Advances in Science, Technology and Engineering Systems Journal Vol. 7, No. 6, 139-150 (2022)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Prototype to Mitigate the Risks, Vulnerabilities and Threats of Information to Ensure Data Integrity

Segundo Moisés Toapanta Toapanta[1,*], Rodrigo Humberto Del Pozo Durango[2], Luis Enrique Mafla Gallegos[3], Eriannys Zharayth Gómez Díaz[4], Yngrid Josefina Melo Quintana[4], Joan Noheli Miranda Jimenez[5], Ma. Roció Maciel Arellano[6], José Antonio Orizaga Trejo[6]

[1]*Universidad Católica de Santiago de Guayaquil (UCSG), Guayaquil 090615, Ecuador*

[2]*Universidad Estatal de Bolívar (UEB), Guaranda, Km. 3 1/2 vía San Simón, Ecuador*

[3]*Faculty of Systems Engineering, Escuela Politécnica Nacional (EPN), Quito, 17-01-2759, Ecuador*

[4]*Research Department, Instituto Tecnológico Superior Rumiñahui, Sangolquí, 171103, Ecuador*

[5]*Department of Investigation, Gestión de Tecnologías para el Mundo (GTM), Quito, N35-100, Ecuador*

[6]*Department of Information Systems (CUCEA), Universidad de Guadalajara (UDG), Guadalajara,* 45100, *México*

ARTICLE INFO

Article history:
Received: 21 August, 2022
Accepted: 10 November, 2022
Online: 08 December, 2022

Keywords:
Information security
Risks
Vulnerabilities
Security models
Information systems
Systems evaluation
Process control

ABSTRACT

The constant evolution of Information and Communication Technologies, Internet, access to different free software, among others; they generate problems in the management of information security in companies; to mitigate risks, vulnerabilities, and information threats, an alternative was presented considering that information security systems are the basis for decision-making at the government, strategic, tactical, and operational levels. The objective is to design a security prototype applied to business management to mitigate risks, vulnerabilities and threats to information. The deductive method and exploratory research were used for the analysis of the information. Turned out prototypes that allow mitigating risks, vulnerabilities and threats in information management for data control and integrity. It was concluded that the security prototype proposed for a commercial information system; it is security system suitable for public and private companies. In the simulation carried out, it was determined that if the number of risks and threats is high, there will be a greater probability that a problem will arise in the security of the system.

1. Introduction

Information security problems are persistent in most public and private institutions according to what the author's state in this document. To mitigate vulnerabilities, threats and information risks, they define a basic methodology based on Coras, Ebios, Magerit, Cramm, Octave, which have relevant advantages. This document is taken as a reference to continue with the investigation with the objective of presenting additional alternatives [1]. With the constant advances in technology and internet access, it has become easier to access information that is not protected, causing more frequent information security problems, putting at risk the proper management of information, which is one of the main assets of commercial companies [2]. Guaranteeing the correct functioning of the data and the transmission of information from one user to another. The misuse, modification or unauthorized access to information, whether commercial or of any other kind, can affect the privacy or well-being of an organization, person and society. Security models based on rules and policies should be used [3]. The vulnerability is a weakness in the operating system that allows to violate the confidentiality, integrity, availability, access control in systems [4]. The existence of vulnerabilities gives way to threats, which can be external or internal. The threat assessment process is the biggest problem in information security, because the source of vulnerability and threat in an information system can be hidden until the attack begins,

[*] Corresponding Author: Segundo Moisés Toapanta Toapanta, moisestoapanta@hotmail.com

https://dx.doi.org/10.25046/aj070614

which generates insufficient security controls that generate a high level of risk to the organization [5]. To minimize the availability of threats and vulnerabilities in organizations, the risk assessment process is defined, which must be carried out by an expert[6]. By information asset, we mean any good or service used so that institutions or organizations can operate and meet the objectives established in their mission and business vision[7]. Adequate information security requires that organizations determine the risks to which they are exposed, since companies that are dedicated to commercial or economic management frequently report losses due to failures and attacks on their servers. Due to the problems that arise, controls are established for the configuration of processes, hardware equipment, applications and operating systems[8]. Currently, security prototypes must be implemented that determine, analyze, evaluate and classify risks, to implement control mechanisms and prevention measures that will be implemented in the short and long term[9]. Avoiding attacks like DDoS (DDoS attacks take advantage of network capacity limits, allowing them to send multiple requests either in the form of emails with malicious files or links to web pages); Black Hat, Gray Hat, etc. taking into account four main strategies of risk treatment such as: risk avoidance, acceptance, transfer and treatment[10].

Why is it necessary to generate a security prototype to mitigate risks, vulnerabilities and threats for the control and integrity of data in business management?

To mitigate risks in information systems, to avoid large financial losses and reputational damage from misuse of technology by users of an organization.

The objective is to design a security prototype applied to business management to mitigate risks, vulnerabilities and threats to information.The deductive method is applied, exploratory research for the analysis of information related to the research topic.Turned out prototypes that allow mitigating risks, vulnerabilities and threats in information management for data control and integrity.

It is concluded that the security prototype proposed for a commercial information system; it is security system suitable for public and private companies. In the simulation carried out, it was determined that if the number of risks and threats is high, there will be a greater probability that a problem will arise in the security of the system.

2. Materials and Methods

The information from the references detailed below was used to analyze the prototypes oriented to information security in different organizations; to determine which prototype is the most suitable and optimal for security. The design of a prototype takes into account the architecture of the security infrastructure validated in different layers using elements suitable for the infrastructure.

2.1. Related Jobs

Information security is important and a priority for business management; the threats put at risk the operations of the companies the same ones that the CIA can protect[11]. They explore the structure of knowledge, development and future trends in the area of information security; in order to provide a comprehensive review of the literature on information security risks; when incidents occur and cause serious damage to information[12]. Risk assessment processes are one of the most important factors for the development of an information system[13]. They present a comprehensive methodology for IT risk management based on globally accepted standards such as ISO 31000 and ISO/IEC 27005, which define the appropriate requirements for risk management; nevertheless[14]. The authors define those cyber threats generate risks for an organization. To quantify the risks, the differences between the risks of cyber threats and other compliance vectors are analyzed. Results determine actual and potential losses from cyber threats[15]. Absolute reliance on control, monitoring and surveillance mechanisms should be considered risky. They prove to be a useful instrument to indicate the importance of successful information system measures and to reveal weaknesses[16]. A security assessment management database can be used that can store and manage all available versions and translations of the ISO / IEC 15408 and ISO / IEC 18045 series, related documents and all intermediate products in a secure and convenient way[17]. Flexible AC transmission system devices and associated data exchange cybersecurity are necessary for the control of wide-area power networks. They verify published cybergraphic which can significantly hide data sharing[18]. This article focused on the vulnerability of software and the internet and the accumulation of raw information in big data, which are serious problems in computing[19]. The authors proposed the technological capacity they have to mitigate internal threats in computer security systems, with a systematic review of mixed methods[20]. The COBIT guide identifies the level of maturity in ICT management; that allows project management to be more effective and efficient in different areas such as: Information security, software development, etc.[21]. The Chinese Wall security model regulates the binary relationship "Conflict of interest", considers the CIR to be an equivalence relationship, using the Chinese Wall policy as a security model. A security model is a design that promotes consistent and effective mechanisms for defining and implementing controls[22].

In the table 1. Contains the best-known security models. These security models are used to guarantee the confidentiality of the information, because the security models are more precise and detailed, and are used as guidelines to create and evaluate systems.

Table 1: Security Models

Model	Concept	Ref.
Clark-Wilson model	Seeks the security of data integrity, managing the modification of the access control mechanism.	[23]

	This model is based on the classification of applications establishing an order.	
Chinese Wall Model	Oriented to guarantee confidentiality by reducing conflicts of interest, implementing security policies. It consists of access policies implemented on the data, whether applications or databases, preventing the same person from entering two databases of different companies that are in the same business area.	[22]
Bell-LaPadula Model	They focus on the roles of users and objects. They consider arrays to be able to provide access. In this model, it must be checked if the user has authorized access in the assigned security mode, based on their role or work profile.	[24]

The authors conclude that cloud computing is an emerging technology that uses the Honey Bee. Which is similar to cloud access control mechanism [24]. The authors determined an area of cognitive cryptography that is connected with universal cryptosystems, to link cognitive computational models with classical cryptographic procedures. With the combination of cryptographic techniques and cognitive approaches define cognitive cryptography [25]. The authors conclude that security solutions are centralized in the scalability of IoT environments. The IoT ecosystem can include DLT as a layer so that more devices can benefit from its features[26]. Define that cloud computing can provide various server attributes to process information in the cloud, which makes Smart-meter a suitable device [27], OCTAVE Allegro is a guide used by banks for information system risk management. The implementation of risk management focuses on the threats and vulnerabilities of each critical asset it owns, the bank can discover the risks, threats, vulnerabilities with their respective impact on each critical asset [28].

Table 2: Types of Risks

Type	Concept	Ref.
Business Risk	It comes from the effect of uncertainty that arises from the organization's business objectives.	[28]
Investment Risk	It comes from the effect of the uncertainty of the investment objectives of the organization.	[28]
Quality Risk	It comes from the effect of uncertainty towards the quality objectives of the organization.	[28]
Operational risk	It comes from the effect of uncertainty of the operational objectives of the organization.	[28]
Technological Risk	It comes from the effect of uncertainty of the technological objectives of the organization.	[28]
Financial risk	It comes from the effect of uncertainty of the financial objectives of the organization.	[28]

In the table 2. Contains the evaluation of the concepts of the different types of risks implemented in relation to the reviewed articles.

They conclude that an artificial intelligent network is a new way of manipulating an electrical network, which combines information and communication technology; in order to provide more effective and efficient services [29]. The authors determined that large parts of an organization's critical data currently reside in databases, making them an attractive target for cyber attackers. At the same time, cyber attackers increased their skill set leading to sophisticated attacks in the recent past [30]. The authors concluded that real threats can be detected through the assessment of risk values using the expression approach based on quantitative values. Assessment of risk values on qualitative scales is easier for practical implementation [31]. They concluded that a cloud model is qualitative and uses three digital features. They determine that the use of an uncertainty transformation model reflects the theories of confounding and randomness [32]. This article focused on demonstrating the value that a formal risk assessment technique such as EBIOS can have when considering the use of the smart grid, with respect to security solutions [33]. The authors proposed the use of cyber risk insurance products to reduce losses from cyber risk, showing future financial rewards and the benefits of obtaining cyber insurance [34]. The authors propose a risk management model based on the OCTAVE-S methodology and the ISO/IEC 27005 standard. The model has a quantitative approach that calculates the residual risks based on the effectiveness of the assigned controls [35]. They propose a CMMI model that allows the identification of gaps or weaknesses to establish continuous improvement processes [36]. The authors propose that companies, in order to optimize ICT management, should consider a customized standard prototype or model to save resources; considering methodologies and standards such as: Cobit, ITIL, Coso, ISO 27001, among others [37]. They propose a MePRiSIA security prototype, designed as a risk prevention methodology; considering the human factor in all phases [38]. This article focuses on comparing different methods for measuring and evaluating security risks, highlighting the importance of risk management assessment standards and methods [39]. The authors mention that when administrative processes are affected by cyberattacks, the management of public organizations has serious problems in decision-making [40]. The authors proposed several types of methods that allow to optimize processes and flow in information security; considering as a starting point the definition of vulnerabilities and risk analysis [41]. The authors analyze the practical architecture of vulnerability information exchange for security risk analysis in the automotive sector [42]. The authors propose a model to determine the threats and to be able to calculate the probability of the attacks and the costs of the attacker. They determine that the logs delivered by the IoTRiskAnalyzer program help IoT specialists to define proper system configurations [43]. The authors proposed an ISRM process model that complements information security risk management processes. The ISRM model was adapted from Endsley's situational awareness model [44]. The authors proposed a quantitative method for risk assessment, using formal mathematical distributions with historical data to improve granularity, and make the assessment more realistic with respect to cyber-physical systems in computer systems that use cloud services in general. This methodology supports risks to associated asset-based processes running in the cloud [45]. The authors proposed a quantitative model, so that the interested parties that use the system quantify the risks they assume with the security of their assets regarding the threats, so that the organizations make adequate security decisions. It also allows defining average costs for the problems that are generated by the failure of the systems [46]. The authors propose a semantically enhanced model for security management; classifying the security threats identified by the IDS. The system allows management decisions regarding the selection of security controls to obtain a maximum return on investment in security [47]. They propose a risk assessment method to assess quantitative risk, using fuzzy rules to assess vulnerabilities and uncertainty [48]. They propose a software system with a web application format, to identify, evaluate and neutralize the risks of information and other systems from anywhere [49]. The CORAS method allows the evaluation of security risks for hierarchical processes that can be considered as the basis for the analysis in this investigation [50]. The ISO31000:2009 that allows enterprise risk management (ERM), to improve security management in companies at the corporate level [51].

2.2. Methods

The related methods are detailed below: Cyber Attacks List, Methodologies and security prototype models, Security Prototype Comparative Table, Risk Matrix and Methodology to generate results.

2.2.1. Cyber Attacks List

Computer attacks are considered as malicious attempts or acts by a group of people seeking to identify vulnerabilities with the aim of causing damage or problems to a computer system or network, they occur as a result of some vulnerability or weakness in software or hardware.

Table 3: Cyber Attacks List

Attack	Process	Ref.
Two	Disables access to a system, an application or a machine, in order to block the service for which it is intended; This attack is known as HTTP DoS.	[52]
Cyber espionage	It involves the attacker obtaining confidential information from a user without permission.	[30]
Black hat	They are based on tricking search engines to obtain sensitive information from vulnerable users for malicious purposes.	[53]
Gray hat	Use artificial links with natural patterns, to be able to access in an unnoticed way without using massive or abusive methods.	[40]
Unauthorized access	It consists of unauthorized access to an information system, to obtain access codes or passwords.	[54]

Table 3. described the different attacks that can affect the different information systems.

2.2.2. Methodologies and security prototype models

The methodologies allow a correct analysis of information security risks, which allow creating security prototypes to mitigate security problems.

2.2.3. MAGERIT

It is a public methodology that belongs to the Ministry of Public Administrations and was developed by the Superior Council of Electronic Administration, determining the threats to generate control and improve the protection of assets. Magerit, supports organizations to carry out the evaluation, audit ertification or accreditation process. The only disadvantage of this methodology is that its implementation is expensive, since the assets are converted into economic values, it uses both a qualitative and quantitative model to perform the risk assessment[45].

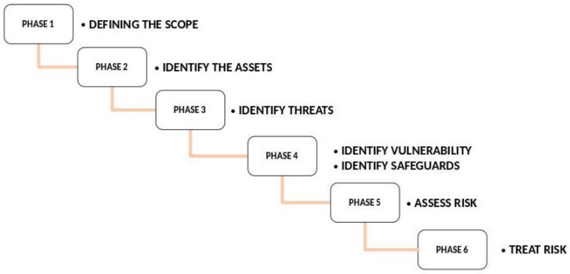

Figure 1: Phases of the Magerit process

In the Figure 1. Each phase a set of equations can be found that will allow to find the value of the estimated annual loss or residual risk. Given the MAGERIT methodology, the following equations can be proposed to find the residual risk value, taking into account the assets that the organization owns, threats and risks that may arise.

$$I = A * D(\%) \tag{1}$$

$$R = I * FA \tag{2}$$

$$RR = [R * (1 - S(\%))] * [0.1 * (1 - ES(\%))] \tag{3}$$

where:
I = Impact
A = Asset Value
D (%) = Percentage of Degradation of a Threat
R = Risk
FA = Estimated annual frequency
S (%) = Percentage of Effectiveness of Safeguards on Impact
ES (%) = Percentage of Effectiveness of Safeguards over frequency
RR = Residual Risk

2.2.4. OCTAVE

This prototype has an account of the operational risks regarding internal users. Identifies and assesses critical assets and/or threats to the organization, tracks risks, and establishes key components and technical vulnerabilities causing the risks[45].

Table 4: Advantages and Disadvantages of the OCTAVE methodology

Advantage	Disadvantages	Reference
Modification of the information system in the early stages of development.	Its administration is difficult.	[45]
It allows the developer to know the requirements of the users and / or clients.	It can only be implemented in medium and small institutions.	[45]
Initial changes during project development are less expensive.	Unforeseen changes arise that slowly down the advance of the prototype.	[45]
Includes risk analysis and management processes in organizations.	Deep technical knowledge is required for its implementation.	[45]

Table 4 shows the advantages and disadvantages of the OCTAVE methodology.

In the figure 2. Shows the operational process of the OCTAVE model, which has three phases. Phase 1 deals with the vision of the organization, in this phase the elements are specified as assets; vulnerabilities; threats and security requirements. This phase is responsible for arranging and organizing the entire plan to be executed in the risk analysis. Phase 2: Technological vision, in this phase the key components and technical vulnerabilities of information systems are analyzed. Phase 3: planning of measures and risk reduction, this phase is responsible for classifying the risk assessment, strategies, risk weighting and the risk reduction network plan, in this phase an appropriate strategy must be sought to risk management.

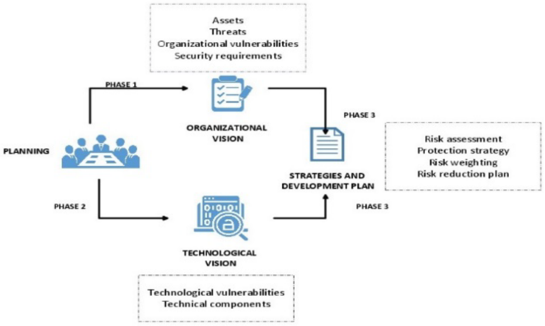

Figure 2. OCTAVE prototype process

A risk assessment is very particular to each organization and it would not be appropriate to develop assessments based on results obtained from other organizations.

2.2.5. MEHARI

It is a methodology that provides a set of tools that allow a quantitative and qualitative risk analysis to be carried out, it is designed to unite the processes of business risk analysis and future risk analysis. Its analysis is carried out based on three criteria [36]:

- Confidentiality
- Integrity
- Availability

This methodology depends on the use of a database of information and computerized techniques to carry out the evaluation of each one of the risks

2.2.6. CRAMM

It is a method of analysis and risk control that allows identifying, measuring and minimizing the attacks to which organizations are exposed. It performs a qualitative and quantitative risk analysis, known as a mixed methodology, in order to have a clear vision of the threats, based on a matrix where the rows represent the assets and the columns the risks that could affect the integrity, availability and confidentiality of the information. CRAMM is a simpler and lower cost methodology compared to the MAGERI methodology[3]. To carry out a risk analysis with the CRAMM methodology, elements such as:

- Goods
- Vulnerabilities
- Risks
- Threats
- Countermeasures
- Implementation
- Audit

2.2.7. EBIOS

Its acronym stands for Expression of Needs and Identification of Security Objects; it is a methodology created by DCSSI (Central Directorate for Information Systems Security). Its objective is to facilitate communication with the internal and external clients of an organization in order to contribute to the process of managing information systems security risks. It allows organizations to have a better knowledge of their assets, identifying the threats and vulnerabilities to which they are exposed[3].

2.2.8. PMI

The PMI prototype is easy to use, because it allows an easy understanding of the information processes, which helps to improve the flaws or vulnerabilities that the information systems have when applying the plans and policies established previously. This prototype is compatible with the Magerit methodology and the Octave prototype, to achieve optimum system performance, successfully controlling the risks that may exist in the information systems for commercial management.

2.2.9. COBIT 2019

It is a reference framework that facilitates the use of information technologies from an investment approach, based on industry standards and best practices. management to provide measures, indicators and processes to take full advantage of the control and implementation of information technologies[2][21].

2.2.10. Risk Matrix

The risk matrix allows us to evaluate the levels of information integrity risks, where a combination of key elements must be used, which are: risks, types of cyber-attacks, impacts and probability of occurrence.

To evaluate the impact of risks and the probability of their occurrence, we use values that are in a range of 1 to 5

Table 6: Impact of risks

Impact level	Punctuation
Mild	1
Low	2
Means, medium	3
High	4
Extreme	5

Table 6 contains the risk impact classification. The chances of a risk occurring are:

Table 7. Probability of Occurrence

Occurrences	Punctuation
Unlikely	1
Probable	2
Very likely	3
Highly probable	4
Extremely Likely	5

Table 7 shows the probability values of certain risks occurring. The criteria of importance of a risk are:

Table 8: Importance of risks

Importance level	Punctuation
Mild	1-5
Low	6-10
Normal	11-15
High	16-20
Critical	20-25

Table 8 contains the index of importance that the risks may have. To find the risk value in our matrix, we are going to use the following formula:

$$VR = POxI \qquad (4)$$

where:

PO = Probability of Occurrence (number of times that event would the impact they may have, both qualitative and quantitative).

Table 9. Risk Matrix

	Probability of:		
Risks	Occurrence (PO)	Impact (I)	Risk Value (VR)
Extraction, modification and destruction of confidential information.	4	5	twenty
Inappropriate use of information.	5	5	25
Red Hat and / or Gray Hat attacks.	4	4	16
Information leakage	3	3	9
Network crash	4	3	12
Organization server failures.	3	4	12
Computer virus attacks.	4	4	16
DDoS attacks	4	3	12
Inadequate logical access controls.	two	one	two

In the table 9. The values that are in a range of 1 to 5, do not indicate a security problem. If the values are from 6 to 10, they generate a low importance level. All the values that are in the range of 20 to 25 are considered extremely high risks, to which we must find a solution immediately. It is clarified that the values used in table 9 come from the simulation of a case study of a company X that can be disclosed according to research ethics.

2.3. Methodology to generate results

2.3.1. Conceptual model

For a security prototype, the following information was taken from the references: phases to obtain the value of a risk [32], risk categories[6], analysis of the development of security strategies and plans[8].

2.3.2. Security prototype

To propose a security prototype, the following references were taken into account[11],[14]. With these references, a three-phase prototype was analyzed and made to mitigate attacks in business management.

2.3.4. Algorithms

To define the algorithms, the following references were taken into account:[9], [35], [38], [39], [49]. In the algorithm of the security prototype, we demonstrate the phases that are required and carry out the verification by means of a formula that the algorithm is stable.

2.3.4.1. Formula

A formula was determined that with the number of risks and the mitigation capacity of the system can mitigate the attacks, based on tables of security levels in order to optimize the proposed prototype.

2.3.4.2. Simulations

The simulations demonstrated the probability of a security problem occurring and the risk assessment, given five different scenarios, which were defined by the authors.

3. Results

This research attempts to reduce attacks on the cloud that occur daily to steal data from different users.

The following results were obtained:

- Conceptual model to protect business data from attacks.
- Security prototype to mitigate vulnerabilities, threats and risks of information for the control and integration of data in commercial management.
- Algorithm in the flowchart to protect data from risks and attacks.
- Formula to find the probability of a simulation and security problem occurring.
- Risk Analysis and Evaluation

The limitations of the results obtained is that they can be applied in small and medium-sized commercial companies. The results obtained are not oriented at the corporate level. The main advantage is that the five results can be applied independently or in turn all to guarantee the process.

3.1. Conceptual model to protect the cloud against attacks

With this proposed model we can analyze that the security information to mitigate vulnerabilities, threats and risks of the information for the control and integration of data in commercial management are:

In the fig. 3. This model was designed to mitigate risks and protect the data of a business management organization. We develop a model where we indicate that we will carry out the identification of assets, vulnerabilities, threats and risks, we will also obtain the real mitigation capacity of our prototype and the probability that the risks found will not affect the organization's data.

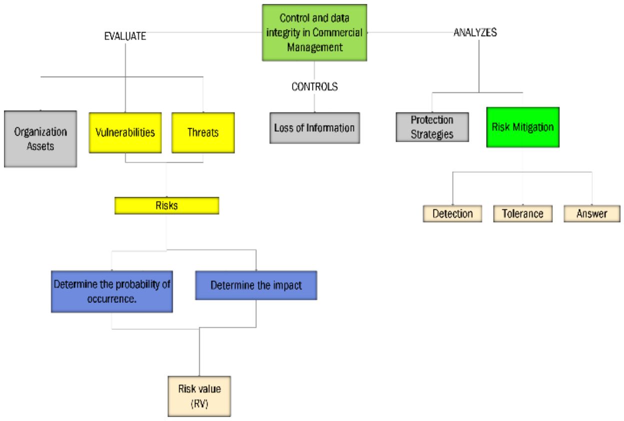

Figure 3: Conceptual model of our proposed protocol

The objective we want to control in the process of finding the value of risks is data loss; the value of the risks will be obtained by determining the probability of occurrence and the impact of each of the risks.

For the calculation of an efficient prototype of the presented conceptual model, the following formula is proposed:

$$x = \frac{\sum_{i=1}^{n}(D+T+R)}{3} \tag{5}$$

where:

X = Average of the sum of mitigation indicators
D = Mitigation detection (range value 0 - 10)
T = Mitigation tolerance (range value 0 - 10)
R = Mitigation response (range value 0 - 10)

$$CM = \frac{x}{CME} = \frac{x}{10} \tag{6}$$

Where:

ACM = Actual Mitigation Capacity

CME = Estimated Mitigation Capacity

$$P(R)\% = \frac{ACM^{R}e^{-ACM}}{R!} * 100 \tag{7}$$

where:

P (R) % = Probability that risks affect the system

R = Number of Risks

e = Euler

$$EP = 100 - P(R)\% \tag{8}$$

where:

EP = Prototype mitigation efficiency

Table 10: Mitigation score

Punctuation	Safe level
80-100	Excellent (E)
50-70	Good (G)
20-40	Regular (R)
0-10	Deficient (D)

Guide to setting measurement values

Example

If we have a system that has a mitigation (Detection = 10, Tolerance = 8, Response 9), in which 9 risks were found.

If we apply the formulas 5, 6, 7 and 8 we have

$$x = \frac{10+8+9}{3}$$

$$x = 9$$

$$CM = \frac{X}{CME} = \frac{9}{10}$$

$$CM = 0.9$$

$$P(R)\% = \frac{CM^{R} e^{-CM}}{R!} * 100$$

$$P(R)\% = \frac{(0.9)^{9} e^{-0.9}}{9!} * 100$$

$$P(R)\% = 4.34x10^{-5}$$

$$EP = 100 - 4.34x10^{-5}$$

$$EP = 99.99\% \tag{9}$$

According to Table 10, our prototype for this scenario shows us that it is optimal.

3.2. Security prototype

It is proposed to have a higher security index, this prototype identifies the vulnerabilities and threats that can generate a risk in the control and integrity of the data, selects mitigation strategies, prepares an action plan, implements and monitors the mitigation strategies implemented.

Mitigation strategies are an important part of data security control, with their help we can reduce the number of information losses, modifications and destruction.

Each section of the prototype is related to security methodologies and prototypes and all these resources to information systems.

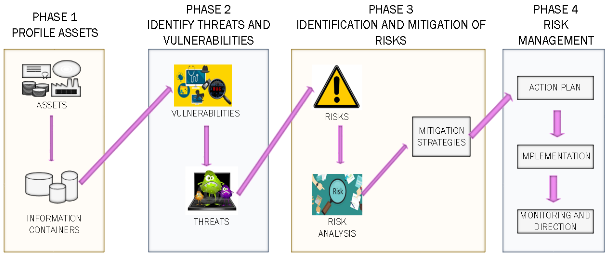

Figure 4: Security prototype

In Figure 4. We find the four phases of our prototype.

First phase:

Here we find the assets that the organization owns and the databases where the organization's data will be stored (information on workers, customers, purchases, sales, etc.).

Second stage:

Vulnerabilities and threats are identified, which give way to information systems risks being generated and which can cause serious security problems.

Third phase:

If there are risks, they must be analyzed and categorized by levels (mild, low, normal, high and critical), in order to implement risk mitigation strategies prioritizing the risks that urgently require attention.

Fourth phase:

Finally, the prototype indicates that an action plan must be generated to carry out the mitigation strategies. Once the action plan is implemented, it must be monitored, to verify that it is being carried out correctly, avoiding loss of information.

3.3. Algorithm in the flowchart to protect data from risks and attacks

The proposed methodology in algorithm and data flow results in the steps that we must take to mitigate vulnerabilities, threats and risks of information for the control and integrity of data in commercial management.

Figure 5. Express the algorithm in a flow diagram, the phases are described below:

Description of the phases:

Phase 1: Profiling assets the assets and information containers owned by the organization must be identified and that can be compromised if a security problem occurs.

Phase 2: Identify threats and vulnerabilities, with the identification of threats and vulnerabilities, we will be able to identify the existing risks in the information systems, since the risks are created thanks to the existence of the vulnerabilities and threats. In the absence of vulnerabilities or threats, the prototype will terminate the control and mitigation processes.

Phase 3: Identify and mitigate risks, the identified risks must have their risk value found, the value of the risks is found by multiplying the probability of occurrence with the impact that each of the risks can generate. Given the value of each risk, they are categorized to know which risks can cause high and critical security problems, the risks that belong to these categories should be solved immediately. The risks are analyzed to be able to select the mitigation strategies, if there are no mitigation strategies, we must create them and re-analyze the risks.

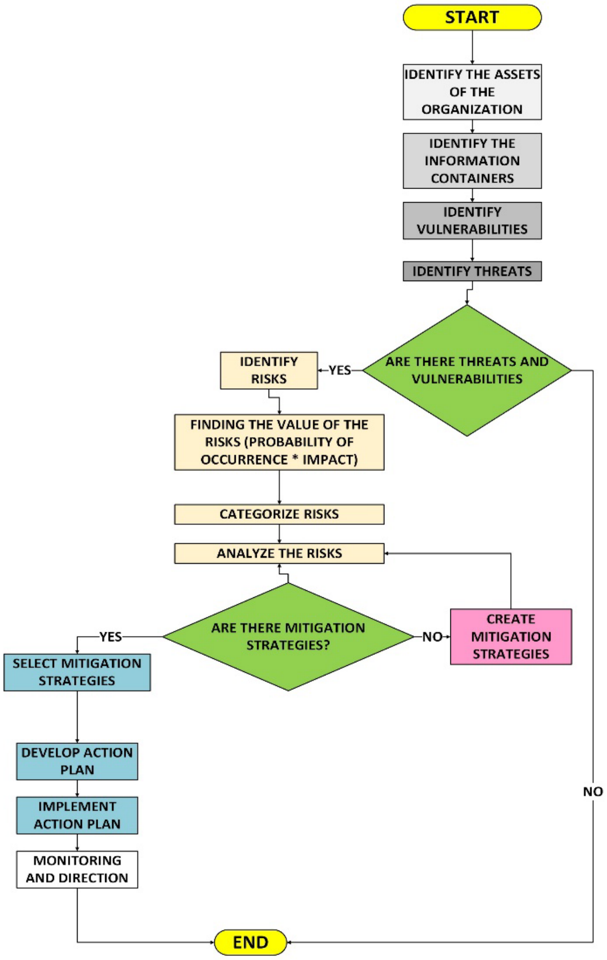
START
IDENTIFY THE ASSETS OF THE ORGANIZATION
IDENTIFY THE INFORMATION CONTAINERS
IDENTIFY VULNERABILITIES
IDENTIFY THREATS
ARE THERE THREATS AND VULNERABILITIES
YES
IDENTIFY RISKS
FINDING THE VALUE OF THE RISKS (PROBABILITY OF OCCURRENCE * IMPACT)
CATEGORIZE RISKS
ANALYZE THE RISKS
ARE THERE MITIGATION STRATEGIES?
YES
NO
CREATE MITIGATION STRATEGIES
SELECT MITIGATION STRATEGIES
DEVELOP ACTION PLAN
IMPLEMENT ACTION PLAN
MONITORING AND DIRECTION
NO
END

Figure 5: Algorithm of the proposed prototype expressed in a flow diagram

Phase 4: Risk Management, the selected mitigation strategies must be executed and described in the action plan, which will then be implemented and monitored, to verify that security problems do not occur.

Algorithm:

Start
Phase 1: Profile assets
The assets and information containers owned by the organization are identified.
Phase 2: Identify threats and vulnerabilities
Vulnerabilities and threats are identified.
If there are no vulnerabilities and threats, the mitigation process will be terminated.
If there are vulnerabilities and threats, the risks must be identified.
Phase 3: Identification and mitigation of risks.
After identifying the risks, the value of each is found, categorized and analyzed.
Once the risks have been analyzed, we must verify that mitigation strategies exist and are selected.
In the absence of mitigation strategies, strategies must be created.
Phase 4: Risk Management
If mitigation strategies were selected, we can develop an action plan.
This action plan will be implemented and monitored.
End.

We demonstrate with our proposed formulas that the protocol is stable:

$$P_o = \frac{1 - \frac{R^*}{R}}{CM} \tag{10}$$

Finally, we calculate the percentage of the formula used:

$$s = P_o(100\%) \tag{11}$$

Where:
R = Number of Risks
R * = Number of high and critical risks
Po = Security Level
CM = Mitigation Capacity
s = Percentage of algorithm stability
Example:

If we have a system that has a mitigation (Detection = 10, Tolerance = 8, Response = 9), in which 9 risks were found, of which 4 are of high and critical level, as shown in Table 9.

Table 11: Security algorithm percentage

Punctuation	Safe level
76-100	Excellent
51-75	Optimum
25-50	Regular
0-24	Deficient

We will calculate the percentage of safety of our algorithm using formula 10:

$$P_o = \frac{1-\frac{4}{9}}{0.9}$$

$$P_o = 0.6173$$

As a last step we calculate the security percentage:

$$s = 0.6173(100\%)$$

$$s = 61.73\%$$

The security percentage is 61.73, according to table 11 our algorithm is optimal to implement it.

Example:

In Figure 6, we can see the percentage of safety of the prototype, the number of risks identified, the number of high risks and the mitigation capacity. For the representation of the simulation, we have 5 scenarios, with different numbers of risks and mitigation capacities. Scenario 2 obtained the highest percentage of safety.

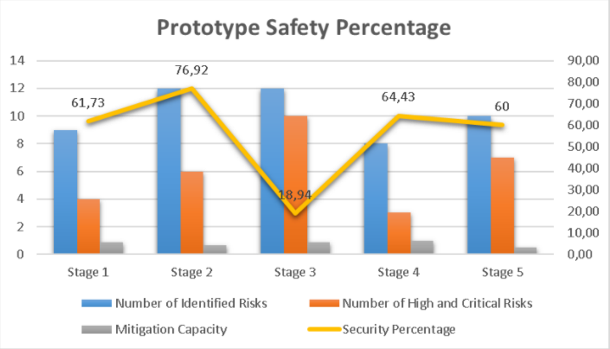

Figure 6: Safety percentage in 5 different scenarios

3.4. *Formula to find the probability of a security problem occurring*

With the following simulations we can observe the probability that security problems occur due to the number of risks and threats presented in 5 different scenarios:

$$P(n) = [(\#R)^n e^{-\#R}]/n! \tag{12}$$

where:
P (n) = Probability of a security problem occurring
n = Number of system threats
#R = Number of System Risks

To determine the probability of a security problem occurring in the system, a scenario with 9 risks was performed, and with 12 threats, using Formula 12, a high percentage of 9.48% probability of a security problem occurring was determined. In the system. Figure 8 shows the simulation of five different scenarios using Formula 12 and shows that there is a higher probability of an information security problem occurring if the threats and risks are high.

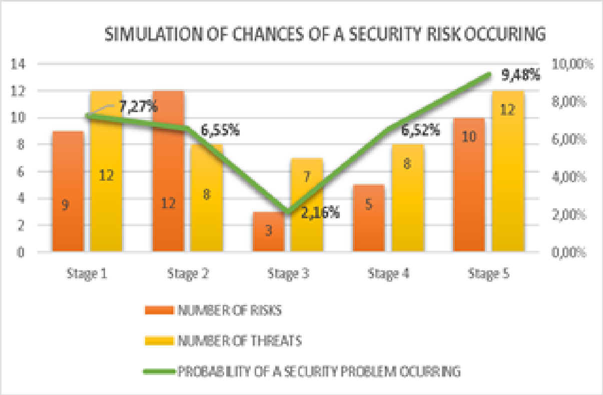

Figure 7: Simulation of the possibilities of a security risk. The simulation is shown in 5 different scenarios

3.5. *Risk Analysis and Evaluation*

Given the analysis carried out on the methodologies and security models, one of the most important and critical processes refers to the identification and evaluation of risk [14].

Within the existing methodologies and methods for the detection and evaluation of risks, MEHARI[9] and OCTAVE[36] are identified as the powerful methodologies that allow the evaluation and management of risks, with the objective of identifying, categorizing and prioritizing the probability and impact of risks on an asset or process, to determine the rate of security problems that risks can cause.

Risk mitigation capacity is made up of several parameters[35], these parameters are defined on a quantitative scale defined between the values 0-10 in which the value 10 represents the highest value for each indicator.

These numerical parameters are used to calculate the actual mitigation capacity of the system, which defines a simple formula for stable critical analyzes on security problems based on quantitative values, Formula 5 and 6.

Through the use of the risk matrix, we will find the potential risks for the generation of actions that mitigate vulnerabilities, threats and information risks.

4. Discussion

In the analysis we carried out, there were cases of security prototypes that adopted a system similar to the one that we have proposed, a security model based on the Magerit methodology was applied to adapt the mitigation prototype. This made it easier for the system to identify vulnerabilities, threats and risks that could arise in the information systems, to have data security.

The proposed prototype does not define the costs for the implementation of the system; The costs will be according to the size of the company and the place where the proposal is implemented.

In the article[49] algorithms were used to assess risks in a system, in the article[32] the probability of security incidents and the losses caused by security incidents allow us to find the value of the risks, in the article[39] algorithms were used to produce a risk treatment plan, selecting measures to reduce; to hold back; to avoid or transfer risks, in the article[11]. A risk management review and control model were used for information security.

According to the information security models, it is necessary to carry out adequate risk management that allows knowing which are the main vulnerabilities that can affect the organization's information assets and which are the threats that could exploit the vulnerabilities found.

In the simulations we have a security percentage of 76.92%. In the simulations we have that the greater the number of risks and threats, the greater the probability that a security problem will occur.

5. Future Work and Conclusions

In the future, we proposed the application of security prototypes to mitigate vulnerabilities, threats and information risks for public and private organizations with a high rate of cyberattacks.

It was concluded that the security prototype proposed for a commercial information system; It is security system suitable for public and private companies. In the simulation carried out, it was determined that if the number of risks and threats is high, there will be a greater probability that a problem will arise in the security of the system.

According to the mitigation efficiency simulation of the prototype, the efficiency percentage can be high if there is good mitigation capacity in the system.

In the first result, we include a concept map that shows us the mitigation efficiency formula of the prototype. In the second result, we conclude that each phase helps to avoid the loss of information in a commercial management system. In the third result, the algorithm was carried out to verify that our protocol is optimal against the risks that are obtained in a system with the proposed formula that we can verify. In the last result, the simulation showed us the chances of a security problem occurring given the number of threats and risks.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The authors thank the: Universidad Católica de Santiago de Guayaquil (UCSG), Universidad Estatal de Bolívar (UEB), Escuela Politécnica Nacional (EPN), Gestión de Tecnologías para el Mundo (GTM), Research Department, Instituto Tecnológico Superior Rumiñahui, Universidad de Guadalajara (UDG) and Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt).

References

[1] J. Miranda Jiménez, Joan Noheli,Llerena Izquierdo, “Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos,” Universidad Politécnica Salesiana Sede Guayaquil, 2021.

[2] Y. Supriyadi and C. W. Hardani, “Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 a case study,” in Proceedings - 2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE, 287–291, 2018, doi: 10.1109/ICITISEE.2018.8721034.

[3] M. a. Tejena-Macías, “Análisis de riesgos en seguridad de la información,” Polo del Conocimiento, **3**(4), 230-238, 2018, doi: 10.23857/pc.v3i4.809.

[4] M. Abomhara and G. M. Køien, “Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks,” J. Cyber Secur. Mobil, **4**(1), 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.

[5] A. N. Kamenskih, M. a. Filippov, and A. a. Yuzhakov, “The Development of Method for Evaluation of Information Security Threats in Critical Systems,” in Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus, 333–336, 2020, doi: 10.1109/EIConRus49466.2020.9038960.

[6] A. Alsalamah, “Security risk management in online system,” in Proceedings - 2017 5th International Conference on Applied Computing and Information Technology, 2017 4th International Conference on Computational Science/Intelligence and Applied Informatics and 2017 1st International Conference on Big Data, Cloud Compu, 119–124, 2020, doi: 10.1109/ACIT-CSII-BCD.2017.59.

[7] S. M. Carta, S. Consoli, A. S. Podda, D. R. Recupero, and M. M. Stanciu, “Ensembling and Dynamic Asset Selection for Risk-Controlled Statistical Arbitrage,” IEEE Access, **9**, 29942–29959, 2021, doi: 10.1109/ACCESS.2021.3059187.

[8] R. Gómez, D. H. Pérez, Y. Donoso, and A. Herrera, “Metodología y gobierno de la gestión de riesgos de tecnologías de la información,” Rev. Ing, **1**(31), 109–118, 2010, doi: 10.16924/riua.v0i31.217.

[9] K. D. R. Gaona Vásquez, “Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala,” Universidad Politécnica Salesiana, 2013.

[10] M. Moyo, H. Abdullah, and R. C. Nienaber, “Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems,” in 2013 Information Security for South Africa - Proceedings of the ISSA, 1–6. 2013 doi: 10.1109/ISSA.2013.6641062.

[11] J. Zarei and F. Sadoughi, “Information security risk management for computerized health information systems in hospitals: A case study of Iran,” Risk Manag. Healthc. Policy, **9**(1), 75–85, 2016, doi: 10.2147/RMHP.S99908.

[12] X. Li and H. Li, “A Visual Analysis of Research on Information Security Risk by Using CiteSpace,” IEEE Access, **6**, 63243–63257, 2018, doi: 10.1109/ACCESS.2018.2873696.

[13] M. Shakibazad and A. J. Rashidi, “New method for assets sensitivity calculation and technical risks assessment in the information systems,” IET Inf. Secur, **14**(1), 133–145, 2020, doi: 10.1049/iet-ifs.2018.5390.

[14] F. M. Arévalo and I. P. C. S. a Moscoso, “Agile Methodology for Computer Risk Management,” Kill. Técnica, **1**(2) 31–42, 2017, doi: 10.26871/killkana.

[15] A. J. Burns and E. Johnson, “The evolving cyberthreat to privacy,” IT Prof, **20**(3), 64–72, 2018, doi: 10.1109/MITP.2018.032501749.

[16] B. Hauer, “Data and information leakage prevention within the scope of information security,” IEEE Access, **3**, 2554–2565, 2015, doi: 10.1109/ACCESS.2015.2506185.

[17] H. Chen, D. Bao, H. Gao, and J. Cheng, “A Security evaluation and certification management database based on ISO/IEC standards,” in Proceedings - 12th International Conference on Computational Intelligence and Security, 249–253, 2016, doi: 10.1109/CIS.2016.63.

[18] H. Parastvand, O. Bass, M. a. S. Masoum, A. Chapman, and S. Lachowicz, “Cyber-Security Constrained Placement of FACTS Devices in Power Networks from a Novel Topological Perspective,” IEEE Access, **8**, 108201–108215, 2020, doi: 10.1109/ACCESS.2020.3001308.

[19] S. Pissanetzky, "On the Future of Information: Reunification, Computability, Adaptation, Cybersecurity, Semantics," IEEE Access, **4**, 1117–1140, 2016, doi: 10.1109/ACCESS.2016.2524403.

[20] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure," IEEE Access, **6**, 25167–25177, 2018, doi: 10.1109/ACCESS.2018.2817560.

[21] R. Rooswati and N. Legowo, "Evaluation of IT Project Management Governance Using Cobit 5 Framework in Financing Company," in Proceedings of 2018 International Conference on Information Management and Technology, ICIMTech, 81–85. 2018, doi: 10.1109/ICIMTech.2018.8528192.

[22] T. Y. T. Y. Lin, "Chinese wall security policies information flows in business cloud," in Proceedings - 2015 IEEE International Conference on Big Data, IEEE Big Data, 1603–1607, 2015, doi: 10.1109/BigData.2015.7363927.

[23] F. Avorgbedor and J. Liu, "Enhancing User Privacy Protection by Enforcing Clark-Wilson Security Model on Facebook," in IEEE International Conference on Electro Information Technology, 155–161. 2020, doi: 10.1109/EIT48999.2020.9208279.

[24] B. Balamurugan, N. G. Shivitha, V. Monisha, and V. Saranya, "A Honey Bee behaviour inspired novel Attribute-based access control using enhanced Bell-Lapadula model in cloud computing," in Proceedings 2015 - IEEE International Conference on Innovation, Information in Computing Technologies, ICIICT, 1–6, 2015, doi: 10.1109/ICIICT.2015.7396064.

[25] M. R. Ogiela and L. Ogiela, "On using cognitive models in cryptography," in Proceedings - International Conference on Advanced Information Networking and Applications, AINA, 1055–1058, 2016, doi: 10.1109/AINA.2016.159.

[26] A. Ahi and A. V. Singh, "Role of Distributed Ledger Technology (DLT) to Enhance Resiliency in Internet of Things (IoT) Ecosystem," in Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI, 782–786, 2019. doi: 10.1109/AICAI.2019.8701282.

[27] S. J. Moon, I. H. Park, B. S. Lee, and J. Ju Wook, "A Hyperledger-based P2P Energy Trading Scheme using Cloud Computing with Low Capabillity Devices," in 2019 IEEE International Conference on Smart Cloud (SmartCloud), 190–192, 2019, doi: 10.1109/SmartCloud.2019.00039.

[28] J. S. Suroso, A. Januanto, and A. Retnowardhani, "Risk Management of Debtor Information System at Bank XYZ Using OCTAVE Allegro Method," in 2019 International Conference on Electrical Engineering and Informatics (ICEEI), 261–265, 2019, doi: 10.1109/ICEEI47359.2019.8988890.

[29] L. Kotut and L. a. Wahsheh, "Survey of Cyber Security Challenges and Solutions in Smart Grids," in 2016 Cybersecurity Symposium (CYBERSEC), 32–37, 2016, doi: 10.1109/CYBERSEC.2016.013.

[30] M. Wegerer and S. Tjoa, "Defeating the database adversary using deception - A MySQL database honeypot," Proc. - 2016 Int. Conf. Softw. Secur. Assur. ICSSA, 6–10, 2017, doi: 10.1109/ICSSA.2016.8.

[31] I. V. Anikin, "Information security risks assessment in telecommunication network of the university," 2016 Dyn. Syst. Mech. Mach, 1–4, 2017, doi: 10.1109/Dynamics.2016.7818967.

[32] L. Huang, Y. Shen, G. Zhang, and H. Luo, "Information system security risk assessment based on multidimensional cloud model and the entropy theory," in ICEIEC 2015 - Proceedings of 2015 IEEE 5th International Conference on Electronics Information and Emergency Communication, 11–15, 2015, doi: 10.1109/ICEIEC.2015.7284476.

[33] B. F. Zahra and B. Abdelhamid, "Risk analysis in Internet of Things using EBIOS," in 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), 1–7, 2017, doi: 10.1109/CCWC.2017.7868444.

[34] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sadhukhan, "Cyber-risk decision models: To insure IT or not?," Decis. Support Syst, **56**(1), 11–26, 2013, doi: 10.1016/j.dss.2013.04.004.

[35] J. Porras, S. Pastor, and R. Alvarado, "Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas," Rev. Peru. Comput. y Sist., **1**(1), 47–56, 2018, doi: http://dx.doi.org/10.15381/rpcs.v1i1.14856.

[36] F. Y. H. García and L. M. L. Moreta, "Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras," RISTI - Rev. Ibérica Sist. e Tecnol. Informação, **31**, 1–17, 2019, doi: 10.17013/risti.31.1-17.

[37] S. M. T. Toapanta, M. A. P. Sánchez, D. W. B. Valencia, and L. E. M. Gallegos, "An approach of models of information technologies suitable to optimize management in a public organization of Ecuador," in 2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4), 207–214, 2019, doi: 10.1109/WorldS4.2019.8904027.

[38] I. C. Satizábal-Echavarría and N. M. Acevedo-Quintana, "MePRiSIA: Risk prevention methodology for academic information systems," Rev. Fac. Ing., **1**(89), 81–101, 2018, doi: 10.17533/UDEA.REDIN.N89A11.

[39] N. Anton and A. Nedelcu, "Security Information and Risk Management Assessment," Appl. Mech. Mater., **809**, 1522–1527, 2015, doi: 10.4028/www.scientific.net/amm.809-810.1522.

[40] S. M. T. Toapanta, I. N. C. Ochoa, R. A. N. Sanchez, and L. E. G. Mafla, "Impact on administrative processes by cyberattacks in a public organization of Ecuador," in Proceedings of the 3rd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2019, 270–274, 2019, doi: 10.1109/WorldS4.2019.8903967.

[41] S. M. Toapanta Toapanta, L. E. Mafla Gallegos, M. J. Chevez Moran, and J. G. Ortiz Rojas, "Analysis of models of security to mitigate the risks, vulnerabilities and threats in a company of services of telecommunications," in 2020 3rd International Conference on Information and Computer Technologies (ICICT), 445–450. 2020, doi: 10.1109/ICICT50521.2020.00077.

[42] Y. Lee, S. Woo, Y. Song, J. Lee, and D. H. Lee, "Practical Vulnerability-Information-Sharing Architecture for Automotive Security-Risk Analysis," IEEE Access, **8**, 120009–120018, 2020, doi: 10.1109/ACCESS.2020.3004661.

[43] M. Mohsin, M. U. Sardar, O. Hasan, and Z. Anwar, "IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things," IEEE Access, **5**, 5494–5505, 2017, doi: 10.1109/ACCESS.2017.2696031.

[44] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," Comput. Secur., **44**. 1–15, 2014, doi: 10.1016/j.cose.2014.04.005.

[45] G. Stergiopoulos, D. Gritzalis, and V. Kouktzoglou, "Using formal distributions for threat likelihood estimation in cloud-enabled IT risk assessment," Comput. Networks, **134**, 23–45, 2018, doi: 10.1016/j.comnet.2018.01.033.

[46] M. Jouini, L. B. A. Rabai, and R. Khedri, "A multidimensional approach towards a quantitative assessment of security threats," Procedia Comput. Sci., **52(**1), 507–514, 2015, doi: 10.1016/j.procs.2015.05.024.

[47] O. T. Arogundade, A. Abayomi-Alli, and S. Misra, "An Ontology-Based Security Risk Management Model for Information Systems," Arab. J. Sci. Eng., **45**(8) 6183–6198, 2020, doi: 10.1007/s13369-020-04524-4.

[48] I. V. Anikin, "Information security risk assessment and management method in computer networks," in 2015 International Siberian Conference on Control and Communications (SIBCON), 1–5, 2015, doi: 10.1109/SIBCON.2015.7146975.

[49] A. Boranbayev, S. Boranbayev, A. Nurusheva, K. Yersakhanov, and Y. Seitkulov, "A Software System for Risk Management of Information Systems∗," in IEEE 12th International Conference on Application of Information and Communication Technologies, AICT 2018 - Proceedings, 1–6, 2018, doi: 10.1109/ICAICT.2018.8747045.

[50] Y. Qi, L. Xiao, and Q. Li, "Information security risk assessment method based on CORAS frame," Proc. - Int. Conf. Comput. Sci. Softw. Eng. CSSE 2008, **3**, 571–574, 2008, doi: 10.1109/CSSE.2008.1001.

[51] B. S. Y. Choo and J. C. L. Goh, "Adapting the ISO31000:2009 enterprise risk management framework using the six sigma approach," IEEE Int. Conf. Ind. Eng. Eng. Manag., 39–43, 2014, doi: 10.1109/IEEM.2014.7058596.

[52] T. Hirakawa, K. Ogura, B. B. Bista, and T. Takata, "A Defense Method against Distributed Slow HTTP DoS Attack," in 2016 19th International Conference on Network-Based Information Systems (NBiS), 152–158, 2016, doi: 10.1109/NBiS.2016.58.

[53] X. Ma, "Research on Black Hat SEO Behaviour Measurement," in 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 1041–1045, 2018 doi: 10.1109/IAEAC.2018.8577831.

[54] D. Kim, D. Shin, and D. Shin, "Unauthorized Access Point Detection Using Machine Learning Algorithms for Information Protection," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 1876–1878, 2018 doi: 10.1109/TrustCom/BigDataSE.2018.00284.