We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

186,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter

An Approach to Optimize the Management of Information Security in Public Organizations of Ecuador

Segundo Moisés Toapanta Toapanta
and Luis Enrique Mafla Gallegos

Abstract

The problems of information security in public organizations in Ecuador are evident, which, as a result, have led to corruptions that are present at all levels of operational, tactical and strategic management. The objective of this chapter is to analyze the available information found in different media, written, spoken, among others. The deductive method was used for the collection of information and observation techniques. It turned out the improve in the administrative processes, prototype diagram of sequence of access of users and services, prototype of integration of technologies of security of the information for public organizations of Ecuador. It was concluded that to avoid corruption in a country change should happen at all levels: the way of thinking and culture of the inhabitants, laws, penalties to politicians without parliamentary immunity, application of information and communications technologies (ICT) in an appropriate manner, and complying with international standards in information security. To improve information security, administrative policies on information security must be changed, and technologies related to immutable security algorithms, Ledger, Hyperledger, etc., must be used.

Keywords: information security, information security management, database security, public organizations of Ecuador, security models, cryptography

1. Introduction

Public organizations in Ecuador have problems in the management of Information Security. The "Ministry of Telecommunications and the Information Society" ratify that information security problems persist. According to the publication of the "White Book of the Information and Knowledge Society", it turned out that only 8% comply with the Security Policies, and those responsible for information security that are part of IT have 51% and that are part of Contingency Plan only have 16%, among other security indicators [1].

The company Deloitte conducted a study in 2017 concerning the problem of information security, and the results were published by the "White Paper on the Information and Knowledge Society," in which more than 50 national and

multinational companies participated to improve information security management and the following was determined:

1. Around 50% had some security breach, and of this, 20% could not determine the impact of this gap, since they did not have an incident management process.

2. Nearly 50% indicated that their main initiative for 2018 will be training and awareness in information security.

3. More than 50% cited as one of their main difficulties the lack of budget, followed, very closely, by aspects such as the lack of visibility and influence and the lack of competent personnel.

4. Around 75% did not measure the return on investments in information security.

5. The 20% were prepared to face security incidents, originated in social networks.

6. The 60% did not have an SOC (Security Operation Center); meanwhile, almost 20% said they will have one by 2018.

7. The 36% did not have a disaster recovery plan.

8. As a result of internal and external reviews of companies, user management remains the most shaky element in the management of CISOs (Chief Information Security Officer (Deloitte, 2017) [1].

Among others defined by the CENDIA published in 2017 that is recorded in the "White Paper of the Information and Knowledge Society".

The implementation projects of the Information Security Management System ISO 27000 ensure all the information assets to have complete control of the organization according to what is stated in the book "Public Companies and Planning" [2].

The security of information is critical today in all public or private organizations; based on this reason, it is necessary that Latin and world universities generate specialized careers in the area of information security to provide qualified personnel considering that information security is a key aspect for the management of an organization [3].

With the foregoing, it is confirmed that public and private organizations in Ecuador and in a large part of the world have serious problems of information security. Information is considered as data, videos, sound, and documents, among others, that can be saved, shared, socialized, etc.

Therefore, mishandling of information can lead to failure of organizations; on the other hand, correct decisions can be made based on information that provides confidentiality, integrity, and authenticity.

In accordance with the current paradigms in information security and computer auditing, the following most relevant points to be considered by public organizations to improve information security management were determined:

1. Change of information security culture in first level executives, so that they consider that information security is not a cost, but is an investment to guarantee the mission, vision, and strategic objectives of an organization.

2. All persons working in public organizations, both the first authority and the lowest office, which may be the custodian or guard, are an important

and responsible party in order to maintain the integrity of the information. One of the main errors in the management of information security in public companies is that we are convinced that only those who handle information or strategic managers are responsible.

3. The structural and functional organizations currently available to public organizations do not allow information and communications technologies (ICT) coordinators/directors/managers to govern the organization.

4. The lack of planning and control in a globalized way for the generation of security plans, contingency, backup, and protection against natural disasters, etc., causes vulnerabilities, risks, and threats in the security of information in the organization.

5. Adequate security models and technologies are required for each public organization considering the mission, vision, and strategic objectives.

6. There should be qualified personnel with experience with an average 10 years in the area of information security and with academic training at all levels (Engineering, Master's, and Doctorate) in the same area of knowledge in accordance with the provisions of UNESCO, SENESCYT, CES (title nomenclature) [4].

7. The World Bank determines that one of the main causes for corruption in Latin America and the Caribbean is that there is no adequate management of Information and Communications Technologies (ICT) in the area of Information Security, and proposes to use it as technologies' alternative such as blockchain, Ledger, and Hyperledger. It also clarifies that as long as there is direct human intervention in the processes and no adequate technologies are used, there will be a greater probability of corruption and the only ones who pay for this incorrect management will be the low-income inhabitants [5].

2. Security of the information

Information security worldwide is considered the main fixed asset of a public or private organization. With the appropriate management of information, corruption in public-private organizations can be avoided, such as transfers of money without due authorization, terrorist attacks, information theft, manipulation of processes and legal reports, kidnappings, violations, accidents, prevention of natural disasters, etc.

2.1 Pillars of information security

To carry out the analysis of information security, the current situation and the functions of the security pillars must be considered clearly: vulnerabilities, risks, threats, which will have a direct relationship with the identity, authenticity, authorization, and audit (IAAA), so that the information is with confidentiality, integrity, and availability (CIA).

The following is a structure for the security of information in public organizations of Ecuador, considering the pillars of security to mitigate the vulnerabilities, threats, and risks of information.

Figure 1 shows that information systems have vulnerability, threats, and risk generation and have two layers of security that are covered first with the identity,

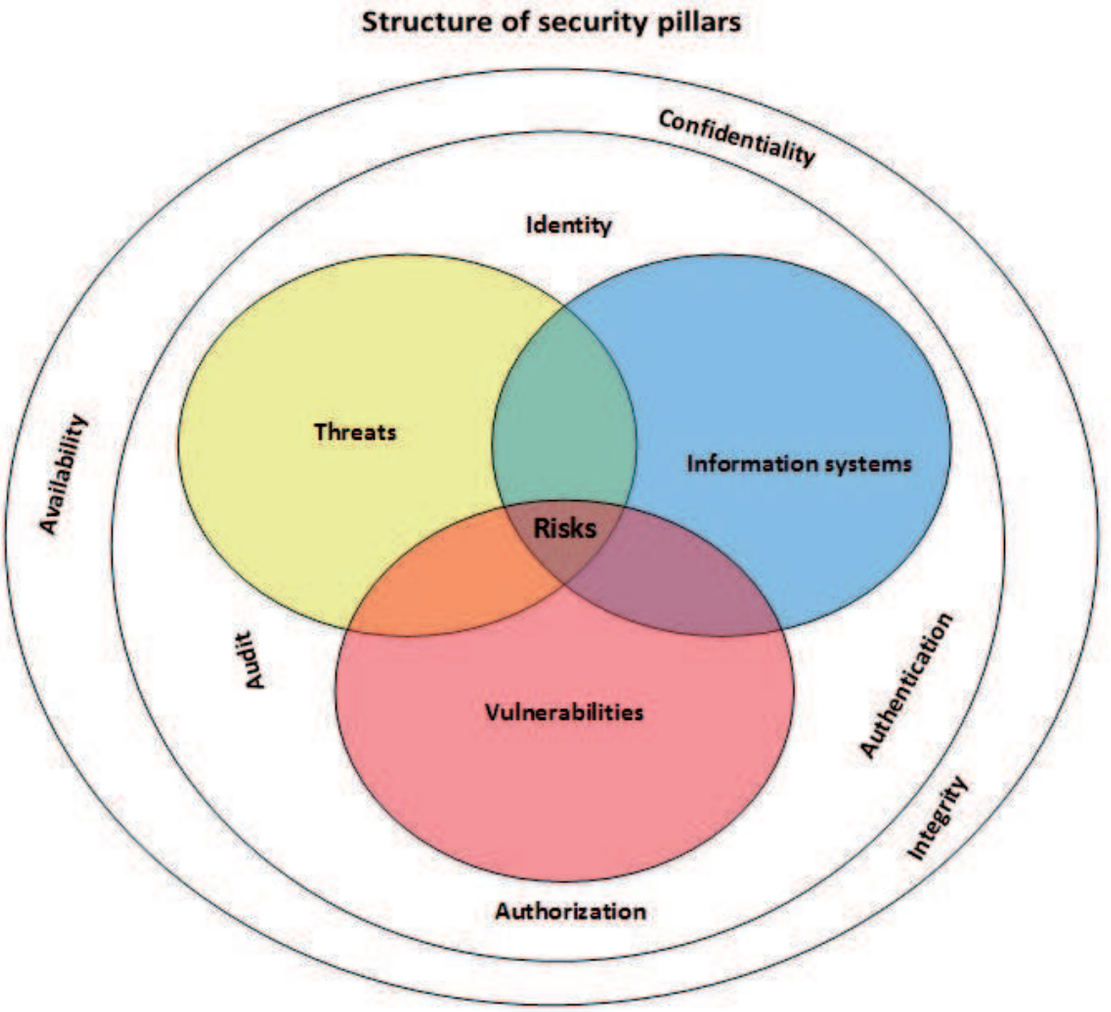

Figure 1.
Pillars of information security.

authentication, authorization, and audit (IAAA) and the second with the confidentiality, integrity, and availability (CIA).

2.1.1 Analysis of information security pillars

Public organizations in Ecuador have vulnerabilities, and as a result, threats and risks are generated for not having adequate procedures for users to have identity, authenticity, authorization, and audit (IAAA), so that the delivery of the information to internal and external users is with confidentiality, integrity, and availability (CIA), then the general description of the following pillars of security will be made.

- Identity is considered to internal or external users who have access to information.
- Authentication corresponds to the identification of users for access through technological or manual system.
- Authorization corresponds to what information the user who has been identified and has an authentication is entitled.
- Audits are the processes and activities performed in the user and recorded in a log to store their identity, authentication, and authorization, to be used at any time in processes of computer audits.

- Confidentiality of the information is considered to be the right that guarantees access only to the personnel that previously have authorization under its responsibility.

- Integrity of the information is when the information is not modified from the beginning of its generation until the final delivery to the authorized persons.

- Availability of information, so that it can be used by users; depending on a technological infrastructure, the availability of information can be guaranteed.

2.1.2 Consequence due to the incorrect management of information security

To solve the problems of the security information of vulnerabilities, risks, threats, which has a direct relationship with the identity, authenticity, authorization, audit (IAAA) and with the security triangle confidentiality, integrity, availability (CIA), one of the alternatives is to carry out the risk analysis; apply the Cobit 5.0 methodology references adapted to the public organization regarding information security ISO 27001; evaluate the degree of knowledge and implementation of information security management systems, based on the norm NCh-ISO 27001, ITIL, COSO; generate or adopt models and appropriate security technologies for each organization; apply immutable security algorithms; generate or adopt own methodologies of the organization for the change of computer culture; and make plans of security, among others.

2.1.3 Alternatives to solve information security problems

To solve the problems of vulnerabilities, risks, threats; which has a direct relationship with the identity, authenticity, authorization, audit (IAAA) and with the security triangle confidentiality, integrity, availability (CIA); one of the alternatives is: Carry out the risk analysis, Apply the Cobit 5.0 methodology references adapted to the public organization regarding information security ISO 27001, evaluation of the degree of knowledge and implementation of information security management systems, based on the norm NCh-ISO 27001, ITIL, COSO, generate or adopt models, appropriate security technologies for each organization, apply immutable security algorithms, generate or adopt own methodologies of the organization for the change of computer culture, make plans of security among others.

Also take as a reference other similar projects such as the one applied in a health institution in Chile [6].

3. Related investigations

3.1 Publications related to the research topic

Below is a list of the articles published in different conferences and scientific journals directly related to the public organizations of Ecuador, in the area of information and communications technologies (ICT) and information security.

Indicator Model for measuring the Alignment between Institutional Strategies and ICT Strategies for a Public Sector Company [7], Las TIC en el Ecuador [8], Tecnologías de Información y Comunicación Impactan la Optimización de los Procesos para el Desarrollo Local [9], Analysis to define management of identities access control of security processes for the registration civil from Ecuador [10], security analysis of civil registry database of Ecuador [11], an approach to information security by applying a conceptual model of identities in smart cities projects [12], adequate

security protocols adopt in a conceptual model in identity management for the civil registry of Ecuador [13], analysis of model Clark Wilson to adopt to the database of the civil registry of Ecuador [14], mitigating the security of the database by applying a conceptual model of integrity for the civil registry of Ecuador [15], a security algorithms approach to apply to the civil registry database of the Ecuador [16], conceptual model for identity management to mitigate the database security of the registry civil of Ecuador [17], adoption of the Hash algorithm in a conceptual model for the civil registry of Ecuador [18], an approach of efficient security algorithms for distribute architectures [19], biometric systems approach applied to a conceptual model to mitigate the integrity of the information [20], algorithms for efficient biometric systems to mitigate the integrity of a distributed database [21], analysis of efficient processes for optimization in a distributed database [22], analysis of HIPAA for adopt in the information security in the civil registry of the Ecuador [23], a blockchain approach to mitigate information security in a public organization for Ecuador [24], analysis of the appropriate security models to apply in a distributed architecture [25], optimization of an electronic signature scheme in a voting system in a distributed architecture [26], ensuring the blind signature for the electoral system in a distributed environment [27], analysis cryptographic for electronic votes in systems of distributed architectures [28], an approach to the efficient security algorithms used in voting scanning in an electoral process [29], a homomorphic encryption approach in a voting system in a distributed architecture [30], analysis of security algorithms for a distributed database [31], a Hyperledger scheme for the deployment of smart contracts in a public organization of Ecuador [32], analysis of adequate bandwidths to guarantee an electoral process in Ecuador [33], appropriate security protocols to mitigate the risks in electronic money management [34], cryptographic algorithms to mitigate the risks of database in the management of a smart city [35], impact on the information security management due to the use of social networks in a public organization in Ecuador [36], an information security approach in the armed forces of Ecuador [37].

3.2 General summary of articles published by segments

- The management of information and communications technologies (ICT), Models of Indicators, allows to visualize all the processes and activities in general form of public institutions that must be analyzed with priority to be considered strategic [7–9].

- The analysis of information security regarding models, technologies, conceptual models, security protocols, prototypes, and cryptographic algorithms, among others, for the civil registry of Ecuador 10–25].

- They support the analysis, design, models, and prototypes of security for the National Electoral Council to mitigate the risks in the integrity of the information that will be delivered from the electoral processes [26–33].

- Analysis of appropriate security protocols to guarantee the cash flow of public organizations using electronic money [34].

- Cryptographic analysis that allows improving the security of data in smart cities that involve the main cities of Ecuador such as Quito, Guayaquil, and Cuenca, among others [35].

- Impact of social networks on information security in public organizations, as it affects both internal and external users to prevent the information from being disclosed without control [36].

Odr.	Public organization name	Priority		
		Low	Half	High
1	National directorate of the civil registry of Ecuador			x
2	National electoral council			x
3	National directorate of public data			x
4	National council of the judiciary			x
5	National assembly			x
6	General comptroller of the state			x
7	Joint command of the armed forces			x
8	Secretaria de gestión de riesgos			x
9	National secretary of higher education science, technology and innovation (SENESCYT)			x
10	Central bank of Ecuador			x
11	National secretary of planning and development, Ecuador			x
12	Ministry of communications and the information society			x
13	Superintendency of banks			x
14	Internal revenue services of Ecuador among others			x

Table 1.
Main organizations of Ecuador that should be evaluated in the first phase.

- The security of information in the joint command of the armed forces of Ecuador is important to analyze because it guarantees the internal and external sovereignty of the country [37].

3.3 Priority of Ecuador's public organizations for the analysis

It defines public institutions that have problems in the management of information and communications technologies (ICT) and information security [1]. For this analysis, public organizations with the highest priority for the evaluation of information security management are considered; the same that in the medium term should be analyzed [7–8]. We must mention that all public organizations in Ecuador must improve the management of information security, but it should be done in phases.

In **Table 1**, the public organizations that should be in the first phase are detailed, considering that they have a high priority for the interrelation they have in state processes, to reduce corruption with the use of appropriate information and communication technologies.

4. Models, security technologies, and good practices

To apply the models, security technologies, and good practices, the mission, vision, and strategic objectives of each organization must be analyzed; it is not appropriate to apply the same to everyone, given that each organization will have its priorities for the application of confidentiality, integrity, and availability of information. Each model, technologies, and good practices have different strengths, which can be applied appropriately [38].

4.1 Security models

4.1.1 Model Clark-Wilson

The Clark-Wilson model is based on four principles: authentication, audit trail, separation of obligations, and well-formed transactions.

Clark-Wilson is a widely used model to protect business information against unauthorized modification. In the CW model, the data in the system are requested in two groups:

- Restricted data elements (CDIs) that are elements or objects whose integrity must be maintained
- Unrestricted data elements (UDIs) that are elements or objects that are not covered by the integrity policy, such as the input data, but which are relevant since they can be transformed into CDIs [39]

4.1.2 Chinese Wall Model

The Chinese Wall model is oriented to guarantee the confidentiality of the information it raises and provides controls to reduce conflicts of interest that may exist between organizations that handle the same business logic [40].

4.1.3 Model Bell-LaPadula

The Bell-LaPadula model's strength lies in multilevel security, which does not allow sensitive information to be filtered by people or entities that do not have the appropriate level of access; this helps maintain a certain degree of confidentiality [41].

4.2 Security technologies

4.2.1 Cryptography

The importance of cryptography is that it is the only current method able to enforce the objective of computer security "maintain privacy, integrity, and authenticity" and enforce nonrejection, related to not being able to deny authorship and reception of a message sent [42].

4.2.2 Log inmutables

Applications require robust and inviolable registration systems, for example electronic voting or bank information systems. At Scytl, we use technologies called immutable records, which are implemented in electronic voting solutions. This technology ensures the integrity, authenticity, and nonrepudiation of the generated records; therefore, in case of any event, the auditors can use them to investigate the problem. To improve the integrity of the information, an implementation for immutability is required, the integrity tests of the secure registers within the chain of blocks known as Bitcoins that is based on SHA-1 [43].

4.2.3 Biometric systems

Biometrics is considered a solution in information security problems; biometrics has the necessary assurances that the information stored in databases in institutions

cannot be manipulated and lose their integrity. There are some types of biometric systems that can be used, such as fingerprint, iris reader, facial recognition, and voice recognition. The use of multimodal biometrics has been considered in the study [44].

4.2.4 Ledger

The Ledger technology is based on the blockchain that ensures the registration of information in a distributed architecture, at the highest possible level, despite being distributed. With Ledger technology, we are thinking of a specific purpose distributed network, a network that shares a local maintenance [45].

4.2.5 Hyperledger

It is a technology that consists of a network infrastructure based on blockchain. Hyperledger fabric (HLF) is an open source implementation of a distributed accounting platform to execute intelligent contracts in a modular architecture. The implementation of Hyperledger technologies will mitigate the risks of information; because in all the transactions you make, you will register through immutable log [46].

4.3 Good practices

All public organizations must apply good information security practices such as those defined in ISO 27001, define appropriate indicators, change of culture in the area of information and communications technologies (ICT) by executives, consider the Cobit 5.0 methodology that the technologies of information and communications govern the organization (separate what is management and government).

In addition, the following good practices are suggested: update systems, limit users, block output systems, separate the most important files, automate, monitor permanently, define safety standards, unify processes, and educate internal and external users.

5. Alternatives to improve information security

In this research, several alternatives were analyzed to improve the security of the information such as mechanical safety that is applied in an appropriate way for each organization and definition of all the processes of each public organization, models, prototypes, and cryptographic security algorithms using techniques of flow chart, etc. [7–33].

5.1 Description in general

It should be noted that in the publications of the reference of [7–33], you can find the following information:

The situation of Information and Communications Technologies (ICT) in Ecuador, definition of processes, conceptual security models, cryptographic algorithms, security models, analysis of security protocols, technological infrastructures, technologies, applied to public organizations in Ecuador in this case to the Civil Registry and National Electoral Council of Ecuador. To be considered as alternatives to improve the management of information security.

6. Proposals to improve information security

After having analyzed all the published articles [5–31] that are directly related to this chapter of the book, the following activities to improve the management of information security are proposed to be carried out.

6.1 Improve administrative processes

In administrative processes, it is important that planning bodies modify the functional structural organization of public organizations, considering the good practices of Cobit 5.0. In the organic structure, the general manager (CEO) and the information and communications technologies (ICT) manager (CIO) must be at the same level.

Figure 2 defines a generic structure chart suitable for public organizations where the manager/coordinator/director of information and communications technologies (ICT) can govern the organization to comply with the recommendations of Cobit 5.0.

6.1.1 Change of culture in information and communications technologies (ICT)

To make the change in the information and communications technologies (ICT) culture, a training plan is required, with an appropriate methodology at all operational, tactical, and strategic levels, especially at the strategic level so that they are clear. For an organization to be competitive and the management of information security to improve, information and communications technologies (ICT) must govern public organizations.

This change of culture at the level of high-level officials of public organizations is necessary to execute, considering that 95% of the authorities of public organizations defined by information and communications technologies (ICT) at the operational level are convinced that they are simply a support for the management of the organization [7].

6.1.2 Processes and activities that should be considered

To carry out this activity, it can be executed through different types of indicators in the information and communications technologies (ICT) area; in this case, the following indicators are used as an alternative: Degree of Utilization, Degree of Support for the Process, Degree of Use, Degree of Online Support,

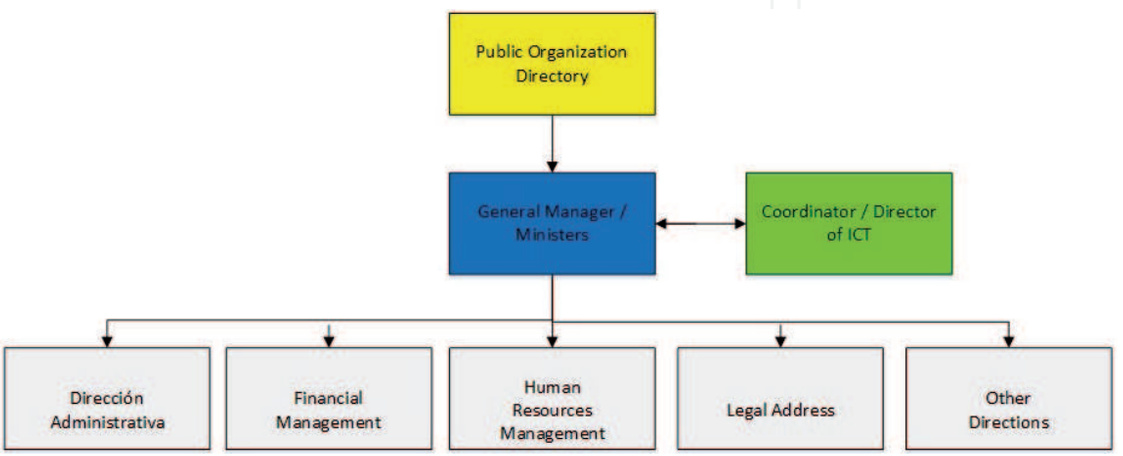

Figure 2.
Generic structural organization chart of a public organization.

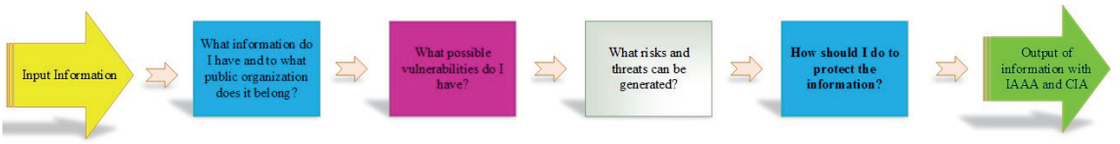

Figure 3.
Frequently asked questions on information security.

Degree of Scope, Degree of Coverage, Degree of Operational Support, Degree of Management Support, and Degree of Support Corporate. This allows to determine the current situation of the organization in all areas. With this information, it is more feasible to identify the information security situation to improve its management [7].

Another alternative to get to identify the current situation of information security is to ask the following frequently asked questions:

In **Figure 3**, the frequent questions are asked with the objective that during this process the entry of the information is determined and also the output of the information with identity, authenticity, authorization and audit (IAAA) and confidentiality, integrity and availability (CIA).

6.1.3 Phases that must be considered to improve the security of information

Consider the results obtained in the different articles published on the public organizations of Ecuador, to consider as an alternative with the objective of improving the security of information [7–33].

1. Adopt or generate a training plan with appropriate methodology for the public organization for the change of computer culture at the operational, tactical, and strategic levels.

2. Perform the analysis and define the organizational structure of the organization considering the Cobit 5.0 methodology as a reference, where the general manager (CEO) and the manager/coordinator/director of information and communications technologies (ICT) equivalent to chief information officer (CIO) have the same level of authority and the CIO is the one who governs the organization.

3. Carry out the analysis to define the vulnerabilities, risks, and threats that are generated.

4. Define the structure for the execution of the project: general coordinator, specialist in information security, process specialist, administrator of information and communications technologies (ICT) infrastructures, etc., all with academic training in the area of knowledge at all levels, engineering, masters, and if the case deserves in the doctorate fulfilling standards of the SENESCYT and UNESCO. Also have a referential budget.

5. Consider the application of ISO 27001:2013 regarding the certification process by FIRST (International Incident Management Community, CSIRTS, and CERTS).

6. Take into account the good practices of the Cobit 5.0, ITIL, and COSO methodologies to integrate information security management in a globalized manner.

7. Define functions for a work group.

8. Define the steps to be taken with the respective responsibility to each officer of the organization.

9. Prepare an information technology strategic plan (ITSP) with their respective security plans, contingency, backup, etc., with the participation of official's at all operational, tactical, and strategic levels.

10. The exposed phases are those that are suggested to be used as an alternative to define a generic methodology for public organizations in the next chapter of the book.

6.2 Prototype sequence diagram of users and services access

A prototype of the sequence of accesses of internal/external users and services to the information of public organizations is defined.

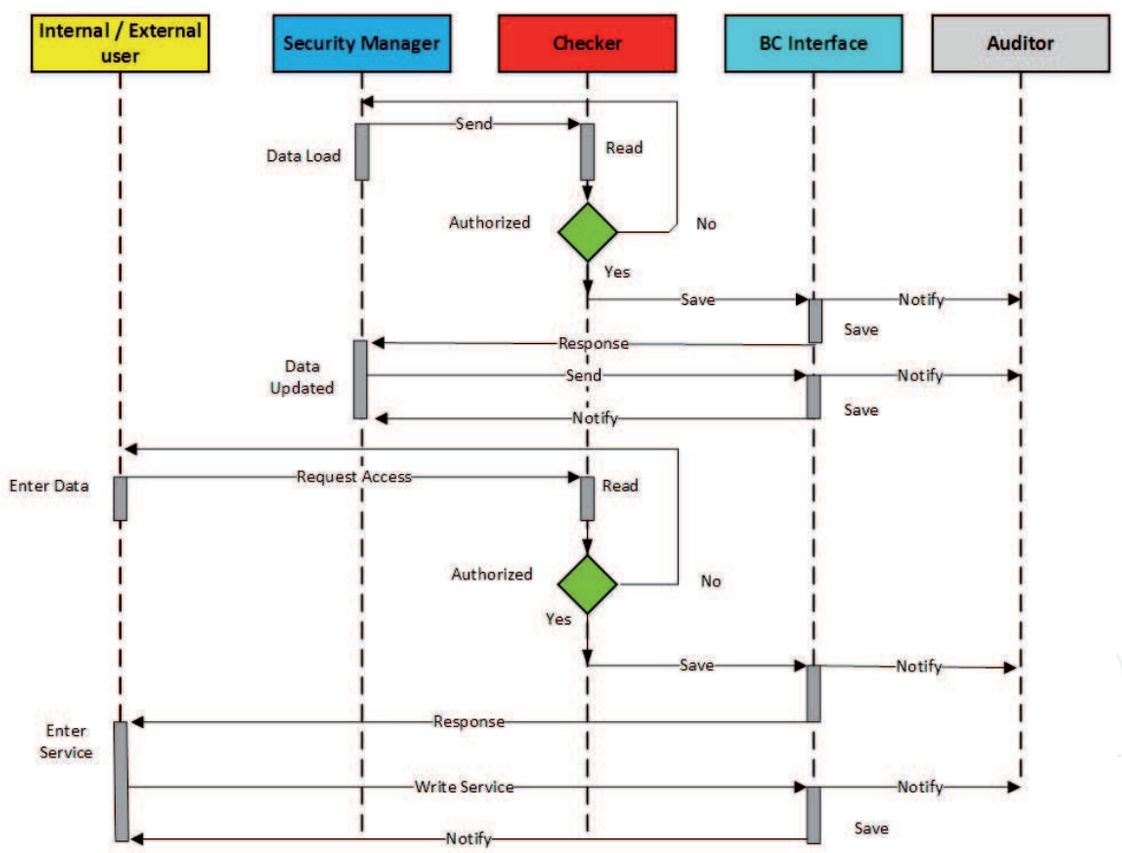

Figure 4.
Prototype sequence diagram of users and services access.

Figure 4 describes the dynamic interaction of the user, administrator, verifier, interface, and auditor to perform the sequence of access to information and services.

6.3 Prototype of security technology integration

In order to generate this prototype, the recommendations of the World Bank for Latin America and the Caribbean are taken into account, which states textifically: "In the midst of all the technological advances we are currently

experiencing, Blockchain, or chain of blocks, has the power to alter current models economic and business, and become a particularly valuable asset for emerging economies. According to the experts, it could also be very useful as a method to fight corruption, especially in Latin America and the Caribbean, where the penetration of mobile telephony can facilitate technological adoptions" [5], the application of Hyperledger Fabric technology with intelligent contracts, provides a starting point to understand a chain of Hyperledger Fabric blocks to consult and update with a Ledger to generate X.509 certificates that are used by applications that interact with a blockchain authorized [47].

Figure 5 describes how the Hyperledger Fabric, which is a set of functions, uses the Ledger to initiate the status information and the read/write requests through the connections.

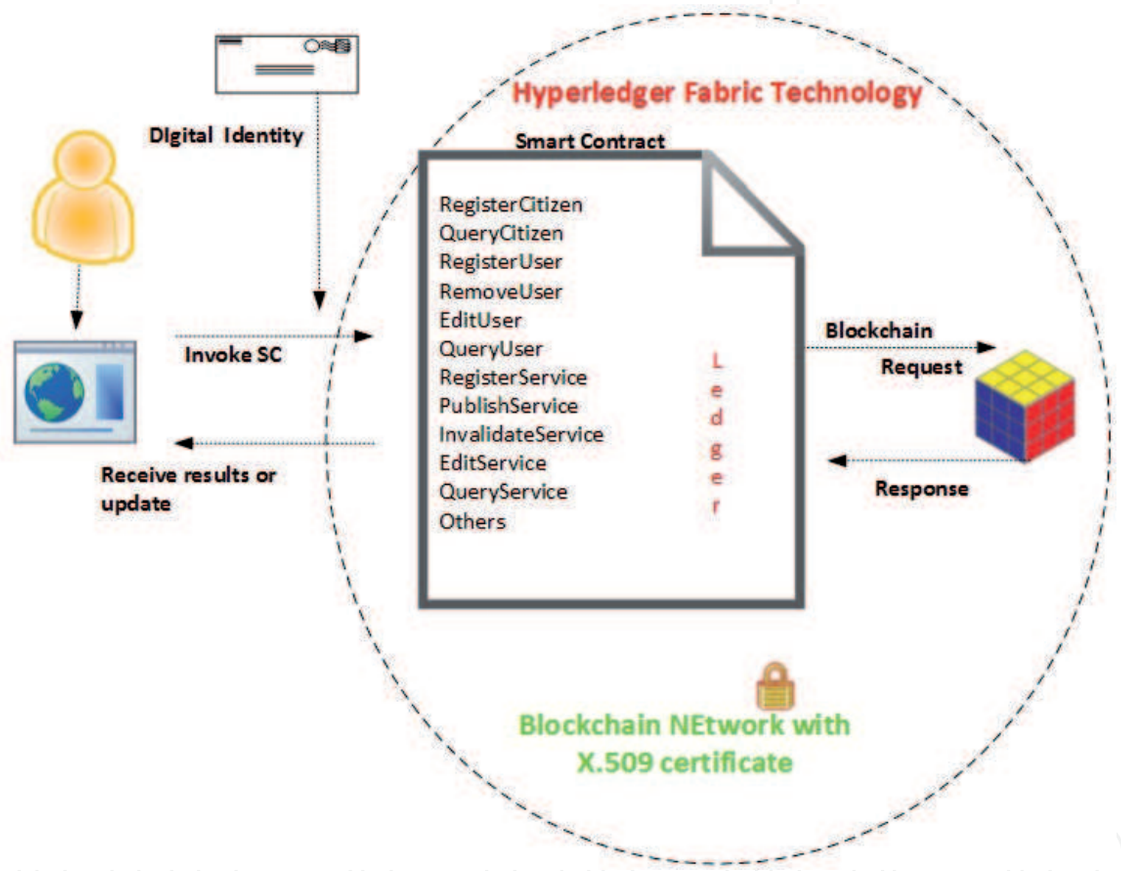

Figure 5.
Prototype integration of security technologies.

7. Conclusions

The security of information is considered strategic and the main asset of public and private organizations. In this chapter, we consider the previous analyzes carried out by the authors in the area of information and communications technologies (ICT) and information security to determine the impact it has on the incorrect management of information. The weakness in the administration of information security is taken advantage of by all officials or workers at an operational, tactical, and strategic level of the public organizations of Ecuador to generate corruption such as incorrect identification of citizens, dead voters, embezzlement in public coffers, false titles especially acquired by the politicians, for all the aforementioned it is concluded that to avoid corruption in a country at

all levels the first matter that we are the inhabitants must be changed, laws with strong sanctions to the politicians without parliamentary immunity, application of information and communications technologies (ICT) in suitable form, to fulfill international standards in administration of security of the information like ISO 27001, Cobit 5.0, definition of profiles for the selection of information and communications technologies (ICT) managers, directors or coordinators who are from the area of knowledge in undergraduate degrees, masters, and doctorates, complying with the provisions of SENESCYT and UNESCO. That planning organisms such as the National Secretariat of Planning and Development-Ecuador (Senplades) and the Ministry of Labor Relations consider the position of manager, director, general coordinator of information and communications technologies (ICT) at the same level as the main authority of the Public Organization, Change of culture in the directive civil servants who must consider that the information and communications technologies (ICT) are those that a public organization must govern to be competitive.

To improve the security of information, administrative policies must be changed in information security, using technologies related to immutable security algorithms, Ledger, Hyperledger, etc..

Acknowledgements

The authors thank the Salesian Polytechnic University of Ecuador, the research group of the Headquarters of Guayaquil "Technology of Computing, Security and Information for a Globalized World" (CSITGW), created in accordance with resolution 142-06-2017-2107-19, and the Secretariat of Higher Education Science, Technology and Innovation (SENESCYT).

Conflict of interest

All the work presented in this chapter is our own research based on several articles that are our responsibility. The points of view expressed, suggested on the management of security in public organizations of Ecuador, correspond to the authors and it is the responsibility of the person who publishes this chapter.

DOI: http://dx.doi.org/10.5772/intechopen.88931

IntechOpen

Author details

Segundo Moisés Toapanta Toapanta[1*] and Luis Enrique Mafla Gallegos[2]

1 Escuela Politécnica Nacional, Universidad Politécnica Salesiana Sede, Guayaquil, Ecuador

2 Faculty of Systems Engineering, National Polytechnic School (EPN), Quito, Ecuador

*Address all correspondence to: stoapanta@ups.edu.ec

IntechOpen

© 2019 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Santacruz GL. Libro Blanco de la Sociedad de la infomración y del Conocimiento. Ministerio de Telecomunicaciones y Sociedad de la Infomración (MINTEL). 2018. Available from: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/07/Libro-Blanco-de-la-Sociedad-del-Información-y-del-Conocimento.pdf [Accessed: April 08 2019]

[2] Campaña JA. Empresas públicas y planificaciòn. Senplades; 2013. Available from: http://www.planificacion.gob.ec/wp-content/uploads/downloads/2014/02/Libro-Empresas-Públicas-web.pdf [Accessed: April 04 2019]

[3] Pacheco F. The need for formal education on information security. IEEE Latin America Transactions. 2013;**11**(1):668-670

[4] Ces. República del ecuador consejo de educación superior rpc-so-24-no.480-2017. no. 289; 2017

[5] Mundial B. Blockchain: cómo asegurarse que cada dólar llegue a quien lo necesita [Online]. 2019. Available from: https://www.bancomundial.org/es/news/feature/2019/01/24/blockchain-como-asegurarse-que-cada-dolar-llegue-a-quien-lo-necesita [Accessed: April 11 2019]

[6] Rienzo A, Ieee M, Bustamante M. Evaluation of the degree of knowledge and implementation of information security management systems, based of the NCh-ISO 27001 standard, in health institutions. In: 2018 IEEE Int. Conf. Autom. Congr. Chil. Assoc. Autom. Control; 2018. pp. 1-6

[7] Sistemas DE. Modelo de indicadores para la medición del alineamiento entre las estrategias institucionales y las estrategias de TIC'S para empresa del sector publico. Escuela Politécnica Naiconal; 2013

[8] Toapanta M. Las TIC en el Ecuador. Revista International Estrategos. 2015;**1**(1):7-19

[9] Maciel R, Toapanta M. Tecnologías de información y comunicación impactan la optimización de los procesos para el desarrollo local. In: I Congreso Internacional Investigación en Desarrollo Local y Emprendimiento Socioeconómico Sustentable y Sostenible; Sección Tecnologías de Información: Guayaquil-Ecuador; Digital 20; 2015. pp. 310-323. ISBN: 978-9942-14-417-1

[10] Segundo S, Toapanta M, Luis PD, Mafla E. Analysis to define management of identities access control of security processes for the registration civil from Ecuador. In: IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life, ISC2 2016-Proceedings; 2016. pp. 1-4

[11] Student PD, Moisés S, Toapanta T, Luis PD, Mafla E. Security analysis of civil registry database of Ecuador. In: Int. Conf. Electr. Electron. Optim. Tech. 2016; 2016. pp. 1024-1029

[12] Moises Toapanta AO, Mafla E. An approach to information security by applying a conceptual model of identities in smart cities projects. Journal of Engineering and Applied Science. 2017;**12**(6):7765-7770

[13] Toapanta M, Mafla E, Orizaga A. Adequate security protocols adopt in a conceptual model in identity management for the civil registry of Ecuador. In: IOP Conf. Ser. Mater. Sci. Eng.; vol. 225; 2017. pp. 1-6

[14] Moisés S, Toapanta T, Enrique L, Gallegos M. Analysis of model Clark

Wilson to adopt to the database of the civil registry of Ecuador. Conf. Open Innov. Assoc. Fruct; vol. 21; 2017. pp. 513-518

[15] Moisés S, Toapanta T, Enrique L, Gallegos M. Mitigating the security of the database by applying a conceptual model of integrity for the civil registry of Ecuador. In: Conf. Open Innov. Assoc. Fruct; vol. 21; 2017. pp. 507-512

[16] Moisés TT, Antonio OT, Enrique MG. A security algorithms approach to apply to the civil registry database of the Ecuador. In: IEEE CITS 2017-2017 International Conference on Computer, Information and Telecommunication Systems; 2017. pp. 287-290

[17] Toapanta M, Mafla E, Orizaga J. Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador. Materials Today: Proceedings. 2018;**5**(1):636-641

[18] Toapanta M, Mafla E, Orizaga A. Adoption of the Hash algorithm in a conceptual model for the civil registry of Ecuador. In: AIP Conference Proceedings; vol. 1952; 2018. pp. 1-9

[19] Moises TT, Enrique MG, Antonio OT. An approach of efficient security algorithms for distribute architectures. In: 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing, ICECDS 2017; 2018. pp. 22-25

[20] Toapanta SMT, Anchundia MAM, Mafia LEG, Orizaga JAT. Biometric systems approach applied to a conceptual model to mitigate the integrity of the information. In: CITS 2018-2018 International Conference on Computer, Information and Telecommunication Systems; 2018. pp. 1-5

[21] Toapanta SMT, Cruz AAC, Gallegos LEM, Trejo JAO. Algorithms for efficient biometric systems to mitigate the integrity of a distributed database. In: CITS 2018-2018 International Conference on Computer, Information and Telecommunication Systems; 2018. pp. 1-5

[22] Toapanta SMT, Gallegos LEM, Quimi FGM, Trejo JAO. Analysis of efficient processes for optimization in a distributed database. In: CITS 2018-2018 International Conference on Computer, Information and Telecommunication Systems; 2018. pp. 1-4

[23] Toapanta SMT, Paredes SJM, Gallegos LEM, Trejo JAO. Analysis of HIPAA for adopt in the information security in the civil registry of the Ecuador. In: CITS 2018-2018 International Conference on Computer, Information and Telecommunication Systems; 2018. pp. 1-5

[24] Toapanta M, Mero J, Huilcapi D, Tandazo M, Orizaga A, Mafla E. A blockchain approach to mitigate information security in a public organization for Ecuador. In: IOP Conf. Ser. Mater. Sci. Eng. 2018;**423**(1):1-7

[25] Toapanta M, Nazareno J, Tingo R, Mendoza F, Orizaga A, Mafla E. Analysis of the appropriate security models to apply in a distributed architecture. In: IOP Conf. Ser. Mater. Sci. Eng. 2018;**423**(1):1-5

[26] Mafla E, Toapanta M, Barona D, Contrera G. Optimization of an electronic signature scheme in a voting system in a distributed architecture. In: 2018 3rd International Conference on Computer Science and Information Engineering (ICCSIE 2018); 2018. pp. 242-248

[27] Mafla E, Toapanta M, Huilcapi D, Cepeda M. Ensuring the blind signature for the electoral system in a distributed environment. In: 2018 3rd International Conference on Computer Science and

Information Engineering (ICCSIE 2018); 2018. pp. 205-212

[28] Mafla E, Toapanta M, Orellana N, Barona D. Analysis cryptographic for electronic votes in systems of distributed architectures. In: 2018 3rd International Conference on Computer Science and Information Engineering (ICCSIE 2018); 2018. pp. 189-196

[29] Mafla E, Toapanta M, Tamayo J, Ortiz J. An approach to the efficient security algorithms used in voting scanning in an electoral process. In: 2018 3rd International Conference on Computer Science and Information Engineering (ICCSIE 2018); 2018. pp. 234-241

[30] Mafla E, Toapanta M, Chávez L, Ortiz J. A homomorphic encryption approach in a voting system in a distributed architecture. In: 2018 3rd International Conference on Computer Science and Information Engineering (ICCSIE 2018); 2018. pp. 182-188

[31] Maciel R, Toapanta M, Mendoza F, Plùa D, Tandazo M, Mafla E. Analysis of security algorithms for a distributed database. In: 2018 3rd International Conference on Computer Science and Information Engineering (ICCSIE 2018); 2018. pp. 197-204

[32] Mafla E, Toapanta M, Espinoza J. A hyperledger scheme for the deployment of smart contracts in a public organization of Ecuador. Smart Innovation, Systems and Technologies. 2018;**1**:1-13

[33] Mafla E, Toapanta M, Aguilar J. Analysis of adequate bandwidths to guarantee an electoral process in Ecuador. Smart Innovation, Systems and Technologies. 2018;**1**:1-12

[34] Mafla E, Toapanta M, Coronel M. Appropriate security protocols to mitigate the risks in electronic money management. Smart Innovation, Systems and Technologies. 2018;**1**:1-12

[35] Mafla E, Toapanta M, Mendoza F. Cryptographic algorithms to mitigate the risks of database in the management of a smart city. Smart Innovation, Systems and Technologies. 2018;**1**:1-12

[36] Mafla E, Toapanta M, Mendoza F. Impact on the information security management due to the use of social networks in a public organization in Ecuador. Smart Innovation, Systems and Technologies. 2018;**1**:1-13

[37] Joseph Guaman AO, Toapanta M. An information security approach in the Armed Forces of Ecuador. In: CITIS 2017; 2017. pp. 366-372

[38] Mafla E, Toapanta M, Orizaga A. Algoritmos y protocolos de seguridad para el registro civil del ecuador. Universidad de Guadalajara. Tesis doctorado, Identificador de la entrega; 2018:930484533

[39] Dennis KH. On the use of the Clark-Wilson security model to protect industrial automation control systems. In: CSIIRW'13 Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop; 2013

[40] Hermann E. The limes security model for information flow control. In: A. Dept. of Secure Inf. Syst., Upper Austria Univ. of Appl. Sci., Linz; 2011

[41] Cui J, Wang Q. An improved BLP model with response blind area eliminated

[42] Manr D, Servicio WMT, Civil R. Seguridad de la Información. Facultad de Ingenieria Universidad de Buenos Aires; 2005. Available from: http://www.cicomra.org.ar/cicomra2/expocomm/TUTORIAL5Heguiabehere-CERTANT.pdf [Accessed: March 19 2018]

[43] Cucurull J, Puiggali J. Distributed immutabilization of secure logs. In: Security and Trust Management, STM 2016; vol. 9871. 2016. pp. 122-137

[44] Parkavi R, Babu KRC, Kumar JA. Multimodal biometrics for user authentication. 2017. pp. 501-505

[45] Ogiela MR, Majcher M. Security of distributed ledger solutions based on blockchain technologies. In: Proceedings-International Conference on Advanced Information Networking and Applications, AINA; vol. 2018: no. c; 2018. pp. 1089-1095

[46] Sukhwani H. Performance modeling of hyperledger fabric (permissioned blockchain network). In: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA); 2018. pp. 1-8

[47] B. with S. using a theme provided by R. the Docs., "Hyperledger Fabric," Writing Your First Application (tutorials, 2019. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.4/write_first_app.html. [Accessed: April 11 2019]