International Journal of Safety and Security Engineering
Vol. 13, No. 4, August, 2023, pp. 763-771
Journal homepage: http://iieta.org/journals/ijsse

Leveraging Security Modeling and Information Systems Audits to Mitigate Network Vulnerabilities

Laberiano Andrade Arenas[1*], Cesar Yactayo-Arias[2], Sheyla Rivera Quispe[3], Jenner Lavalle Sandoval[3]

[1] Facultad de Ciencias e Ingeniería, Universidad de Ciencias y Humanidades, Lima 15304, Peru
[2] Departamento de Estudios Generales, Universidad Continental, Lima 12001, Peru
[3] Facultad de Ingeniería y Negocios, Universidad Privada Norbert Wiener, Lima 15046, Peru

Corresponding Author Email: landrade@uch.edu.pe

https://doi.org/10.18280/ijsse.130420

Received: 18 March 2023
Revised: 26 July 2023
Accepted: 13 August 2023
Available online: 28 September 2023

Keywords:
ISO 27001 standards, IT infrastructure security, protection of valuable assets, cyber-attacks, organizations

ABSTRACT

Advancements in digital technologies have significantly enhanced the functional capabilities of consumers and businesses alike, yet have concurrently amplified the complexities associated with cybersecurity, including theft and cyber-attacks. Consequently, auditing of information systems has emerged as a crucial security apparatus for organizations aiming to safeguard their data assets, specifically with respect to customer information. This study aims to design an information systems security and audit model that emphasizes the fortification of an organization's crucial assets via IT infrastructure security and information security management systems, in alignment with ISO 27001 standards. The proposed model seeks to assure information confidentiality, integrity, availability, and compliance with legal mandates. The study adopted the OCTAVE v2.0 method, executed in three distinct phases. In the first phase, profiles of asset-based threats were constructed. The second phase involved the identification of infrastructure vulnerabilities, whereas the final phase focused on the development of a security strategy and plans. The implementation of the proposed model yielded a marked impact, with a positive shift from 46% to 94% following the establishment of IT infrastructure security policies. The study underscores the importance of conducting a comparative analysis prior to implementation and asserts that well-defined and identified security models and information systems auditing can effectively counteract potential data leaks and cyber-attacks such as malware, phishing, spam, and ransomware. The findings suggest that a meticulous and preemptive approach to auditing and security planning can significantly bolster the resilience of an organization's digital infrastructure.

1. INTRODUCTION

Throughout history, technology has played a pivotal role in the evolution of human society [1]. The advent of the internet and subsequent digital tools has catalyzed unprecedented advancements, reshaping the economic landscape and established business practices. This rapid evolution has necessitated organizations globally to adapt to this digital transformation [2, 3]. From altering sales processes to introducing cost leadership strategies and diversification, digital transformation has expedited service delivery, enhanced customer satisfaction, and broadened business scopes, resulting in consumer empowerment.

According to the 2022 Threat Landscape report by Kaspersky, malware and Trojans were identified as the most prevalent patterns in cyber-attacks. These forms of malicious software have been engineered to exfiltrate data from organizations, with some even designed to facilitate bank fraud and scams, thereby posing significant threats to financial institutions. The report further illustrated that an average of 2,366 malware attacks and 110 fraudulent messages were intercepted every minute in South America. Specifically, Brazil (1,554), Mexico (298), Peru (123), Colombia, and Ecuador (84), followed by Argentina (30) and Chile (28), were identified as the countries with the highest volume of attempted cyberattacks.

The frequent and sophisticated nature of these attacks puts Latin America in a precarious situation for organizations and consumers alike. This situation is exacerbated by the dense concentration of businesses in metropolitan areas, high population, and bustling economic activity, which culminates in intense business competition. Consequently, the region becomes an attractive target for cybercriminals while simultaneously rendering it highly susceptible to cyber-attacks. Challenges related to IT infrastructure further compound these vulnerabilities, primarily due to organizations' limited response capacity in terms of their IT security strategy. This limitation can be attributed to the lack of up-to-date hardware and software resources in areas that safeguard an organization's most valuable assets.

However, this digital progression has also paved the way for sophisticated cyber threats. As reported by Kaspersky's Threat Landscape in 2022, malware and Trojans emerged as the predominant patterns in cyber-attacks. These malicious software were specifically designed to compromise organizational data, posing significant threats to financial institutions [4]. The report further illuminated that South America experienced an average of 2,366 malware attacks and 110 fraudulent messages per minute. Countries such as Brazil, Mexico, Peru, Colombia, Ecuador, Argentina, and Chile were

particularly targeted given their dense metropolitan areas, high population, and significant economic activities, making them attractive yet vulnerable for cybercriminals [5].

In light of these challenges, the proposed security model in this study aims to implement an IT security plan that addresses key vulnerabilities such as insufficient financial resources, inefficient software management, and lack of technical expertise among IT managers. Emphasizing the importance of physical and operational inventories, antivirus software, strict data access controls, and resilience training for personnel, this model seeks to bolster the cybersecurity defenses of organizations [6].

This information security model's primary objective is designed to efficiently and effectively review, monitor, maintain, and optimize an organization's asset security. This involves the identification and mitigation of vulnerabilities to minimize potential cyber thefts and the restriction of sensitive information access to authorized personnel only. Additionally, the model is intended to foster a culture of security within the organization by measuring and evaluating the competence, knowledge, capacity, and preparedness of the IT staff in the face of potential security incidents. This is with the aim to safeguard business systems and information. Utilizing the ISO 27001 standards for IT infrastructure and information security management systems, the model can assist organizations in establishing security policies and objectives, thereby improving their data management. This approach is designed to counteract the daily cyber-attacks that cause losses and instability within organizations. The ultimate aim of this paper is to establish a precedent for strategic responses to cyberattacks, benefiting organizations, communities, and society at large. The evaluation of the proposed model's success is primarily based on each organization's specific needs and objectives, aligning with the goals of this research. This is evident as the proposed model enables the effective assessment of vulnerability management, the incidence and severity of security incidents, and the level of staff awareness, as measured through knowledge and feedback evaluations.

Moreover, the proposal includes an evaluation phase that necessitates a comprehensive comparative report. This is to ascertain whether the implementation of cybersecurity policies has had a positive impact on organizations.

2. METHODOLOGY

OCTAVE v2.0 (Operationally Critical Threat, Asset and Vulnerability Evaluation) is a risk analysis methodology, which was developed by Carnegie Mellon University to identify and evaluate the security risks of government agencies, like the U.S. Department of Defense; as a matter of fact, since it is launched in 2001, it has gone through several updates and changes, which has allowed it to have broad applicability. According to the author [7], this methodology not only allows us to identify and evaluate security risks but also to make improvements in the decision-making process towards data resource management in a medium and large organization.

Regarding the OCTAVE v2.0 method implementation, the author [8] points out that because of the applicability that these criteria have, it is simpler and more interesting to the market, mainly because it adjusts to different types of organization's policies that day after day increases its confidential information, whether it is confidential customer data or confidential employee information, which neither most employees nor senior managers have access to. It reinforces the need to strengthen the IT infrastructure and the cyber-security system. Through risk identification, we can prepare for potential internal and external vulnerabilities that may negatively impact the organization's outcome at any time.

It is important to highlight that this methodology uses a three-phase: Operational risk, security practices, and technology [9] being its core, a set of criteria based on principles, attributes, and results. Hence, the processes carried out by OCTAVE v2.0 begin with an evaluation of the most valuable asset for the organization nowadays, which is "the data"; when analyzed, it allows one to determine the organizational level and their level of Cyber security. After showing the results, we set protection strategies based on the identified operational risks, and best Cyber security practices so that they can fix the vulnerabilities as they arise in the organization.

2.1 Phases of the octave methodology

According to Pacheco et al. [10], the methodology OCTAVE v2.0 has a three-phase approach, which can be seen in Figure 1. where it can be seen that representative graphs and diagrams were made to organize and detail the phases, processes and identify the problems in the areas of the organization, which were worked with the online diagram software draw.io, a tool with which you can create flow charts, process diagrams, organization charts, etc.

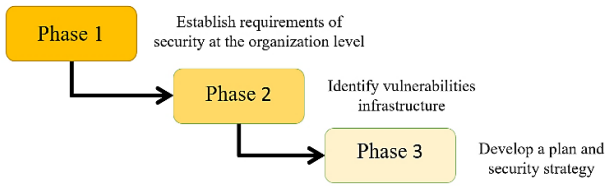

Figure 1. Main phases of the Octave V2 methodology

2.1.1 Phase 1: Build asset-based threat profiles

In this phase, we do an organizational evaluation, basically, we proceed to identify the team's knowledge of the organization’s business and operational areas. Likewise, we identify operational area management knowledge of the organization's most important assets identified, as well as the perceived threats and current protection strategy practices, meaning, what's being done to protect those critical assets [11]. It's noteworthy that, during this phase, we determine the security requirements in order to collect information that helps to create a new design of the protection strategy practices by creating a threat profile for that asset.

2.1.2 Phase 2: Identify infrastructure vulnerabilities

In phase 2, we use the information collected from phase 1, then analyze the key operational components that have a higher vulnerability. In other words, it can be a risk to the organization's assets. In this phase, the missing policies and procedures are identified, as well as a mapping of high-priority assets per the organizational level and conducting a vulnerability assessment.

2.1.3 Phase 3: Develop security strategy and plans

In phase 3, we analyze the information gathered from phases 1 and 2. Then, the team creates protection strategies to

solidify the organization's assets and analyze the information to identify the information security risks, and critical asset vulnerabilities. Also, in the worst-case scenario, if we identify computer risks, there are mechanisms designed to fix the problem, such as the use of access codes, antivirus, firewall, etc. As the author [12] claims, the purpose of this phase is to mitigate potential cyber-risks that may arise in an organization.

2.2 Development of the phases

In accordance with the method OCTAVE v2.0 [13], we establish the phases and processes we follow toward the objective.

2.2.1 Establish security requirements at the organization level

(A) Process 1. Identify the knowledge of senior management. Compile information on the main assets of the organization. As can be seen in Figure 2, the employees who hold high management positions are selected so we can identify the most important assets through security levels, in order to avoid potential threats that may have a negative impact on the organization's software and hardware. Also, according to the security requirements, in order to set protection strategies, we must gather information regarding cyber threats and vulnerabilities. This information must be gathered from a representative set of senior managers.

Figure 2. Identify business knowledge

Select senior managers. This is relevant to the method Octave v2.0 because senior managers are the leaders of an organization. They have excellent knowledge of the organization's workflow and the operations of their department. Therefore, it's crucial to collect information from them. Note that, in Peru, the hierarchy business model states that there must be at least a general manager per location and several lower-level managers per department.

Identify the most valuable assets. We cannot deny that in order to establish the security requirements it is a must to know what the organization's most valuable assets are. Hence, there should be strategies implemented based on the department. Furthermore, there should be an agenda to prepare for a meeting with the employees who are directly in charge of these valuable assets, for example, the IT manager. These employees oversee the servers, software, hardware, and the organization's network, so this is one of the most important departments, as they manage data and sensitive information such as passwords, and business and customer banking.

Perceived threats. With the e-commerce boom and the popularity of social media, organizations have become an easy target for cybersecurity threats like malware, phishing, spam, ransomware, etc. If we don't identify them on time, it could put at risk an organization's most valuable assets. Therefore, we must prevent this and elaborate a contingency plan to back up the organization's data in case they get cyber-attacked.

Security requirements. In order to counteract the threats and avoid potential cyber-attack, we must perform a deep evaluation, which will be applied based on the security requirements and protection strategies to protect their most valuable assets. Moreover, in this section, a vulnerability assessment is conducted to be aware of the security weakness and establish authentication methods for all devices.

Current security practices. As reported by the author [14] regarding digitalization and the new and major types of cyber-attack in Peru's commercial sector, the current security practices are preventive measures against any type of cyber-attacks and when this happens, the IT manager should be prepared to face them.

Organizational vulnerabilities. The vulnerabilities or weaknesses in the organization's IT system are analyzed, expecting to reinforce them to protect the assets that can easily become a target. Mainly, as a result of using software without a license, network issues, and technological limitations; this is when cybercriminals take advantage of the situation. In order to neutralize the cyber-attacks, we must identify the vulnerabilities, which can be a threat to the organization [15].

In Figure 3 it can be seen the main departments that are more exposed to vulnerabilities. Through Ishikawa diagram shows the potential causes and effects if we don't properly protect the organization's most valuable assets. Also, this graphic diagram helps to do a deep analysis of all departments in the organization. The results show the need for investment in cybersecurity analytics, preventive measures, providing training to employees, and updating their security models.

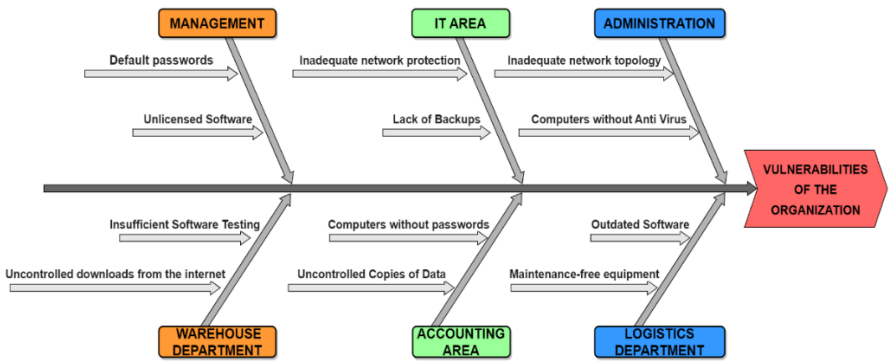

Figure 3. Ishikawa diagram of possible causes and effects

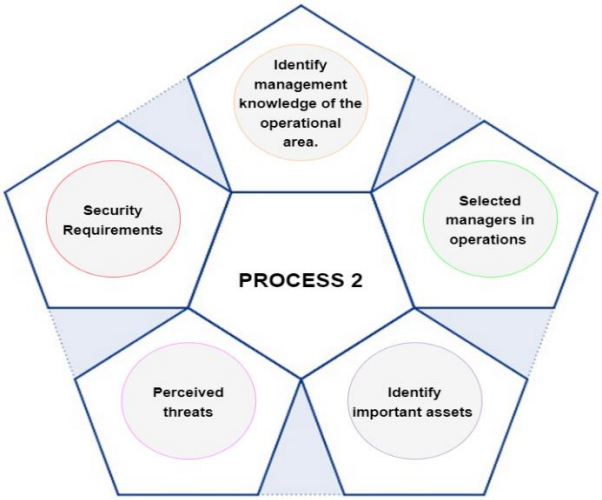

Figure 4. Identify operational area management knowledge

(B) Process 2. Identify operational area management knowledge**.** In this part of the process, the activities are defined, and the security requirements and assets' perceived threats are identified by selected operational area managers. Based on an operational point of view, we gather information like important assets, security requirements, and others, with a scope on a tactical level (see Figure 4).

(C) Process 3. Identify staff knowledge**.** In this process, we collect information from selected IT and general staff as they are knowledgeable and/or have access to confidential information. For example, an IT employee is the main character as is visible in Figure 5. Not only because they give technical support, but also because they back up the internal information of an organization in between departments, such as management, accounting, sales, logistics, warehouse, administration, etc.

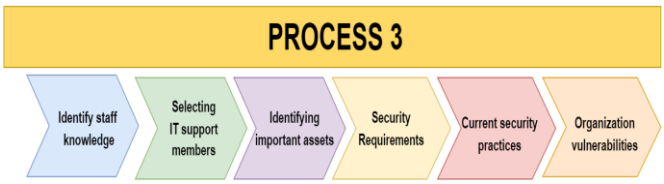

Figure 5. Identify staff knowledge

(D) Process 4. Create threat profiles. In the process, the team analyses the information gathered from processes 1,2, and 3 and contrasts them based on perceived threats, current security practices, and risk indicators regarding the critical assets in this organization. That have previously determined the security requirements for high-priority assets. This process 4, helps to determine the security requirements and the fundamentals for a protection strategy, to give sufficient information that at the same time helps to design strategies concerning all the activities, assets, threats, and risk indicators to design protection strategies by creating threat profiles.

2.2.2 Identify infrastructure vulnerabilities

Regarding the analyses of the information gathered from phase 1, we proceed to classify the IT infrastructure's components per priority levels. Once this is done, we can identify the asset's vulnerabilities [16] in order to mitigate security risks and give a cyber-security [17] solution. The objective of this phase is to know in detail the procedures, elements, policies, and IT infrastructure risks.

(E) Process 5. Identify key factors. Regarding high-priority assets, the author [18] states that in order to efficiently map the high-priority assets, we need the employee in charge of these assets to assist. They know every detail of the IT infrastructure, as well as the physical and logical aspects, so their input is crucial to identify its most critical components. It is important to get information about the IT department regarding the information assets, cashflow statement, location of the assets, and network architecture access routes, mainly as we aim to get a security model [18] based on a hierarchical identity-based Blockchain System to get better network security [19].

As you can see in Table 1, you can identify the organization's assets, which let you oversee what hardware an organization in Peru has, and, consequently, with this inventory we can implement improvements in an organization. Also, these components are exposed to potential threats and vulnerabilities. Table 1 shows, the cyber-assets the organization has are 2 database servers, a web server, PCs, monitors, laptops, etc. This states that the organization must reinforce some departments by implementing a cyber-security system to block unauthorized access to computers and their servers, as they have the organizations and customers' information. Hence, it's important to do a hardware inventory as it shows the devices, we should keep versus the ones we should either replace or reinforce the cyber-security system to avoid cyber-attacks. Mainly, as they must do financial transactions, as well as communicate with other locations, customers, providers, etc.

Table 1. Hardware Inventory

No.	Hardware	Quantity
Hardware Inventory		
1	Database Servers	2
2	Internet Server	3
3	PCs	14
4	Monitors	14
5	Laptops	13
6	Switch	2
7	Router	3
8	Printers	9
9	Ups	2
Others		
10	Current Stabilizers	12
11	Barcode Scanner	2
12	Access Point	4
13	Projectors	3

Table 2 is shown one of the other important and valuable assets in an organization, which operates through software systems. As you can see, an inventory was done with all commercial software used in an organization in Peru (Table 2). This allows us to know if it is software with or without a license, in order to replace them if needed, to avoid exposure to cyber-attacks.

(F) Process 6. Evaluate selected components. As part of this process, it evaluates the key systems and the components of IT infrastructure to identify vulnerabilities. Its main objective is to recognize technology weaknesses by using vulnerability tools, as well as determine the procedure and security policies the organization lacks. The purpose is to point out the vulnerabilities and components of the IT infrastructure to classify them based on threat profiles.

Table 2. Software inventory

No.	Software	Quantity
	Operating Systems	
1	Windows Server 2019	2
2	Ubuntu Server 22.04.1	1
3	Windows 10	13
4	Windows 11	14
	DataBase Engines	
5	MySQL	2
6	SQL Server 2019	1
	Development Tools	
7	Visual Studio Professional 2022	1
	Office Tools	
8	Office 2021 Professional	14
	Web Design Tools	
9	Adobe Creative Cloud	4
	Antivirus	
10	Panda Dome Premium	14
11	McAfee	13
	Others	
12	Any Desk	14
13	Microsoft Teams	27
14	TeamViewe	27
15	Siscont	3
16	OBS Studio	4

2.2.3 Develop security strategy and plans

During this phase, strategies based on cyber-security management are established, as well as the analyses of vulnerabilities and threats to an organization to identify high-priority risks to the assets. In other words, the objective is not only to identify and expose these risks but also to develop protection strategies to solidify the Cyber security system.

(G) Process 7. Conduct risk analysis. In this process, the analysis team determines the activities the organization must follow to identify the highest priority risks that are threats to the organization (see Table 3). To accomplish objectives, the threats must be defined by the team using the knowledge obtained from the information collected, like the exposed assets, threats and their impact on the organization, current security practices and the lack of those, as well as determine the probability that the risk can materialize by creating criteria to evaluate the risk and conduct a multidimensional risk analysis (Figure 6). The purpose of this process is to make a list according to the criteria to evaluate the risk and two aspects: the impact and probability.

(H) Proceso 8. Desarrollar una estrategia de protección. The analysis team defines activities to develop protection strategies to reduce any security risks. The main objective is to design protection strategies and risk mitigation plans. The organization's employees must be compliant with the data protection strategies to safeguard the customer and organization's information.

In Figure 7, it's shown that in this process, protection strategies are developed based on criteria assets and their risk profiles, explained in process 7. There was a risk evaluation per criteria asset after the establishment of risk profiles, as the purpose is to determine how effective this is and its efficiency regarding the mitigation plans. After establishing the severity of these criteria assets, the risk profile is categorized. Each risk profile has a numerical value assigned plus the associated cost of its implementation, in order to simplify the decision-making process.

Table 3. Data network vulnerability

Infrastructure	**Networks**	
	Vulnerabilities	**Threats**
Data Network	- Undocumented network layout makes it difficult to identify the exact points in the event of damage to a company's network. - Outdated security policies.	- Partial detection of certain activities in a company. - The different events that affect equipment and information are not adequately controlled.

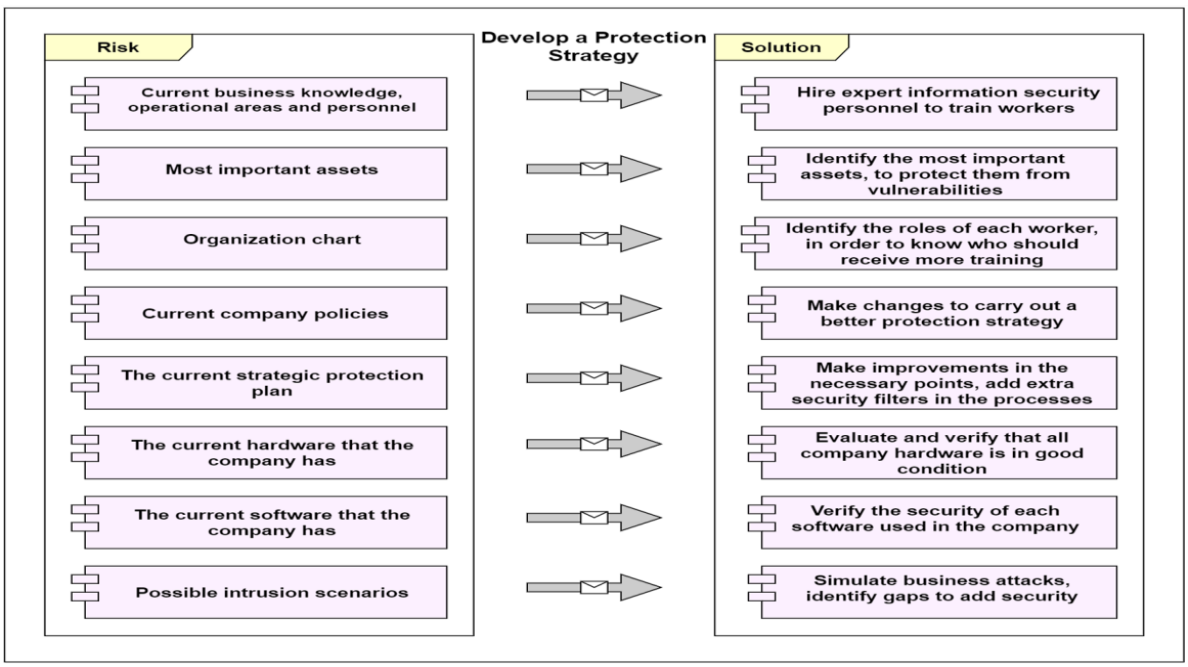

Figure 6. Multidimensional risk analysis

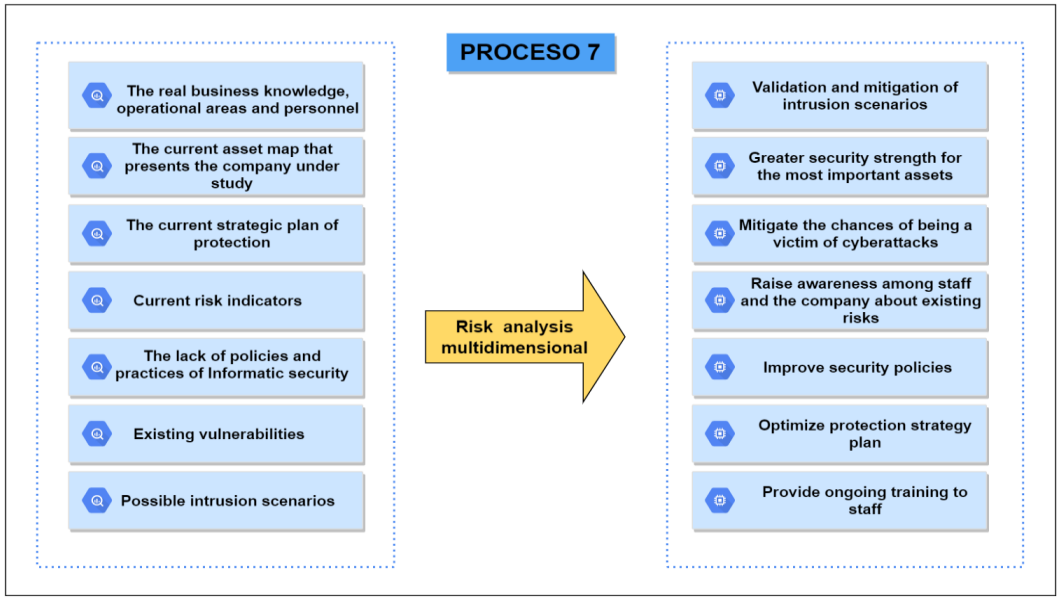

Figure 7. Develop a protection strategy

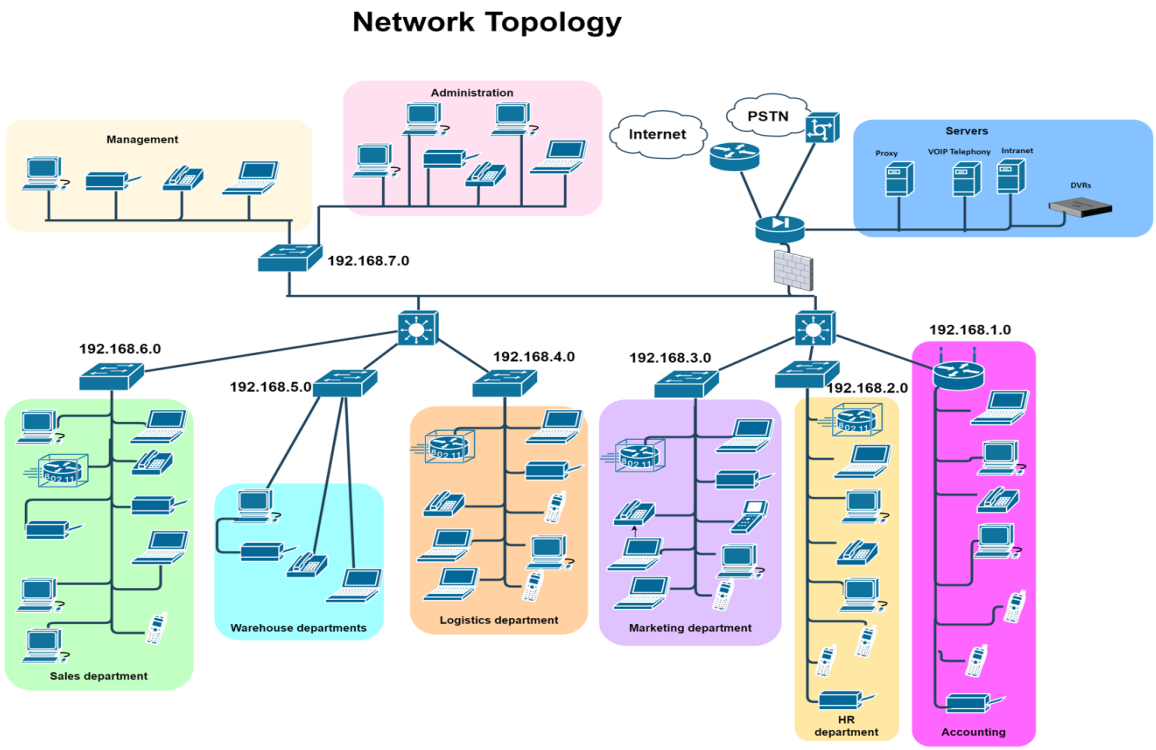

Figure 8. Network topology proposal

To determine what risks will be mitigated, it's crucial to determine the expected opportunity loss, which will dictate what investment is reasonable and viable, including its self-financing. In pursuance of implementing protection strategies, it is important to know what criteria assets have a higher impact regarding the risk. Along with verifying if the organization's current employees can apply these business practice improvements to the current processes.

In addition, it is relevant to evaluate the risk trigger, as these identified risks might be triggered by other risks, that in the worst-case scenario could increase its criticality, which can generate a business loss. Also, cybercriminals can take advantage of this through phishing, ransomware, smishing, vishing, etc. [20] that will confirm the data breach, and as a result, will affect the organization's reputation.

3. RESULTS AND DISCUSSIONS

In Figure 8, a network topology is used to mitigate cyber risk in an organization [21]. At first, the criteria assets and mitigation plans are established [22, 23]. The Active Directory allows them to store information from the organization's electronic devices, making it easy to access the data and blocking unauthorized users from the network. Together with the use of the VLAN configuration in all the departments in order to block unnecessary access and safeguard confidential information, as well as this proposal is also suggesting the implementation of a firewall to provide a higher level of protection and security. Along with the DVR access to store images and videos from network manipulation. Also, this access will be controlled through VNP. This is because

regardless of the size of the company, whether it is an SME or a large enterprise, all businesses that handle confidential employee, customer and supplier information are in some way vulnerable to spam, DDoS attacks, mobile malware and data theft, and many other cybersecurity challenges.

It should be clarified that the topology was designed considering the organizational structure and functional areas of a commercial company in the Peruvian market. The topology was designed as a tree topology, known as such because it maintains a configuration in which the nodes are placed in the form of a tree. It should be noted that this topology presents a series of advantages that favor organizations such as, for example, hierarchy and control in terms of entry, administration and access to information within the network, which provides a higher level of security.

This topology is very useful to be able to carry out a network extension, as well as to perform centralized monitoring that allows users to easily control and manage the organization's network, as well as to detect errors, find faults in the network, and promptly allow the administrator to correct the error on the spot.

3.1 Comparison chart

In Figure 9, it is demonstrated that the implementation of security policies based on this proposal had a positive impact. According to the author [24], in order to set security policies in the IT infrastructure it is recommended to do a report before and after its implementation [25], to do an accurate comparison and know if the changes did work or need to be reformulated back to the initial stage. Regarding this, during the developing process of this proposal, it was taken into consideration the evaluation of preconditions and postconditions of these assets and security policies in the IT infrastructure to evaluate the risks and show the input of the new updates and changes (see Table 4).

According to Podrecca et al. [26] and Martín [27], Cyber security is based on policies regarding ISO 27001, an international standard, whose best practices help develop effective Information Security Management Systems. Along with Figure 9, the graphs and percentages evidence that there was not a proper risk evaluation [28], and in some cases, they were not aware of the vulnerabilities in the IT infrastructure [29]. However, after the implementation of this proposal, you can see an increase in risk and vulnerability mitigation [30], and as a result, good cyber-security practices [31-33].

Table 4. Comparison of beginning and end

Domain Description	Start	Final
Knowledge of Vulnerable Areas	40%	93%
Personnel Trained for Cyber Attacks	45%	99%
Information Access Control	65%	97%
Information Backup	40%	99%
Security Policy	55%	99%
Secure Network Topology	53%	99%
Protection Strategy Plan	40%	89%
Suitable Hardware	58%	95%
Certified Software	53%	97%
Security Practices Computing	45%	80%
Acquisition, Development and Maintenance	45%	98%
Suspicious Threats Blocked	20%	91%
Compliance	40%	90%
% Total Compliance	**46%**	**94%**

Undoubtedly, the role played by the ISO 27001 standard is fundamental in the protection of data and privacy in organizations, since information security can be protected in any type of company, regardless of its size and the economic activity to which it is dedicated. In addition, ISO 27001 standards ensure compliance by identifying requirements, establishing the Information Security Management System (ISMS), documenting the ISMS, implementing the ISMS, evaluating the ISMS and continually improving the organization, which means that the business has followed appropriate information security practices to manage any potential risks effectively.

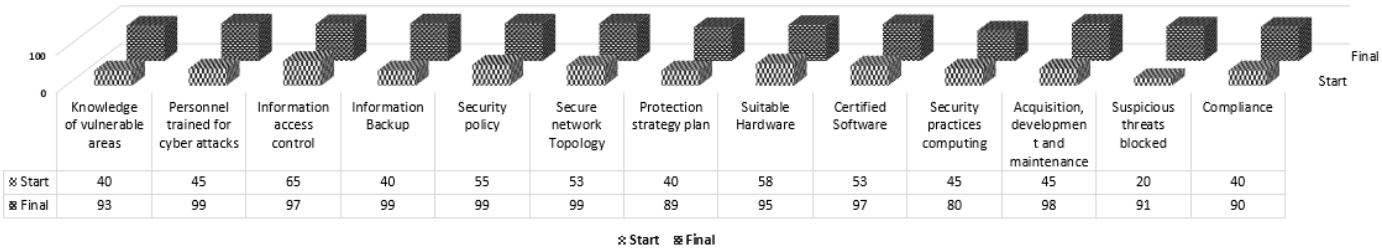

Figure 9. Comparative chart of indicator analysis

4. CONCLUSIONS

From this proposal, we conclude that the security and audit models of information systems based on the Octave v2.0 methodology improve the management of the most valuable assets of an organization in Peru or in any other country in the region, regardless of its location, size, complexity or industrial sector, allowing the business to analyze the situation from a strategic perspective in order to prevent any possible cyber-attack or information breach in any of its areas. Likewise, the importance of hardware and software in an organization is vital, as it provides an overview of the needs of a company such as the absence of an adequate network topology, in addition to the use of equipment with unlicensed software, poor management of cabling, the lack of a diagnosis by department in an organization, leaving it exposed to potential cyber threats and vulnerabilities in unprotected systems.

Considering this in mind and after making a diagnosis, it concluded that several organizations do not have an efficient network architecture that protects their most valuable assets from cyber-attacks or network vulnerability. This represents a major problem regarding the network topology and if there's no appropriate implementation of the network architecture, it would be harder to manage the information and accomplish the expectation set, such as availability, functionality, security, manageability, usefulness and feasibility. Furthermore, most

of the organizations which have been affected by this, do not invest in cyber-security to keep the network, electronic devices, and data safe to face potential cyber-attacks, nor follow international standards, such as ISO 27001, in order to safeguard sensitive information regarding the principle of confidentiality; this increases the number of organizations that are victims of cyber-attacks at a regional level.

On the other hand, several organizations don't have trained staff that have knowledge of departments that have critical assets; or employees that can counteract any type of cyber-attack. Regarding this, we recommend that organizations invest in technological solutions that help them detect spam emails, outdated software, and obsolete electronic devices that are compliant with our security policies. Besides, a risk evaluation takes place to protect the organization's information and evaluate where we can find weaknesses, making an incident report as a preventive measure for potential cyber-attacks. Although there were some difficulties such as limited access to the security policies used in the private sector, there are also ethical limitations, since the research involves the use of sensitive or confidential data, which became a challenge at the time of collecting the information. This research is conducted as a support for future research and activities that can follow up on the quality of information regarding the security policies used in Peruvian organizations, but also so that future researchers can conduct an analysis of the economic and non-economic benefits brought about by the implementation of ISO 27001 in organizations. Finally, this work also includes a list of indicators and dimensions that can help to improve their weaknesses in this area.

REFERENCES

[1] Chupin, A., Chupina, Z., Pavlova, A., Skudalova, T., Andreeva, E. (2023). Innovation and IT Technologies as the Main Element of a Dynamic Business Model. In: Guda, A. (eds) Networked Control Systems for Connected and Automated Vehicles. NN 2022. Lecture Notes in Networks and Systems, vol 509. Springer, Cham. https://doi.org/10.1007/978-3-031-11058-0_114

[2] Al-Rwaidan, R.M., Aldossary, N., Eldahamsheh, M.M., Al-Azzam, M.K.A., Al-Quran, A.Z., Al-Hawary, S.I.S. (2023). The impact of cloud-based solutions on the digital transformation of HR practices. International Journal of Data and Network Science, 7(1): 83-90. https://doi.org/10.5267/J.IJDNS.2022.12.003

[3] Suryanto, A., Nurdin, N., Irawati, E., Andriansyah. (2023). Digital transformation in enhancing knowledge acquisition of public sector employees. International Journal of Data and Network Science, 7(1): 117-124. https://doi.org/10.5267/J.IJDNS.2022.11.011

[4] Guru, K., Raja, S., Sasiganth, J., Sharma, D.K., Tiwari, M., Tiwari, T. (2023). The future impact of technological developments on digital marketing through artificial intelligence. Smart Innovation, Systems and Technologies, 290: 217-225. https://doi.org/10.1007/978-981-19-0108-9_23

[5] Mittal, A., Garg, U. (2022). A review for insider threats detection using machine learning. Innovations In Computational and Computer Techniques: ICACCT-2021, 2555: 020006. https://doi.org/10.1063/5.0108887

[6] Salami Pargoo, N., Ilbeigi, M. (2023). A scoping review for cybersecurity in the construction industry. Journal of Management in Engineering, 39(2). https://doi.org/10.1061/JMENEA.MEENG-5034

[7] Singh, M., Aujla, G.S., Bali, R.S. (2022). Derived blockchain architecture for security-conscious data dissemination in edge-envisioned Internet of Drones ecosystem. Cluster Computing, 25(3): 2281-2302. https://doi.org/10.1007/s10586-021-03497-9

[8] Alberts, C.J., Dorofee, A.J. (2001). OCTAVE SM Method Implementation Guide Version 2.0 Volume 1: Introduction. https://insights.sei.cmu.edu/documents/17/2001_012_001_51564.pdf.

[9] Pyka, M., Sobieski, Ś. (2012). Implementation of the OCTAVE methodology in security risk management process for business resources. Advances in Intelligent and Soft Computing, 118: 235-252. https://doi.org/10.1007/978-3-642-25355-3_21/COVER

[10] Pacheco, A.E., Luis, F., Santamaría, I.S., Hover, J., Chacón, G. (2010). Aplicar la Metodología OCTAVE de Identificación de Amenazas y Vulnerabilidades en una Entidad Bancaria.

[11] Alberts, C., Dorofee, A., Stevens, J. (2003). Introduction to the OCTAVE ® Approach.

[12] Pupentsova, S., Livintsova, M. (2022). The Enterprises Risk Management in the Context of Digital Transformation. In: Manakov, A., Edigarian, A. (eds) International Scientific Siberian Transport Forum TransSiberia - 2021. TransSiberia 2021. Lecture Notes in Networks and Systems, vol 403. Springer, Cham. https://doi.org/10.1007/978-3-030-96383-5_129

[13] Luh, R., Temper, M., Tjoa, S., Schrittwieser, S., Janicke, H. (2020). PenQuest: A gamified attacker/defender meta model for Cyber security assessment and education. Journal of Computer Virology and Hacking Techniques, 16(1): 19-61. https://doi.org/10.1007/S11416-019-00342-X

[14] Alfarisi, S., Surantha, N. (2022). Risk assessment in fleet management system using OCTAVE allegro. Bulletin of Electrical Engineering and Informatics, 11(1): 530-540. https://doi.org/10.11591/EEI.V11I1.3241

[15] Stanikzai, A.Q., Shah, M.A. (2021). Evaluation of cyber security threats in banking systems. 2021 IEEE Symposium Series on Computational Intelligence, SSCI 2021 – Proceedings, Orlando, FL, USA. https://doi.org/10.1109/SSCI50451.2021.9659862

[16] Shokry, M., Awad, A.I., Abd-Ellah, M.K., Khalaf, A.A.M. (2023). CORAS model for security risk assessment in advanced metering infrastructure systems. Lecture Notes on Data Engineering and Communications Technologies, 152: 449-459. https://doi.org/10.1007/978-3-031-20601-6_39

[17] Gerunov, A. (2023). Risk in Digital Assets. In: Risk Analysis for the Digital Age. Studies in Systems, Decision and Control, vol 219. Springer, Cham. https://doi.org/10.1007/978-3-031-18100-9_3

[18] Li, B., Ma, M. (2023). An advanced hierarchical identity-based security mechanism by blockchain in named data networking. Journal of Network and Systems Management, 31(1): 13. https://doi.org/10.1007/S10922-022-09689-X

[19] Alkanhel, R., Abouhawwash, M., Sangeethaa, S.N., Venkatachalam, K., Khafaga, D.S. (2023). Wireless network security using load balanced mobile sink technique. Intelligent Automation and Soft Computing,

35(2): 2135-2149. https://doi.org/10.32604/iasc.2023.028852
[20] Chanti, S., Chithralekha, T. (2022). A literature review on classification of phishing attacks. International Journal of Advanced Technology and Engineering Exploration, 9(89): 446-476. https://doi.org/10.19101/IJATEE.2021.875031
[21] Fakiha, B. (2021). Business organization security strategies to cyber security threats. International Journal of Safety and Security Engineering, 11(1): 101-104. https://doi.org/10.18280/ijsse.110111
[22] Noel, S., Swarup, V., Johnsgard, K. (2021). Optimizing network microsegmentation policy for cyber resilience. Journal of Defense Modeling and Simulation, 20(1). https://doi.org/10.1177/15485129211051386
[23] Lainjo, B. (2020). Network security and its implications on program management. International Journal of Safety and Security Engineering, 10(6): 739-746. https://doi.org/10.18280/ijsse.100603
[24] Chillur, N., Patel, A., Patel, S., Swain, D. (2022). Deep Analysis of Attacks and Vulnerabilities of Web Security. In: Singh, P.K., Wierzchoń, S.T., Chhabra, J.K., Tanwar, S. (eds) Futuristic Trends in Networks and Computing Technologies. Lecture Notes in Electrical Engineering, vol 936. Springer, Singapore. https://doi.org/10.1007/978-981-19-5037-7_78
[25] Pasino, A., De Angeli, S., Battista, U., Ottonello, D., Clematis, A. (2021). A review of single and multi-hazard risk assessment approaches for critical infrastructures protection. International Journal of Safety and Security Engineering, 11(4): 305-318. https://doi.org/10.18280/ijsse.110403
[26] Podrecca, M., Culot, G., Nassimbeni, G., Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. Computers in Industry, 142: 103744. https://doi.org/10.1016/J.COMPIND.2022.103744
[27] Martín, T.R. (2021). Automation of an information security management system based on the ISO/IEC 27001 standard. Universidad y Sociedad, 13(5): 495-506.
[28] Pandey, S.K. (2012). A comparative study of risk assessment methodologies for information systems. Bulletin of Electrical Engineering and Informatics, 1(2): 111-122. https://doi.org/10.11591/EEI.V1I2.231
[29] Dorothy, R., Sasilatha. (2017). Smart grid systems based survey on cyber security issues. Bulletin of Electrical Engineering and Informatics, 6(4): 337-342. https://doi.org/10.11591/EEI.V6I4.862
[30] Al-Hazaimeh, O.M., Abu-Ein, A.A., Al-Nawashi, M.M., Gharaibeh, N.Y. (2022). Chaotic based multimedia encryption: A survey for network and internet security. Bulletin of Electrical Engineering and Informatics, 11(4): 2151-2159. https://doi.org/10.11591/EEI.V11I4.3520
[31] Negabi, I., El Asri, S.A., El Adib, S., Raissouni, N. (2023). Convolutional neural network based key generation for security of data through encryption with advanced encryption standard. International Journal of Electrical and Computer Engineering (IJECE), 13(3): 2589-2599. http://doi.org/10.11591/ijece.v13i3.pp2589-2599
[32] Tabassum, N., Devanagavi, G.D., Biradar, R.C., Ravindra, C. (2023). Survey on data aggregation based security attacks in wireless sensor network. International Journal of Electrical and Computer Engineering (IJECE), 13(3): 3131-3139. https://doi.org/10.11591/IJECE.V13I3.PP3131-3139
[33] Nandalal, D.K., Bhakthavatchalu, R. (2023). Design of programmable hardware security modules for enhancing blockchain based security framework. International Journal of Electrical and Computer Engineering (IJECE), 13(3): 3178-3191. https://doi.org/10.11591/IJECE.V13I3.PP3178-3191