ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 2, 673-682 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Analysis of Vulnerabilities, Risks and Threats in the Process of Quota Allocation for the State University of Ecuador

Segundo Moisés Toapanta Toapanta[1,*], Andrés Aurelio García Henriquez[1], Luis Enrique Mafla Gallegos[2]

[1]*Department of Computer Science, Universidad Politécnica Salesiana (UPS), Guayaquil, 010102, Ecuador*

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

ARTICLE INFO

Article history:
Received: 15 January, 2020
Accepted: 02 April, 2020
Online: 17 April, 2020

Keywords:
Allocation of quotas Vulnerability
Risks
Quotas
College entrance
Security Information

ABSTRACT

Different models and standards of information security were analyzed, to adopt a model that mitigates vulnerabilities, risks and threats in the quota allocation process for the State University in Ecuador. The main objective is defining a prototype for the management of processes and information security in this type of organization. It was used the deductive and exploratory research method to analyze the information in the references. In this work, the characteristics of the attacks were analyzed. It turned out a model performs the detection and defense of attacks based on the differences in data and time between them and the browsing behavior of normal users. It was concluded that the prototypes presented as results are an alternative to improve the security of the processes and the flow of information and that these can be used as a reference in this type of organization.

1. Introduction

Universities State of Ecuador, for the admissions process students have implemented "Ser Bachiller", which platform since the beginning of its implementation in 2018 has presented security problems that jeopardized the integrity of the system hurting students' rights in their application. Higher education in Ecuador has undergone changes since the last decade, in the current Constitution the right to this is guaranteed, observing the principle of equal opportunities and permanency through the Organic Law on Higher Education (LOES), implemented in 2010, as it stated in the art. 71 on access and management of higher education institutions (IES) on art collecting tariffs.73 Higher education platform of the State, has disadvantages in the application process for admission to universities, since there is the possibility of being manipulated by external agents, which makes seeing the process trustworthy, So that applicants can be affected in their desire to pursue a college career [1].

The aim of this study is to analyze vulnerabilities, threats and risks in the process of allocation of quotas for State Universities Ecuador and a quantitative methodology is applied, descriptive cross-sectional study under.

Although the computer platform uses reference frameworks to streamline and operationalize the admissions process, however, applied technology does not offer the best assurance to ensure non-interference of irregular actions that violate the integrity and confidentiality of the system.

Results affectation seen from the interface authentication of users "Ser Bachiller" system, problems in the security system for identifying risks, inconvenience for authentication and loss of access control on the intake system of education higher.

According to OWASP list errors most dangerous security-related software affect Web applications [2].

What are the benchmarks or standards that can be applied to prevent vulnerabilities, threats and risks in the process of allocation of quotas for state universities in Ecuador?

There are frameworks for optimization and good management of technological resources, technical criteria that are applied through effective systems. A typical system with service-oriented architecture (SOA) is front-end web applications, web services intermediary databases and background; They work in a harmonized way [3].

It is concluded that it is important to implement and apply the methodology OWASP Top Ten, so that the "Ser Bachiller" system cannot be hacked to attack any cyber as add-on armor and

*Corresponding Author: Segundo Moisés Toapanta Toapanta, Email: stoapanta@ups.edu.ec

protection to COBIT and COSO methodologies implemented in the allocation process quota system.

2. Materials and Methods

2.1 Prevention measures

The first vector in which can be implemented security layers is the network infrastructure as services is the entry route offered. Any measures to keep in mind is that, for example, in the case of online services within a corporate network, due to the fact that we can easily conFigureure security layers as a check list (ACL) , which controls network access based on IP applicants or firewall. The ISP is providing this router, but not always, the ISP not always allows us to conFigureure these security measures, taking into account that in this case we should have an additional internal router in our network firewall how we allow to apply these security measures,

- ConFigureuration: it is essential to review in detail the conFigureuration of routers and firewalls to stop all IP that are not valid. Currently, the router is given adequate control of connections through logging options. Contingency plan: in any business, it is essential to have a protocol of action against any attacks from DOS. Thus, to produce the attack, security experts have a plan to follow, significantly minimizing the damage.
- IS / IPS: to explain IDS / IPS can detect any misuse valid as possible attack vectors protocols.
- Traffic: It is recommended to limit the tax on traffic coming from a single host in order to warn of a DoS attack that aims to saturate the server.
- DOS protection: These are services that will oversee the redirection of heavy traffic, thereby avoiding many requests affect the operation of the web.
- IP Block list: Blacklists allow identification of critical IP addresses and packet discard. This security measure can be done manually or automatically through block lists of the firewall.
- Filters: You can set limits on the amount of data processed simultaneously to filter, therefore, all kinds of abnormal packets. At this point, it is important to note that often, proxy servers allow many clients to connect from the same IP address of the server, which can generate the lock for no apparent reason.
- SYN cookies: if this security measure is used, information about SYN packets are no longer stored on the server but is sent as an encrypted cookie to the client. This way, a SYN flood attack compromises the ability of the equipment, but not the memory of the system.
- Load balancing: an effective measure against overload is the load distribution in the different systems. The use of load balancers can extend services to multiple physical machines. Thus, to some extent, controls the denial of service attacks.
- The need for complementary security technologies: in addition to using firewall systems and intrusion prevention, companies must have security solutions that certify successful mitigation of attacks known and unknown, including tools for analyzing network behavior, which systems can detect real-time signature. The intrusion prevention systems against application vulnerabilities known. Active defense mechanism application levels. Active counter strategies emergency, alerting capabilities.
- Prepare for counterattacks, with a proactive and offensive defense system simultaneously: the design of a solid plan to integrate real-time technicians to ensure that tools, alerts, correlation and mitigation are properly managed. Make sure the team is ready to provide immediate assistance and active mitigation; or Figureht defensive actions as soon as the system is under attack. Active defense is equivalent to a backlash if it conforms to the last vestiges of DoS attacks and the incident is adjusted.
- Encryption: If engineering data security protects the network and other physical assets, such as servers, computers and databases, encryption protects the actual data and files stored on them or that travel between them over the Internet. Encryption strategies are crucial for any company that uses the cloud and are a great way to protect hard drives, data and files that are in transit via email, browsers or on their way to the cloud. If data is intercepted, encryption makes it difficult for hackers to do something with them. This is because encrypted data is unreadable to unauthorized users without the encryption key.
- Detection and response to a security breach: If suspicious actions occur in the network, for example, someone or something tries to enter, intrusion detection is activated. Systems network intrusion detection (NIDS) continuously monitor traffic network and passively to detect behaviors that appear illegal or abnormal mark for review. NIDS not only block this type of traffic, but also gather information about it and alert network administrators. However, despite all this, security violations continue to occur. That is why it is important to have a plan to respond to a data breach. They are prepared to act as an effective system. That system can update as often as necessary, for example,
- Strict access controls: a major concern is the loss of control of data for companies if the data is outside your firewall. This control extends to the belief that some employees of the cloud provider have general access to your sensitive data. A cloud provider is properly managed will have several features sharing responsibilities for the entire cloud solution without a single person who has full access to all components of the solution. In other words, no person has access level necessary to put the security or confidentiality of customer data at risk.
- Mitigation: once a threat has been detected, it must be mitigated. In the case of denial of service mitigation, it is to implement a series of measures that reduce the damage and, if possible, restore the compromised system services normally. These usually consist of increasing the pool of resources available for eliminating bottlenecks, increasing restriction of authentication systems through puzzles and lures, or update access lists and encryption policies.

2.2 Materials

The means and methods used in this research are based on the review of reference articles and general information sequence still steps to get the results. As users should check the conFigureuration of our routers and firewalls for invalid or false IP detect that come from potential attackers. Overall, our internet

service provider (ISP) ensures that the router is updated with this conFigureuration. On the other hand, state universities must protect both your network and your entire infrastructure to prevent attacks affect performance and safety of their customers.

We used information about items that have studied the situation in several universities in the world, for determining admission tests applied and what types of vulnerabilities have processes for allocating quotas in these institutions and likewise consider the situation of universities the public of Ecuador, with the application of the system of income, using tools to ensure the safety of students, to obtain a quota allowing him to study the career of their choice.

It is important for the Government of Jakarta, the measures in the field of education, because it affects the academic achievement of certain universities as a whole [4]. In Kazakhstan, this information technology and communication (ICT) improve and secure the quality of life in different areas including medicine, educational process and safety [5]. China's admission to the University is not only an examination system, it has also become a phenomenon of the social system [6]. Instead, Brazil is considered the entrance exam at several universities [7]. Also, at the Polytechnic University Timisoara (UPT) in Romania, the entrance exam for technical profile covers up to twelve math questions chosen at random from the exercise book [8]. All of them are considered, of utmost importance, to have a clear and fair entry process.

2.2.1 Vulnerability scan

Hackers are used to analyze networks actively or passively for holes and vulnerabilities. Analysts' data security professionals and vulnerability assessment are key elements in identifying potential holes and close them. Software safety analysis is used to exploit any vulnerability of a computer, network or communications infrastructure, prioritize and address each of them with safety plans that protect data, detect and react.

2.2.2 Frequency of vulnerabilities

Very high frequency: One or more times a day
High frequency: 1 time per week
Average frequency1 time a month
Low frequency: 1 time every two months
Very low frequency: 1 time every six months.

2.2.3 Testing Intrusion

The vulnerability analysis (identifying potential threats) may also include knowingly investigating a network or system to detect failures or intrusion testing. It is an excellent way to identify vulnerabilities in advance and devise a plan to solve them. If there are flaws in operating systems, problems with the default values, the code of some applications or other similar problems, an administrator expert network penetration testing can help you locate these problems and apply patches to make it less likely to have an attack.

Penetration testing involves performing manual or automated processes that disrupt servers, applications, networks and even end-user devices to see if it is possible intrusion occurred and where this division. From this, you can generate a report for auditors as proof of compliance. A complete intrusion test can save you time and money on costly warn of attacks on weak areas not known.

Table 1: Comparison - Methodologies Security Applications

Frequency	**Time**
Very high frequency	1
High frequency	2
Half frequency	3
Low frequency	4
Very low frequency	5

In Table 1. The frequency that can be generated for each process threats an organization defined.

Downtime of the system can be another annoying side effect of unbridled attacks, so regular intrusion tests are an excellent way to avoid problems before they arise. Manufacturing division chewing establishes a framework for data leakage prevention to protect sensitive data and prevent unauthorized disclosure to third parties. DLP storage based tools apply to supervisors or even block any user activities and confidential data transmissions.

2.3 Methods

A quantitative, descriptive methodology under a cross-sectional applied also under a criterion Deductive information related articles were analyzed for:

- Identifying information related to the process for allocating quotas.
- Identify vulnerabilities or risks of universities in computer admissions process.
- Evaluate reference models leading to neutralize the risks and threats to the security of the admissions process.

In order to apply for a place at a public university in the country it is required to apply to the test designed by the SENESCYT, but in cities across the country have filed complaints, which can be reviewed in several newspapers of the city, also in the news and common citizenship, which, since its inception, has expressed dissatisfaction with the process.

It is important to review the steps for allocating quotas and the different problems presented in it.

2.3.1 Allocation of quotas

The institution responsible for the allocation of quotas is the Ministry of Higher Education, Science, Technology and Innovation (SENESCYT), who works for the benefit of students who want to aspire to a place in a public university, through the surrender of an examination It applied digitally, but has also been criticized by the public for various reasons, whether nonconformity by the mechanism adopted for a quota or for failing to assigning the desired career, on the other hand, some problems are attributed the platform used.

Computing services is the economic backbone of many different types of information systems [9].

For the system of income produces the best results in the

allocation of quotas is necessary to identify, first, information assets, then the possible threats also may recognize the vulnerabilities of the system, hence analyze the impact on the allocation quota, which can lead to finally manage systems that minimize or prevent damage to the system applied in universities. It is worth noting that in the midst of all this, the rate by which organizations and government are adopting the use of the web as they increase the useful resources [10].

Moreover, to combat increasing security risks, many software engineers recognize and analyze the abuse or misuse of the system to provide greater security to the beginning of the development of the system [11]. Firewalls analyze all incoming traffic, detect attacks using rules for policy expressions and blocks attacks detected [12].

In addition, in order to establish protection mechanisms on the platform, you should review the different articulated proposed by the Ecuadorian government, which are beneficial to students, so they can choose a career according to their profile, while their rights are violated citizens.

2.3.2 *External computer threats*

Because internal or external agents can threaten a digital platform, it is important to have a technical team that can identify, assess and eliminate or reduce their impact.

Regarding external threats, according PwC's Global Economic Crime Survey 2016 reports that there are organizations that had suffered losses from cybercrime for more than $ 5 million, and these nearly a third reported losses in excess of $ 100 million. In addition, Juniper Research reports that cybercrime increased the cost of data breaches to $ 2.1 trillion worldwide by 2019; four times the estimated cost of violations in 2015 [13]. This alarmed security analysts, for which, before investing resources and efforts to defend itself, require first acknowledge the attacks received.

2.3.3 *Internal computer threats*

Internal threats affect the image of the institution as well as processes carried out, hurting users who use it. Institutions sometimes detected easily solved problems they have, like removing a magnetized article, which can affect the information, but also major issues such as the intrusion of unauthorized persons. At the organizational level are emerging efforts to improve security systems where filtering of information, analysis, penetration testing, development of best practices and defensive coding using a frame includes fully automated [14].

2.3.4 *Vulnerabilities in the system*

For the security of a system is considered to have access, some require web access to upload real-time information, the gateway is a channel to be careless, becomes vulnerable. For efficient mitigation of web-based attacks, the system must understand the context of the content of the information is processed and the ability to filter content based on their effect on the target application [15].

Moreover, vulnerabilities become increasingly common in the computing environment, where in addition to the system, you should care for other peripherals that can give people access remote ill-intentioned, hurting the theft of information. Machine learning approaches for protecting texts have been applied to research in cybersecurity in the last decade [16].

2.3.5 *Impact on quota allocations*

Within the management of quotas for students who aspire to go to college, is a minority group that can

Enter, with the largest group, through preferential treatment in quotas.

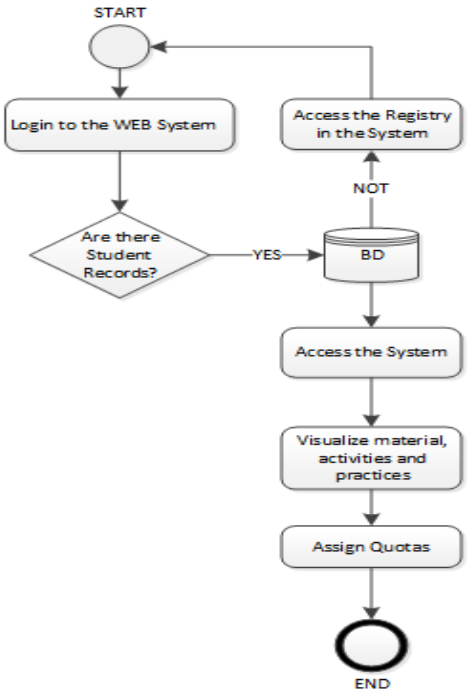

Figure.1: Description of the quota allocation process

In Figureure 1 shows how the process of allocating quotas in state universities in Ecuador, do not maintain sufficient controls to ensure we get a quota for aspiration of university courses.

2.4 Security Tools

After establishing the threats and vulnerabilities, it is important to present alternatives to such security systems that may be compatible with other programs and can be more effective in their results. The threat to cyber security has increased exponentially [17].

2.5 *Cobit (Control Objectives for Information and related technologies):*

Is a framework designed to help implement strategies in technology, with the aim of unifying the processes presenting a comprehensive approach to business, ranked IT processes, criteria and information technology resources.

The components of the development and implementation of

the COBIT that allow streamline processes stand as follows:

2.5.1 Information criteria

This component is intended to adapt the control criteria, allowing requirements apply quality assurance processes quota allocation under the following aspects:

2.5.2 Effectiveness

It is related to the results of the selection process.

2.5.3 Efficiency

It is related to the ability to expedite the process of allocating quotas.

2.5.4 The integrity

It is to protect the information recorded by students in quota allocations, preventing it from being manipulated.

2.5.5 Disponibility

It refers to the application alternatives if the student was unable to complete the process within the platform.

2.5.6 Compliance

It is to follow the instructions recommended by the university to make quota allocations processes successfully. Also considering the introduction of IT processes, where this component is to establish strategies offering a better approach to the processes applied technology, classified in the following domains:

2.5.7 Plan and organize

Establishes strategies to attract students by offering them a good academic service.

2.5.8 Acquire and Implement

It allows for solutions in the classroom processes in view there is disagreement on the means of payment, so it is forced to enable electronic channels to perform them.

2.5.9 Monitor and evaluate

Evaluates the processes of quota allocations for their quality and performance.

2.5.10 Technological resources

This component aims at investing technology resources to the needs of the institution named below:

2.5.11 The applications

It provides applications for managing users based procedures manuals.

2.5.12 Information

Stores the data in quota allocations for your application.

2.5.13 Infrastructure

It is related to the application of physical and logical components that enable the proper functioning of the applications.

2.5.14 People

Are those responsible for managing resources and monitoring systems implemented to mitigate the risks and threats that could arise [18].

2.5.15 The main features of the COBIT 5.0 include

- Identifies the most common risks within the organization.
- Implements technological resources best suited to form a robust technology architecture.
- Develops strategies for automating software.

2.5.16 Advantage

- Is a targeted approach to the needs of the business
- It comprises using the technology to improve its processes.
- Improves the functionality of integrated systems, using the availability of both technological and human resources.

2.5.17 Disadvantages

- It applies to all types of organizations involving information technology.
- It requires large investment of technological resources for standards compliance.
- It requires technical knowledge and commitment of all staff of the organization.

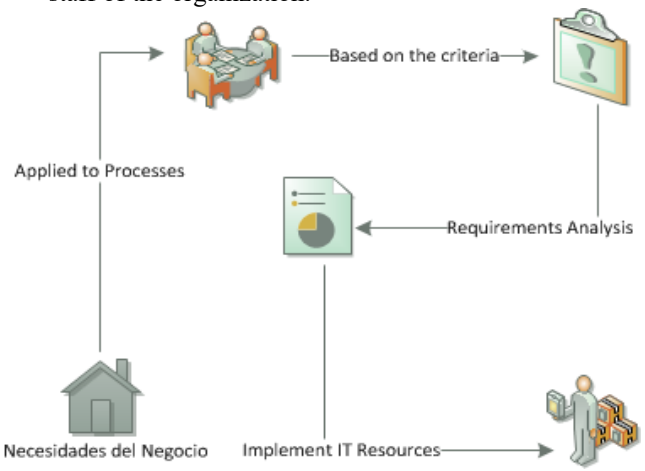

Figure.2: Overview of the COBIT 4.1

In Figureure 2 the application of the COBIT 4.1 and the process, which a company, which also can be used for the allocation of quotas in a college is observed.

2.6 *COSO ERM*

This framework was created with the aim of identifying risks by obtaining data collected through the events presented, providing alternatives to mitigate risks in the business. Recently in research on corporate governance, internal control issues and Complex Enterprise Risk Management (ERM) have been the most debated in academic circles [19].

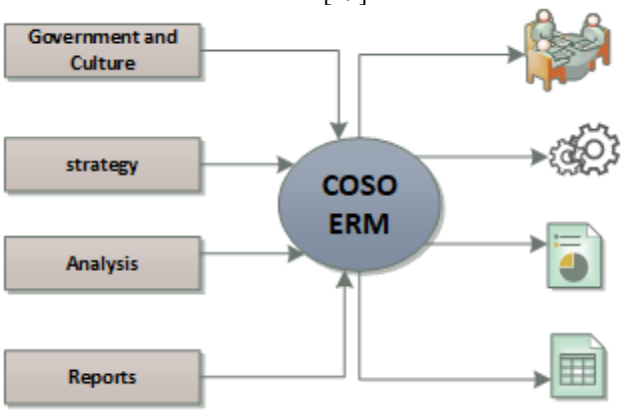

Figure.3: Description of the COSO ERM

In Figureure 3, the complementary process is observed following this type of resource applied to a platform to solve problems presented.

The framework for the assessment and risk control comprises eight elements, which are described below:

2.6.1 Control environment

It refers when processes are vulnerable and can significantly affect the assets of the institution.

2.6.2 Setting objectives

It is to establish strategies to identify risks to address them adequately staffed.

2.6.3 Even ID

Locates vulnerable events in which it is exposed top-level platform and appropriate to mitigate the risks.

2.6.4 Risks evaluation

Classifies risk events by drawing heat maps to measure their impact on us platform quota allocations.

2.6.5 Risk Response

It is to obtain possible solutions once the threats that may affect the institution identified.

2.6.6 Information and communication

Is to communicate to all members within an organization, measures to address risks to take.

2.6.7 Supervision and control

Monitors and monitor the activities assigned to those responsible for each vulnerable area in the institution.
This framework of risk management and internal control includes the following benefits:

- Sets strategies by identifying risk events.
- It allows staff to raise awareness about what steps to take response to risk events.
- Reduce the number of events and damaging consequences for the organization.
- Assesses the risks identified by developing heat maps to classify, reducing negative impacts.

2.6.8 Advantage and disadvantages

The advantage is that it understands the risks to which it is exposed to the organization. It establishes controls in their processes by identifying risks to the fulfillment of its objectives. Offers action plans, which involves the entire organization to achieve its strategic objectives.

The disadvantages are that it requires large investment of technological resources for standards compliance. It requires technical knowledge and commitment of all staff of the organization.

2.7 *OWASP Top Ten (Project Open Web Application Security*

WASC addition, there are plans open up web applications (OWASP) makes visible security software [20]. This security system applications, was designed to raise awareness among organizations about the risks and threats that are exposed through the consequences this brings, with the aim of identifying the most critical risks, providing techniques and tools to counter increased risk events, as many methodologies applied are based on streamlining processes and identify risks without knowing how to counter them. Measures taken to protect network systems and data against attacks or intrusions: it is, by definition, a risk issue [21].

This project shows the most common problems presented in web applications, according to their criticality, taking into account any risks associated with exposure of sensitive data, which will be applied on the platform Bachelor Being under the following aspects:

2.7.1 Broken Authentication

It is used passwords with alphanumeric validations to prevent improper authentication session, in which they may be exposed when they expire passwords or credentials remembering, exposing sensitive information from intruders.

2.7.2 Loss of Access Control

It occurs when the parameters role assignment does not have validations on options granted, due to lack of functional testing by developers.

2.7.3 Registration and Monitoring Deficient

It refers to the lack of oversight that should have systems since submitted an incident does not have the capacity for immediate response.

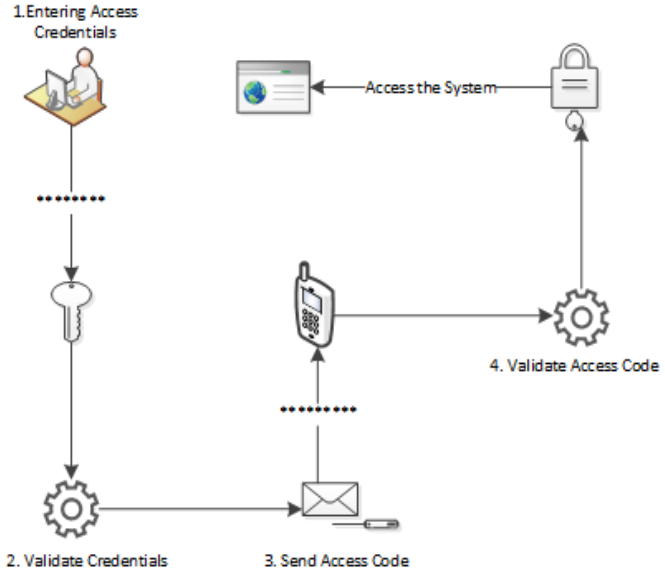

Figure.4: Hazard Identification Description OWASP TOP TEN

In Figureure 4, the following process is observed OWASP TOP TEN to minimize security problems.

Functionality OWASP TOP TEN system:

- Assesses the results by the findings on the platform of higher education.
- Executes scan tests source code, allowing detecting potential vulnerabilities to which the web application is exposed.
- Establishes security controls to measure the impact can cause a cyber-attack.
- Validates the inputs and outputs of the application to rule no authentication Access to the user.
- It requires the implementation of tools to validate the quality of the code to prevent data leakage.
- To find solutions, but also new risks, which in the detection can be useful to identify technological resources.

2.7.4 Advantage

Applies in the cycle of software development considering Web security requirements. Explores possible threats through the most common risks presented. Implement mitigation strategies classified by types of threats.

2.7.5 Disadvantages

It requires specialized computer security analysts for troubleshooting. You need to know the business processes to be applied. No implementation is favorable when the software is developed.

3. Results

3.1 Comparative Methodology OWASP TOP TEN.

Shows that the methodology OWASP TOP TEN meet the acceptance criteria, as to the level of security it offers, by identifying and preventing threats that can occur on web platforms, providing responsiveness to counter events present.

Table 2: Comparison - Methodologies Security Applications

Evaluation criteria	COBIT	COSO ERM	OWASP Top Ten
Ensure access to application from secure locations.	DO NOT	DO NOT	YES
Ensure compliance with security policies and procedures.	YES	YES	YES
Determine the impact of events identified risks.	DO NOT	YES	YES
Implement technological resources to ensure the infrastructure.	YES	YES	YES
Monitor the behavior of services.	YES	YES	YES

Table 2 shows the comparison between COBIT, COSO ERM, OWASP TOP TEN observed.

Ecuador remains a country that is developing at the level of ICT [22]., It is for this inexperience, which is considered most work systems and cyber security risk [23].

Thus, the Ministry of Telecommunications and Information Society, "confirms that security problems persist Information [1].

In this paper the characteristics of the attacks are analyzed, active defense model is proposed and describe the corresponding model. This model makes detection and defense of attacks based on differences in the data and the time between them and the browsing behavior of ordinary users. Propose algorithms to detect attacks incoming, outgoing and forwarded. In addition, cooperatively they detect attacks by delivering its own detection statistics. To mitigate the potential risks to the integrity of an organization, it is necessary to define security policies in the strategic, tactical and operational level and to define the ICT department-level strategic management.

3.2 Monitoring attacks

The system is the victim of a denial-of-service attack. The network monitoring is done through tools, protocols, and control analysis records through applications. Finally, once you have identified the symptoms and vulnerabilities detected on the network, security measures are applied. The indicators were tested in trials are the alteration and packet loss. Since these are the parameters that directly, affect the quality of the service. Finally, the most notable indicator is the downtime that allowed the exact time who allowed us to know the exact time in which the service is no longer available.

3.3 ISO 27001

The standards give the organization the basis for developing a security management framework, which allows you to protect your important information assets, minimizing risks and optimizing investments and efforts required for protection. ISO

17799 presents a number of areas to manage, by applying controls or protection mechanisms, ranging from security systems, to aspects of physical security, human resources and general aspects of the organization.

A model offering a new cooperation between enterprises, can build dynamically. They are using a temporary network of independent organizations connected through information and communication technologies. Community projects can be directed by sharing resources, skills and practical skills and should implement security policies to protect resources from harmful attacks, preventing consequences such as loss of business. A security policy defined global information can be constructed as an extension of the local security policy of different organizations, avoiding start from scratch.

This solution offers the opportunity to focus only on security issues, respecting those who define govern trade within an organization. The question is, as an implant, a system of this type, which must be reliable, simple and must ensure the separation of the different fields.

Security services such as authentication, permission, confidentiality, integrity and traceability must be guaranteed within the infrastructure. ISO 27001 is an evaluation chart of the operating system information security. This prototype is based on ISO / IEC 27001; to mitigate the risks of information security, the variables that will be used are:

- Number = N
- Process = P
- Threat = X
- Frequency = Y
- Impact = Z
- Risk value = VR

Table 3: Risk Matrix

N	P	X	Y	Z	VR
one	Management strategies	The application of standards irregularly	3	4	12
		Difficulty in violation of the processes	3	4	2
		Acts of non-application process	7	8	9
two	IT security	Failure to follow the activities of political organizations	3	2	3
		Failure of processes	7	4	3
		Loss of resources (time, established agreements)	9	3	2

The number of processes in each organization will vary depending on their strategic objectives.

In Table 3 it can be determined that all the processes that are equal to or less than six obtained in risk value (RV) have no problems and all those that are greater than or equal to seven in the value of irrigation (RV) have to formulate strategies at the administrative level, technological, to define security policies that reduce the level of risk.

3.4 Equations

To mitigate the potential risks to the integrity of an organization, it is necessary to define security policies in the strategic, tactical and operational level and to define the ICT department-level strategic management.

The following formula applies in Table 3

$$N \rightarrow (P \subset X) \Rightarrow (Y * Z) = VR \quad (1)$$

In the formula 1 wherein determining the process number (N), process (P), threats (X) Frequency applied (Y) multiplied by the impact (Z) and the result obtained is the resistance value (VR). For the TVR is the sum of all risk values

$$TVR = \bar{X} = \frac{\sum x}{n} \quad (2)$$

Apply the formula two are:

$$TVR = (12 + 2 + 9 + 3 + 3 + 2) / 6$$

$$TVR = 31/6 = 5.16 \quad (3)$$

For the percentage of total risk values was:

$$PTTR = ((TVR / TTR) / 10) * 100\% \quad (4)$$

Apply the formula 4 which we are:

$$PTTR = (5.16 / 10) * 100\% = 51.6\% \quad (5)$$

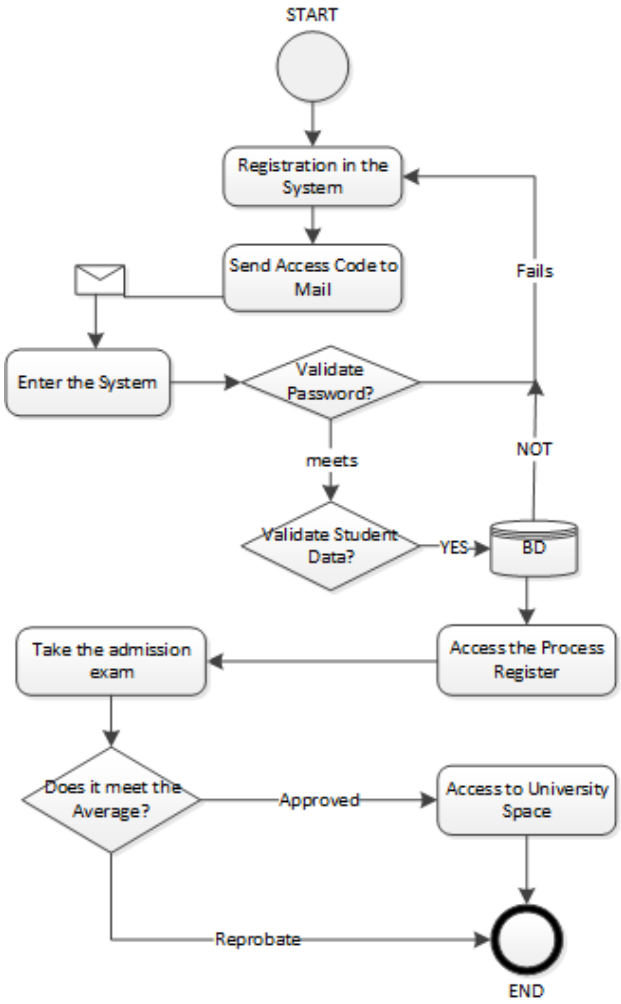

Figure. 5: Diagram of the methodology OWASP Top Ten

3.5 Flowchart of the methodology OWASP Top Ten

Figureure 5 provides the application of the methodology OWASP Top Ten, applying validations authentication must meet the quota allocation system to confront threats that may be exposed.

4. Discussion

Achievements in this research are generic so they can follow the methodology and adapt to any specific organization considering your requirements. This research does not solve the security problems of telecommunications companies; only offered an alternative that mitigates risk levels in information security.

The results are directly related to other research in this regard; for each process security model that is carried over the Internet, you should be evaluated and should set up new processes and should be integrated models deemed appropriate. We believe that the use of our risk matrix we can find safety deficiencies for which state are in addition to this, we can learn a rating of overall risk that state universities may have.

The comparison between security processes applying each of the computing methodologies provides important knowledge about COBIT, COSO ERM, OWASP TOP TEN.

Methodologies do not provide complete assurance that the platform of Higher Education is not to be violated, because there are multiple threats on the web, which should be studied, such as lack of precision, failure to prevent surprises and lack of effectiveness.

To increase security in the identification process to minimize vulnerabilities, it is also the Transport Layer Security (TLS) tool is applied under a cryptographic protocol that ensures Internet communications to prevent attacks.

The methodology OWASP Top Ten is showing greater compatibility, it presents the necessary and reliable conditions to reduce the amount of potential threats.

5. Conclusions and Future Work

In the future, it will analyze how it affects the security problems in the student population of the country.

After conducting research, we can conclude the following:

- The matrix-defined risk is an alternative to improve process safety and the flow of information and can be used as reference in these organizations.
- The different points presented in this research enable companies to create a clear picture of the different threats that are daily affected by day in order to take precautionary measures constants ratings director to its staff and consider the physical different topics day of its facilities to be much more organized models of their processes.

6. Acknowledgment

The authors thank the Salesian Polytechnic University of Ecuador, a research group Guayaquil Headquarters "Computing, security and information technology for a Globalized World" (CSITGW) created in accordance with resolution 142-06-2017-07 -19 and the Ministry of Education. Superior Science, Technology and Innovation (Senescyt).

7. References

[1] S. Moisés Toapanta Toapanta and L. Enrique Mafla Gallegos, "An Approach to Optimize the Management of Information Security in Public Organizations of Ecuador," *Fault Detect. Diagnosis Progn.*, no. November, 2020, doi: 10.5772/intechopen.88931.

[2] F. Spoto *et al.*, "Static identification of injection attacks in Java," *ACM Trans. Program. Lang. Syst.*, vol. 41, no. 3, 2019, doi: 10.1145/3332371.

[3] S. Jan, A. Panichella, A. Arcuri, and L. Briand, "Automatic Generation of Tests to Exploit XML Injection Vulnerabilities in Web Applications," *IEEE Trans. Softw. Eng.*, vol. 45, no. 4, pp. 335–362, 2019, doi: 10.1109/TSE.2017.2778711.

[4] E. Khudzaeva, F. Mintarsih, A. T. Muharam, and C. Wirawan, "Application of Clustering Method in Data Mining for Determining SNMPTN Quota Invitation UIN Syarif Hidayatullah Jakarta," *2018 6th Int. Conf. Cyber IT Serv. Manag. CITSM 2018*, no. Citsm, pp. 1–4, 2019, doi: 10.1109/CITSM.2018.8674329.

[5] A. Zhamanov, Z. Sakhiyeva, R. Suliyev, and Z. Kaldykulova, "IoT smart campus review and implementation of IoT applications into education process of university," *2017 13th Int. Conf. Electron. Comput. Comput. ICECCO 2017*, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/ICECCO.2017.8333334.

[6] Y. X. Li, Y. N. Miao, and S. Y. Lue, "A comprehensive analysis method of application in college entrance examination," *Proc. - 2017 Int. Conf. Netw. Inf. Syst. Comput. ICNISC 2017*, vol. 131, no. 1, pp. 131–134, 2017, doi: 10.1109/ICNISC.2017.00036.

[7] I. C. Silveira and D. D. Maua, "University Entrance Exam as a Guiding Test for Artificial Intelligence," *Proc. - 2017 Brazilian Conf. Intell. Syst. BRACIS 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/BRACIS.2017.44.

[8] A. Robu, I. Szeidert, I. Filip, C. Vasar, and R. Robu, "Online platform for university admission," *2018 9th Int. Conf. Information, Intell. Syst. Appl. IISA 2018*, 2019, doi: 10.1109/IISA.2018.8633616.

[9] H. C. Huang, Z. K. Zhang, H. W. Cheng, and S. W. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls," *Computer (Long. Beach. Calif).*, vol. 50, no. 6, pp. 81–85, 2017, doi: 10.1109/MC.2017.183.

[10] O. M. Awoleye, B. Ojuloge, and M. O. Ilori, "Web application vulnerability assessment and policy direction towards a secure smart government," *Gov. Inf. Q.*, vol. 31, no. S1, pp. S118–S125, 2014, doi: 10.1016/j.giq.2014.01.012.

[11] K. Qian, R. M. Parizi, and D. Lo, "OWASP Risk Analysis Driven Security Requirements Specification for Secure Android Mobile Software Development," *DSC 2018 - 2018 IEEE Conf. Dependable Secur. Comput.*, pp. 1–2, 2019, doi: 10.1109/DESEC.2018.8625114.

[12] R. Ranchal, B. Bhargava, P. Angin, and L. Ben Othmane, "EPICS: A Framework for Enforcing Security Policies in Composite Web Services," *IEEE Trans. Serv. Comput.*, vol. 12, no. 3, pp. 415–428, 2019, doi: 10.1109/TSC.2018.2797277.

[13] N. S. Ali, "Investigation framework of web applications vulnerabilities, attacks and protection techniques in structured query language injection attacks," *Int. J. Wirel. Mob. Comput.*, vol. 14, no. 2, p. 103, 2018, doi: 10.1504/ijwmc.2018.10012241.

[14] S. Braun, N. Dwenger, D. Kübler, and A. Westkamp, "Implementing quotas in university admissions: An experimental analysis," *Games Econ. Behav.*, vol. 85, no. 1, pp. 232–251, 2014, doi: 10.1016/j.geb.2014.02.004.

[15] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," *Proc. - 2017 Eur. Intell. Secur. Informatics Conf. EISIC 2017*, vol. 2017-Janua, pp. 91–98, 2017, doi: 10.1109/EISIC.2017.20.

[16] M. O. K. Qhw, "&\ EHU % XGJHW 2SWLPL] DWLRQ 7KURXJK 6HFXULW \ (YHQW," pp. 1026–1031, 2017.

[17] G. Husari, X. Niu, B. Chu, and E. Al-Shaer, "Using entropy and mutual information to extract threat actions from cyber threat intelligence," *2018 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2018*, pp. 1–6, 2018, doi: 10.1109/ISI.2018.8587343.

[18] J. S. Suroso and B. Rahadi, "Development of IT risk management framework using COBIT 4.1, implementation in it governance for support business strategy," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1306, pp. 92–96, 2017, doi: 10.1145/3124116.3124134.

[19] M. Rubino and F. Vitolla, "Corporate governance and the information system: How a framework for IT governance supports ERM," *Corp. Gov.*, vol. 14, no. 3, pp. 320–338, 2014, doi: 10.1108/CG-06-2013-0067.

[20] E. Semastin *et al.*, "Preventive measures for cross site request forgery attacks on Web-based Applications," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 130–134, 2018, doi: 10.14419/ijet.v7i4.15.21434.

[21] A. Razzaq, Z. Anwar, H. F. Ahmad, K. Latif, and F. Munir, "Ontology for attack detection: An intelligent approach to web application security," *Comput. Secur.*, vol. 45, no. 3, pp. 124–146, 2014, doi: 10.1016/j.cose.2014.05.005.

[22] 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," *Proc. 3rd World Conf. Smart Trends Syst. Secur. Sustain. WorldS4 2019*, no. July, pp. 270–274, 2019, doi: 10.1109/WorldS4.2019.8903967.

[23] N. M. Scala, A. C. Reilly, P. L. Goethals, and M. Cukier, "Risk and the Five Hard Problems of Cybersecurity," *Risk Anal.*, 2019, doi: 10.1111/risa.13309.