Machine Learning and Artificial Intelligence
A.J. Tallón-Ballesteros and C. Chen (Eds.)

doi:10.3233/FAIA200796

Analysis for the Adoption of Security Standards to Improve the Management of Securities in Public Organizations

Segundo Moisés Toapanta Toapanta[a*], Madeleine Lilibeth Alvarado Ronquillo[b], Luis Enrique Mafla Gallegos [b], Alberto Ochoa Zezzatti[c]

[a]*Department Computer Science, Salesian Polytechnic University of Ecuador (UPS), Chambers 227 and June 5, Ecuador*
[b]*Faculty of Systems Engineering, National Polytechnic School (EPN), Ladrón the Guevara E11·253, Ecuador*
[c]*Industrial and Manufacturing Department, Autonomous University of Ciudad Juarez (UACJ), Av. Plutarco Elías Calles #1210, México*

Abstract. Public organizations have the ongoing task of properly managing the security of the information they handle. The objective of this research is to analyze the security standards adopted by public organizations in Ecuador to improve their management of information security. The deductive method was applied for the review and analysis of appropriate standards for public institutions. As a result, information was obtained on the different security policies, standards and guidelines that apply, national and international public organizations. A Diagram of activities for the adoption of standards for public organizations resulted; a prototype standards-based Information Security Management Model; and an Information Security Management Matrix, from which the Risk Mitigation Percentage was calculated. It was concluded that maintaining high levels of security in public organizations requires the adoption of control standards in different areas and the collaboration of the different organizational and hierarchical levels of public organizations.

Keywords. security standards, security management, public organization, information security

1. Introduction

Public organizations have the ongoing task of properly managing the security of the information they handle. For that reason, they have had to seriously consider protecting their information through normally accepted standards that seek to prevent the institution from being a victim of cyber criminals [1]. In reference to the above, a figure from the International Telecommunication Union (ITU) mentions that Ecuador is the sixth most cybersecure country in Latin America of a total of 19 countries. At the Latin American

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

level, the most cybersecure countries are Uruguay and Brazil. While worldwide dominate Singapore and the United States [2].

Standards are written standards that are contained in a document available to the public, established by consensus and adopted by a recognized body; it establishes the rules, requirements, characteristics, guidelines or general recommendations that must be followed to achieve an optimal level of regulation in a particular area in relation to current problems or problems that may arise in the future [3].

Failure to implement security standards can bring with it a series of problems for ecuadorian public institutions, such as theft or leakage of information, whether due to digital techniques such as embedding malicious software, viruses that affect the system, keyloggers to reveal access codes, spyware to maliciously collect information from systems and use it; SQL injection attacks, denial of service attacks [4]. Then there is the social engineering through which certain people outside or related to the organization, access the internal information of the company and use it to harm it [5]. And we must not forget natural disasters such as fires, landslides, floods or human error [6].

Ecuador's public institutions are a group of organizations designed to provide and facilitate services to the community. Currently there are 3,251 public institutions that are directly part of the central public administration or others that belong to decentralized autonomous governments. These institutions have implemented a series of Comprehensive Information Systems, which has facilitated citizen processes or procedures. They are also required to integrate their information into the National Information System and their Information Security Management is evaluated by the Ministry of Telecommunications and the Information Society (MINTEL).

Several significant flaws have been identified in current management systems that have allowed:

- The data leak of 20 million Ecuadorian data between living and dead people, which included personal, banking and even tax information.
- Alteration of citizen data in databases of the Civil Registry and the National Council for Equality of Disabilities (CONADIS) in order to obtain benefits or commit criminal acts.
- Denial of service attacks on websites of public entities.

As a result of the events that have become public knowledge in recent years, citizens distrust the capacities of public institutions to ensure the confidentiality, integrity and availability of information.

At an international level, organizations such as The International Standard Organization (ISO), have elaborated the family of the ISO/IEC 27000 standard, which contains the best practices for the development, implementation and continuous improvement of Information Security Management Systems (ISMS) in organizations [7]. Implementation of this standard allows organizations of any type to properly manage the security of their assets, their financial information, intellectual property, employee details and information entrusted by third parties related to the institution in some way in Ecuador, the Ecuadorian Standardization Service (INEN) is the entity in charge of ensuring compliance with quality requirements of public and private institutions, in this sense it has powers to regulate and comply with requirements to guarantee the safety of users and the provision of a quality service. Ecuadorian Standardization Service has adopted ISO technical standards and under the Government Information Security Scheme (EGSI) together with the Ministry of Telecommunications and the Information Society (MINTEL), periodically evaluate the Security Management of the Information from Ecuadorian public organizations.

The objective of this research is to analyze the security standards adopted by public organizations in Ecuador to improve their management of information security.

¿Does the implementation of security standards in a public organization help improve the management of information security?

The adoption of security standards based on international regulations allows organizations to establish policies, procedures and controls with the aim of reducing the risks to which the information is exposed. Due to the security controls installed, an improvement in security management can be achieved, in terms of efficiency and continuous improvement.

Assessing information security levels in each of its dimensions will ensure business continuity, as well as early identification of security risks and potential damage to information. The evaluation of security controls and metrics is necessary since they provide information for decision-making at the three decision levels of organizations: operational, tactical and strategic [8].

Related references: An approach of National and International Cybersecurity Laws and Standards to Mitigate Information Risks in Public Organizations of Ecuador [9], An Empirical Study of Information Security Management Success Factors [10], Critical Success Factors Analysis on Effective Information Security Management: A Literature Review [11], Cyber-security Policy Framework and Procedural Compliance in Public Organisations [12], Identifying factors of "organizational information security management" [13], Organizational factors to the effectiveness of implementing information security management [14], Security Related Issues In Saudi Arabia Small Organizations: A Saudi Case Study [15], Analysis of Appropriate Standards to solve Cybersecurity problems in Public Organizations [16], Adapting ISO 27001 to a Public Institution [17], Ecuadorian Standardization Service [18].

The deductive method was applied for the review and analysis of appropriate standards for public institutions that allow the improvement of information security management.

The results obtained were: a Diagram of activities for the adoption of standards for public organizations; a prototype standards-based Information Security Management Model; and an Information Security Management Matrix, from which the Risk Mitigation Percentage was calculated.

Maintaining high levels of security in public organizations requires the adoption of control standards in the different areas and the collaboration of the different organizational and hierarchical levels of public organizations.

2. Materials and Methods

In the first instance in Materials, was made a search for information from different sources that allowed defining the standards used in public government organizations and the adoption process. Secondly, in Methods, the steps to achieve the results were defined.

2.1 Materials

2.1.1 Governmental Information Security Scheme – EGSI

Ecuadorian public organizations have the obligation and responsibility to protect the information they handle, much of this information has to do with citizens and another

part strictly with the internal management of the company. In any case, with the advancement of Information and Communication Technologies (ICT), state organizations have given greater attention to the protection of their information assets and thus generate confidence in citizens that their data is safe [16].

In Ecuador, Ministerial Agreements have been issued in order to efficiently and effectively manage information security in public entities. In turn, it maintains the Commission for Computer Security and Information and Communication Technologies in charge of computer security issues for government entities [16]. This commission was created with the purpose of analyzing the situation of information security in public institutions belonging to the Ecuadorian state and has come to determine the need to apply rules and procedures for information security, and incorporate culture and institutional processes, its permanent management, for this purpose the Government Information Security Scheme (EGSI) was prepared.

The objective of the EGSI is to increase the security of information in public entities. The implementation of the EGSI is carried out through the Continuous Improvement Cycle (PDCA), which has four steps: Plan, Do, Act and Verify.

Table 1: EGSI Compliance Classification

% of milestones met	EGSI Compliance Level Weighting
90% a 100%	High
75% a 89%	Medium
50% a 74%	Regular
<50%	Low

The EGSI is divided into 11 sections and has 126 priority guidelines or milestones that must be evaluated and met by public organizations in Ecuador [16]. The final qualification of compliance with the EGSI is performed according to Table 1.

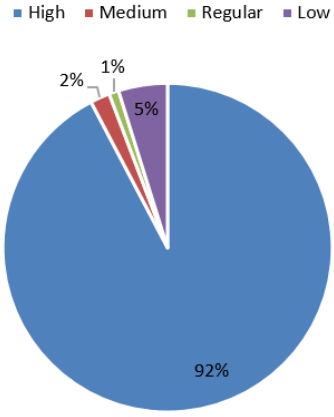

Figure 1. EGSI compliant entities

Figure 1 shows the level of compliance of public organizations in Ecuador, according to the milestones that organizations must meet.

2.1.2 ISO/IEC 27001: 2013

ISO/IEC 27001: 2013 is the international standard that governs the management of information security. It specifies the requirements that organizations must follow regarding the implementation of an Information Security Management System (ISMS) [17]. ISO/IEC 27001: 2013 defines information security as a preservation of the confidentiality, integrity and availability of information, essential dimensions that must be covered to a greater or lesser extent, controls, standards established in an organization [11].

2.1.3 ISO/IEC 27002: 2013

Describes the Code of Practice for the implementation of information security controls. ISO / IEC 27002: 2013 provides guidelines for organizational information security standards and information security management practices, including the selection, implementation and management of controls taking into account the information security risk environments of the organization [13]. Through ISO / IEC 27002: 2013, institutions will be able to select the appropriate standardized controls that will form part of the Information Security Management System for the organization. Through this standard, companies can also develop their own information security management guidelines. The standard has 114 controls, grouped into 14 domains and 35 control objectives that organizations can adapt according to their nature [6].

2.1.4 INEN ISO/IEC 27002

INEN ISO / IEC 27002 is the Ecuadorian technical standard, aimed at institutions derived from the Central Public Administration, whose objective is the adequate Management of Information Security. This standard is a translation of the ISO / IEC 27002 standard, so its structure is the same as that of the international standard. The implementation of the standard established by INEN serves as a reference for public institutions to select and adopt commonly accepted controls as part of the implementation process of the Government Information Security Scheme (EGSI) [18]. According to this standard, the assets of an organization are in constant threat of being affected, in which processes, systems, networks and people are involved. Changes in processes, business systems and other external changes can be causes of risks for information security, so it is necessary to implement a set of appropriate controls: policies, processes, procedures, organizational structures using resources software and hardware to ensure an organization meets its security objectives and strategic objectives.

2.2 Methods

The objective of this study was to analyze the security standards that Ecuadorian public organizations can adopt to improve their management of information security. For this, the deductive method was applied to review and analyze the appropriate standards for public institutions.

With the objective of evaluating the impact on the Management of information security produced by the adoption of security standard controls, scales of assessment of Confidentiality, Integrity and Availability of information were developed and used.

The creation of the prototype of the Information Security Management model was carried out based on the analysis of the ISO IEC 27001 and 27002 standard. From the 27001 standard, the dimensions of information security were considered: confidentiality, integrity and availability. In the same way, the 14 domains of the 27002 standard were considered, resulting from the analysis of 4 proposed dimensions that are part of public organizations.

For the evaluation of the impact produced by the adoption of controls in the Information Security Management, an agency of the Civil Registry of Ecuador was taken as a reference, which is part of the institutions that have completed the first phase of the EGSI.

Table 2: Scale to assess Confidentiality of information

Scale	Value	Criterion
High	3	Control is essentially important and has a crucial effect in ensuring the confidentiality of information
Medium	2	The control in place is moderately important to ensure the confidentiality of the information
Low	1	The established control is important to ensure the confidentiality of the information

Table 2 shows the rating scale of the Confidentiality of the information. The integrity and availability of the information were assessed based on the same scale. The objective of this assessment was to provide qualitative values to each quantitative value, depending on the importance of establishing control to ensure company information. The quantitative assessment of the dimensions of information security, then allowed calculating the assessment of the impact of controls, which was carried out by applying the following formula:

$$VIC = \frac{C + I + D}{n} \tag{1}$$

Where C is Confidentiality, I is Integrity, D is Availability, VIC is Control Impact Assessment and n is the Number of security dimensions evaluated, which for the case is 3.

Table 3: Control Impact Assessment Scale

Scale	Value	Criterion
High	3 - 2	Must be installed immediately
Medium	1,99 - 1,01	It must be established in the shortest possible time
Low	1	Must be established when resources are available

The results of the Control Impact Assessment were weighted using the scale in Table 3. Then the Risk Mitigation Percentage is calculated. To do this, first calculate the average VIC using the formula:

$$\bar{X} = \frac{\sum x}{n} \tag{2}$$

Finally, with the mean of X the Risk Mitigation Percentage was calculated, dividing the mean of X for the maximum score that each control can obtain, in this case 3 and multiplying by 100%.

$$PRM = \frac{\bar{X}}{3} * 100\% \tag{3}$$

3 Results

3.1 Diagram for the Adoption of Standards in Public Organizations

The improvement of Information Security Management in public organizations can be achieved through the adoption of standards, this requires that a series of basic steps be followed:

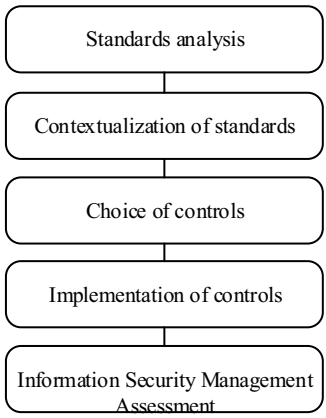

Figure 2. Adoption of standards to improve information security management

Figure 2 shows the activities that must be followed to improve Information Security Management in Public Organizations. The first step is the review and analysis of national and international standards, the second step is to contextualize the standards according to the nature of the organization to know if the controls belonging to that standard are applicable to the public organization, the third step is the choice of the information

security controls most appropriate to the nature of the organization, the fourth step is the implementation of said controls, the last step is the evaluation of the Information Security Management achieved with the implementation of the controls.

3.2 Prototype of a Standards-based Information Security Management Model

The analysis of the national and international norms and standards to which the public institutions of Ecuador must abide, allowed the creation of the following prototype of the Information Security Management Model based on standards.

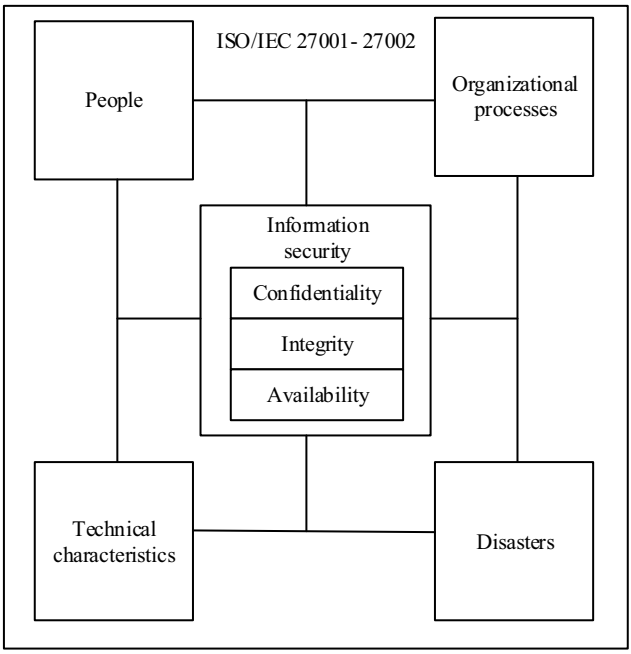

Figure 3. Standards-based information security management

This prototype integrates the domains of the ISO/IEC 27002 standard which were classified into 4 dimensions: People, Organizational Processes, Technical Characteristics, and Disasters. Information security management is carried out on these 4 dimensions to achieve satisfactory levels of information security in terms of its 3 dimensions: Confidentiality, Integrity and Availability.

The different controls of ISO/IEC 27002 that are part of the 4 dimensions represented in the model in Figure 3, can be evaluated with the Minimum Distance Method. The Minimum distance to an ideal point method is a method that allows evaluating different object parameters in a n-dimensional unit mathematical space. The minimum distance method is a methodology that can be used to assess computer security in organizations [6]. With this method, public organizations can evaluate controls from adapted standards, using the following equation:

$$d = \sqrt{(X_i - X_1)^2 + (X_i + X_2)^2 + \cdots (X_n - X_m)^2} \quad (4)$$

Eq. 4 calculates the Euclidean distance, distance from any point in n-dimensional space to the perfect point (1, 1, 1, ...) or the point that the user defines as an ideal point taking into account their requirements and available resources, from there you can decide how to spend resources to manage computer security, this is very useful when it comes to optimizing resources and it is required to give higher priority to some controls than others. Depending on whether (1, 1, 1, ...), or any other point was set as the ideal point, the parameter values can take values very close to one or the ideal point, which means that they are more important than the others; and therefore, the organization will spend more resources to control said parameters.

3.3 Information Security Management Matrix

A security management matrix was carried out in which different controls that the public organizations implement were weighted, according to the impact that said control produces in maintaining the security of the information evaluated in its 3 dimensions.

Table 4: Information Security Management Matrix

Controls	Impact on information security				Scale
	C	I	D	VIC	
Biometric	3	1	1	1,67	Medium
Security cameras	3	1	1	1,67	Medium
Firewalls	2	2	2	2	High
Antivirus	2	2	1	1,67	Medium
Wireless controller, access points	2	1	1	1,33	Medium
Hard disk backups	1	3	3	2,33	High

The generated matrix is shown in Table 4, where the backup of hard drives obtained the highest impact value in Information Security Management, followed by the implementation of firewalls. The wireless controller for access points is the control that obtained the lowest rating.

It was determined that the backup of hard drives and the implementation of firewalls, are controls that cause a high impact in the improvement of Information Security Management, so these controls must be implemented immediately in order to safeguard the information and organization assets. The installation of biometrics, security cameras, antivirus and configuration of wireless controller of access points, are controls that cause a medium impact so they must be implemented in the organization in the shortest possible time.

3.4 Calculation of Risk Mitigation Percentage

The results obtained in the Control Impact Assessment were used to calculate the Risk Mitigation Percentage.

$$\bar{X} = \frac{1,67 + 1,67 + 2 + 1,67 + 1,33 + 2,33}{6} = 1,78 \tag{5}$$

Eq. 5 calculated the average of the impact evaluations of the controls.

$$PRM = \frac{1,78}{3} * 100\% = 59,3\% \tag{6}$$

The calculation of the Risk Mitigation Percentage was carried out by applying Eq. 3 and allowed determining areas in which controls should be improved to reduce the risks related to information.

4 Discussion

This work presents an analysis for the adoption of Security Standards in order to improve Security Management in Public Organizations. Any public organization that intends to adopt national and international standards may apply the methodology proposed in this work.

The Information Security Management model developed considered the dimensions described in ISO / IEC 27002, in another study [17], and the ISO / IEC 27001.

In this study, an Information Security Management Matrix was developed based on the impact produced by the selected controls of the ISO / IEC 27002 standard according to the nature of the organization; contrary to what has been done in other studies where they analyze the impact of a risk becoming a threat, which helps determine the level of risks according to their impact and probability of occurrence; however, the proposal developed in this study is a more simplified alternative that focuses on Safety Management for risk mitigation.

The Risk Mitigation Percentage found for a public organization was 59.3%. In a similar investigation [9], this percentage was 58.6%.

5 Future Word and Conclusion

In the future, the factors that positively or negatively influence the adoption of standards in public organizations should be investigated.

Maintaining high levels of security in public organizations requires the adoption of control standards in different areas and the collaboration of the different organizational and hierarchical levels of public organizations.

The improvement of Information Security Management requires its evaluation in its three dimensions: Confidentiality, Integrity and Availability and is achieved with adequate management of people, organizational processes, technical characteristics and disasters around the controls described in the standard. ISO / IEC 27002.

The backup of hard drives and the implementation of firewalls are controls that produce a greater impact to ensure the security of the information, so they must be implemented immediately in all public institutions in order to over-safeguard the

information of the organization. The installation of biometrics, security cameras, antivirus and wireless access point controller configuration are controls that cause a medium impact, therefore they must be implemented in public organizations in the shortest time possible.

Most of Ecuador's public organizations have implemented the Government Information Security Scheme (EGSI) in conjunction with the INEN ISO / IEC 27002 standard, which demonstrates the progress of Ecuadorian public organizations in the area of protection and management of information security.

Acknowledgments

The authors thank to Universidad Politécnica Salesiana del Ecuador, to the research group of the Guayaquil Headquarters "Computing, Security and Information Technology for a Globalized World" (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaría de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

References

[1] Cannon G, Statham P, Yamada A. Biometric Security, Standardization. Encycl Biometrics. 2009;122–9.
[2] Ministerio de las Telecomunicaciones y de la sociedad de la información. Ecuador ocupa sexto lugar en la región, según Índice de Ciberseguridad. [Internet]. [Consulted 10 Jul 2012] Available in https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/
[3] Olifer D. Evaluation metrics for ontology-based security standards mapping. 2015 Open Conf Electr Electron Inf Sci eStream 2015 - Proc. 2015;17–20.
[4] Heimes R. Global InfoSec and Breach Standards. IEEE Secur Priv. 2016;14(5):68–72.
[5] Sedinić I, Perušić T. Security Risk Management in complex organization. 2015 38th Int Conv Inf Commun Technol Electron Microelectron MIPRO 2015 - Proc. 2015;(May):1331–7.
[6] Felipe FD, Acevedo EM, Sanchez MM. Evaluating informatics security in an organization: The minimal distance method. Proc 2017 IEEE 24th Int Congr Electron Electr Eng Comput INTERCON 2017. 2017;17–9.
[7] Lontsikh PA, Karaseva VA, Kunakov EP, Livshitz II, Nikiforova KA. Implementation of information security and data processing center protection standards. In: 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. 2016. p. 138–43.
[8] Doynikova E, Fedorchenko A, Kotenko I. Ontology of metrics for cyber security assessment. ACM Int Conf Proceeding Ser. 2019.
[9] Toapanta SMT, Gurumendi AJ, Gallegos LEM. An approach of national and international cybersecurity laws and standards to mitigate information risks in public organizations of ecuador. ACM Int Conf Proceeding Ser. 2019;(December):61–6.
[10] Zammani M, Razali R. An empirical study of information security management success factors. Int J Adv Sci Eng Inf Technol. 2016;6(6):904–13.
[11] Tu Z, Yuan Y. Critical success factors analysis on effective information security management: A literature review. 20th Am Conf Inf Syst AMCIS 2014. 2014;1–13.
[12] Lubua EW, Pretorius PD. Cyber-security policy framework and procedural compliance in public organisations. Proc Int Conf Ind Eng Oper Manag. 2019;(July):1847–56.
[13] Singh AN, Gupta MP, Ojha A. Identifying factors of "organizational information security management." J Enterp Inf Manag. 2014;27(5):644–67.
[14] Chang SE, Ho CB. Organizational factors to the effectiveness of implementing information security management. Ind Manag Data Syst. 2006;106(3):345–61.
[15] Almubayedh D, Khalis M Al, Alazman G, Alabdali M, Al-Refai R, Nagy N. Security Related Issues in Saudi Arabia Small Organizations: A Saudi Case Study. 21st Saudi Comput Soc Natl Comput Conf NCC 2018. 2018;1–6.
[16] T SMT, E GSG, Enrique L, Gallegos M. Analysis of Appropriate Standards to solve Cybersecurity

problems in Public Analysis of Appropriate Standards to solve Cybersecurity problems in Public Organizations. In 2020.
[17] Carvalho C, Marques E. Adapting ISO 27001 to a Public Institution. Iber Conf Inf Syst Technol Cist. 2019;2019-June(June):19–22.
[18] Servicio Ecuatoriano de Normalización. NTE INEN-ISO/IEC 27002. 2017.