that are more focused on processes, infrastructure, and systems. Therefore, these concepts, habits, practices, and constant updating must be integrated into education from an early age, and made available to people of all origins and ages, which would collectively foster a safer and more responsible digital environment, thus protecting information assets in general.

In this train of ideas, Table 1 summarizes and reflects on the most relevant aspects of the importance of information security for both individuals and institutions, collected from diverse reported analyses [26–28,31].

Table 1. Aspects of the importance of information security for individuals and institutions.

Aspect of Importance	For Individuals	For Institutions
Protection of Personal Data	Safeguards against identity theft and privacy violations.	Compliance with data protection regulations and laws.
Financial Security	Prevents financial losses due to fraud and cybercrime.	Avoids financial losses, legal fines, and reputational damage.
Online Reputation	Preserves trust and credibility in personal and professional spheres.	Avoids damage to reputation and the loss of customers and partners.
Privacy Preservation	Protects personal information and online privacy.	Maintains the privacy of customer and employee data.
Protection from Cyber Threats	Guards against malware, phishing, and ransomware attacks.	Mitigates the risk of cyberattacks and data breaches.
Data Access Control	Ensures control over personal data and who can access it.	Controls access to sensitive corporate information.
Preventing Data Loss	Prevents the loss of personal data and digital assets.	Safeguards intellectual property and sensitive data.
Business Continuity	Ensures the ability to access online services and resources.	Maintains business operations during cyber incidents.
Trust in Online Services	Enhances confidence in online services and transactions.	Builds trust among customers, clients, and partners.
Adherence to Regulations	Ensures compliance with data protection and privacy laws.	Avoids legal penalties and regulatory sanctions.
Protection from Insider Threats	Guards against accidental or intentional data leaks.	Prevents insider threats, data theft, and sabotage.
Preventing Disruptions	Minimizes disruptions due to cyberattacks and service outages.	Reduces downtime and financial losses from cyber incidents.
Intellectual Property	Protects personal creative work and inventions.	Safeguards proprietary information and trade secrets.

Relevant aspects of the importance of information security for individuals and institutions.

2.4. Information Security Training and Awareness

Information security training and awareness involves teaching people how to protect their information and use the Internet safely. It aims to give them the skills and knowledge to keep their online activities secure, just like when people learn to lock their doors to keep their homes safe and to be careful with whom they give entry.

Preparing users to apply effective security controls on the information they handle involves, for example, the creation of secure passwords; the identification of risks, such as those related to malicious emails (phishing); the protection of personal data, such as passwords and account access data (for example, bank accounts and social network profiles, or access to other systems); the safe use of the Internet, including avoiding dangerous sites and preventing the downloading of unknown elements, and the delivery of data; recognizing cyber threats, as well as avoiding the installation of viruses and malware; emphasizing responsible online behavior; staying updated and informed regarding the latest threats and forms of cyberattacks; and, last, but not least, teaching users to report incidents or suspicions of these, and the importance of this action for collective protection and the adjustment of existing security controls or the implementation of new ones [7,28,31].

According to researchers, an awareness and training program in information security and cybersecurity should include the following three fundamental aspects in the delivery of information and the development of user skills: education, through general and specific theories of the sector to which the organization belongs; awareness, highlighting the importance of information security and the implications of not addressing these issues; and training, which contributes to the hardening of threat recognition skills but also to support the modification of behaviors that are misaligned with information security. Additionally, it is recommended that these programs be accompanied by the implementation of change management models, a recognition program, support for strengthening the cognitive skills of users, and the creation of an Information Security Culture and community [6,7,16,31].

2.5. Benefits of Implementing an Information Security Awareness and Training Program

An ISACA explains the multifaceted benefits and various compelling reasons to develop and implement an information security awareness and training program [34], some of which are explained in the following list:

- Regulatory Benefits: This is one of the primary rationales behind this process. However, while specific laws governing information security and privacy vary across countries, their fundamental purpose remains constant: safeguarding citizens and organizations from potential harm. In most legal and regulatory requirements, the adherence to these protocols is pivotal, and awareness training serves as evidence of compliance. Typically, following the process is mandatory for all employees; such training can also be tailored to cater to the needs of executives and business lines.
- Benefits to Business Organizations: Serving to establish organizational policies, foster a secure environment, and cultivate a uniform security posture throughout the organization. These programs assist in defining the levels of data sensitivity, addressing concerns related to mobile media, and accentuate the prevention of identity theft. Furthermore, they act as a shield for the organization's reputation by pre-empting security breaches and data losses, ultimately nurturing a secure and compliant operational milieu.
- Personal and Employee Benefits: Beyond the organizational sphere, these training programs extend tangible benefits to individuals and employees. They educate individuals about the legal and ethical aspects of safeguarding data, thereby underscoring personal accountability for data mishandling, particularly within a professional context. By imparting knowledge and promoting responsible cybersecurity practices, employees could also assume the role of mentors, sharing insights into cybersecurity best practices with colleagues. These training programs not only fortify personal cybersecurity but also extend to securing sensitive family information and reinforcing ethical conduct in online interactions.

2.6. The Higher Education Industry

The field of higher education is complex, as it encompasses a mix of public and private institutions of various sizes, including a variety of state universities and community colleges in the public sector, nonprofit schools, ranging from research universities to world-renowned schools, such as Harvard and Stanford, to prestigious liberal arts colleges, such as Swarthmore and Williams, in addition to the many less selective schools, including those with religious affiliations [35]. This industry generates substantial income and offers employment opportunities. For example, higher education (private for-profit institutions) in the United States alone generated around USD 13.06 billion in revenue in the period 2019–2020 [36].

According to [37], there were an estimated 31,097 universities from all over the world as of July 2021, where the top five countries with more universities are India, with 5288, the United States of America, with 3216, Indonesia, with 2595, China, with 2565, and Brazil, with 1297. Bringing together these five countries, 48.15 v% of the total number of universities are registered in the statistics.

In terms of the challenges facing HE, it is clear that changes are needed. The World Economic Forum suggests that higher education should be geared toward active learning and teaching skills that remain valuable in an ever-evolving world. Formative assessment, which involves continuous assessment, is more effective in equipping students with the skills they need to succeed compared to high-stakes testing [38]. The recent COVID-19 pandemic has forced schools and universities to move an important part of their teaching online. They discovered that it is possible to manage a certain part of the industry in this way, facilitating the expansion of study centers without the need to expand infrastructure to enable classrooms or buildings in general, and, combined with the convenience of avoiding the transfer of people to a physical location, this has led to a large part of higher education being maintained online [39].

2.7. Why Has the HE Industry Become More Desirable to Cyber Attackers?

In the Introduction and Problem Background sections, the state of the art of information security and cybersecurity in the HE industry was explained; however, the cause of the increase in attacks in the industry was not developed in-depth, a point on which this section focuses.

The higher education industry's attractiveness to cyber attackers stems from valuable data, research assets, personal information, and potential financial gains. Another factor is the cultural factor inherent to the industry, where people tend to be free and open in sharing information [8,39].

In addition, other industries such as retail, corporate banking, financial services, insurance, service providers, energy, manufacturing, and healthcare have reinforced their security systems, both in the implementation of technological solutions and in the preparation of employees in the safe use of systems related to their work and participation in the industry [2,40].

To mitigate these risks, universities and colleges must invest in robust cybersecurity measures, raise awareness among their academic communities, and stay vigilant against evolving cyber threats [31]. Table 2 shows a resume of the most common causes of why the HE industry has become more desirable to cyberattacks. This resume comes from the interpretation of the work conducted by [8,31,39,41].

Table 2. The most common causes of why the HE industry has become more desirable for cyberattacks.

Group of Causes	Details	Example/Explanation
Source of valuable data and intellectual property	Rich Data Stores	Student records, financial information, and research data.
	Research and Intellectual Property	Valuable studies and innovation.
	Personal Information	Social Security numbers and credit card data.
Financial incentives	Financial Resources	Ransomware attacks for financial gain.
Security vulnerabilities	Weaker Security Awareness	Diverse user base with varying security awareness.
	Limited Resources for Cybersecurity	Budget and resource constraints.
	Open Networks	Collaborative and open network environments
Attack methods	Credential Harvesting	Stealing login credentials for various services.
	Botnets and Distributed Attacks	Compromising connected devices.
	Supply Chain Attacks	Targeting the broader supply chain.
Nation-state interest	Nation-State Actors	Espionage, research access, and intelligence gathering.
Longer attack windows	Holidays and Vacations	Extended periods of low activity during breaks.

2.8. Comparison Between the Security Level Applied in HE and Other Industries

The security levels applied in the HE industry may vary due to factors like regulatory requirements, data sensitivity, budget constraints, and the diverse user base. Other industries, especially those that are highly regulated, tend to prioritize cybersecurity more extensively due to the critical nature of the data that they handle and the regulatory pressures that they face. While HE institutions have unique challenges, they must continue to invest in cybersecurity to protect their data, research, and reputation. One of the most important comparison factors for this study is the regulatory environment because, although the higher education industry is subject to certain regulations, they may not be as strict as those in highly regulated sectors such as finance (the banking) or healthcare, which are regulated by the HIPAA and are mandated to meet strict data privacy and security standards, with strong penalties for non-compliance. Conversely, in the case of compliance requirements, higher education almost always focuses on protecting students' online payment data and personal information [42].

Higher education institutions deal with diverse data types, including student records, financial data, research data, intellectual property, and faculty information. While some of these data are sensitive, they have not been managed or considered as critical as financial or healthcare data in general terms; however, as has been mentioned before, this information still represents an attractive target for cyber attackers due to being lucrative data [8,39,41]. On the contrary, finance deals with highly sensitive financial data, and healthcare manages protected health information, therefore prioritizing data security and privacy so to protect against severe consequences [43].

Considering budget and resources, many HE institutions may have limited budgets and resources allocated to cybersecurity. This limitation can impact the level of security measures and staff available. Conversely, highly regulated industries often allocate significant budgets for cybersecurity initiatives, including the employment of dedicated security teams, advanced security technologies, and regular security audits. An example of

this is the healthcare industry, which registered an increase in its budget allocation by at least 25 percent in 2021 compared with the registered number in 2020 [44].

In the case of the user base, HE institutions often have a diverse user base, including students, faculty, and staff. This diversity can make it challenging to maintain a consistent security awareness culture [41]. However, this can be analogized to the user base of health institutions, since students tend to be homologous with patients or the users of the medical services, and professors with doctors, and both industries need administrative personnel. On the other hand, some industries, like finance, have a more controlled user base, comprising employees with a strong focus on security protocols.

Concerning the research focus, universities and colleges emphasize research and collaboration, which can result in open and collaborative network environments. While this fosters innovation, it may introduce vulnerabilities, making it more attractive for cyberattacks [31,39]. Meanwhile, highly regulated industries prioritize security over collaboration, often resulting in more closed and controlled network environments.

Finally, as has been explained in previous sections, HE institutions face a broad range of cyber threats, including phishing attacks, data breaches, and intellectual property theft. They may also be targeted by nation-state actors seeking research data. For example, financial institutions are prime targets for financial fraud and cyberattacks, and healthcare is susceptible to ransomware attacks.

2.9. Information Security Frameworks and Its Contributions to Awareness and Training Programs

According to the work described by Mercer [45], and in a general context related to regulatory compliance and the standardization of regulatory processes, a regulatory framework refers to a structured and organized set of guidelines, principles, recommendations, and rules that provide a basis for establishing, implementing, and evaluating specific practices or processes.

In other words, a regulatory framework helps to progressively organize the implementation of processes in an orderly manner in such a way that all elements of the involved areas of the organization work coherently and asynchronously to achieve a common objective. In this case, the design, implementation, control, and continuous evolution of user awareness and training programs on cybersecurity and information security issues involves individuals internal and external to the organization itself but who, in turn, make use of and manage the institution's information assets and systems.

For the specific case of information security frameworks, improving awareness and training programs is essential to ensure the protection of confidential information and to reduce the risk of security breaches within organizations. This is supported by various specialists and researchers, who indicated that security must be a combination of the benefits that properly configured technological systems can provide, security controls specifically applied and adapted to the institution, with the training of the users who manage and have access to organizational information [4,16,34,46,47]. Therefore, not everything is in the hands of technology. It is also required that people know the risks, threats, and best practices related to the information they manage according to their role, and the implications of not taking this into account alongside the seriousness and consequences that this represents.

To emphasize the distinctiveness of the proposed Cybersecurity Awareness and Training Framework for Higher Education (CA&TF for HE), a comparative analysis was conducted against widely adopted frameworks, including the NIST NICE, ISO/IEC 27001, and the ENISA Cybersecurity Culture Guidelines (Table 3). While these frameworks offer general cybersecurity guidance, they often fall short of addressing the nuanced and dynamic context of higher education institutions.

Table 3. Comparison of CA&TF for HE with existing frameworks.

Feature	NIST NICE	ISO/IEC 27001	ENISA Guidelines	CA&TF for HE (Proposed)
Target Sector	General workforce	All organizations	Public/private sectors	Higher education-specific
Role-based Segmentation	Partial (job categories)	Not detailed	Limited	Explicit (students, faculty, staff, admin)
Training Content Customization	Moderate	Minimal	Moderate	High (based on user role and access level)
Adaptive Learning Paths	No	No	No	Yes (AI/ML suggested for future implementation)
Feedback Loop for Dynamic Threats	Not embedded	Not embedded	Basic	Yes (threat intelligence integration)
Decentralized Institution Readiness	Not addressed	Centralized control model	Not addressed	Yes (designed for distributed HE systems)
Integration of Emerging Technologies	Low	Low	Moderate	High (planned AI, blockchain-based protection)
Implementation Guidance	Structured	Highly formalized	Guideline-based	Roadmap with practice-oriented stages
Evaluation Mechanisms	Not defined	Requires audit	General recommendations	Simulation-based and survey feedback suggested

This segment of the literature review of this research is dedicated to the study of some of the most popular information security frameworks, such as the NIST Cybersecurity Framework, ISO/IEC 27001 and 27002, the SANS Security Awareness Maturity Model, the Center for Internet Security Controls Version 8 (CIS Controls v8), the Control Objectives for Information and Related Technologies (COBIT), and the Cybersecurity Awareness Framework for Academia (CAFA), focusing specifically on their contributions to the development of awareness and training programs, and the opportunities for improvement concerning the topic.

2.9.1. National Institute of Standards and Technology (NIST)

The NIST is an institution that is part of the United States Department of Commerce. However, currently, the NIST is one of the global leaders in measurement solutions and standards, with a high level of inclusion, integrity, and excellence. It has also contributed substantially to standards and publications that promote the responsible management of information security, which includes, as a fundamental part of the standardization of the design, the implementation of awareness processes and the training of users in information security, starting with the establishment of information security areas [48].

Speaking specifically of the NIST's contribution to establishing information security for institutions, it has developed a framework that is divided into the following three basic components: the central framework, implementation levels, and profiles. The central framework is subdivided into 5 high-level functions, 23 categories, and 108 subcategories, which is explained in a non-technical language and transversal to all areas in such a way that it can be understood by people who are not specialists in the security areas of information or related [49].

Figure 2 illustrates that the Awareness and Training category in the NIST's framework falls under the 'Protect' function (PR.AT) [50], and shares connections with other frameworks, like the CIS CSC, COBIT 5, ISA, ISO/IEC 27001, and NIST Special Publication

800-53, which will be discussed in this section. Regarding the levels of implementation, these are related to the alignment of the institution to the framework, where this will depend on the strategic objectives of the institution and not on its level of maturity. The implementation levels range from partial implementation to the adaptive phase, indicating the level of integration of the framework with risk decisions that impact broad levels of the organization and that, in turn, have inter-relation with parties external to the organization, such as suppliers or customers, and the information that flows to and from them.

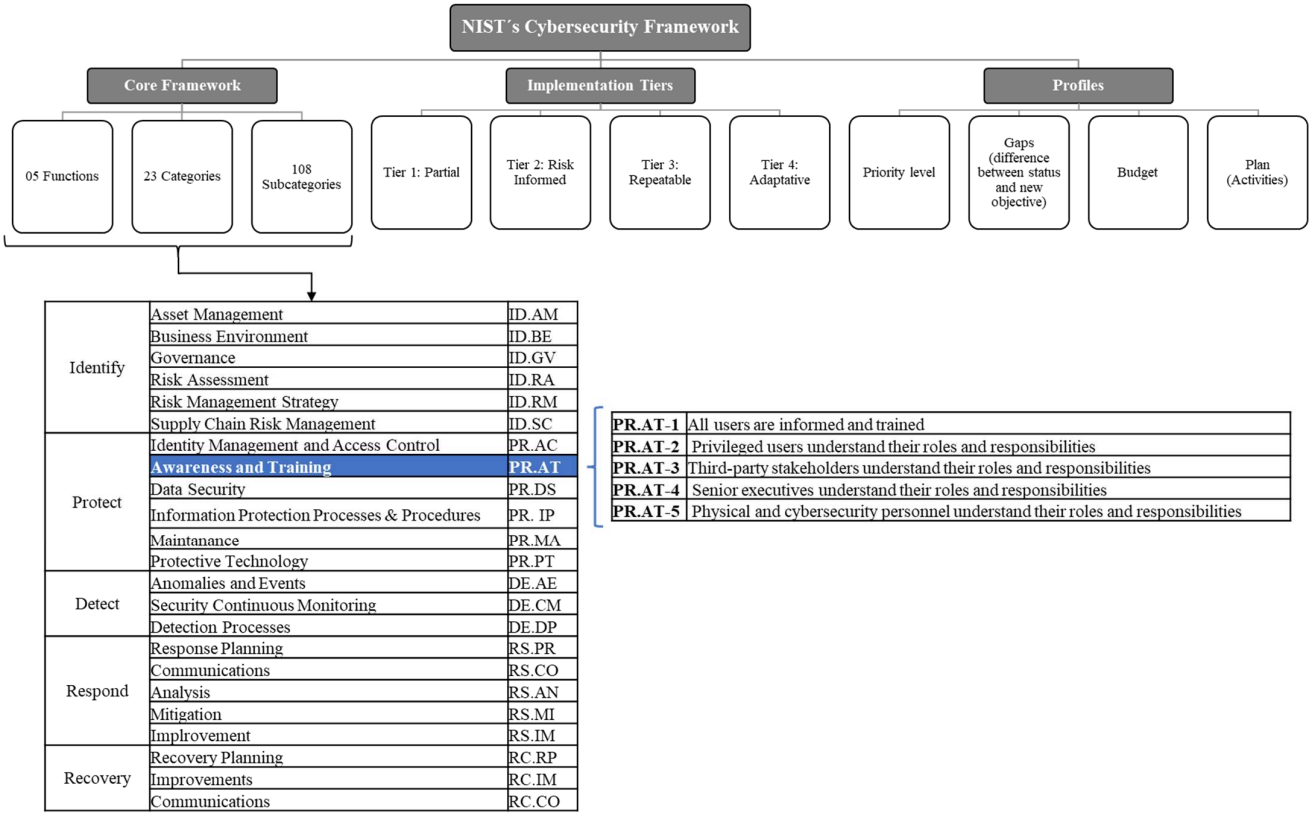

Figure 2. NIST's Cybersecurity Framework structure.

Therefore, the levels of the implementation of this framework will depend specifically on how functional and compatible they are with the operation of the organization. As for the profiles, this helps to identify and align the organization's objectives with the implementation and fulfillment of functions, categories, and subcategories, and, in turn, the risk tolerance and resources of an organization with the current results achieved and the following objectives. This contributes to the identification of opportunities for improvement in cybersecurity, thereby becoming a process of continuous improvement [49].

An interpretation of the information published on the NIST official website [49] and the NIST's Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 [50], is the base used to develop Figure 2, which depicts the specific contribution of the NIST's Cybersecurity Framework in user awareness and training. This contribution is organized into the second function, "Protect" (PR), the category "Awareness and Training" (PR.AT), and the five subcategories from PR.AT-1 to PR.AT-5.

Concerning the development levels of the subcategories, the NIST establishes four levels, which are explained below in Table 4, from the point of view of awareness development. This table is an excerpt from the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 [50].

Table 4. Description of the NIST's Cybersecurity Framework implementation tiers.

TIER	Risk Management Process	Integrated Risk Management Program	External Participation
1: Partial	Not formalized; reactive	Limited awareness Case-by-case implementation	Unaware of the cyber supply chain risks.
2: Risk-Informed	Practices are approved but may not be established as policy	There is an awareness of the cybersecurity risk, but an approach to managing this risk has not been established	There is an awareness of the cyber supply chain risks but does not act consistently or formally upon those risks.
3: Repeatable	Formally approved and expressed as policy	Personnel possess the knowledge and skills to perform their roles and responsibilities	There is an awareness of the cyber supply chain risks and formal mechanisms to communicate baseline requirements, governance structures, and policy implementation.
4: Adaptative	Cybersecurity practices are based on previous and current cybersecurity activities, including lessons learned and predictive indicators	Cybersecurity risk management evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks	It receives, generates, and reviews prioritized information that informs the continuous analysis of its risks as the threat and technology landscapes evolve.

To address and focus on the need for support that exists in the areas of awareness and user training on cybersecurity issues, the NIST has developed special publications that complement its cybersecurity framework by delivering detailed documents, such as those indicated below.

- NIST SP 800-16. This special publication contains a model that supports the establishment of a professional team in charge of information security, highlighting the awareness, training, and education that each individual needs according to the role that they play in the institution, thereby providing a guide for management of training programs in information technology and cybersecurity [17].
- NIST SP 800-50. This special publication is a compendium of detailed requirements for the creation of an awareness and information security training program divided into the following four sections: the first is dedicated to the design of the program, the second to the development of material to be used in the program, the third to the implementation of the program, and, finally, the fourth to the processes related to post-implementation [16].
- NIST SP 800-53. Chapter 3.2 of this publication provides specific aspects related to user awareness and training. It provides a list of requirements necessary for developing an awareness and training program based on roles, policy, and procedures, literacy training and awareness, the control of the training carried out, the interpretation of its results, and feedback [51].

Based on the above description, the NIST's contribution is based on comprehensive, detailed, and complete guidance, which allows it to be molded in a certain way to be implemented by different organizations belonging to various fields. Additionally, it offers a flexible framework that can be adapted to the unique security needs and risks of each organization. It can be integrated with other standards, such as ISO/EIC 27001, providing a more robust approach to information security.

However, this framework also has weaknesses, as the NIST guidelines can be complex and resource-intensive to fully implement. Furthermore, since the framework is so broad and generic, specific points and needs of certain organizations or industries may escape the context.

Additionally, this framework focuses on regulatory needs in the United States, which may not align or consider some of the needs of organizations in other countries relative to the particularities of other regions. Therefore, points of improvement that can be applied to this framework could be to expand certain aspects to make it more applicable at a global level by considering international standards and regulations. Another improvement that could be suggested is to develop specific guides that adapt to different industries so to summarize the adaptive work for those smaller institutions, or those whose core is not technology and that lack a mature area of information security.

2.9.2. ISO/IEC 27001

The International Organization for Standardization (ISO) is a non-governmental institution currently made up of 169 members (national standards bodies) whose objective is to develop international standards, which are based on the consensus for the standardization of operational aspects, production, and innovation-relevance in various markets. These standards are generated from the convergence of the knowledge and expertise of the members that comprise it [52].

For the specific case of information security, the ISO has developed an international standard under the name ISO/IEC 27001, which supports organizations that decide to align themselves with the standard to implement an information security management system (ISMS) to protect their information assets through information security risk management. This framework recommends the development, establishment, and continuous improvement of policies, processes, technology, and training of people to maintain optimal levels of confidentiality, integrity, and the availability of information assets. Moreover, it promotes the identification and constant evaluation of the environment of security threats related to the institution, which is one of the main sources of information for the creation, establishment, and modification of security controls, ranging from technological and operational aspects to cultural aspects. Additionally, ISO/IEC 27001 establishes the periodic evaluation cycles of the ISMS so to adapt it to the organization's strategic objectives, the changes present in the market, new emerging risks, and new needs in general. Therefore, one of the key topics for establishing an efficient ISMS is periodic risk assessments and monitoring, which leads to establishing the ISMS as a continuous improvement process [18].

Figure 3 shows the ISO/IEC 27001 structure and its contribution to developing an awareness and training program based on the normative interpretation of information published in ISO/IEC 27001 [18].

ISO/IEC 27001 emphasizes the importance of security awareness and training throughout the standard. However, as Figure 3 shows, this standard does not have a section specifically dedicated to user awareness and training, but these factors are integrated into various clauses and controls, particularly into subclause 7.3 (Awareness), that, in turn, is decomposed into three controls that aim to keep employees informed about security policies, their relationship with the ISMS, and the implications of not meeting information security requirements. Regarding Annex A, in Section A.7 (Human Assets Security), control A.7.2 (During employment) demands the awareness and training of employees about the security aspects of the company. On the other hand, in Annex A.12 (Operational Security), control A.12.2 (Protection from malware) recommends the implementation of a control against malware [18].

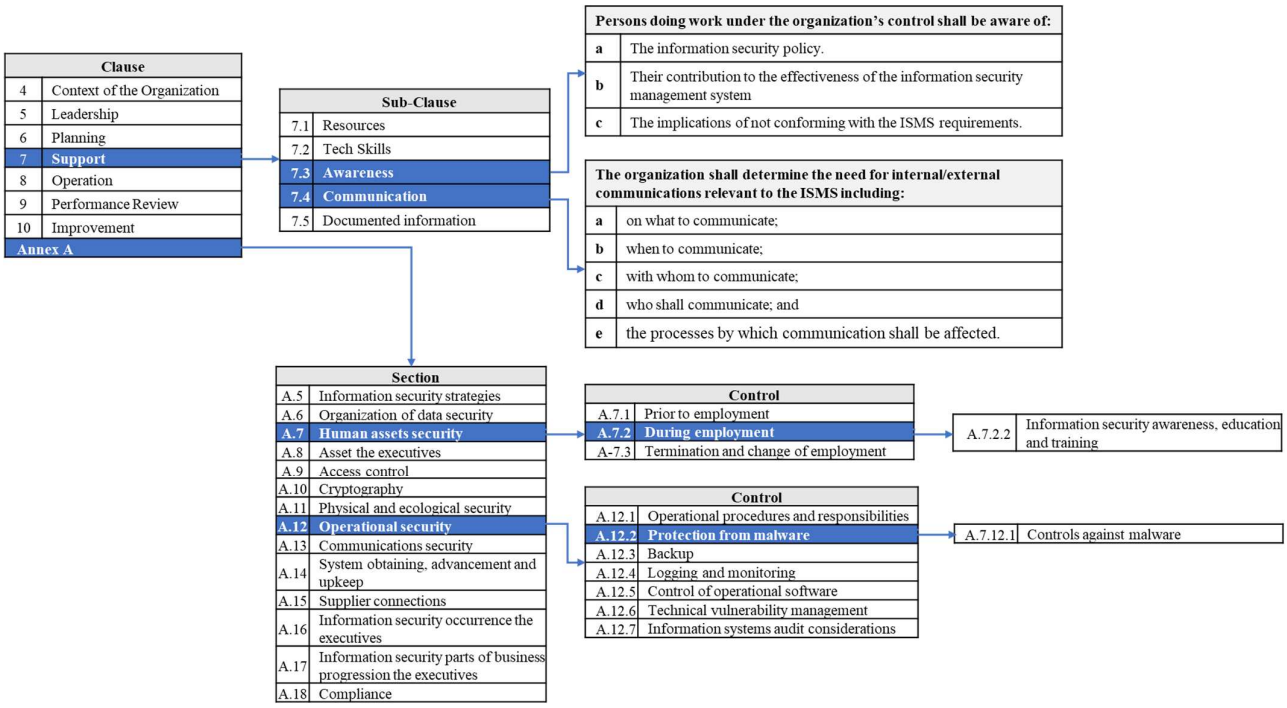

Figure 3. ISO/IEC 27001 structure and its contribution to an awareness and training program.

Another aspect indirectly related to the annexes and the specific controls of awareness and user training is subclause 7.4 (Communication), which is added to this analysis due to the importance of the transmission of information and the critical and confidential information assets. This subclause lists five fundamental aspects that must govern the flow of information (internal and external) in the organization [18].

Given the above, it can be said that the fundamental strengths of the ISO/EIC 27001 standard lie in the fact that it has international recognition, which makes it a valuable credential for organizations in global markets. Additionally, it offers a holistic approach to information security, addressing both the technical and cultural aspects of organizations. Another positive point is that, being a standard based on risk management, it allows organizations to prioritize security efforts based on their risk levels and unique requirements.

On the other hand, the level of complexity involved in the implementation of ISO/EIC 27001 can be high, and requires many resources, since it is not a specific regulation, because it lists the controls to be implemented but does not indicate how exactly they should be performed, as occurs in many regulations, standards, and frameworks. Being a broad regulation, like the NIST security framework, it is necessary to delve deeper into aspects specific to each industry, where it is necessary to address singularities that affect specific sectors.

2.9.3. ISO/IEC 27002

ISO/IEC 27002 is a complementary standard to ISO/IEC 27001, whose objective is to provide practical and detailed guidelines for implementing an ISMS and its associated security controls. The specific contribution of this standard to the topics of awareness and user training in cybersecurity is summarized in the recommendations provided in Section 7.2.2, which provides a general guide for security awareness, education, and training. It is established that the user awareness and training program should not only be applied to employees but should also be extended to contractors and suppliers. Said program must provide indications about the company's security policies, alignment with the guidelines established in the ISMS, and information management. Additionally, it is recommended

that the program be accompanied by other types of periodic and recurring activities that stimulate and promote good information security practices, thereby emphasizing their importance and benefits, for example, newsletters and publications of lessons learned [53].

This standard was updated in 2022. This version is composed of 4 categories and 94 controls, where category 6, entitled People Controls, in control 6.3 (Information Security Awareness Education and Training), provides the relevant and updated aspects of this subject [19].

Figure 4 represents the structure of ISO/IEC 27002:2022 and its contribution to the awareness and training of users in information security according to the interpretation of the information published in Information security, cybersecurity, and privacy protection—Information security controls [19].

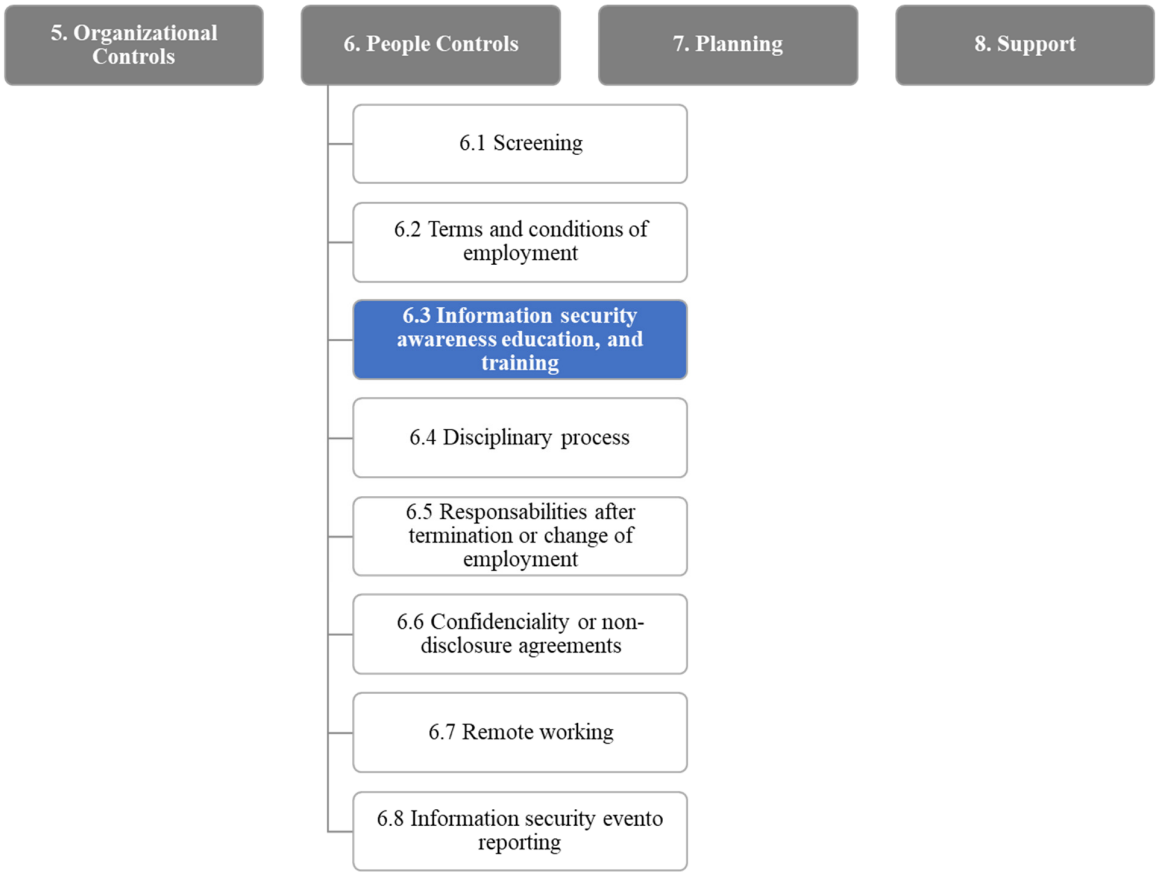

Figure 4. ISO/IEC 27002:2022 structure and its contribution to awareness and training programs.

In general, this standard allows organizations to tailor their security controls based on their unique risk profiles and requirements. However, there are enhancements to apply; these could focus on simplification, providing practical implementation guidance, and ensuring that the standard remains current and adaptable to emerging security challenges.

2.9.4. SANS Security Awareness Maturity Model

The SysAdmin, Audit, Networks, and Security (SANS) institution is a leading organization specializing in cybersecurity training and information security research. One of its notable activities is the development of cybersecurity training and awareness materials [54].

In 2011, SANS developed the SANS Security Awareness Maturity Model, which is still valid today with certain visual modifications. This guide establishes a model that helps organizations evaluate and improve the maturity of their security awareness programs. It provides a structured approach for organizations to assess their current state

of awareness, identify areas for improvement, and develop a roadmap to improve their awareness initiatives. The model proposes the following five stages of maturity: stage 1 (Non-existent), stage 2 (Focused on compliance), stage 3 (Promoting awareness and behavior change), stage 4 (Long-term sustainability and cultural change), and, finally, stage 5 (Metrics framework). Each stage of the model is well described and is complemented with proposed indicators to measure the program implementation and the level of the organization's cybersecurity culture. It also provides metrics, times, and next steps on the critical paths to increase the maturity of the institution [46,55].

The SANS Security Awareness Maturity Model is a useful tool for organizations looking to evaluate and improve their security awareness initiatives. Its strengths lie in its focus on security awareness, maturity levels, and practical guidance. However, it could be improved by considering a perspective that more specifically covers all aspects of the organization's cybersecurity posture, aligning the program more to the types of audiences that may coexist within the organizations, which would avoid leaving gaps in the overall security management. In addition, as [46,55] mention, it is important to understand what motivations inspire people to want to be responsible when it comes to information security; therefore, it is important to be able to complement these frameworks with change management models or other models that provide knowledge as to how people learn and are encouraged.

2.9.5. Center for Internet Security Controls Version 8 (CIS Controls v8)

The Center for Internet Security Controls (CIS), specifically Version 8, is a list of best practice guidelines for cybersecurity that provides a set of actions and measures designed to improve an organization's security posture. These controls are organized into three Implementation Groups (IGIGs) to serve organizations of different sizes and capabilities. IG1 is dedicated to small organizations, IG2 is dedicated to medium-sized organizations, and IG3 is dedicated to large organizations [56].

The controls grouped in IG1 aim at the implementation of basic and generic aspects of information security, generally covering the scope and objectives of small companies that do not have an established information security area, and that focus on maintaining operational continuity. The controls listed under the IG2 group are aimed at companies with at least one person responsible for the security area, which needs to align and comply with specific regulators in their field, with their main objective being regulatory compliance and maintaining an optimal level of security, as well as the company's reputation concerning information management. The third group of controls (IG3) applies to companies with consolidated information security areas that have information security experts and those related to them [20].

Specifically for the awareness training aspect, CIS has designated control 14, titled "Security Awareness and Skills Training", which is divided into nine Safeguards in total, with eight Safeguards grouped into GI1 (for small organizations) and nine in GI2 and GI3 (for medium and large organizations), as indicated in Figure 5, which is an extraction from the information published in CIS Critical Security Controls® Version 8 [57].

Although CIS control 14 emphasizes the importance of establishing and maintaining a security awareness program to influence people's behavior so that they are security aware and have the appropriate skills to reduce cybersecurity risks, the framework does not delve into this topic with much dedication. Therefore, one of the points of improvement could be to provide a more specific implementation guide for its controls so that it can deliver the tools that provide specifications according to the industry.

Control	Description
1	Inventory and Control of Enterprise Assets
2	Inventory and Control of Software Assets
3	Data Protection
4	Secure Configuration of Enterprise Assets and Software
5	Account Management
6	Access Control Management
7	Continuous Vulnerability Management
8	Audit Log Manageent
9	Email and Web Browser Protection
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	**Security Awareness and Skills Training**
15	Service Provider Management
16	Applications Software Security
17	Incident Response Management
18	Penetration Testing

Safeguard	Description	IG1	IG2	IG3
14.1	Establish and Maintain a Security Awareness Program	X	X	X
14.2	Train Workforce Members to Recognize Social Engineering Attacks	X	X	X
14.3	Train Workforce Members on Authentication Best Practices	X	X	X
14.4	Train Workforce on Data Handling Best Practices	X	X	X
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	X	X	X
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	X	X	X
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	X	X	X
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	X	X	X
14.9	Conduct Role-Specific Security Awareness and Skills Training		X	X

Figure 5. CIS Controls V8 structure and its contribution to awareness and training programs.

2.9.6. Control Objectives for Information and Related Technologies (COBIT)

COBIT is a framework developed by the ISACA (Information Systems Audit and Control Association) for enterprise IT governance and management. This framework provides a structured approach to align IT processes with an organization's business objectives. For this, COBIT defines a set of principles, processes, and controls to help organizations effectively manage and govern their information and related technologies. Typically, this framework is used for IT governance, risk management, and regulatory compliance. In 2019, the ISACA published the latest version, COBIT 2019 [58], which consists of six objectives related to the awareness and training of users in cybersecurity, which could be mapped with CIS Controls v8, as depicted in Table 5, which provides an excerpt from CIS Controls v8 mapped to ISACA COBIT 19 [58].

The main purpose of the BAI08 objective is to guarantee that the necessary management information is always available, updated, verified, and reliable, which is achieved with the constant training of users and periodic updating in all areas of the management program. Objective DSS05 is aimed at protecting information assets in such a way that the risk is maintained at an acceptable level and is in compliance with its security policies, thereby establishing information security roles and access privileges, which are complemented by user training so to recognize threats and possible attacks related to social engineering [58].

In the case of objective DSS06, the aim is to define and maintain controls for the secure flow of information in the processes that involve internal and external transactions of the organization so that these are carried out by following the established compliance with the principles of confidentiality, availability, and integrity of information. The information that is processed, received, or generated in each of the organization's processes can be achieved through the training of collaborators about the causes, consequences, and implications of the poor management of the company's information assets. The APO01 objective is to design an information technology management system that is aligned with business objectives and other design factors, which is achieved by aligning the information security awareness program with the company's security policies and values so that it adapts to the specific roles of each area depending on the functions that they perform [58].

Additionally, the CIS lists the objectives not mapped by its 18 controls, in which 2 objectives related to the awareness and training of users on cybersecurity issues are identified. The first is APO04, which, when applied to the program, establishes that it must be able to stay up to date with technological trends, identify opportunities for

innovation, and ensure that these contribute positively to the company's business and information technology objectives. The second unmapped objective is MEA02, which aims to continuously monitor and evaluate security controls, which also includes self-assessments and self-awareness, which allows for identifying points of improvement and weaker areas [58].

Although COBIT 2019 is a valuable framework for organizations seeking effective IT governance and risk management, one of the weaknesses of this framework is that it provides high-level principles and guidelines but may lack specific, prescriptive guidance, which could be a drawback for organizations seeking step-by-step instructions.

Table 5. CIS Controls v8 Information Security Awareness and Training Mappings to ISACA COBIT 19.

Safeguard	Description	COBIT 19-Objective #	Management Objective
14. 1	Establish and Maintain a Security Awareness Program	BAI08	Managed Knowledge
14. 2	Train Workforce Members to Recognize Social Engineering Attacks	DSS05	Managed Security Services
14. 5	Train Workforce Members on Causes of Unintentional Data Exposure	DSS06	Managed Business Process Controls
14. 9	Conduct Role-Specific Security Awareness and Skills Training	APO01	Managed IT Management Framework
Unmapped COBIT 19-Objective #			
-	-	APO04	Managed Innovation
-	-	MEA02	Managed System of Internal Control

2.9.7. Cybersecurity Awareness Framework for Academia (CAFA)

CAFA is a framework for the development of user training and awareness programs in information security, specifically for the field of higher education, which was developed by [59]. This framework is based on a gamified assessment strategy and is divided into four training modules, all of which must be designed and adjusted by the Cybersecurity Awareness Center (CAC) established at the institution. The framework is designed to facilitate modules to remain aligned with the latest cybersecurity trends in the market and the institution's policy and procedure adjustments.

Additionally, the CAC is tasked with completing test banks associated with training modules in the Learning Management System (LMS), where the modules must be included within the study programs offered by the institutions, thereby allowing the use of instances within the courses to deliver awareness-raising and training material to students, as well as reporting the assessment results and recommending actions. All of this information is loaded into the student information system (SIS), which connects to the information and communication technology support (ICTS) [59].

The ICTS is responsible for creating logistics for training modules in the LMS, providing technical support, and conducting surveys. It should be in constant communication with the CAC to provide feedback so to enhance processes and the module design, as well as receive the latest updates and changes in the structure and contents of the program, which depicts a clear continuous improvement process [59].

On the other hand, it is important to note that this framework does not cover the following aspects:

- The framework is mainly aimed at the integration of security modules with study programs, but it does not include other audiences that are also part of the organization;

not including them in the program is a risk for the organization. In the specific case of HE, students, administrative staff, professors, senior executives, third-party stakeholders, and physical and cybersecurity personnel clearly define how to classify content according to the type of audience, as the NIST's Framework for Improving Critical Infrastructure Cybersecurity recommends [50]. In addition, ISO/IEC 27001 and the CIS Critical Security Controls indicate that every member of the organization must be included in the awareness and training program during the period that they are part of the institution [18,20,50,53].

- The process to define and establish roles for the management of the program, as stated by NIST SP 800-16 and the CIS Critical Security Controls [17,20,50].
- Since this is a theoretical framework, this will be felt more in training being evaluated based on games, which represents an opportunity for improvement by combining it with periodic phishing campaigns that allow for the emulation of real attacks, and thus to complement the feedback for the design and program adjustment [18,20,50,53].
- Another opportunity for improvement comes from other complementary activities, such as sending periodic newsletters, where, in addition to delivering content related to the organization's cybersecurity culture, it is also constantly reporting on latent threats [16].
- Finally, the development of an Information Security Culture that constantly promotes and serves as a reminder on the topic of information security across the organization is encouraged through awards and recognition [51].

2.10. Technical Enhancements and Emerging Technologies

2.10.1. AI/ML for Adaptive Training and Threat Prediction

By facilitating continuous monitoring, predictive analytics, and enhanced threat identification, AI and ML are revolutionizing cybersecurity. Static rules and signature-based detection, which are inadequate against new and changing threats, are frequently used in traditional security systems. Large volumes of data can be analyzed by AI/ML algorithms to find trends, abnormalities, and indicators of compromise (IOCs) that might otherwise go overlooked. AI/ML models can anticipate future assaults and proactively reduce risks by learning from historical data [60,61]. The capacity of AI/ML to offer adaptive training is one of its main advantages in cybersecurity. By tailoring training programs according to user behavior and skill levels, AI algorithms can make sure that staff members are prepared to identify and handle common dangers, such as social engineering attempts and phishing assaults. Compared to conventional, one-size-fits-all training methods, our adaptive approach is more effective [60].

Through the analysis of system logs, network traffic, and other data sources, AI/ML systems can be trained to anticipate such attacks. Security teams may react swiftly and efficiently thanks to these predictive models' ability to recognize vulnerabilities, spot malicious activities, and rank security warnings [60,62]. However, concerns of algorithmic bias, data privacy, and the requirement for explainable security judgments are brought up by the incorporation of AI and machine learning into Zero-Trust frameworks [63]. In AI-driven healthcare systems, differential privacy is a crucial technique for maintaining patient confidentiality [64]. To protect privacy, methods like k-anonymity, multi-tier distributed ledgers, data encryption, and de-identification can also be used [65].

2.10.2. Blockchain for Data Integrity and Privacy Protection

A decentralized, unchangeable ledger provided by blockchain technology can be used to guarantee data integrity in cybersecurity systems. Blockchain guards against manipulation and unwanted changes by storing data in cryptographically connected blocks [66].

This is especially helpful in situations like healthcare, supply chain management, and financial transactions, where data integrity is crucial [66,67].

Blockchain can be utilized to improve cybersecurity systems' privacy protection. Sensitive information can be protected while enabling verification and validation using methods such secure multi-party computing, ring signatures, and zero-knowledge proofs [68–70]. Blockchain-enabled federated learning (FL) provides a machine learning technique that improves privacy, particularly in smart healthcare systems (SHSs) [71]. The integrity and security of healthcare data are guaranteed when FL, PETs, and blockchain are combined, underscoring their importance in creating a reliable SHSs that protect private patient data [71].

Implementing scalable federated learning (FL) systems has several issues, including privacy, integrity, and fairness. Combining blockchain technology, local differential privacy, and zero-knowledge proofs can result in FL systems that transparently and scalably balance secrecy, trust, and financial incentives [69]. PPBFL, a blockchain-based federated learning model with privacy protection, improves federated learning security and promotes nodes' active involvement in model training [68]. According to Hu et al. [72], multiblockchain architecture can improve the ecosystem with the main consortium chain and data side chain. These architectures save medical data in JSON format in side chain structures in the ecosystem's implementation methods. A point nomination system and dynamic RBAC access mechanism were used to improve the Practical Byzantine Fault-Tolerant (PBFT) consensus. They tested this method's record retrieval, consensus mechanism, and storage execution time in a multi-node blockchain context. This article shows that the proposed strategy improved the query time efficiency by 30% over a single-chain structure. Blockchain has several advantages for protecting privacy and data integrity, but it also has drawbacks in terms of the efficiency, scalability, and regulatory compliance. Careful planning, creative problem solving, and cooperation between industry stakeholders and regulatory agencies are necessary to overcome these obstacles [73].

2.10.3. Zero-Trust Architecture (ZTA)

The security concept known as Zero-Trust Architecture (ZTA) is founded on the tenet "never trust, always verify" [60]. ZTA mandates that all users, devices, and applications be authenticated and permitted before gaining access to resources, in contrast to conventional perimeter-based security models that presume network trust [14,74]. By removing implicit trust and shrinking the attack surface, this method makes it harder for hackers to access private information and systems [75]. Implementing a ZTA involves ensuring that only expressly authorized resources have least privilege access, providing robust identity verification and confirming device compliance before granting access [74]. A Zero-Trust approach must include data protection, device and network security, and identity and access management (IAM) [67]. A Zero-Trust framework can be implemented using the Software-Defined Perimeter (SDP), a secure overlay network technique [75].

New technologies like blockchain, AI/ML, and quantum computing are changing how Zero-Trust systems are implemented and how effective they are [63]. These technologies push the limits of conventional Zero-Trust models by enabling more advanced trust evaluation algorithms, improved threat intelligence, and dynamic access control mechanisms [63]. Blockchain technology is used to introduce confidence in the banking sector using a zero-confidence model-based framework that includes identity and access management (IAM), data protection, and device and network security [67]. A decentralized Zero-Trust framework built on the blockchain guarantees security and reliability in O-RAN (Open Radio Access Network) [76]. By using a Zero-Trust Architecture, government organizations may protect digital assets while enhancing public trust and service delivery [61].

3. Materials and Methods

The method used to investigate and subsequently build the Cybersecurity Awareness and Training Framework for Higher Education (CA&TF for HE) was a deductive approach, which is defined by [77] as a study based on an established theory. This method was deliberate and well-suited to the nature of this investigation for several specific reasons that align with the research goals of this work. First and foremost, this research aims to address a pressing problem in the HE industry (the need for a tailored Cybersecurity Awareness and Training Framework) that enhances security levels, particularly in the context of user behavior, and the implementation of best security practices.

This need is substantiated by a thorough analysis of statistical data presented in the Problem Background and Problem Statement sections of this document. These statistics reveal a growing trend of cybercriminal interest in the HE sectors and a noticeable increase in cybersecurity attacks within this industry. Therefore, this research aims to point to the analysis of the following three aspects, which are described in a general view below:

- Prove that there is a need for a tailored Cybersecurity Awareness and Training Framework that contributes to improving the security levels of HE institutions, specifically in aspects related to people's behavior and the implementation of best security practices, so to protect the information that these users handle during their time in the organization; this information is explained and developed in the Problem Statement section of this document.
- Analyze the best-known international information security frameworks and previous studies, as well as their contribution/recommendations in establishing user awareness and training programs, which are presented in the Literature Review section of this research work.
- Make use of the information collected to create a framework specifically adapted to the HE industry, with the flexibility that it can be adapted for organizations of different sizes and at different levels of maturity. This, in turn, will allow HE institutions to stay updated and remain in a process of continuous improvement in the construction of information security systems, supported by trained users capable of identifying threats related to social engineering and errors due to lack of knowledge or lack of education in this matter, which is explained in the next section of this document.

Additionally, according to the explanation provided by [77], it can be indicated that the purpose of the study is of the explanatory and reporting type, since it is based on the results from the search for a solution to an existing problem, and is demonstrated according to statistics and studies from previous research work. Given this, the explanatory purpose is fulfilled by comparing the different information security frameworks, the specific sections of each of them dedicated to user awareness and training, and, subsequently, in the construction of a CA&TF for HE, which is explained in detail as the progressive implementation of a process that becomes a cycle of continuous improvement. This is achieved with a research philosophy that combines the analysis of quantitative data from statistics and the numerical results of previous studies that support the Problem Statement. Moreover, it stems from the analysis of qualitative data resulting from the examination of generic baseline frameworks and previous studies on this subject.

Hence, the research strategy is based on archival analysis and a later comparative [77], where an investigation was carried out in statistical sources like Statista.com and the United States Census Bureau using keywords such as "Cybersecurity in higher education", "Cyber threats in universities", "Statistics of cyberattacks in higher education industry", "Information security trends in higher education institutions", "Cybersecurity awareness framework in academic institutions", "University Data Breach Statistics", "Security gaps in higher education", "Cybersecurity risks in universities", among others, as well as annual

reports prepared by institutions dedicated to researching market behavior and trends, technological areas, and other specific information security, such as Deloitte, Apricorn, BakerHostetler, IBM, SonicWall, Verizon, and Symantec.

This is followed by an analysis of frameworks like NIST SP 800-16, NIST SP 800-50, NIST SP 800-53, ISO/IEC 27001, ISO/IEC 27002, and ISACA COBIT 19, all of which are available on the official websites of the organizations that are in charge of their creation.

Moreover, we perform an analysis and comparison of previous studies obtained in information bases such as the University Canada West Library, Science Direct, Information, Research Gate, Harvard Business Review, and Elsevier, where the same keywords were applied to the research statistics, and other similar ones were also used.

4. Cybersecurity Awareness and Training Framework for Higher Education (CA&TF for HE)

The Cybersecurity Awareness and Training Framework for Higher Education Institutions (CA&TF for HEIs) is composed, in its most general level, of three blocks that are interconnected. Starting with block 1, which lays the foundations for a Cybersecurity Training and Awareness Program for Higher Education Institutions (CA&TP for HEIs). This block aims to create the team responsible for leading the program and the identification of the main stakeholders that connect the CA&TP for HEIs with the specific institution, adapting it to the strategic objectives of the organization, as recommended by [17].

Next is block 2, Cybersecurity Training and Awareness Program for Higher Education Institutions (CA&TP for HEIs), which aims to design, integrate, and implement the program; this section is a complement between [18,49,53,57,59]. Finally, block 3, Information Security Culture development, aims to establish user awareness and training through complementary activities that help to keep users on alert and to integrate a cybersecurity culture within the organizational culture, as suggested by [78], and which is complemented by an adaptation from [79], taking the benefits beyond the organizational boundaries, preparing future professionals to face the challenges related to information security in their future work environments, and transmitting their knowledge to other institutions and industries.

Figure 6 depicts the most general scheme of the Cybersecurity Awareness and Training Framework for Higher Education Institutions (CA&TF for HEIs), which is an interpretation and integration of previous works [16–19,55,58,59,79].

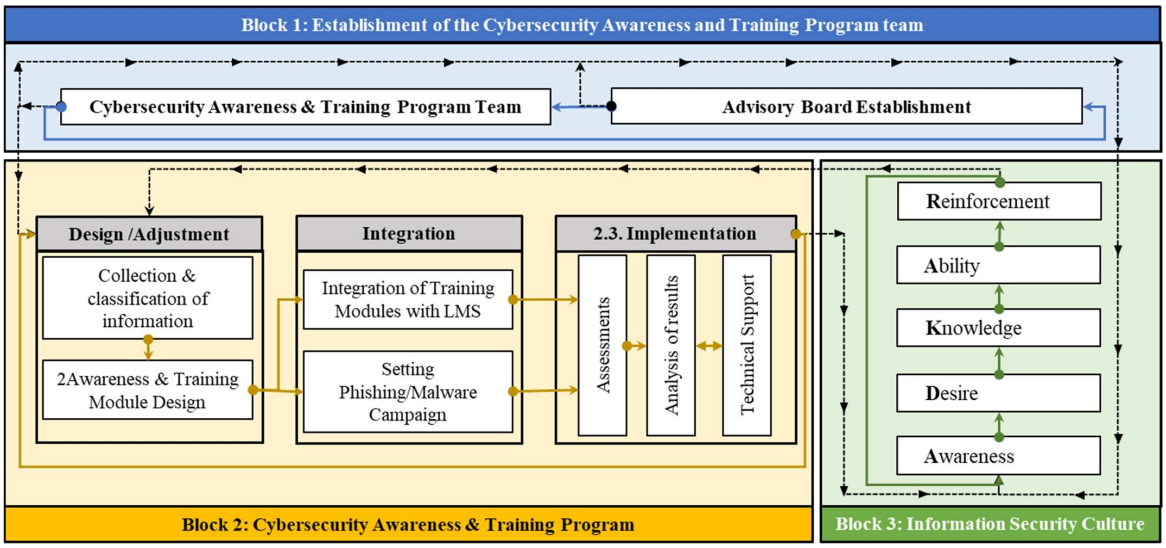

Figure 6. High-level scheme: Cybersecurity Awareness and Training Framework for Higher Education Institutions (CA&TF for HEIs).

4.1. Block 1: Establishment of the Cybersecurity Awareness and Training Program Team

This block is made up of two sections, the Creation of the Cybersecurity Awareness and Training Program team and the Advisory Board Establishment, as illustrated in Figure 7, through the interpretation of [16–19,55,58,59,79] (SANS, n.d.; Klein & Toth, 2014; Hash & Wilson, 2003).

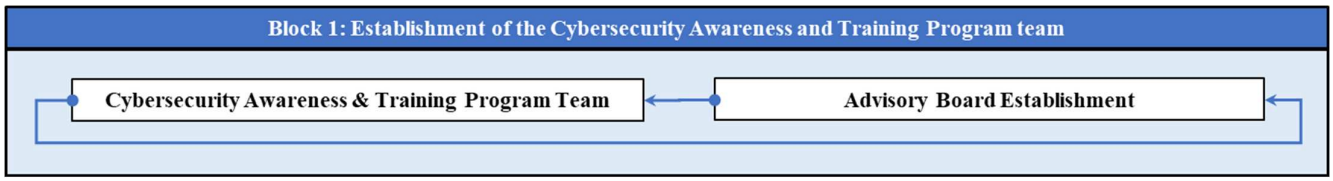

Figure 7. Block 1: Establishment of the Cybersecurity Awareness and Training Program team.

4.1.1. Cybersecurity Awareness and Training Program Team Establishment

According to [17,55], the institution must create an area or team dedicated to the continuous design/adjustment, implementation, management, measurement, control, and continuous improvement of the Cybersecurity Awareness and Training Program, which must report to the organization's security team. The area objectives aligned with the organizational culture, values, and security strategy therefore must be defined [55]

4.1.2. Cybersecurity Advisory Board Establishment

There needs to be a team from the information security area that leads the awareness and training program of the institution [17]. However, this must be complemented with a table of advisors that provides information from the other areas that structure the institution [55]. This will allow for a better audience approach and the adaptation of the program to each of their needs. Therefore, the Advisory Board must be made up of at least one member from each audience, including the faculties, administrative and complementary areas, student center, and government [55]. The responsibilities and contributions of the Advisory Board members are listed in Table 6, according to their own experience and the interpretation of previous works developed by [16,17,55].

Table 6. Advisory Board accountability and contribution.

Area Representatives	Accountability and Contribution
Information Security	• Provide security policies, processes, and procedures. • Establish/define best practices. • Define the information security strategy.
Cybersecurity Awareness and Training Center (CA&TC)	• Define the awareness and training strategy for each audience. • Lead the information security awareness and training program. • Contribute to researching trends in information security, threats, attacks, security risks, news, and other information of importance for the design/adjustment of program content. • Design/adjust and structure the Cybersecurity Awareness and Training Program. • Design/adjust the assessment process. • Apply the assessment process and analyze/report the results. • Development of a cybersecurity culture and awards.
Information and Communication Technology Support (ICTC)	• Provide technical support to users on the tools and platforms to use in the program. • Assist in the integration of the tools and platforms to be used in the program with the institution's operating and registration systems. • Technical support in the assessment of the audience groups.

Table 6. *Cont.*

Area Representatives	Accountability and Contribution
Faculty	• Support in the integration of the content of the cybersecurity program with the content of the different academic programs offered by the institution. • Support in the development of the applicability of information security and cybersecurity in the careers and courses offered by the institution.
Human Resources	• Inclusion of an Information Security Culture and cybersecurity in the organizational culture. • Support in the monitoring and control of the participation of members of organizational governance, employees, and contracts in the program. • Contribute to the design and management of activities related to the program.
Marketing and Communication	• Audience segmentation. • Program identity development and support material. • Support the program with marketing campaigns and internal communication related to the program. • Support in the planning and management of activities associated with the program.
Finance	• Make financial resources available. • Budget calculation/monitoring/control.
Student Center	• Promote the culture of cybersecurity among students. • Promote and participate in program activities.

4.2. Block 2: Cybersecurity Awareness and Training Program

This is the second block of the CA&TF for HE, which is created from an adaptation and interpretation of the CIS Critical Security Controls Version 8 [56], the Cybersecurity Awareness Framework for Academia [59], the SANS Security Awareness Maturity Model TM [55], the NIST Especial Publication 800-6 [17], and the NIST Special Publication 800-50 [16]. As illustrated in Figure 8, this block is divided into the following three sections: Design/Adjustment, Integration, and Implementation.

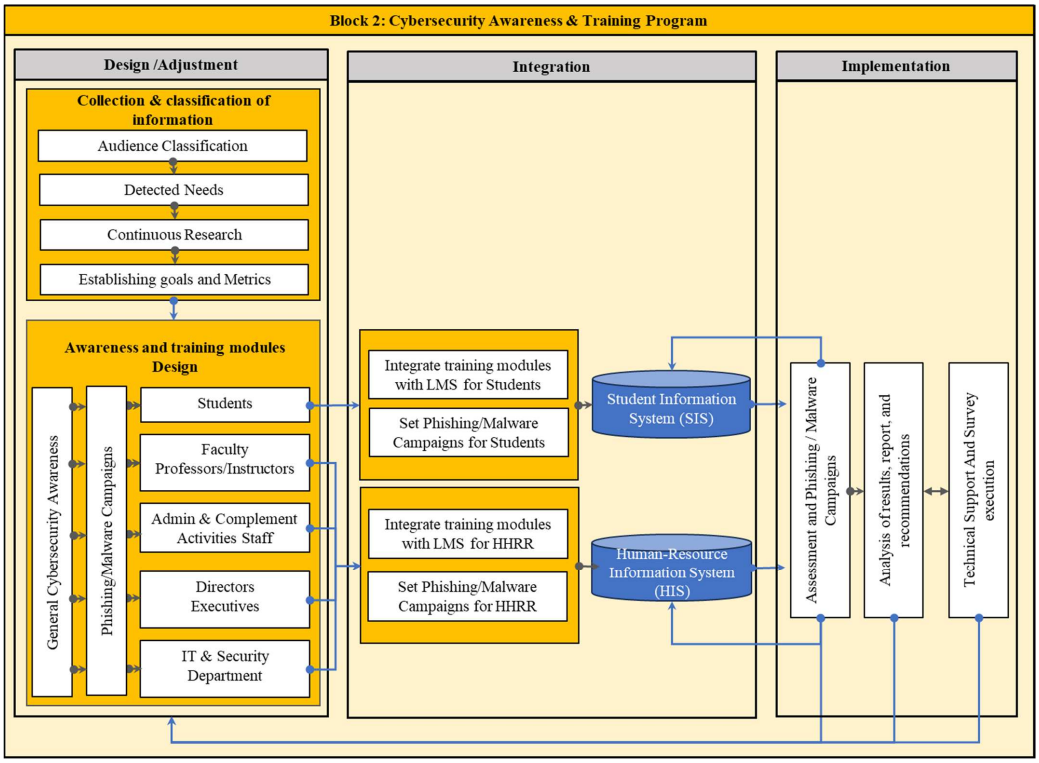

Figure 8. Block 2: Information Security Awareness and Training Program.

4.2.1. Design/Adjustment

In this section, two important processes are carried out for the creation and adjustments of the program. Firstly, there is the Collection and Classification of Information, and, secondly, based on the results obtained, it proceeds to the Awareness and Training Module Design.

Collection/Classification of Information. Integrated by the modules of Audience Classification, Detected Needs, Continuous Research, and Establishing Goals and Metrics.

Audience Group Classification. Identifying the specific groups to raise awareness and train; in the case of HE, within these groups, users, support groups, and those responsible for the Cybersecurity Awareness and Training Program will be identified.

According to the authors' experience, stakeholders' classification by [80], and the interpretation of requirements from the SANS Security Awareness Maturity Model TM [55], the NIST Especial Publication 800-6 [17], and the NIST Special Publication 800-50 [16], Figure 9 is developed, depicting a general audience group classification for HE institutions according the following:

- Students: the largest group/audience.
- Faculty: professors and instructors.
- Administration and Support Activities Staff: Finance, Human Resources, the Registry Office, Student Services, and Marketing, Legal, and Compliance.
- Directors and Executives: President or Chancellor, directors, deans, and executives.
- Information Technology (IT) and Security Department: This department oversees the technology infrastructure, including networks, computer labs, and academic technology support. They will define and implement security controls and ensure the security, integrity, and availability of information assets.

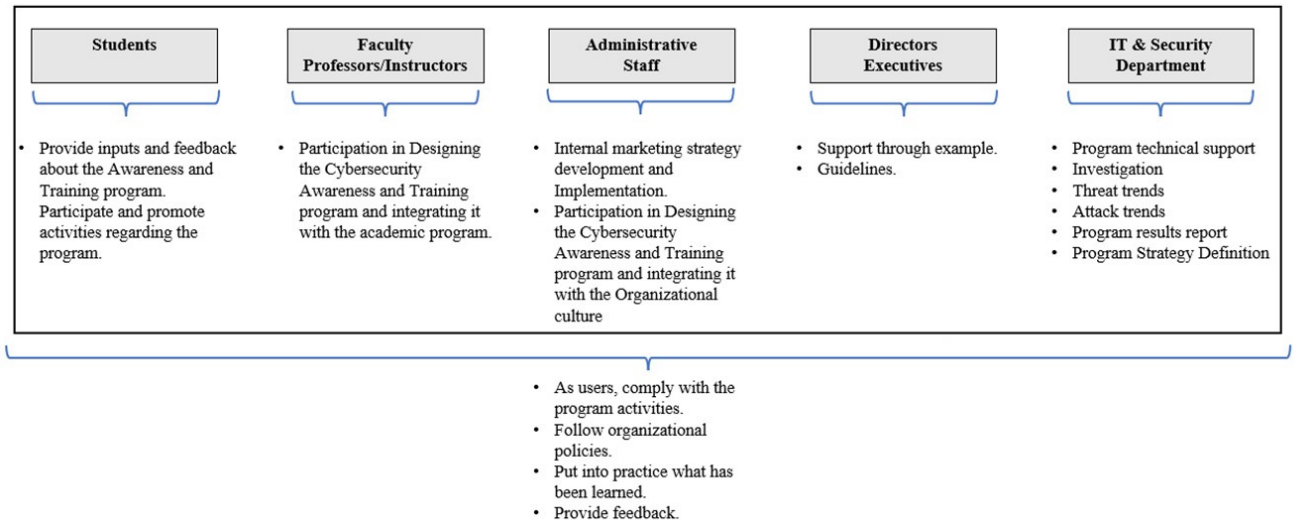

Figure 9. General classifications of audience groups in HE institutions.

Identification of the Needs of Each Audience Group. As identified in the previous section, within higher education institutions, there are five general groups of audiences with specific characteristics and roles that all share some similar needs, which will be the basis of the cross-organizational awareness plan. In addition, there are also characteristic needs associated with the specific risk levels of the role, which is why these areas require a special approach and training according to the criticality of the information that these people handle.

For example, a finance manager requires different training than a student due to the criticality of the information handled by the finance areas and the tasks inherent to their

role, the systems they manage, and the information to which they have access. Therefore, in this case, training sections related to the role, its privileges, and/or functions are defined. Figure 10 describes the initial structure of the design of the awareness and training program for HE institutions by the interpretation of the requirements and recommendations in the SANS Security Awareness Maturity Model TM [55], the NIST Especial Publication 800-6 [17], and the NIST Special Publication 800-50 [16].

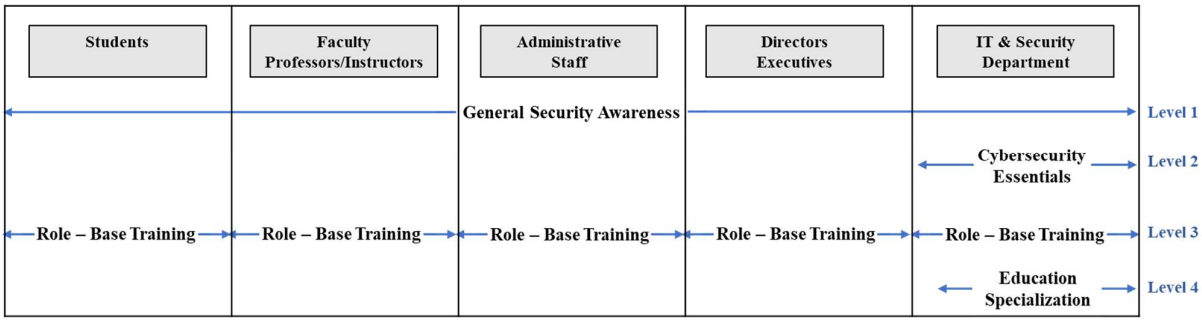

Figure 10. The general structure of the design of the CA&TP for HE institutions.

Continuous Researching. This is one of the key activities that feeds the program, and keeps it updated and in context with what is happening in the market, as well as the different trends, threats, vulnerabilities, and experiences of both the HE industry and others that share commonalities or use the same technologies/systems [16,55,59]. This activity must be under the responsibility of the Cybersecurity Awareness and Training Program team, and the line of research must be based on, but not limited to, information security and cybersecurity market trends, emerging threats and vulnerabilities, updates on defense, prevention, detection, and recovery techniques, related technological advances, attack vectors, regulator updates, states of the art from other industries, reporting of incidents in the industry and the lessons learned from case studies on the subject, and the statistics in this area.

The research, in combination with the results obtained from the application of the program and the feedback from the users, is what will shape the program, periodically adjusting it to current market conditions, the specific objectives of the organization, and its organizational and technological structure [59,78].

Establishing Goals and Metrics. Once the panorama of the institution is known, it is important to determine what the initial design objectives of the program will be for organizations that are starting or the adjustment objectives for those that already have the process established [55]. These objectives must be aligned with the strategic objectives of the organization and can be configured according to the example below [49].

Initiation Stage

IS-1. The design of the General Security Awareness Program, focused on compliance with regulations and attention to the critical points identified.

IS-2. Integration of the program with the entry processes of new members of each audience.

IS-3. Establishment of the periodic updating and review of the program according to obtained results and the inputs from the continuous research process.

Stage 2

S2-1. Deepen and reinforce the General Security Awareness Program to cover new trends, meet new needs, and cover other areas that had not been included in the previous stage.

S2-2. Initial design of the cybersecurity essential program according to the industry and the technology implemented in the institution. This section is dedicated only to the IT team and the Security Department.

S2-3. Integration of the cybersecurity essential program with the onboarding and orientation program for new members of the IT team and the Security Department. In addition, the list of skills and knowledge established in the program design may be used as a description of the positions and roles when publishing a vacancy or needing to expand the team.

S2-4. Initial design of the Role-Based Security Awareness and Training Program. For this stage, the roles to be addressed are defined according to priority and criticality established by the institution.

S2-5. Integration of the Role-Based Security Awareness and Training Program with the onboarding and orientation program for new members of the organization.

Stage 3

S3-1. Deepen and reinforce the General Security Awareness Program and the role-based training so to cover new trends, meet new needs, and cover other areas that had not been included in the previous stage.

S3-2. Update the essential security knowledge of the IT team and the Security Department.

S3-3. Initial design of the education specialization security awareness and training program for the Security Department. For this stage, the roles to be addressed are defined according to the criticality established by the institution.

Program Consolidation Stage

By this time, the organization already has an established process for the application of the Cybersecurity Awareness and Training Program. All of its areas must already be involved with the security strategy and the objectives of the organization. They must be attentive to improving the metrics and to the periodic adjustment of the program.

Cybersecurity Awareness and Training Modules Design. The model shown in Figure 10 provides four levels of awareness and cybersecurity training according to the needs of the identified audience. This section explains how to develop the set of modules of the specific program for each audience; for this purpose, the section is divided into the four levels of training and, at the same time, explains how to design the modules for each audience, as appropriate.

General Cybersecurity Awareness and Training Program. This must be the base content of the program, which must be taught to each member of all the audiences identified in the institution upon joining the organization.

This subprogram must be updated periodically, either by reinforcement during the period that the individual remains in the institution; each time there is a new need, a change in the market, or a change or upgrade in the institution's processes, technologies, or systems; when adding new programs; when there are structural changes; and/or when any other agent of change occurs. All of the individuals must complete this subprogram before they are assigned access to the organization's systems. For the following periodic training related to this subprogram, the Cybersecurity Awareness and Training Program team, in conjunction with the Cybersecurity Awareness Board, must determine if the members of the institution must repeat the entire subprogram, or a part of it, depending on the amount of information that is required to be updated and the time that has passed since the previous training [16–18,20,49,53,55–59,81]. They will also be able to define which of the audience groups should be enrolled in the subprogram.

According to the recommendation in NIST SP 800-50 [16], the construction of this program may include, but is not limited to, the following:

- General and transversal alignment with the Cybersecurity Awareness Strategy of the institution;
- Institutional cybersecurity policies alignment;
- Users' accountabilities;

- Good practices of information security;
- General IT security concerns and those related to the HE industry;
- Threat and vulnerability trends related to the users;
- Focused attention and recognition of threats and vulnerabilities;
- A process to report detected and possible threats, vulnerabilities, and incidents;
- Cybersecurity news;
- Implications for not accomplishing the institutional policies and cybersecurity best practices.

Role-Based Cybersecurity Awareness and Training Program. For the development of an awareness plan and training based on roles, it is not enough to only focus on the first classification level of audiences proposed by this document. Instead, it is recommended that there is a role-type identification within each of the audiences so to develop a granular program, which can be achieved as the program increases in maturity and as the institution goes through the cycle repeatedly, combined with a consideration of the feedback and needs of each audience.

Although NIST SP 800-16 [17] generally addresses the classification of roles in the technology and security area of the institution, it is important to consider the criticality of the information and the associated risk managed by other areas, and to not leave everything in the hands of the technical and security controls applied by the technology and security areas of the organization [46].

Therefore, it is highly recommended to make a more detailed classification of the roles that are in line with the criticality of the information assets that they manage. For example, in the Finance area, certain roles manage access information to bank accounts, access to systems where payment plan approval information can be modified, and the status of students' financial responsibilities.

Another example is related to the Registry Office or the area that manages the registration of grades and the current standing of students. These roles have a much greater associated risk than others in the organization; therefore, they will require specific training related to the security of the information and the systems that they manage.

Therefore, to design role-based training, we recommended aligning with the guidelines recommended by NIST SP 800-16, starting with identifying the needs to strengthen knowledge and threat identification skills specifically related to the systems and information handled by each role. In the case of the technology and security roles, these needs are more aligned with technical knowledge and technical skills, but they must also be focused on the type of technology and processes specific to each institution [17].

Once the specific needs of each role have been identified, the common needs of each role must be validated, and, based on this, the content of each module of the training program must be defined and created. It is recommended that an order of priorities be defined according to what is most critical initially, as established in the "Establishing Goals and Metrics" section of this framework [17].

Once the bank of modules is built, it is possible to choose which modules apply to each role; therefore, the following approach is recommended:

- Role-Based Cybersecurity Awareness and Training Program—Students. As recommended by [59], a basis for the design of this subprogram is the creation of educational modules that can be merged with the academic content taught in each year of study of the program (in the case of studies that are completed in at least one year). However, to adjust this model to any program taught by HE institutions, regardless of their completion time, it is established that all students should at least be enrolled in the General Security Awareness and Training Program and the first module of Role-Based

Awareness and Training for Students in such a way that this program may also include short academic programs.

Following the model proposed by [59], the module scheme consists of two components, a general one that includes content and gamification/interactive exercises related to the content of the General Security Awareness and Training Program, and a specific one that consists of complementary activities that serve as input or study material, such as readings, analyses, case studies, or those related to the more technical courses, which can be included in the different courses of the academic program.

The second component could be developed in conjunction with the faculty members in charge of developing the academic programs. Figure 11 shows a scheme for the proposed nomenclature for the Role-Based Cybersecurity Awareness and Training Module for Students through the interpretation and adaptation of previous works [59].

- Role-Based Cybersecurity Awareness and Training Program—Faculty Members: Faculty members fulfill a dual role within the program; in the same way, they are the audience, as they support the creation of the CATMS, which is why they require prior training on the topics defined in the continuous research phase, including recommendations from the report of results of previous cycles of evaluation and feedback obtained from the student audience. This is to provide them with a better definition of the material with cybersecurity information, which will complement and adjust the academic content and the CATMS according to the needs of each course. Therefore, following what was suggested by [59], faculty members will receive an induction consisting of a workshop that contains all of the information prepared in the Continuous Research section whenever it is necessary to modify or adjust the program for the student's audience.

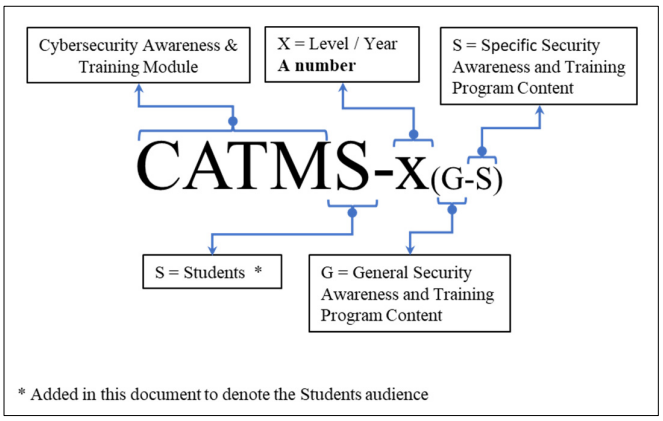

Figure 11. Role-Based Cybersecurity Awareness and Training Program: Students Module nomenclature.

Consequently, the faculty member's modules will be adjusted so that they are compatible with the CATMS. Figure 12 shows a scheme of the proposed nomenclature for the Role-Based Cybersecurity Awareness and Training Module for Faculty Members through the interpretation and adaptation of previous works [59], where F represents the faculty members' audience, X is the year or level of the module, G represents the specific general information module based on gamification/interactive exercises for faculty members, and S refers to the specific content in activities and support material to align with the academic program of the course.

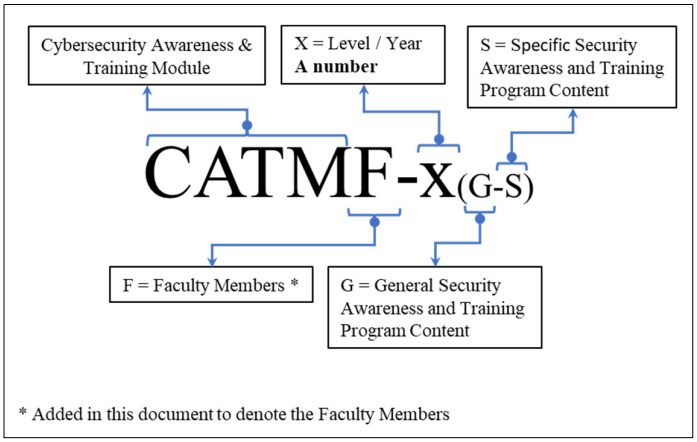

Figure 12. Role-Based Cybersecurity Awareness and Training Program: Faculty Members Module nomenclature.

- Role-Based Cybersecurity Awareness and Training Program—Administrative and Complementary Activities Staff. As for the two previous audiences, for the Administrative and Complementary Activities Staff, the creation of modules based on gamification/interactive exercises, specifically adjusted to the type of information, systems managed, and possible attack vectors related to this type of roles within of the institution, is recommended [17].

Figure 13 shows a scheme of the proposed nomenclature for the Role-Based Cybersecurity Awareness and Training Module for Administrative and Complementary Activities Staff through the interpretation and adaptation of previous works [59], where A refers to the audience in question and vx corresponds to the version of the module, which must be adjusted or updated depending on the corresponding updates with the continuous research activities, the results obtained from previous program cycles, audience feedback, or any change produced within the organization [16–18,53,55,57–59].

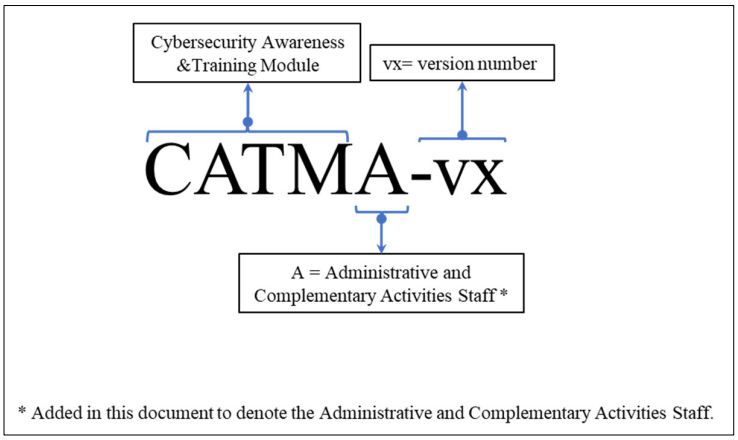

Figure 13. Role-Based Cybersecurity Awareness and Training Program: Administrative and Complementary Activities Staff Module nomenclature.

- Role-Based Cybersecurity Awareness and Training Program—Directors and Executives Members. The description of this subprogram is very similar to the previous one, only adapted to the specific needs of this audience. Figure 14 shows a scheme for the proposed nomenclature for the Role-Based Cybersecurity Awareness and Training Module for Directors and Executive Members through the interpretation and adaptation of previous works by [59], where D refers to the audience in question and vx corresponds to the version of the module.

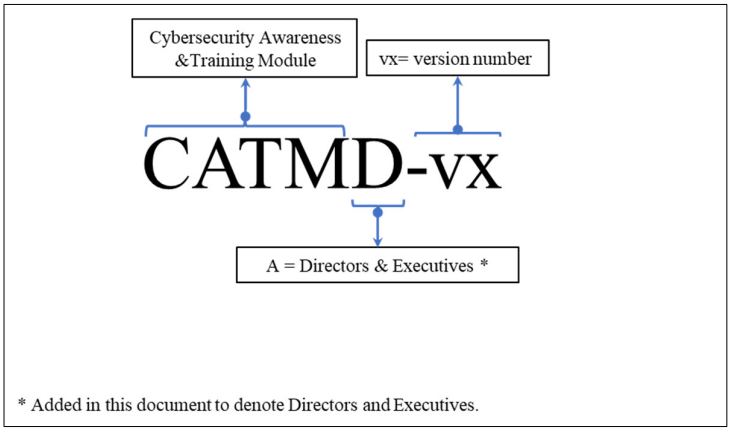

Figure 14. Role-Based Cybersecurity Awareness and Training Program: Directors and Executives Members Module nomenclature.

- Role-Based Cybersecurity Awareness and Training Program—IT and Security Departments. The content of the program for this audience points more to specific technical knowledge of the subject, adapted to the roles that make up the area, the technology on which the organization's infrastructure is based, and its internal processes. Figure 15 shows a scheme of the proposed nomenclature for the Role-Based Cybersecurity Awareness and Training Module for IT and Security Departments through the interpretation and adaptation of previous work by [59], and the requirements from NIST Especial Publication 800-16 [17] and NIST Special Publication 800-50 [16].
- Cybersecurity Essentials Program. This section is most related to roles in the Tech and Security team, and aligned with NIST SP 800-16 [17]. It recommends continuously updating the specialists and technical team in the fundamental base of knowledge aligned to the processes, infrastructure, and technology implemented in the organization. Therefore, it is recommended that the topics that the training of this audience can at least cover aspects such as basic concepts related to information security, cybersecurity, intrusion, social engineering, and challenges associated with the HE industry; common vulnerabilities and threats related to the type of system implemented in HE institutions, for example, eLearning systems; the most common attack vectors and those related to the HE industry; the weaknesses found in successful attacks; cryptography; perimeter defense infrastructure, incident prevention, security status monitoring, event log, attack prevention, and security controls; and the construction and development of information security and cybersecurity.
- Education/Specialization Cybersecurity Program. In favor of the continuous development and specialization of the relevant roles that require it, it is highly recommended that the organization develop a specialized education program for those professionals who must occupy positions with highly critical functions and which serve as experts in the subjects, thereby allowing them to keep the knowledge base updated and aligned with the latest technologies, trends, certifications, and high-level education. This will direct the formation of a robust technical team capable of delivering the most accurate recommendations and with the level of depth required for decision-making support, both at the high levels of governance and the direction of the organization, as well as in more specific aspects [17].

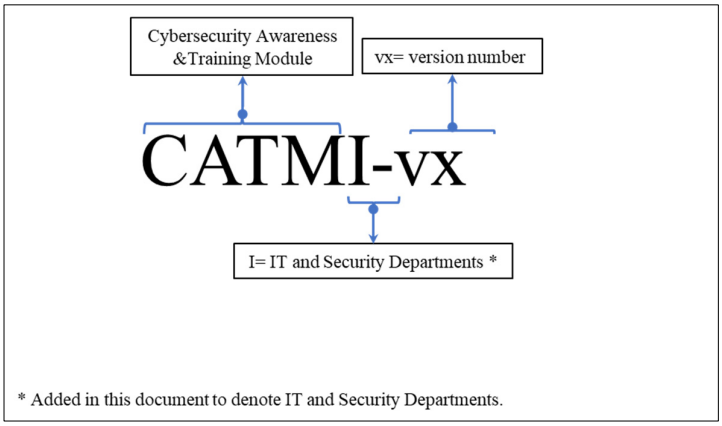

Figure 15. Role-Based Cybersecurity Awareness and Training Program: IT and Security Departments Module nomenclature.

Phishing/Malware Campaigns. In addition to the delivery of content related to this program, audiences must be tested, not only on their theoretical knowledge and the identification of attack scenarios exposed in games, videos, or any other interactive material where the user is aware that it is being evaluated, but periodic phishing/malware campaigns must also be included that emulate real attacks on the audience's everyday use systems so to detect the real level of education, awareness, and training of the members of the institution, and that, in turn, this evaluation is as close to reality as possible [16,18,20,53]. To this end, the following points are proposed:

- Prepare periodic phishing campaigns where the contents of the theoretical modules can be evaluated in a real environment.
- Design campaigns that allow for the determination of the level of education of the users and that, in turn, is related to the risk levels of the organization according to the type of information and access to the system managed by each audience and each role. For example, a phishing campaign based on sending a trap email that contains a link, a downloadable file, and a request for data delivery. Each action can be associated with the level of risk it represents, allowing for adjustments to be prioritized in the design of the content based on risk mitigation.
- Design campaigns adjusted to real scenarios where each audience develops, to the season of the year, and to the specific events of the moment so to make them more realistic. For example, an email promoting the purchase of a book associated with a specific program at the beginning of an academic cycle.

4.2.2. Integration

Once all of the program modules have been designed, they must be integrated into the learning system used by each audience so that they are available when configuring the subprograms [59]. This phase consists of three sections. The first section is to Integrate Cybersecurity Awareness and Training Modules on the Learning Management Systems (LMSs), the second section is to Set Phishing/Malware Campaigns, and the third section is Integration with Students' Information Systems (SISs) and the Human Resource Information System (HIS).

- Integrate Cybersecurity Awareness and Training Modules on the LMS. For this specific case, the CATMS is integrated into the LMS that the institution uses to deliver the academic content of each course [59]. In the case of the rest of the audience, if the company has a training platform for its employees, the module groups CATMF, CATMA, CATMD, and CATMT can be integrated into this tool. Another option to make the content of the modules available can be on an Intranet. Other institutions may choose to

purchase an eLearning platform license that allows them to adapt/customize/update the content to the context of each audience.

- Set Phishing/Malware Campaigns. Once the phishing campaigns are designed, they must be integrated and programmed to run on the systems used by the audiences, for example, email and directory service-developed whitelists within the company's systems, so to prevent these campaigns from being blocked by the security infrastructure of the institution [82]. This activity is based on the configuration/activation of the program modules for each of the audiences according to the needs detected and the modules assigned, thus giving the level of awareness and training for each individual [16,17,55,56,58].
- It is important to note that the execution of phishing campaigns must be carried out in a controlled manner and by the support areas that will be involved in the activity [82]. For example, the institution may have a process for reporting attacks or threats detected by end-users, and already educated and trained users are expected to report the threat; if, in this case, the support or management team of this type of report is not aware of the exercise, the entire process is activated, and resources will be used unnecessarily.
- Integration with Information Systems. The organization's information systems will integrate the information available from the Cybersecurity Awareness and Training Program with the information and management of processes within the organization, thereby allowing the registration of available material, the results obtained, and the feedback resulting from the activities carried out in this process [59].

4.2.3. Implementation/Execution

This section summarizes the implementation of the program, including the following activities:

Assessment and Phishing/Malware Campaigns. Once all of the program modules have been loaded and programmed according to each audience, people will be able to take their courses as scheduled. In the case of the execution of phishing/malware campaigns, these can be carried out and grouped according to the audience, the area of the institution, and new income. The Cybersecurity Awareness and Training Program team must coordinate activities with the areas that may be involved with the exercise, such as the technical support area and human resources management, so to execute a controlled exercise [82].

Analysis of Results, Reports, and Recommendations. The results must be analyzed from various points of view to collect information regarding

- Specific individuals. For example, those individuals who occupy critical positions and manage the relevant information of the organization, as well as individuals who remain at a low level of awareness and training, and who possibly require greater attention and focus to advance through the levels of the program [82].
- Groups, such as audiences, areas of the organization, and other relevant specific analyses according to the needs of the institution [16,17,55].
- The organization in general, which will give a general look at the level of awareness and the training of the institution [55,82].

All of these data will provide information that will guide the adjustment of the program and strategy, as well as the decision making in general. In addition to the application of the program modules and phishing/malware campaigns, user satisfaction surveys must be applied, where users can additionally provide their feedback regarding the program, which will also serve as input for future process adjustments.

All of the information must be gathered in a report with data analytics, which, in turn, is contrasted with the results of previous cycles and the initially agreed strategy objectives

so to measure the fulfillment of goals and the progress of the strategy, thereby generating recommendations from the group of security experts. This report must be reviewed by the information security team and the Cybersecurity Advisory Board, thereby completing a cycle and generating inputs for the next cycle of the program.

Technical Support and Survey Execution. As proposed by [59], the technical support team supports tasks related to

- The integration of the modules with the LMS, SIS, and SIHR.
- Monitoring of the correct functioning of the program modules.
- Attention to issues reported with the operation of the systems.
- In addition, it can also serve as the first instance in receiving reports of incidents and threats detected by users so to make a first filter or to discard false positives, for example, those reports made during a phishing/malware campaign, or errors in linking harmless emails with threats detected by a user.
- Additionally, the support team must record metrics related to the reports made by users and the generation of surveys related to the technical functioning of the program. These last two points serve as relevant inputs that must be included in the results report of the cycle in execution.

4.3. Block 3: Information Security Culture Program for Higher Education (ISCP for HEIs)

As recommended by [78], it is important to accompany the CA&TP for HEIs (block 2 of the CA&TF for HEIs) with a cybersecurity culture establishment program based on complementary activities that constantly reinforce the knowledge taught in block 2 of the framework, making the program become part of the organizational culture of the institution.

In this case, the ADKAR change management model is proposed and adapted to introduce/integrate the Information Security Culture into/with the organizational culture of the institution; as explained by [79], the meaning of the ADKAR framework is an acronym that follows the initials of the words Awareness, Desire, Knowledge, Ability, and Reinforcement. These words are associated with the five stages of the implementation and change management cycle. The method focuses on reinforcing the preparation of the members of an organization and, at the same time, providing them with the necessary support during the change process. Figure 16 depicts the adaptation of the ADKAR model to the ISCP for HEIs through the adaptation and interpretation of previous works on this subject [78,79], as well as the SANS Security Awareness Maturity Model TM [55].

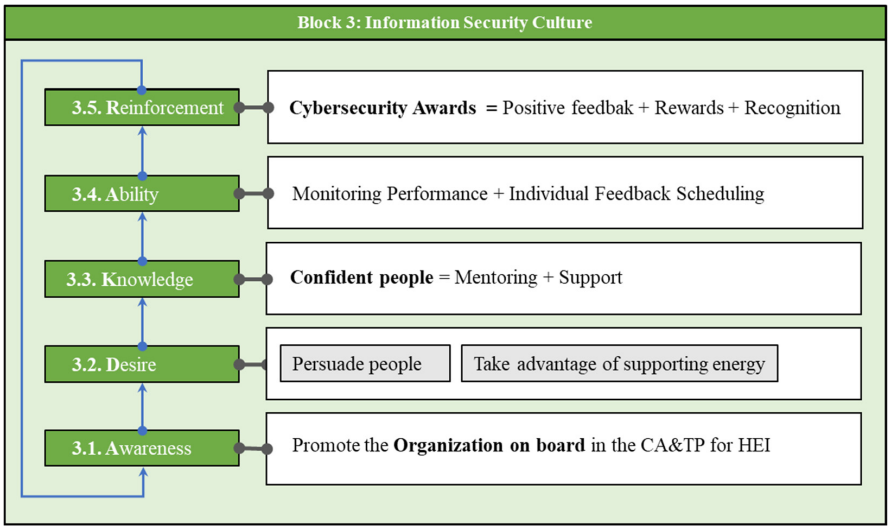

Figure 16. Block 3: Information Security Culture Program for higher education (ISCP for HEIs).

It is important to note that the following roles and departments are relevant to the design, execution, and control of this program, as is explained in Table 7.

Table 7. Department contribution to the success of the Information Security Culture Program for higher education (ISCP for HEIs).

Department/Area	Specific Role	Contribution
Marketing and Communications	Creates awareness and promotes the Information Security Culture Program.	• Creation of Visual and Audio Material, including posters, videos, and infographics, to raise awareness about the program. • Campaign Planning and Execution to promote the culture of information security. • Branding and Messaging aligned with the institution's values.
Cybersecurity Awareness and Training Program Team	Manages the cybersecurity awareness and training aspects of the program, ensuring that it aligns with the ADKAR model stages.	• Content Development and continuous research to create training materials, workshops, and courses that cater to the stages of the ADKAR model. • Booking and Scheduling of training sessions and coordinating with different departments to ensure that the training is well-integrated into the program. • Progress Tracking the progress of participants at each stage of the ADKAR model and to provide support when necessary.
Directors, Executives, and Leaders	Drives the Information Security Culture within the institution.	• Promotion and Alignment of the Information Security Culture by setting an example through behavior and actions. • Resource Allocation, including budgets and personnel, to support the implementation of the ISCP for HEIs. • Policy Advocacy for and enforcement of information security policies and practices within the institution, thus demonstrating commitment to the program.
Student, Faculty, and Complementary Activities Leaders	Leaders within the academic and administrative departments serve as champions for information security and act as role models.	• Championing Information Security by actively supporting and promoting information security within their respective areas of influence, thereby encouraging others to follow suit. • Training Facilitation, where the leaders can facilitate training sessions, workshops, or discussions within their departments to reinforce the knowledge and skills related to information security. • Feedback and Improvement so to provide valuable feedback on the effectiveness of the program, thereby helping to identify areas for improvement and adjustment.

4.3.1. Awareness

In addition to the CA&TP for HEIs, this framework also proposes an awareness section aimed at the execution of activities that promote the need to adopt information security processes and good practices, and their importance, thereby reinforcing the knowledge and training acquired during their stay at the institution. Some of these cybersecurity awareness activities are based on suggestions from [16,55,78,79]. This could be

- Sending periodic newsletters with information relevant to audiences and updated according to data linked to the industry.
- Information pill videos that are sent periodically through emails or work groups, for example, weekly 3-min videos.
- Posting on the institution's communication channels.
- Workshops that educate people about information security in general (applied in the personal sphere).
- ISCPs for HEI mascot election.
- The celebration of Cybersecurity Day/Week.
- A cybersecurity-themed brunch.
- Posters in places with a greater influx of people, among others.

4.3.2. Desire

The second step established by the ADKAR model is to promote the desire for change. In this case, to develop the desire or willingness to support and participate in the inclusion of information security as part of the organizational culture of the institution. At this point, people need to see the benefits of the change being promoted [79].

For them, this module integrates activities such as Persuading People and Taking advantage of Supporting Energy, which are explained below.

Persuading People. Maintain the activities of the awareness campaigns and emphasize the need to implement the Information Security Culture within the institution. Encourage people to take ownership of cybersecurity within their respective roles. Tailor campaign messages and approaches to address the specific needs and concerns of different groups within the institution, as different stakeholders may have different levels of awareness and motivation [79].

Taking Advantage of Supporting Energy. Identify the individuals in favor of the change, those who are most interested, those with a desire for collaboration, and team leaders who can serve as spokespersons in favor of the Information Security Culture within the institution, and involve them in a more close and participatory way in information security activities and campaigns. Some of the key activities that [78] recommend in their research are establishing a brand that distinguishes the institution's cybersecurity team and creating a team of promotional leaders (champions) of information security.

4.3.3. Knowledge

The knowledge stage of this change management model goes hand-in-hand with the CA&TP, empowering and preparing people to advance in the integration of information security with the culture of the institution. For this point, it is possible to establish periodic activities related to information security, such as a ritual or tradition of the organization [79].

4.3.4. Ability

At this point, the institution already has more prepared individuals, with knowledge and skills that allow them to identify threats and implement the notification processes, actively contributing to compliance with established security policies, and being attentive to making use of the best security practices [79]. Therefore, this point is linked to the process of the assessment, monitoring, and analysis of results of the implementation of the CA&TP and phishing/malware campaigns.

4.3.5. Reinforcement

Following the recommendation outlined by [16,55,78,79], at this stage, it is important to highlight the positive results. One of the alternatives is through awards or recognition to individuals and/or outstanding areas in meeting the objectives of the information security strategy to those outstanding leaders who fulfilled the role of a change agent, and to others

who have been relevant to the organization or who have complied outstandingly with the program. An example of this could be the closing of Cybersecurity Week with an awards ceremony. For the establishment of reinforcement practices, some criteria for awards are recommended below.

Criteria for Awards

- Performance Metrics. Awards will be based on specific performance metrics aligned with the objectives of the information security strategy. These metrics may include adherence to security protocols, participation in training, incident response efficiency, or other relevant key performance indicators established by the Cybersecurity Awareness and Training Program team leaders and the Advisory Board.
- Impact on Culture. Nominees will be evaluated not only on their adherence to security practices but also on their contributions to fostering a culture of information security. This can encompass efforts to promote awareness, mentorship, or innovative solutions.
- Leadership as Change Agents. A key criterion for awards will be the extent to which individuals have acted as effective change agents, driving positive behavioral changes in their departments or teams.
- Nominations. Nominations for awards can come from peers, supervisors, or self-nominations, highlighting a democratic and inclusive approach to recognizing achievements.

Selection Process

- An Award Committee: A dedicated Award Committee will be established, consisting of representatives from various organizational levels, including senior management, information security professionals, and key stakeholders. The committee will ensure a fair and unbiased selection process. This activity could also be carried out by the Advisory Board.
- Evaluation and Scoring: The Award Committee will evaluate nominations based on the established criteria and score each nominee. This evaluation will be data-driven, with a focus on quantifiable achievements.
- Transparent Process: The selection process will be transparent and communicated to all stakeholders. The award categories and criteria will be publicly available.
- Award Ceremony: A culminating event, such as the closing ceremony of Cybersecurity Week, will serve as the platform for announcing and celebrating the award recipients. This ceremony will be an opportunity to share best practices and inspire others to excel in the realm of information security.

Award Categories

To ensure comprehensive recognition, various award categories will be established, including awards for individual excellence, outstanding teams or departments, and special categories for contributions to the ISCP for HEIs. Specific award titles and categories will be determined in consultation with the Award Committee or the Advisory Board.

5. Discussion

Analyzing the implementation of the Cybersecurity Awareness and Training Framework for Higher Education (CA&TF for HE) at a general level, it is of utmost importance to first establish block 1 (Establishment of the Cybersecurity Awareness and Training Program team), since the definitions of the objectives, responsible parties, and metrics that are the basis of the program start from this. After establishing the first block, the institution can choose between dedicating itself exclusively to establishing block 2 (Cybersecurity Awareness and Training Program) or working on block 2 and block 3 (Information Secu-

rity Culture); this will depend on the resources it has at its disposal (time, budget, and professionals/responsible).

The adaptation of the CA&TF for HE framework may vary significantly based on the institution's size, structure, and funding model. For instance, larger or public universities may have more resources and dedicated IT departments, allowing for the parallel development of blocks 2 and 3. Conversely, smaller or private institutions with limited budgets may benefit from a phased or modular implementation, prioritizing essential awareness modules before tackling culture change initiatives. This flexibility is key to ensuring the framework's practical adoption in diverse educational environments.

5.1. Establishment of the Cybersecurity Awareness and Training Program Team and Cybersecurity Advisory Board

The fundamental basis and beginning of the creation of the CA&TF for HE is the definition of the teams of professionals who will oversee the direction of the program, but also identify who will occupy the roles in charge of the different departments or areas of the institution that will serve as feedback providers and internal communicators, in this case, the Cybersecurity Advisory Board. This team's role is of vital importance, as they are responsible for the design, implementation, management, measurement, control, and continuous improvement of the cybersecurity awareness and training program. Additionally, the team should be aligned with the organization's security team and should define objectives that are in harmony with the institution's culture, values, and overarching security strategy.

5.1.1. Creation of the Cybersecurity Awareness and Training Program Team

It is highly recommended that this team be made up of personnel who are related to or in charge of the institution's information systems in case it does not have a defined information security area [55].

These professionals will play a pivotal role in shaping the awareness and training program, ensuring that it is well-suited to the institution's unique needs and objectives. The design and adjustment of the program start with the construction of this team, since they are responsible for the execution of key activities, such as the integration of the internal information of the organization (results, feedback, insight, strategies in general, and organizational objectives) with external information related to market trends, threats, and attacks carried out in other institutions in the same and different areas, which constantly shapes the program and the processes linked to it.

On the other hand, it is also of great relevance to mention that the results obtained from the application of the program may also affect other areas of the organization, its processes, and its security control environment. By analyzing the results, in addition to modeling the awareness program and user training on security issues, improvements can be suggested in other areas, for example, the implementation of technologies that support information security. Therefore, this team must be able to prepare reports with different levels of language so to clearly transmit the information to other departments whose core is technology or information security.

The effectiveness of this team is highly dependent on the active support of top management. Their commitment ensures the allocation of necessary resources, legitimizes the program across departments, and fosters a security-centric culture. Strategic endorsement by leadership also signals the institutional importance of cybersecurity initiatives, which can significantly enhance participation and compliance.

5.1.2. Cybersecurity Advisory Board Establishment

Members of the Cybersecurity Advisory Board may be delegates of each of the areas. These people do not need to be specialists in information security, but they must be aware of the strategic objectives of the institution, its processes, the interconnection between the different areas, and information flow process, the systems they manage, and the interaction with suppliers and/or external to the organization that are indirectly linked to it. The main function of the board is to provide information for the design and modification of the CA&TF for HE.

Once the Cybersecurity Awareness and Training Program team and Advisory Board are established, meetings or workshops must be held to share points of view and extract relevant information about the institution, which will serve as a basis for subsequent phases of the program. This information may include, but is not limited to, the following list:

- Strategic objectives of the institution.
- Institutional culture.
- Operation and integration of processes, systems, and people.
- Learned lessons.

5.2. Cybersecurity Awareness and Training Program

This is the most complex and extensive block of the CA&TF for HE. Due to this complexity, it is recommended that the Cybersecurity Awareness and Training Program team and Cybersecurity Advisory Board analyze and establish the objectives and scope of the design and implementation of the program; this will also depend on the resources and time available to the institution and its strategic objectives.

5.2.1. Design/Adjustment

The recommended steps for program design are as follows:

- Based on the information obtained from the organizational analysis meetings between the Cybersecurity Awareness and Training Program team and the Advisory Board, the organization must be segmented into audiences according to the groups that make it up (students, faculty/professors, administrative staff, directors/executives, the IT and Security Department, and others that cannot be classified in the previous groups).
- Identify the awareness and training needs of each audience according to their role, and the information and systems that they manage.
- Establish a continuous research process that can be based on, but which is not limited to, the investigation of HE industry trends, tech trends, incidents, vulnerabilities trends, and case studies of cyberattacks in other institutions in the same and different areas. This activity can be performed in parallel with the beginning of the organization's analysis, so that people's knowledge needs also influence the research strategy and objectives.
- Based on the above, the Cybersecurity Awareness and Training Program team and the Advisory Board must establish metrics and indicators to monitor compliance with the strategy. An awareness and training schedule must also be established.
- At this point, it is important to have defined the scope of the program and whether the design of the awareness and training modules will be developed partially or completely.

Some institutions prefer to start the first cycle by developing the General Cybersecurity Awareness module, which is transversal to the institution and lays the foundations of the program. This can be accompanied by phishing/malware campaigns. Subsequently, institutions may progressively include the following modules of the program according to their criticality and risk management. This will depend on the strategic objectives of each institution.

5.2.2. Integration

It is of great relevance to develop a roadmap for the integration of the designed modules with the organization's systems. This work will be led by the Cybersecurity Awareness and Training Program team, but the technology areas will be involved to make said integration possible, which is why it is important that this plan is communicated to the areas involved and that it can also be executed without affecting the operation of the institution. This is one of the points that have been formed since the establishment of the Cybersecurity Advisory Board. A summarized way of grouping the steps to be executed in this phase of the program is the following:

- Once the program design is completed, it will be important to confirm the systems and areas with which it must interact and that were initially identified by the Cybersecurity Advisory Board. This is to ensure that all actors are involved in the process.
- Develop an integration plan for the training modules with the LMS for students and the HHRR of the institution, as well as the student and HHRR information systems.
- Establish test times before releasing the program into production so to validate that the system and the program are working without problems.

Aligning the integration roadmap with external accreditation or regulatory compliance requirements (such as ISO/IEC 27001, NIST 800-50, or local educational standards) can enhance the institutional value of the framework. This alignment may facilitate smoother audits, improve the institutional reputation, and provide measurable benchmarks for evaluating the cybersecurity maturity.

5.2.3. Implementation/Execution

This section deals with the execution of the program as such, following the established schedule of user awareness and training, which specifically corresponds to the first module (Assessment and Phishing/Malware Campaigns). In addition to executing the program, the Cybersecurity Awareness and Training Program team must monitor and control it. Being able to send reminders of pending activities, and reaching out to those individuals who are not complying with what was scheduled so to ensure compliance with what was planned, is important.

The second module of this section is an analysis of the results, reports, and recommendations. It is important to implement this module, independently of whether the Cybersecurity Awareness and Training Modules are completed or not, since this section of the framework is the one that will gather the results and provide feedback on the operation of the implemented program. Whereby it is highly recommended that the collection of results be carried out in the form of data that allow for analysis, thus allowing for easy comparisons between one cycle and another. This will shorten the time for analyzing the results, allow for the easy identification of points for improvement, and facilitate the modification of the program strategy.

The third module, the Technical Support and Survey execution, will oversee the information technology area of the institution, since they manage the company's systems, and could address operating situations and visualization of the program based on the records of the LMS and information systems. In this module, statistics, such as reported malfunctions and users served, among others that are defined as relevant to the institution, must also be recorded.

To ensure the sustainability of the awareness and training efforts, it is essential to institutionalize a feedback loop. After each cycle, collected data should be used not only for analysis but also for refining future modules. The institution should also establish regular intervals for revisiting its objectives, threats, and user needs so to adapt the program

accordingly. This iterative process is central to aligning the program with evolving security landscapes and educational environments.

5.3. Information Security Culture Program for Higher Education (ISCP for HEIs)

This is the third block of the framework, which is recommended to be designed and implemented in parallel to block 2, since, as indicated by [46], it is important to accompany the user awareness and training strategy with activities that encourage the practice of security in a positive way. The complexity of the activities carried out in this part of the program will again depend on the company's resources; however, different low-cost options could work in the case of smaller institutions or those with fewer resources, for example, security talks led by those responsible for the security or IT area of the organization, newsletters, and sharing emails with periodic information regarding information security.

5.4. Integration of CA&TF for HE Blocks and Information Flow

The CA&TF for HE is a framework that works in the form of cycles, where its three modules are also interconnected by the flow of information, which serves as the input for the readjustments and redesign of the strategy based on the results obtained and the trends and situations of the markets.

As an initial phase, the framework establishes a first block (Establishment of the Cybersecurity Awareness and Training Program team), where the Cybersecurity Awareness and Training Program team and the Cybersecurity Advisory Board are consolidated. Once the Cybersecurity Advisory Board is established, the Cybersecurity Awareness and Training Program team receives specific information on each of the areas, their people, systems, and processes. This, together with the active research carried out by the Cybersecurity Awareness and Training Program team, are inputs for the design and modification of block 2 (Cybersecurity Awareness and Training Program) and block 3 (Information Security Culture).

Given that block 2 includes integration and execution activities, and the evaluation of the results of the modules, assessments, and campaigns executed, it is also able to produce information that contributes to its own improvements, as well as serving as the input for block 3. These are the starting points for the design and adjustment of the complementary activities that accompany the education and training carried out in block 2. The outputs of block 3, in addition to serving as the input for its improvement, also contribute to the design adjustments of block 2.

In this way, the interconnection between the three blocks and the flow of information as input to make readjustments turns the framework into a process of continuous improvement, which is illustrated in Figure 17.

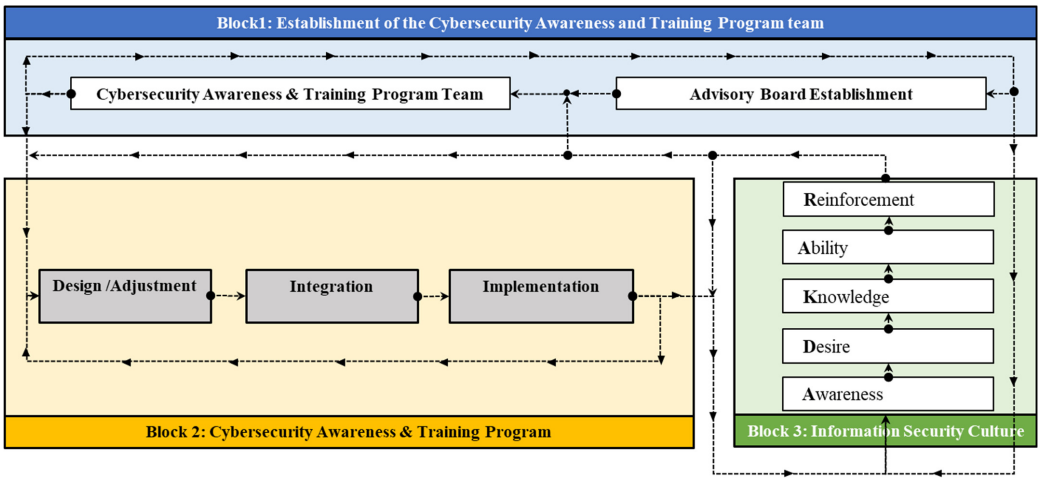

Figure 17. Integration of the CA&TF for HE blocks and information flow.

6. Conclusions

A specific information security awareness and training framework tailored to the higher education (HE) industry is essential for several reasons. Starting with the fact of the coexistence of various user groups within HE institutions, and the wide and valuable amount of data and information contained in their systems, this represents unique challenges in terms of cybersecurity education and awareness. This is one of the main reasons why these institutions are often targeted by cybercriminals. Therefore, a dedicated framework is needed to address these challenges effectively. In this context, the Cybersecurity Training and Awareness Framework for Higher Education (CA&TF for HE) is designed to provide a comprehensive and institution-specific approach to cybersecurity education, aiming to empower users with the knowledge and skills necessary to protect against cyber threats. It also focuses on cultivating a culture of cybersecurity within the HE institutions, which is crucial for long-term security.

Currently, there are several existing frameworks for building awareness and training users in information security and establishing an information security system in general. While these frameworks may serve as valuable references, they often require adaptation to meet the unique needs and challenges of specific industries. Often, they also align to a single framework that does not guarantee covering all of the aspects in question. As demonstrated throughout this research, many of these frameworks and standards overlap at certain points, but, in other areas, there are still gaps to cover, or the information does not have the depth that is needed.

The CA&TF for HE draws upon the best practices and methodologies from various cybersecurity frameworks, including the NIST and its special publications NIST SP 800-16, NIST SP 800-50, and NIST SP 800-53; ISO/IEC 27001 and ISO/IEC 27002; the SANS Security Awareness Maturity Model; the CIS Control V8; COBIT 2019; and the CAFA, a framework based on a previous work which proposes the inclusion of security topics within the academic program of HE institutions, which contributes to the preparation of future professionals in matters related to information security, best practices in information management, and the importance of constantly applying this knowledge in one's personal and professional life.

However, this last framework needs to be expanded to other audiences beyond students and professors, such as directors and executives, other departments that perform administrative tasks, and the same team that manages the information technology and security of the institutions, adding practical components that simulate real social engineering attacks, like phishing campaigns, and complementary activities that encourage changing user behavior so that this is integrated into the organizational culture.

The careful combination of the aforementioned frameworks and standards makes the CA&TF for HE adapt and integrate elements to create a specialized approach suitable for HE institutions so to address the challenges regarding the education and awareness of users grouped in the different audiences that coexist in HE institutions, thus organizing the CA&TF for HE in three connected blocks, each of which contributes to the main objective but which is focused on specific sections of the institutions.

The first block of the CA&TF for HE is focused on the establishment of the team responsible for the Cybersecurity Awareness and Training Program and the Cybersecurity Advisory Board. These two entities play a key role in the planning, implementation, and management of the program, aligning it with the institution's strategic objectives, and ensuring a comprehensive and effective approach. In the specific case of the Cybersecurity Advisory Board, it is integrated by members from different areas of the institution, which allows them to add valuable information to customize the program for specific audiences and the current organization's state of the art.

The second block, the Cybersecurity Training and Awareness Program, is the result of a careful adaptation of various cybersecurity methods. It covers planning, adjustments, integration, and implementation to empower users with the knowledge and skills necessary to protect against cyber threats.

The third part, the Information Security Culture Program for Higher Education (ISCP for IES), complements the Cybersecurity Training and Awareness Program by promoting a cybersecurity culture within the general culture of the institution. Moreover, the use of the ADKAR change management model prepares people to meet information security challenges and become cybersecurity advocates. The CA&TF for HE works in a cycle, where its three blocks are interconnected, and the information flowing between them and the knowledge of each part helps to improve the entire framework, thus creating a continuous improvement process.

Finally, the CA&TF for HE is a relevant tool that aims to provide the knowledge and skills to protect the information of students, faculty, and staff, while also strengthening the culture of cybersecurity. This proposal contributes as part of the solution to the growing increase in attacks in the HE industry. This could be considered an important step in preparing the workforce of the future to face the challenges of a constantly changing and evolving world. However, it also is important to acknowledge its limitations. The lack of empirical validation limits this study's unique conceptual framework for cybersecurity awareness and training in higher education. Further study may be needed to assess the framework's efficacy in other institutional and cultural situations. Attack simulations, user awareness tests, and feedback systems will demonstrate the framework's applicability and efficacy. To adapt to new cybersecurity threats and educational demands, the framework must be evaluated and adjusted. Future research can examine the integration of AI-driven adaptive learning systems and threat intelligence feedback loops, and the framework's long-term influence on higher education cybersecurity issues. Based on this research, future studies can improve cybersecurity awareness and education in the HE industry.

Author Contributions: Conceptualization, H.T.; methodology, H.T.; validation, H.T.; formal analysis, R.A.; resources, R.A.; data curation, R.A.; writing—original draft preparation, R.A.; writing—review and editing, H.T.; visualization, R.A.; supervision, H.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: Author Hamed Taherdoost is employed by Q Minded | Quark Minded Technology Inc., Vancouver, BC V6E 1C9, Canada. The remaining author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Statista Research Department. *Spending on Digital Transformation Technologies and Services Worldwide from 2017 to 2026 (in Trillion U.S. Dollars)*; Statista: Hamburg, Germany, 2022.
2. Statista Research Department. *Global Annual Growth Rate of Spending on Cyber Security from 2019 to 2026, by Industry Sector*; Statista: Hamburg, Germany, 2023.
3. IBM Security. *X-Force Threat Intelligence Index 2023*; IBM: Armonk, NY, USA, 2023; p. 42.
4. Amorosa, K.; Yankson, B. Human Error—A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *Holistica J. Bus. Public Adm.* **2023**, *14*, 110–132.

5. Armas, R. *Information Security Awareness in Higher Education: The Need for a Tailor-Made Suit*; C2SA: Agadir, Morocco, 2023.
6. Ben-Asher, N.; Gonzalez, C. *Effects of Cyber Security Knowledge on Attack Detection*; Elsevier: Amsterdam, The Netherlands, 2015; pp. 51–61.
7. Ikram, N.; Ikram, N.; Murtaza, H.; Javed, M. Evaluating Protection Motivation Based Cybersecurity Awareness Training on Kirkpatrick's Model. *Comput. Secur.* **2023**, *125*, 103049.
8. Ulven, J.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet* **2021**, *13*, 39. [CrossRef]
9. IBM Security. *Cost of a Data Breach Report 2023*; IBM: Armonk, NY, USA, 2023; p. 20.
10. SonicWall. *2023 SonicWall Cyber Threat Report*; SonicWall: San Jose, CA, USA, 2023.
11. Microsoft Security Intelligence. *Global Threat Activity*; Microsoft: Redmond, WA, USA, 2023.
12. CheckPoint. *Check Point Press Releases*; CheckPoint: Tel Aviv-Yafo, Israel, 2023. Available online: https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed/ (accessed on 8 August 2022).
13. Arina, A. Cyber security strategies for higher education institutions. *J. Eng. Sci.* **2021**, *23*, 72–92.
14. Astudillo, F.; Astudillo-Salinas, F.; Tello-Oquendo, L.; Sanchez, F.; Lopez-Fonseca, G. Information security management frameworks and strategies in higher education institutions: A Systematic Review. *Ann. Telecommun.* **2021**, *76*, 255–270.
15. EDUCAUSE. *Cybersecurity and Privacy Guide*; EDUCAUSE: Louisville, CO, USA, 2023. Available online: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-policies#:~:text=The%202016%20EDUCAUSE%20Core%20Data%20Service%20found%20that,20%25)%20CIS%20Critical%20Security (accessed on 16 July 2023).
16. Hash, J.; Wilson, M. *NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program*; NIST Computer Security Resources Center: Gaithersburg, MD, USA, 2003.
17. Klein, P.; Toth, P. *NIST Especial Publication 800—16—A Role-Based Model for Federal Information Technology/Cybersecurity Training*; NIST Computer Security Resources Center: Gaithersburg, MD, USA, 2014.
18. *ISO/IEC 27001*; International Standard: Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO/IEC: Geneva, Switzerland, 2013.
19. *ISO/IEC 27002:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Controls. Online Browsing Platform (OBP) n.d; ISO/IEC: Geneva, Switzerland, 2022. Available online: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en (accessed on 16 July 2023).
20. CIS. *CIS Critical Security Controls Version 8*; CIS: East Greenbush, NY, USA, 2021.
21. CDC. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*; Center for Diseases Control and Prevention: Atlanta, GA, USA, 1996. Available online: https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html?CDC_AAref_Val=https://www.cdc.gov/phlp/publications/topic/hipaa.html (accessed on 27 June 2022).
22. NIST. *Information Technology Laboratory: Computer Security Resource Center*; NIST: Gaithersburg, MD, USA, 2025. Available online: https://csrc.nist.gov/glossary/term/information (accessed on 23 August 2023).
23. Cawthra, J. Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. Available online: https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html (accessed on 16 September 2023).
24. ISACA. *Glossary*; ISACA: Schaumburg, IL, USA, 2023. Available online: https://www.isaca.org/resources/glossary (accessed on 16 September 2023).
25. IBM. *What Is a Cyberattack?* IBM: Armonk, NY, USA, 2025. Available online: https://www.ibm.com/topics/cyber-attack (accessed on 16 September 2023).
26. Statista. PHISHING. In *DIGITAL & TRENDS*; Statista: Hamburg, Germany, 2023.
27. Threat Hunter Team. *The Ransomware Threat Landscape: What to Expect in 2022*; Symantec by Broadcom Software: Palo Alto, CA, USA, 2022.
28. Zadelhoff, M.V. The Biggest Cybersecurity Threats Are Inside Your Company. *Harv. Bus. Rev.* **2016**, *19*, 45.
29. Bahorski, Z.C.; Droujkova, M. *Personal Computers*; EBSCO Research Starters: Ipswich, MA, USA, 2024. Available online: https://www.ebsco.com/research-starters/computer-science/personal-computers (accessed on 20 August 2023).
30. Dobrow, S. *Rise of the Internet and the World Wide Web*; Salem Press Encyclopedia: Ipswich, MA, USA, 2023.
31. Shillair, R.; Esteve-González, P.; Dutton, W.H.; Creese, S.; Nagyfejeo, E.; von Solms, B. *Cybersecurity e Ucation, Awareness Raising, and Training Initiatives: National Level Evidence-Based Results, Challenges, and Promise*; Elsevier: Amsterdam, The Netherlands, 2022; p. 119.
32. Petrosyan, A. *Number of Internet Users Worldwide from 2005 to 2022*; Statista: Hamburg, Germany, 2023.
33. United States Census Bureau. *U.S. and World Population Clock*; United States Census Bureau: Suitland-Silver Hill, MD, USA, 2023.
34. Wlosinski, L. The Benefits of Information Security and Privacy Awareness Training Programs. *ISACA J.* **2019**, 1.
35. Asch, E.; Ballou, J.; Weisbrod, B. *Mission and Money: Understanding University*; Cambridge University Press: Cambridge, UK, 2008.

36. Statista Research Department. *Revenue from Tuition and Fees of Degree-Granting Postsecondary Institutions in the United States from 2010/11 to 2019/20*; Statista: Hamburg, Germany, 2023.
37. Statista Research Department. *Estimated Number of Universities Worldwide as of July 2021, by Country*; Statista: Hamburg, Germany, 2023.
38. El-Azar, D. *4 Trends That Will Shape the Future of Higher Education*; World Economic Forum: Cologny, Switzerland, 2022.
39. Pavlova, E. Enhancing the Organisational CULTURE related to Cyber Security during the University Digital Transformation. *Inf. Secur.* **2020**, *40*, 239–249. [CrossRef]
40. Bernard, J.; Golden, D.; Nicholson, M. *Reshaping the cybersecurity landscape*; Deliotte Ingsight: Westlake, TX, USA, 2020. Available online: https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (accessed on 23 November 2023).
41. Clark, C.; Fishman, T. *Elevating Cybersecurity on the Higher Education Leadership Agenda*; Deloitte Insights: Westlake, TX, USA, 2018.
42. Kaplan, J.; Kaplan, J.; Kazimierski, B.; Lewis, C.; Telford, K. *Organizational Cyber Maturity: A Survey of Industries*; McKinsey & Company: Chicago, IL, USA, 2021.
43. Bowlin, E. *Cybersecurity and Privacy in the Future of Health*; Deloitte: Westlake, TX, USA, 2020. Available online: https://www2.deloitte.com/us/en/pages/advisory/articles/data-privacy-and-cybersecurity-in-the-future-of-health.html (accessed on 23 November 2023).
44. Petrosyan, A. *Percentage Change in the Cyber Security Budget Allocation in U.S. Healthcare Organizations from 2020 to 2021*; Statistic: Suitland, MD, USA, 2023.
45. Mercer, T. *What Is a Framework in Cybersecurity? (A Beginner's Guide)*; Forbes: Jersey City, NJ, USA, 2020. Available online: https://books.forbes.com/author-articles/what-is-a-framework-in-cybersecurity-a-beginners-guide/ (accessed on 13 November 2023).
46. Bhaskar, R. Better Cybersecurity Awareness Through Research. *ISACA J.* **2022**, *3*, 1–10.
47. Constantin, A. Information Security Management—Part of the Integrated Management System. *Acta Univ. Cibiniensis* **2015**, *66*, 102–107.
48. NIST. *About NIST*; NIST: Gaithersburg, MD, USA, 2022. Available online: https://www.nist.gov/about-nist (accessed on 11 January 2022).
49. NIST. *Cybersecurity Framework Components*; NIST: Gaithersburg, MD, USA, 2023. Available online: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components (accessed on 16 March 2023).
50. NIST. *Framework for Improving Critical Infrastructure Cybersecurity*; NIST: Gaithersburg, MD, USA, 2018.
51. NIST. *Security and Privacy Controls for Information Systems and Organizations*; NIST: Gaithersburg, MD, USA, 2020.
52. ISO/IEC. About ISO. n.d. Available online: https://www.iso.org/about-us.html (accessed on 20 August 2023).
53. *ISO/IEC 27002:2013*; INTERNATIONAL STANDARD Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO/IEC: Geneva, Switzerland, 2013. Available online: https://www.iso.org/standard/54533.html (accessed on 20 August 2023).
54. SANS Institute. *About SANS Institute*; SANS Institute: Cleverdale, NY, USA, 2023. Available online: https://www.sans.org/about/?msc=main-nav (accessed on 20 August 2023).
55. SANS. *SANS Security Awareness Maturity Model TM*; SANS: Cleverdale, NY, USA, 2022.
56. CIS. *CIS Critical Security Controls Version 8*; CIS: East Greenbush, NY, USA, 2023. Available online: https://www.cisecurity.org/controls/v8?sc_camp=BB43A1FDB3874AABA535F539EDD34A19&utm_source=bing&utm_medium=cpc&utm_campaign=bing_controls&msclkid=0df2e9b6556514dcbf8a8ca18af5b7dc (accessed on 20 August 2023).
57. CIS. *Download the CIS Critical Security Controls® v8*; CIS: East Greenbush, NY, USA, 2021.
58. CIS. *CIS Controls v8 Mappings to ISACA COBIT 19*; CIS: East Greenbush, NY, USA, 2023.
59. Karam, M.; Khader, M.; Fares, H. Cybersecurity Awareness Framework for Academia. *Information* **2021**, *12*, 417. [CrossRef]
60. Austin-Gabriel, B.; Hussain, N.Y.; Ige, A.B.; Adepoju, P.A.; Amoo, O.O.; Afolabi, A.I. Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Res. J. Eng. Technol.* **2021**, *1*, 047–055. [CrossRef]
61. Abikoye, B.; Agorbia-Atta, C. Securing the Cloud: Advanced Solutions for Government Data Protection. *World J. Adv. Res. Rev.* **2024**, *23*, 901–905. [CrossRef]
62. Rebouças Filho, W.L. The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. *Braz. J. Dev.* **2025**, *11*, e76836. [CrossRef]
63. Joshi, H. Emerging Technologies Driving Zero Trust Maturity Across Industries. *IEEE Open J. Comput. Soc.* **2024**, *6*, 25–36. [CrossRef]
64. Williamson, S.M.; Prybutok, V. Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Appl. Sci.* **2024**, *14*, 675. [CrossRef]
65. Padmanaban, H. Privacy-preserving architectures for AI/ML applications: Methods, balances, and illustrations. *J. Artif. Intell. Gen. Sci. (JAIGS)* **2024**, *3*, 235–245.

66. Wang, M.; Zhang, H.; Wu, H.; Li, G.; Gai, K. Blockchain-based secure medical data management and disease prediction. In Proceedings of the Fourth ACM International Symposium on Blockchain and Secure Critical Infrastructure, Nagasaki, Japan, 30 May 2022.
67. Daah, C.; Qureshi, A.; Awan, I.; Konur, S. Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. *Electronics* **2024**, *13*, 865. [CrossRef]
68. Li, Y.; Xia, C.; Lin, W.; Wang, T. PPBFL: A privacy protected blockchain-based federated learning model. *arXiv* **2024**, arXiv:2401.01204.
69. Rückel, T.; Sedlmeir, J.; Hofmann, P. Fairness, integrity, and privacy in a scalable blockchain-based federated learning system. *Comput. Netw.* **2022**, *202*, 108621. [CrossRef]
70. Yun, J.; Lu, Y.; Liu, X.; Guan, J. Bio-Rollup: A new privacy protection solution for biometrics based on two-layer scalability-focused blockchain. *PeerJ Comput. Sci.* **2024**, *10*, e2268. [CrossRef] [PubMed]
71. Ngoupayou Limbepe, Z.; Gai, K.; Yu, J. Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey. *Blockchains* **2025**, *3*, 1. [CrossRef]
72. Hu, J.; Hajlaoui, N.; Touati, H.; Hadded, M.; Muhlethaler, P.; Boudjit, S. *A Secure Medical Information Storage and Sharing Method Based on Multiblockchain Architecture*; IEEE Transactions on Computational Social Systems: Piscataway, NJ, USA, 2024.
73. Ghanmi, H.; Hajlaoui, N.; Touati, H.; Hadded, M.; Muhlethaler, P.; Boudjit, S. Blockchain-cloud integration: Comprehensive survey and open research issues. *Concurr. Comput. Pract. Exp.* **2024**, *36*, e8122. [CrossRef]
74. Tsohou, A.; Karyda, M.; Kokolakis, S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Comput. Secur.* **2015**, *52*, 128–141. [CrossRef]
75. Akbar, W.; Rivera, J.J.D.; Ahmed, K.T.; Muhammad, A.; Song, W.-C. Software Defined Perimeter Monitoring and Blockchain-Based Verification of Policy Mapping. In Proceedings of the 2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS), Takamatsu, Japan, 28–30 September 2022.
76. Abou El Houda, Z.; Moudoud, H.; Khoukhi, L. Blockchain Meets O-RAN: A Decentralized Zero-Trust Framework for Secure and Resilient O-RAN in 6G and Beyond. In Proceedings of the IEEE INFOCOM 2024-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 20 May 2024.
77. Taherdoost, H. *Research Skills; The Essential Step-By-Step Guide on How to Do a Research Project*; Kindle Edition: Vancouver, BC, Canada, 2021.
78. Cheng, E.; Wang, T. Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information* **2022**, *13*, 192. [CrossRef]
79. Ali, M.; Usman, Z.; Asif, M.; Muhammad, N. The Power of Adkar Change Model in Innovative Technology Acceptance under the Moderating Effect of Culture and Open Innovation. *LogForum* **2021**, *17*, 485–502.
80. Enders, J.; Jongbloed, B.; Salerno, C. Higher education and its communities: Interconnections, interdependencies and a research agenda. *High. Educ.* **2008**, *56*, 303–324.
81. ISACA. *COBIT an ISACA Framework*; ISACA: Schaumburg, IL, USA, 2023. Available online: https://www.isaca.org/resources/cobit (accessed on 20 August 2023).
82. Gür, G.; Gür, G.; Sutter, T.; Tellenbach, B. Don't click: Towards an effective anti-phishing training. A comparative literature review. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 33.