Articles

Vulnerability of the technological infrastructure of the Salinas Fire Department, year 2023

Vulnerabilidad de la infraestructura tecnológica del Cuerpo de Bomberos de Salinas, año 2023

Luigi Villafuerte Clavijo*
Byron Oviedo Bayas*

REVISTA TECNOLÓGICA
ciencia y educación
Edwards Deming

ISSN: 2600-5867

Edited by: Tecnológico Superior Corporativo Edwards Deming
July - December Vol. 8 - 2 - 2024
https://revista-edwardsdeming.com/index.php/es
e-ISSN: 2576-0971
Received: Febrary 19, 2024
Approved: June 12, 2024
Page 10-31

ABSTRACT

The present research addressed the critical issue in the field of cybersecurity. The technological infrastructure of the Salinas Fire Department is exposed to significant risks due to the growing threat of cyber attacks. Given this situation, the main objective of the research was to assess the cyber risks present in the institution's information technology (IT) infrastructure. To achieve this objective, the methodology of risk analysis and management of information systems known as MAGERIT was employed, providing a systematic and structured framework to identify, analyze, and manage risks related to information security in an organization. In the context of this research, this methodology was applied to conduct a comprehensive risk analysis of the institution's infrastructure. During the analysis, risk levels were verified in each department, identifying critical areas of vulnerability that could compromise the integrity and operational effectiveness of the institution. The results confirmed the existence of critical areas of vulnerability that require immediate attention. For this reason, the creation of a contingency plan was proposed to reduce the risks identified during the analysis. This plan includes specific measures to strengthen the security of the Salinas Fire Department's technological infrastructure and ensure its operational effectiveness against potential cyber attacks.

* Msc. Universidad Península de Santa Elena | Facultad de Posgrado | La Libertad-Santa Elena | Ecuador, https://orcid.org/0009-0003-9995-5551, Email: luigi.villafuerteclavijo0878@upse.edu.ec

* Ph.D Universidad Técnica Estatal de QuevedoQuevedo - Los Ríos, Ecuador, https://orcid.org/0002-5366-5917, boviedo@uteq.edu.ec

Articles
Revista tecnológica ciencia y educación Edwards Deming
ISSN: 2600-5867

Keywords: cybersecurity, technological infrastructure, MAGERIT, risk management, vulnerabilities

RESUMEN

La presente investigación abordó la cuestión crítica en el campo de la ciberseguridad. La infraestructura tecnológica del Cuerpo de Bomberos de Salinas está expuesta a importantes riesgos debido a la creciente amenaza de los ciberataques. Ante esta situación, el objetivo principal de la investigación fue evaluar los riesgos cibernéticos presentes en la infraestructura de tecnologías de la información (TI) de la institución. Para alcanzar este objetivo, se empleó la metodología de análisis y gestión de riesgos de los sistemas de información conocida como MAGERIT, que proporciona un marco sistemático y estructurado para identificar, analizar y gestionar los riesgos relacionados con la seguridad de la información en una organización. En el contexto de esta investigación, esta metodología se aplicó para realizar un análisis de riesgos exhaustivo de la infraestructura de la institución. Durante el análisis, se verificaron los niveles de riesgo en cada departamento, identificando las áreas críticas de vulnerabilidad que podrían comprometer la integridad y la eficacia operativa de la institución. Los resultados confirmaron la existencia de áreas críticas de vulnerabilidad que requieren atención inmediata. Por esta razón, se propuso la creación de un plan de contingencia para reducir los riesgos identificados durante el análisis. Este plan incluye medidas específicas para reforzar la seguridad de la infraestructura tecnológica del Cuerpo de Bomberos de Salinas y garantizar su eficacia operativa frente a posibles ciberataques.

Palabras clave: ciberseguridad, infraestructura tecnológica, MAGERIT, gestión de riesgos, vulnerabilidades

INTRODUCTION

The growing dependence on technology in contemporary institutions has led to a significant increase in the vulnerability of their infrastructures to cyber threats (Mogollón Flores, 2017). We live in an era of constant challenges in the battle to preserve data privacy, where cybercriminals lurk in every corner, taking advantage of technology to conduct detailed vulnerability analysis and discover flaws in security devices previously considered secure (Robles Puentes, 2018).

Articles
Revista tecnológica ciencia y educación Edwards Deming
ISSN: 2600-5867

In an information system, failures can affect all elements, with information being considered the most vulnerable factor. While hardware and other physical components are replaceable, damaged information is not always recoverable, which can cause economic and reputational damage to the organization, as well as harm to individuals. It is emphasized that most security failures are attributable to human error (Baca Urbina, 2017).

Damage resulting from lack of security can result in financial or reputational loss to an organization. These damages can originate fortuitously, such as accidental errors, power outages or natural catastrophes, or fraudulently, through malicious software, intruders, misconduct of personnel with access to the system, theft and provoked accidents (Baca Urbina, 2017).

Companies such as Uniscan and CNEL EP have conducted an analysis of their network infrastructure with Kali Linux, Nessus, NMAP tools to identify risk levels in data transfer. In this context, it was crucial to examine the security of key entities, such as the Salinas Fire Department (CBS), which not only plays a vital role in protecting the community, but also manages a technological infrastructure essential to its internal operations.

The CBS not only has a dedicated systems unit, but also hosts a network consisting of approximately 21 computers, a database server, router and switch. In addition, the institution uses institutional e-mail and maintains an official website that hosts administrative information crucial to its operation. This set of technological elements, although fundamental for optimizing internal operations, also becomes a potential target for various types of computer attacks.

To mitigate the negative effects of these attacks, procedures and best practices were employed that facilitated the fight against criminal activities, significantly reducing the margin of action of the attacks (Mieres, 2009). (Mieres, 2009).

Education stands out as one of the most crucial steps in security. Understanding the most common weaknesses susceptible to exploitation and understanding the associated risks provides insight into how a cyber attack is carried out. This helps to identify weaknesses and risks, allowing the strategic and intelligent implementation of effective security measures. (Mieres, 2009).

In the past, the CBS network has faced a series of threats, ranging from DNS attacks to intrusions using techniques such as SQL injection and the propagation of malware. These events underscored the urgent need to evaluate and strengthen the security of the institution's technological infrastructure, thus guaranteeing the integrity, confidentiality and availability of the administrative information circulating on its network.

This study focused on analyzing and identifying the vulnerabilities of CBS's technological infrastructure, applying a methodology that revealed the weaknesses of the infrastructure and allowed correcting the problems, highlighting the importance of implementing effective security measures to protect not only critical administrative data, but also the operational capacity of an entity vital to the security and well-being of the community.

Articles
Revista tecnológica ciencia y educación Edwards Deming
ISSN: 2600-5867

The scientific problem addressed in this study focused on the vulnerability of the CBS technological infrastructure to constantly evolving threats.

In their paper entitled "Prevention in Cybersecurity: Focus on Technological Infrastructure Processes", M. Cando and P. Medina (2021) focused on reviewing the existing literature on processes related to the prevention of cyber-attacks targeting technological infrastructures. This review was carried out by examining Spanish and English sources indexed in databases such as Scopus, Scielo, Dialnet and Microsoft Academic Search. The findings of their study were synthesized to define and establish good technological practices, as well as to propose actions aimed at preventing attacks and fostering the creation of innovative and adaptable technological environments for companies.

J. Delgado (2019) conducted a research entitled "Analysis and Evaluation of Risks in the Technological Infrastructure of the Second Local of the Piura Regional Government using the Magerit Methodology". In this study, the MAGERIT methodology was used and the identification of 348 assets was carried out, including computers, communication assets, information support, auxiliary equipment, among others. For data collection, the author used observation guides in the form of log sheets, where information assets, threats, vulnerability analysis and safeguards were recorded.

H. Bolaños, J. Cruz, and J. Reyes. (2018) conducted an assessment of the security platforms and servers in the technological infrastructure, which revealed that the Keralty entity lacked well-defined security policies in general. As a result, they proceeded to debug internal firewall policies and perform a vulnerability scan on servers in the company's pre-production environment. In addition, they presented a proposal to improve the vulnerabilities identified in the servers, and for the firewall, they carried out an intervention following the best practices manual provided by the manufacturer. The authors developed a proprietary methodology consisting of five phases: Initial, Planning, Execution, Analysis of Results and Delivery of Results.

A. Sossa (2017) conducted a study with the purpose of establishing a remediation plan for critical vulnerabilities identified during an intrusion assessment conducted on the technological infrastructure of a Colombian bank in October 2016. To develop this plan, the author used two methodological approaches: one based on penetration testing, consisting of four stages (evasion of network access controls, remote privilege escalation, discovery of assets and services, inspection and exploitation of vulnerabilities), and another based on risk management according to ISO 27005.

B. Aviles (2023) in his research entitled "Application of the threat hunting process for the detection of vulnerabilities and countermeasures in the network infrastructure of the Ambato Fire Department" proposed the creation of a detailed manual to deploy the Threat Hunting process in the network of that entity. In this process, several specialized cybersecurity tools were used, such as Wireshark, Nessus and Advanced IP Scanner. This research not only identified security weaknesses, but also facilitated the planning of several corrective measures aimed at reinforcing the vulnerable points found in the network.

Articles
Revista tecnológica ciencia y educación Edwards Deming
ISSN: 2600-5867

M. Guamán et al. (2023) conducted a study focused on analyzing cybersecurity risks and threats affecting Ecuadorian government assets. The researchers employed the MAGERIT methodology to identify and classify threats, vulnerabilities and risks, assigning them to critical assets in areas such as government, health and energy. Threats were categorized according to their origin, such as user error, technical failures, deliberate attacks, and natural disasters. The evaluation of the potential impact of each threat in terms of confidentiality, integrity and availability, together with the estimation of the probability of occurrence, made it possible to calculate the level of risk in order to prioritize mitigation actions. The results highlighted that the assets with the highest risks include citizens' personal and financial data, medical records and confidential government information.

The objective of the research project "Evaluation of Information Security under the ISO/IEC 27001 Standards in the Technological Infrastructure of the State University of Milagro" carried out by R. Ramírez (2022) was to identify the vulnerabilities present in the entity with the purpose of improving its technological infrastructure. This was done in accordance with the ISO/IEC 27001 standard, in order to reduce risks in the institution's information systems. The author used the Failure Mode and Effects Analysis (FMEA) methodology to evaluate the risk level of each component, which allowed him to take mitigation measures to protect the integrity of the information. As a result of this research, a list of recommendations aimed at improving information security, based on the vulnerabilities identified, was drawn up.

Researchers R. Avila and J. Cuenca (2021) in their study entitled "Risk Analysis and Evaluation: Applied to EMAPAL-EP, based on the MAGERIT Methodology version 3.0", set out to obtain a quantitative evaluation of risk analysis management in the company. Using the Magerit methodology, the result of their research was the formulation of a plan to address the risks identified and analyzed, with the objective of mitigating them or leaving them in an acceptable state.

Y. Viteri, M. Cano and A. Zambrano (2019) carried out an analysis of the vulnerabilities present in the technological infrastructure of the Universidad Laica Eloy Alfaro de Manabí. For this purpose, they used the Failure Mode and Effects Analysis methodology to evaluate the probability and impact levels of the risks. In addition, they used the MAGERIT methodology to identify the unit's assets and the threats to which they could be exposed. As a result of this study, they developed a Continuity Management Model, which consists of several phases, including Business Continuity Plan Scoping, Risk Assessment, Business Impact Analysis, Recovery Strategies and Plan Development.

In their research project entitled "Exploration of Vulnerabilities in the Technological Infrastructure of an Enterprise using Intrusion Testing Tools," researchers E. Yánez and L. Parra (2017) conducted a detailed examination of the vulnerabilities present in the infrastructure of the educational institution "Culinary School of the Americas". Their main objective was to identify potential security threats in the network, employing the Open Security Testing Methodology (OSSTMM) and network auditing tools in the analysis process.

Articles
Revista tecnológica ciencia y educación Edwards Deming
ISSN: 2600-5867

The MAGERIT methodology (Methodology for the Analysis and Management of Information Systems Risks) is a framework developed by the Spanish National Cryptologic Center (CCN-CERT), and has been conceived as a comprehensive approach to risk management in information systems. Its design provides a structured and comprehensive framework that facilitates the assessment, analysis and effective management of the risks associated with information security (Andrade Talero, 2021).
The main phases of the methodology are:
Start: This phase involves establishing the objectives and scope of the risk analysis, identifying the relevant information assets and defining the criteria for assessing risks.
Asset analysis: In this phase, the organization's information assets are identified and classified, including data, systems, infrastructure and human resources.
Identification of threats and vulnerabilities: Potential threats that could affect information assets are identified, as well as vulnerabilities that could be exploited by these threats.
Risk assessment: The probability of occurrence of the identified threats and the potential impact they would have on the information assets is evaluated. This allows prioritizing risks and focusing mitigation efforts on the most critical areas.
Risk treatment: In this phase, strategies are developed to mitigate, transfer, avoid or accept the identified risks. Controls and security measures are established to reduce the probability of occurrence of threats and minimize their impact should they occur.
Monitoring and review: The risks and controls implemented are monitored and reviewed periodically to ensure that they remain effective and adequate as conditions in the organization's environment change.
Author R. Naveiro (2022) defines risk analysis in his book as a systematic and analytical procedure to assess, manage and communicate risks in order to mitigate or eliminate them as far as possible. Its purpose is to understand the potential negative consequences of hazards on human life, health, our assets or the environment. Similarly, the author of the book "IT Risk Analysis Methodology" considers that IT risk assessment involves identifying and assessing the threats and vulnerabilities that impact information security, in order to determine the level of risk to which it is exposed. This process provides the organization with a detailed and accurate understanding of the areas where security controls should be implemented and their specific nature. (Pagliari and Eterovic, 2012)..
Risk analysis comprises three fundamental stages (Naveiro Flores and Ríos Insúa, 2022):
1. Risk assessment: Focused on gathering information on the probability and impacts associated with threats that could affect a system should they materialize.
Risk management: Includes activities aimed at controlling threats in order to reduce the probability of their occurrence and/or reduce their impact should they occur.
3. Risk communication: Consists of the exchange of opinions and information about risks and related factors between assessors, managers and any other party involved in the problem.
The level of risk is based on probability and impact levels, as shown in Table 1:

Table 1. *Risk Levels*

Risk Level	Action required for risk treatment
High	Unacceptable: action must be taken as soon as possible.
Medium	Actions required and to be taken within a reasonable period of time.
Under	Acceptable: no actions are required as a result of the risk assessment.

CCN-CERT defines the term "impact" as the measure of the damage suffered by an asset as a result of the materialization of a threat. By knowing the value of assets in different dimensions and the degradation caused by threats, it is possible to directly determine the impact that these would have on the system.

Probability

In the context of risk management, the term "probability" is used to express the possibility of an event occurring, the occurrence of which may be established, measured or determined objectively or subjectively, both qualitatively and quantitatively, and is described using general terms or mathematically.

Technological Infrastructure

Resources are defined as the assets, both tangible and intangible, available to carry out tasks. Available information is considered an intangible asset, including customer databases, suppliers, production manuals, research and patents. On the other hand, tangible assets include the company's physical resources, such as servers, network equipment, computers, smartphones, vehicles, real estate, among others. (Romero Castro et al., 2018)..

The basis of any organization at the global level is found in the IT infrastructure or equipment, which includes servers, network equipment, computers and their management tools. (Cando Segovia and Medina Chicaiza, 2021).. The security applied to this infrastructure is a critical factor that ensures the operational continuity, image and integrity of the organizations. (Santiago Chinchilla and Sánchez Allende, 2017).. According to the analysis of Gómez and Parra the protection of technological infrastructures that support essential services has acquired a significant priority for nations and organizations, given the growing dependence on these that is increasing exponentially every year (Gómez and Parra, 2017).. Similarly, Roy highlights that cybersecurity aims to preserve the availability and integrity of networks and technological infrastructures, as well as to maintain the confidentiality of the information hosted on these platforms (Roy, 2017).

Computer security encompasses the development of standards, procedures, methods and techniques designed to achieve a secure and reliable information system. (Aguilera

Articles
Revista tecnológica ciencia y educación Edwards Deming
ISSN: 2600-5867

López, 2010). Other authors define it as a discipline that, supported by the company's internal and external policies and regulations, is responsible for safeguarding the integrity and privacy of the information stored in a computer system. Its objective is to prevent any type of threat, minimizing both physical and logical risks to which the information may be exposed (Baca Urbina, 2017)however, despite the security precautions applied to an information system, there is always a level of inherent risk (Aguilera López, 2010).
The author Aguilera in his book indicates that in order to establish a security system, it is crucial to understand the following aspects (Aguilera López, 2010):
The composition of the elements that make up the system, obtained through interviews with those responsible for the organization and direct observation.
Hazards that may affect the system whether accidental or intentional, revealed through data provided by the organization and direct testing of the system.
The measures necessary to know, prevent, impede, reduce or control potential risks, involving the decision on the services and security mechanisms that will minimize risks.
After conducting a risk study and implementing measures, it is essential to carry out periodic monitoring to review and update the measures taken.
The researcher and author specialized in computer security considers that a system is secure when it complies with the properties of integrity, confidentiality and availability of information, each of which requires the implementation of specific security services and mechanisms. (Aguilera López, 2010). However, the COBIT enterprise not only considers the aforementioned properties, it also adds effectiveness, efficiency, compliance with standards, and reliability (Baca Urbina, 2017).
The aspects that IT security must address can be categorized into three fundamental areas: users, information and infrastructure. (Romero Castro et al., 2018).
Vulnerabilities refer to weaknesses in security systems or in those that the user employs to carry out their activities, which could allow a threat to successfully cause problems (Romero Castro et al., 2018)..
Today, the presence of both intentional and unintentional attacks is recognized, to which a company is always exposed to varying degrees of vulnerability. When an IT security vulnerability is identified, it is usually the result of a flaw in the design, implementation or operation of the system (Baca Urbina, 2017).
A computer attack implies taking advantage of any vulnerability or failure in the software, hardware or even in the people that make up a computer environment, with the aim of obtaining a benefit, generally of an economic nature, and generating a negative impact on the security of the system, directly affecting the assets of the organization. (Mieres, 2009).
Mieres in his research identifies five common stages of a computer attack when it is executed: Phase 1 Reconnaissance, Phase 2 Scanning, Phase 3 Gaining Access, Phase 4 Maintaining Access, Phase 5 Covering Tracks.
The term "ethical hacking" was initially used by professionals for the purpose of strengthening the security and reliability of systems. A person is designated as an ethical

hacker when he or she works to improve the security of systems, showing caution and safeguarding the system from the perspective of a hacker (Sanchez Avila, 2019).
However, the UNAM-CERT entity mentions that the fundamental purpose of Ethical Hacking lies in taking advantage of the vulnerabilities present in the "target" system by means of intrusion tests, which evaluate both the physical and logical security of information systems, computer networks, web applications, databases, servers, among others. This approach seeks to gain access and "prove" the vulnerability of a system, providing valuable information for organizations to take preventive measures against possible malicious attacks. (UNAM-CERT, 2010).

MATERIALS AND METHODS

The MAGERIT methodology (Methodology for the Analysis and Management of Information Systems Risks) was applied in this study. The application of this methodology sought to identify, evaluate and manage the risks associated with possible threats to information security and the continuity of the institution (CBS), therefore, it was important to adapt this methodology to the specific characteristics of the CBS, considering its technological infrastructure, its operating environment and the most relevant threats. In addition, the active participation of those responsible for and key users of the system was essential for the successful implementation of security measures. The phases that were carried out are presented below.
Asset Identification: The critical assets of the Salinas Fire Department's technological infrastructure were identified, including servers, databases, communication systems and computer applications.
Threat Analysis: Potential threats to the technological infrastructure, such as cyber-attacks, hardware failures, natural disasters and human error, were evaluated.
Vulnerability Analysis: Vulnerabilities in critical assets were identified, considering aspects such as lack of security patches, incorrect configurations and weaknesses in physical and logical access.
Risk Analysis: The impact and probability of occurrence of the risks associated with the identified vulnerabilities were evaluated using the Magerit risk matrix.
Mitigation Strategies: Strategies were designed to mitigate the risks identified, prioritizing those measures that reduce both the probability of occurrence and the impact of the risks.
Phase 1. Contextualization and Scope:
Identification of the operational context of the Salinas fire department, including its critical functions and associated technological infrastructure.
Clear definition of the scope of the analysis, identifying systems, applications and data critical to operations.
Phase 2. Risk Analysis:
Asset Identification: Listing of all technological assets, from servers and communication equipment to software and databases.

Threat Identification: Analysis of potential threats, such as cyber-attacks, natural disasters, hardware failures or human error.
Vulnerability Assessment: Identification of weaknesses in systems that could be exploited by threats.
Impact Assessment: Measurement of the potential impact in terms of interruption of services, loss of data and impact on rescue operations.
Probability Assessment: Determination of the probability of occurrence of identified hazards.
Phase 3. Risk Management:
Risk Prioritization: Classification of risks according to their impact and probability.
Development of Mitigation Strategies: Proposed security measures and plans to reduce the probability or impact of risks.
Contingency Plan: Establishment of plans to respond to incidents and ensure service continuity.
Assignment of Responsibilities: Definition of roles and responsibilities for the implementation and monitoring of security measures.
Phase 4. Security Audit:
Implementation of regular audits to evaluate the effectiveness of security measures.
Updating the risk analysis based on changes in the technological infrastructure or in the threat environment.
Phase 5. Documentation and Communication:
Detailed documentation of all findings, risk analysis and security measures implemented.
Communication of results to stakeholders, including fire department personnel and decision makers.
Phase 6. Follow-up and Continuous Improvement:
Establishment of a continuous safety monitoring and review process.
Learning from past incidents and adjusting security strategies as needed.
The use of this methodology in this project provided a structured and systematic approach to identify, analyze and manage information security risks in the CBS technology infrastructure. It also facilitated informed decision making on the implementation of security measures to protect the integrity, confidentiality and availability of information critical to emergency operations.

RESULTS

This case study consisted of identifying the assets with their respective risks involved in the services provided by the Salinas Fire Department following the MAGERIT methodology.
The analyses performed are qualitative, considering the institution's assets, risks and safeguards, which will help the department in charge of information security to carry out the evaluation and implementation by asset according to priorities.
The results of this research on the vulnerability of CBS's technological infrastructure have highlighted a number of key points that underscore the urgent need to address the

deficiencies in the security of the information and technologies employed by this vital institution for the community. Using the MAGERIT methodology, the identification and assessment of various aspects of the technological infrastructure, from information assets to specific vulnerabilities in web, network and server services, has been carried out.

This study made it possible to identify the threats facing key information assets such as web services, user devices and the server. These threats range from hacker attacks and exposure of confidential data to potential network and server integrity failures. The detailed results of the assessments are presented in the corresponding tables, providing a holistic view of the identified vulnerabilities and associated risks.

Identification of IT assets.

The assets that facilitated the detection of the threats to which they are exposed were identified. Table 1 details these relevant assets, each of which is considered equally important after analyzing their advantages and disadvantages.

Table 2. *CBS Assets*

Number	Information asset
1	Web services
2	User teams
3	Information supports
4	Structured cabling
5	Server
6	Network access equipment

Identification of vulnerabilities and risks.

Different aspects of the CBS's technological infrastructure were identified and evaluated. The results are presented below, detailing the vulnerabilities found and their associated risk level.

Table 3: *Vulnerabilities of the CBS Technological Infrastructure*

N.	Vulnerability	Description	Risk Level
1	Lack of software updates	Outdated operating system and applications	High
2	Weak password management	Weak or shared passwords	Medium
3	Lack of physical and logical access control	Unauthorized access to	High

		facilities and systems	
4	Lack of redundancy in critical systems	Lack of backup in case of hardware failure	Medium
5	Insufficient computer security training	Lack of awareness and training in good practices	Medium

These results underscore the critical need to address the vulnerabilities identified in the technological infrastructure. The implementation of corrective and preventive measures, in line with the recommendations derived from the MAGERIT methodology.

In order to measure the security risk present in the Information Technology (IT) infrastructure of the CBS, it is crucial to select the appropriate tools that are aligned with MAGERIT's principles and objectives. Below is a comparative table of tools that could be considered for this purpose.

Table 4. *Comparative table of tools*

Tool	Type	Vulnerability Scanning	Network Scanning	Protocol Analysis	Web Application Security	License
Open VAS	Vulnerability Scanner	Yes	No	No	No	GPL v2
Nessus	Vulnerability Scanner	Yes	No	No	No	Commercial with free version

Nmap	Network Analysis Tool	Through scripts	Yes	No	No	GPL v2
Wireshark	Protocol Analyzer	No	No	Yes	No	GPL v2
OWASP ZAP	Web Application Security	No	No	No	Yes	Apache 2.0

The choice of Nmap and OpenVAS for the analysis of vulnerabilities in the institution's infrastructure is based on their versatility, efficiency and ability to use custom scripts. The tools stand out for their ability to perform exhaustive network scans in a short time, being compatible with a wide range of operating systems. However, its most notable feature lies in the use of scripts written in the Nmap scripting language (NSE), which automate complex security assessment tasks and allow for the analysis of

Table 5: *Results obtained with the OpenVAS tool*

Department	**High**	**Medium**	**Low**	**Total devices**
Information technology	7	8	4	19
Financial Administrative	1	4	4	9
Accounting	0	4	4	8
Secretary	0	2	6	8
TOTAL	**8**	**18**	**18**	44

The risk analysis was carried out in the Information Technology (I.T.), Administrative Finance (A.F.), Accounting (C.) and Secretariat (S.) departments. Using the OpenVAS tool, the following findings were determined:

In the IT area, 19 IT devices were evaluated, of which 7 are at high risk of suffering a computer attack. It is recommended that immediate mitigation measures be taken. In addition, 8 devices were identified with medium risk and 4 with low risk, suggesting that the high risk level in this area is 36.84%.

In the F.A. area, 9 computing devices were analyzed. Unlike I.T., only 1 device is considered high risk, but 4 devices were found with medium risk and 4 with low risk. This implies that the high risk level in this area is 11.11%.

At the Secretariat, 8 computing devices were examined, with the good news that no high-risk devices were identified. However, as in A.F., 4 devices were found with medium

risk and 4 with low risk, which suggests taking action within a reasonable timeframe. The high risk level in this area is 0%.
As for Accounting, 8 computer devices were also evaluated, without identifying high-risk devices. Two devices were found with medium risk and six with low risk. The high risk level in this area is 0%.

Table 6: *Percentage of the risk level of the CBS's technological infrastructure*

	High Risk Level	**Medium Risk Level**	**Low Risk Level**	**TOTAL**
# of computing devices	8	18	18	44
% of computing devices	18,18%	40,91%	40,91%	100%

In summary, according to the OpenVAS report, CBS has 8 computing devices with a high risk, equivalent to 18.18%, 18 with medium risk, equivalent to 40.91%, and 18 with low risk, also equivalent to 40.91%.

Identification of safeguards
Following the study conducted and the identification of threats and vulnerabilities, the importance of the safeguard measures proposed to mitigate the risks identified in assets, web services, the network and the CBS server is emphasized. These measures are designed to strengthen the security of the technological infrastructure, protecting the confidentiality, integrity and availability of critical information.
The safeguarding measures are presented below in an organized table with the respective dimension to be addressed, highlighting the contingency plan to reduce risks and improve the security of the institution.

Table 7: *Information Assets and Safeguarding Measures*

Information Assets	Safeguard	Dimension
Web services	Implement regular security updates	Availability
User teams	Establish strong password policies and change them periodically.	Confidentiality
Information supports	Enforce data encryption and strict access control	Confidentiality, Integrity

Structured cabling	Implement physical security and redundancy measures	Availability, Integrity
Server	Maintain a secure and up-to-date operating system	Availability, Integrity, Confidentiality
Network access equipment	Perform regular firmware and software upgrades	Availability, Confidentiality

Contingency plan for risk reduction

The analysis conducted in the institution presents vulnerabilities that put at risk its most valuable asset, which is the information, so the following contingency plan is proposed as a comprehensive guide to address and reduce the risks identified in the technological infrastructure of the CBS. This model is designed to improve information security, protect critical assets and strengthen the institution's resilience to potential threats.

Table 8: *Proposed Solution for Risk Reduction Web Services*

Category	Vulnerability	Proposed Solution
Web Services	Lack of security updates in web services	Implement regular security updates to patch known vulnerabilities.
	Poor protection against denial-of-service attacks on web services	Use DoS mitigation solutions to protect web services against malicious attacks.
	Lack of encryption in data transmission in web services	Configure SSL/TLS encryption to ensure the confidentiality of information transmitted via web services.

	Exposure of sensitive information in error messages in web services	Modify the server configuration to avoid exposing sensitive information in error messages.
	Vulnerabilities in web applications	Perform periodic security testing and employ web application security solutions to mitigate vulnerabilities.

A proposal for Web Services Risk Reduction is provided, addressing several critical areas of concern in terms of security. First, the lack of security updates in web services can expose the organization to significant risks due to the exploitation of known vulnerabilities. Implementing regular security updates is critical to patch these vulnerabilities and maintain the integrity of web services. In addition, poor protection against denial of service (DoS) attacks can result in serious disruption to web services. Adopting DoS mitigation solutions can help prevent or mitigate the effects of such malicious attacks. Also, the lack of encryption in data transmission represents a major breach in the security of web services, which could compromise the confidentiality of transmitted information. Configuring SSL/TLS encryption is an essential measure to ensure the security of communication between clients and servers. In addition, exposing sensitive information in error messages can provide attackers with valuable information to carry out targeted attacks. Modifying the server configuration to avoid this exposure is a crucial preventive action. Finally, vulnerabilities in web applications are a common concern, and it is critical to perform regular security testing and employ web application security solutions to proactively identify and mitigate these vulnerabilities.

Table 9: *Proposed Solution for Network Risk Reduction*

Category	Vulnerability	Proposed Solution
Web	Lack of network segmentation	Implement network segmentation to limit access between segments and reduce the attack surface.
	No packet filtering	Configure firewalls and intrusion

		detection systems to filter and block unauthorized traffic.
	Vulnerabilities in network devices	Keep network devices up to date with the latest security patches and secure configurations.
	Weak network security configurations	Establish strong security policies, including strong authentication and access control, on network devices.
	Insufficient network monitoring	Implement network monitoring solutions to detect and respond to malicious activity.

Network risk reduction focuses on addressing common vulnerabilities that compromise the security of the network infrastructure. This includes implementing regular security updates to mitigate known vulnerabilities, properly configuring network devices to restrict unauthorized access, implementing SSL/TLS encryption to protect the confidentiality of transmitted information, and implementing intrusion detection solutions to monitor and respond to malicious activity on the network. In addition, the importance of establishing robust data backup and recovery policies along with redundancy mechanisms to ensure continuous availability of network services in the event of failures or incidents is emphasized.

Table 10: *Proposed Risk Reduction Solution for the Server*

Category	Vulnerability	Proposed Solution
Server	Lack of server security patches	Keep the server up to date with the latest security patches and software updates.

	Insecure server service configurations	Configure services securely and disable unused functionality to reduce the attack surface.
	Poor protection against malware and brute force attacks on the server	Use anti-virus and anti-malware solutions to detect and prevent the execution of malware.
	Lack of monitoring and logging of server events	Configure event and audit logs to monitor and record suspicious activity.
	Insufficient access control on the server	Implement strict access control policies and ensure strong authentication of users and administrators.

The lack of security patches on the server represents a significant vulnerability, as known gaps can be exploited by attackers to compromise data integrity and confidentiality. The proposed solution of keeping the server up-to-date with the latest security patches and software updates is essential to close these gaps and ensure protection against known threats. In addition, insecure service configurations on the server can create entry points for attacks, underscoring the importance of configuring services securely and disabling unused functionality to reduce the attack surface. Poor protection against malware and brute force attacks on the server can compromise its integrity and availability, so the use of anti-virus and anti-malware solutions is recommended to detect and prevent the execution of malicious software. Likewise, the lack of monitoring and event logging on the server makes early detection of malicious activity difficult, so the configuration of event logs and audits is essential to quickly identify and respond to potential threats. Finally, insufficient access control on the server can result in unauthorized access and compromise the security of stored data, highlighting the importance of implementing strict access control policies and ensuring strong authentication of users and administrators to protect the integrity and confidentiality of critical data.

DISCUSSION

The collection of data on CBS assets has provided a comprehensive view of its infrastructure and associated vulnerabilities. This process has been crucial in the initial phase of the investigation, making it possible to identify the institution's current weaknesses and the level of risk to which the information circulating within its network is exposed.

Given the diversity of tools available for assessing security risk in an infrastructure, an exhaustive comparative analysis of various options was carried out. As a result of this process, the OpenVAS and Nmap programs were selected to carry out the vulnerability scan. The results obtained with these tools contribute significantly to the evaluation of the level of risk in the infrastructure of the Salinas Fire Department.

The results of the vulnerability scan provided an accurate picture of the current level of risk in the infrastructure of the Salinas Fire Department. Based on these findings, a contingency plan has been proposed with the objective of reducing these risks and guaranteeing greater security for the information available in said institution.

This contingency plan will establish clear guidelines for those in charge of the Salinas Fire Department, in order to strengthen data protection, especially administrative information, which plays a crucial role in the operation of the institution.

REFERENCES

Aguilera López, P. (2010). *Seguridad Informática.* Madrid: Editex. https://doi.org/8497717619, 9788497717618.

Andrade Talero, D. L. (2021). *Analysis of the concepts, elements and techniques of risk management oriented to SMEs in the telecommunications sector based on magerit v3*. UNAD.

Avila-Torres, R. A., & Cuenca-Tapia, J. P. (2021). Risk analysis and assessment: applied to EMAPAL-EP, based on the MAGERIT version 3.0 methodology. *Dominio De Las Ciencias, 7*(4), 363-376. https://doi.org/https://dx.doi.org/10.23857/dc.v7i4.2425. https://doi.org/https://dx.doi.org/10.23857/dc.v7i4.2425

Avilés Vasco, B. J. (2023). Application of the threat hunting process for the detection of vulnerabilities and countermeasures in the network infrastructure of the Ambato Fire Department. *Degree dissertation prior to obtaining the degree of Engineer in Information Technology.* Technical University of Ambato, Ambato. https://repositorio.uta.edu.ec/bitstream/123456789/39618/1/t2416ti.pdf

Baca Urbina, G. (2017). *Introducción a la seguridad informática.* Mexico: Grupo Editorial Patria. https://doi.org/6077444715, 9786077444718

Baloch, R. (2017). *Ethical Hacking and Penetration Testing Guide.* New York: CRC Press. https://doi.org/148223162X, 9781482231625.

Bolaños González, H., Cruz Cuellar, J. M., & Reyes Peñaloza, J. (2018). Identification and proposal of an improvement solution to the computer vulnerabilities of the network and pre-production server environment of the Keralty entity. *Specialization in telematic network security.* Universidad El Bosque, Bogotá. https://repositorio.unbosque.edu.co/server/api/core/bitstreams/887a6923-50ef-4314-8be4-521af12ae051/content

Cando Segovia, M. R., & Medina Chicaiza, P. (2021). Cybersecurity prevention: focused on technological infrastructure processes. *3C TIC. Cuadernos de desarrollo aplicados a las TIC, 10*(1), 17-41. https://doi.org/ https://doi.org/10.17993/3ctic.2021.101.17-41

Delgado Mena, J. E. (2019). Analysis and risk assessment of the technological infrastructure in the second local of the Piura Regional Government using the Magerit methodology. *Thesis to obtain the professional degree of Systems Engineer.* Universidad César Vallejo, Piura. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/59829/Delgado_MJE-SD.pdf?sequence=1&isAllowed=y. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/59829/Delgado_MJE-SD.pdf?sequence=1&isAllowed=y

Gómez, Á. (2022). *Computer security auditing.* Bogotá: Ediciones de la U. https://doi.org/9587628195, 9789587628197.

Gómez, F. S., & Parra, J. L. (2017). Public-private cooperation in infrastructure protection. *Cuadernos de estrategia, 185*, 11-216.

Guamán, M., Carrillo, J. A., Flores Urgilés, C., Flores Urgilés, C., & Ron Egas, M. (2023). Analysis of cybersecurity risks and threats in the Ecuadorian state, using the Magerit methodology. *Pro Sciences: Journal of Production, Science and Research, 7*(49), 139-165. https://doi.org/https://doi.org/10.29018/issn.2588-1000vol7iss49.2023pp139-165

Mieres, J. (January 2009). *Computer attacks: Commonly exploited security weaknesses.* Retrieved January 10, 2024, from https://www.evilfingers.org/publications/white_AR/01_Ataques_informaticos.pdf

Mogollón Flores, F. S. (2017). Cybersecurity challenges and state responses: the case of the Ecuadorian state in the period 2008-2015. *Thesis for the postgraduate degree.* Pontificia Universidad Católica del Ecuador.

Naveiro Flores, R., & Ríos Insúa, D. (2022). *Análisis de riesgos.* Los Libros De La Catarata. https://doi.org/8413524598, 9788413524597

Pagliari, G. A., & Eterovic, J. (2012). *Computer Risk Analysis Methodology.* Editorial Academica Espanola. https://doi.org/3848471841, 9783848471843

Quishpe, H. (2016). Analysis of vulnerabilities in the hierarchical LAN network of the National University of Loja in the area of energy, industries and non-renewable natural resources. *Thesis prior to obtaining the degree of Systems Engineer, Systems Engineering Career.* UNL, Loja.

Ramírez Anormaliza, R. I. (2022). Evaluation of Information Security under the ISO/IEC 27001 Standards in the Technological Infrastructure of the State University of Milagro. *Project prior to obtaining the degree of Magister in Information Technology.* State University of Milagro, Milagro.

Robles Puentes, H. A. (2018). Current overview of computer security or cybersecurity, at the country level and current and future trends globally. *Specialization in computer security.* Universidad Nacional Abierta y a Distancia UNAD, Neiva. https://repository.unad.edu.co/bitstream/handle/10596/24018/haroblesp.pdf?sequence=1&isAllowed=y. https://repository.unad.edu.co/bitstream/handle/10596/24018/haroblesp.pdf?sequence=1&isAllowed=y

Romero Castro, M. I., Figueroa Morán, G. L., & Vera Navarrete, D. S. (2018). *Introduction to computer security and vulnerability analysis.* Portoviejo: 3Ciencias. https://doi.org/8494930613, 9788494930614

Roy, A. M. (2017). Cybersecurity, the external auditor and OCEXs. *Auditoría pública: revista de los Organos Autónomos de Control Externo, 70*, 27-38.

Sánchez Avila, M. A. (2019). Ethical hacking: Impact on society. http://repository.unipiloto.edu.co/handle/20.500.12277/4919.

Santiago Chinchilla, E. J., & Sánchez Allende, J. (2017). Cybersecurity risks in Enterprises. *Technology and Development, XV*, 1-33. http://www.uax.es/publicacion/riesgos-de-ciberseguridad-en-las-empresas.pdf. http://www.uax.es/publicacion/riesgos-de-ciberseguridad-en-las-empresas.pdf

Sossa López, A. M. (2017). Remediation of critical vulnerabilities identified from a penetration test to the technological infrastructure of a Colombian banking institution. *Specialization in computer security*. Universidad Piloto de Colombia, Bogotá. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2655/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2655/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

UNAM-CERT. (October 25, 2010). *Ethical Hacking*. Retrieved January 8, 2024, from https://d1wqtxts1xzle7.cloudfront.net/33438256/VpsUZIU0FmrhWifPrxevcZJonofCM-hAj5Dy1M~1Q7J3LcbZ3W8bvS7Xo06DyWg8VAc1b1uLS2Lo66gtdkMrO1hrQKI5zGVRF05~8hl8h5Ck~a-eJZx1jpA6uw8cevDu4nV5NQJC70Xgp6jLjg6fCr8EEL7ebP7m~zYfS4IRCFwcTMsjOylARG3KzmxDMLHbt0O0WicPziLkx5VT

Viteri Alcívar, Y. A. (2019). Evaluation of the incidences and risks present in the technological infrastructure of the Universidad Laica Eloy Alfaro de Manabí-Ecuador. *Universidad, Ciencia y Tecnología, 23*(94), 62-68. https://doi.org/2542-3401/ 1316-4821.

Yánez Cedeño, E. S., & Parra Barzola, L. M. (2017). Analysis of vulnerabilities in the technological infrastructure of a company using penetration testing tools. *Thesis - Networking and Telecommunications Engineering*. University of Guuayaquil, Guayaquil. https://repositorio.ug.edu.ec/server/api/core/bitstreams/b0d17af0-4885-4d35-8e31-8853ebf609b4/content.