Metadata of the chapter that will be visualized in SpringerLink

Book Title	Applied Technologies	
Series Title		
Chapter Title	Towards the Information Security Governance for Institutions of Higher Education: Harmonization of Standards	
Copyright Year	2020	
Copyright HolderName	Springer Nature Switzerland AG	
Corresponding Author	Family Name	**Heredia**
	Particle	
	Given Name	**Hugo**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Instituto Tecnológico Superior Cordillera
	Address	Quito, Ecuador
	Division	Maestría en Sistemas de Información
	Organization	Universidad Técnica de Ambato
	Address	Ambato, Ecuador
	Email	hugo.heredia@cordillera.edu.ec
		hugoheredia79@gmail.com
	ORCID	http://orcid.org/0000-0001-5534-8934
Corresponding Author	Family Name	**Merchán**
	Particle	
	Given Name	**Vicente**
	Prefix	
	Suffix	
	Role	
	Division	
	Organization	Universidad de las Fuerzas Armadas ESPE
	Address	Sangolquí, Ecuador
	Division	
	Organization	Universidad de Otavalo
	Address	Otavalo, Ecuador
	Email	vrmerchan@espe.edu.ec
		vmerchan@uotavalo.edu.ec
	ORCID	http://orcid.org/0000-0002-4456-0689

Abstract

Institutions of Higher Education have been continually threatened by the lack of direction and control from the perspective of information security in the context of information technology governance. The ISO/IEC 27014:2013 standard represents an opportunity to govern information security; however, it suffers from a clear alignment that allows it to articulate its activities with the IT governance and provide visibility to the organizational government. This exploratory and document-level study has carried out a harmonization

process between the ISO/IEC 27014:2013 and ISO/IEC 38500:2015 standards with the purpose of identifying overlapping problems and strongly related elements that contribute to a consistent model of information security governance at three levels: principles (responsibility, performance, strategy, risk analysis, compliance and human behavior), objectives and indicators. As a result, the components of the information security governance model have been defined as strongly related to information technology governance. This work contributes to the knowledge and collaboration of decision-makers in the strategic steering and information security control committees of Ecuador's higher education institutions. Future work will focus in the relation of substantives components of law of higher education, the factorial analysis of components of the model with the participation of actors from the institutions, in order to consolidate it towards what the institutions cannot do without.

Keywords Information security - Information security government - Information technology government

Towards the Information Security Governance for Institutions of Higher Education: Harmonization of Standards

Hugo Heredia[1,2(✉)] and Vicente Merchán[3,4(✉)]

[1] Instituto Tecnológico Superior Cordillera, Quito, Ecuador
hugo.heredia@cordillera.edu.ec, hugoheredia79@gmail.com
[2] Maestría en Sistemas de Información, Universidad Técnica de Ambato, Ambato, Ecuador
[3] Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador
vrmerchan@espe.edu.ec
[4] Universidad de Otavalo, Otavalo, Ecuador
vmerchan@uotavalo.edu.ec

Abstract. Institutions of Higher Education have been continually threatened by the lack of direction and control from the perspective of information security in the context of information technology governance. The ISO/IEC 27014:2013 standard represents an opportunity to govern information security; however, it suffers from a clear alignment that allows it to articulate its activities with the IT governance and provide visibility to the organizational government. This exploratory and document-level study has carried out a harmonization process between the ISO/IEC 27014:2013 and ISO/IEC 38500:2015 standards with the purpose of identifying overlapping problems and strongly related elements that contribute to a consistent model of information security governance at three levels: principles (responsibility, performance, strategy, risk analysis, compliance and human behavior), objectives and indicators. As a result, the components of the information security governance model have been defined as strongly related to information technology governance. This work contributes to the knowledge and collaboration of decision-makers in the strategic steering and information security control committees of Ecuador's higher education institutions. Future work will focus in the relation of substantives components of law of higher education, the factorial analysis of components of the model with the participation of actors from the institutions, in order to consolidate it towards what the institutions cannot do without.

Keywords: Information security · Information security government · Information technology government

1 Introduction

A good implementation of information security government must offer a strategic alignment, risk management, and resource management, for this, it is essential to identify the critical factors that allow achieving the strategic success of information security in the long term in organization [1].

M. Botto-Tobar et al. (Eds.): ICAT 2019, CCIS 1195, pp. 1–15, 2020.
https://doi.org/10.1007/978-3-030-42531-9_37

Similarly, [2] in the proposed information security governance framework show the relevance of adopting and employing a mature approach to the ability to manage and control information security with the use of a common business-focused language that allows organizations to establish appropriate security standards according to the nature of each business and leverage resources to achieve a level of information security, generating confidence and business advantage.

On the other hand, [3] states that the benefits of an information security government enhance trust in customer relationships, protect the reputation of the organization, hand over responsibility for safeguarding information from critical business activities; meanwhile, Luqman Ayodele [4] concludes that inadequate governance over information security affects organizations in the management and processing of information by inconsistency in the configuration of their information systems.

Da Veiga and Eloff [5] that in order to implement an information security governance framework, behavior and a level of culture must be generated at all levels of the organization, that is, from the top executives to the operational levels, with a view to reducing the impact generated by the loss or theft of information in the organization.

It is important that the organization effectively governs information security, its components, policies, and metrics holistically by developing behaviors among the actors that go hand in hand with an information security governance model.

Clark and Sitko [6] ensure that the implementation of an information security framework will allow the organization to significantly improve its corporate governance processes; just as CGI Group [7] that security and governance cannot be separated nor can they be achieved by deploying technical solutions alone.

Carcary et al. [2] argue that governance processes are intended to enhance the ability of any organization to direct, supervise, and control actions, processes, and procedures to safeguard information assets, as well as to provide confidentiality, integrity, availability, and accessibility of data found in information systems.

That is why Bowen, Hash and Wilson [8] establish a conceptualization of what information security governance is guaranteeing its implementation proactively while at the same time managing it. An information security government has a set of requirements, challenges, activities, and structures that allows it to identify key roles and responsibilities that influence the implementation of information security policies and procedures.

Finally, De Oliveira Alves, Rust da Costa Carmo and Ribeiro [9] conclude that while corporate governance concepts are well known, information security governance remains a major challenge for organizations.

These definitions help us to thinking that many institutions of higher education have yet to establish real information security governance. There are many reasons behind this; our goal is not to list them but rather, to propose a model to facilitate the implementation of a governance process adapted to the realities of each institution. But, first, let's harmonization look at governance and management activities to better understand what we are talking about and why it is important together worked in information technologies and information security.

In particular, the ISO/IEC 38500:2015 standard for the Governance of IT, not only covers all the good governance principles, e.g. responsibility, accountability and outcomes strategy alignment but also includes (implicitly) the governance of information security. The same applies for the ISO/IEC 27014: 2013 standard which is not limited to those areas of organizational governance that are specifically related to information security activities. Information security governance include subjects such as defining the governance structure; strategic alignment, value creation, accountability, security adequacy, investment decision process, and compliance with standards.

We believe that both standards: have overlapped issues, need some coordination and compatibility to be coherent and moreover, there should be some hierarchy between them. All these possible design issues produce practitioner's misunderstandings and standardization drawbacks in the current version of both standards.

The present work has been structured. In Sect. 2, the theoretical background. In Sect. 3, the research methodology is presented. In Sect. 4, the results obtained are analyzed. In Sect. 5, the discussions and conclusions of the study are presented.

2 Background

2.1 ISO/IEC 38500:2015

ISO/IEC 38500:2015 is the international standard that speaks about elements of governance of Information Technology (IT) in organizations, it sets standards for processes, procedures and decision making in terms of reference to information systems and technologies, on the other hand, describes that a model is a set of components that are related to describing the functioning of an object, system or concept [10].

The ISO/IEC 38500:2015 governance model is based on three main axes, the first evaluating the current and future use of IT, the second preparing for the implementation of policies and strategies to ensure that the use of IT meets business objectives, and the third establishing the monitoring of compliance with policies and performance in relation to established strategies, i.e., it shows a governance model that Evaluates, Directs and Monitors [10].

Figure 1 shows the model for IT governance proposed by ISO/IEC 38500:2015 in which three main elements can be seen to evaluate, direct and monitor strategies, policies, plans and purposes in the achievement of the organization's strategic objectives [10, 11].

Merchán and Rodríguez [12] that within the ISO/IEC 38500:2015 standard, guiding principles are also defined, which are applied to any organization. The principles of responsibility, strategy, procurement, performance, compliance establish the conduct by which directors, executives and will be guided in the best decision making. On the other hand [10] establishes a model composed of three main activities: management (Direct), evaluation (Evaluate) and follow-up (Monitor).

2.2 ISO/IEC 27014:2013

ISO/IEC 27014:2013 [13] is a guide to information security governance, providing concepts and principles by which organizations can assess, manage, monitor and communicate information security- related activities, as well as develop a holistic view in the organization's board of directors on security governance issues.

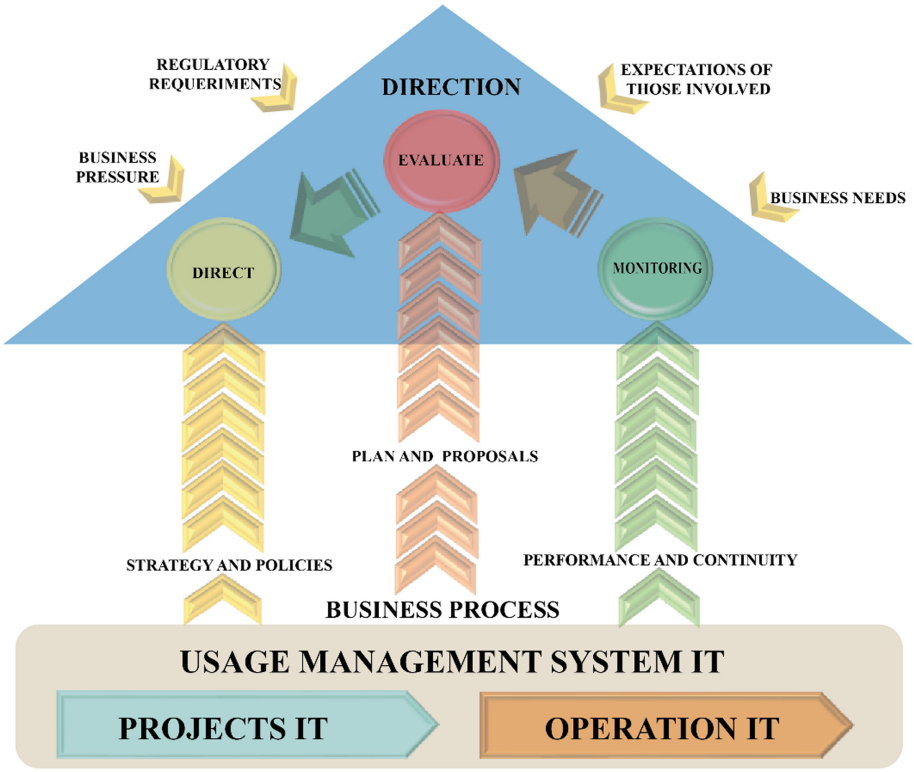

Fig. 1. Model for IT governance [10]

However, ISO/IEC 27014:2013 establishes certain results that must be evaluated when implementing information security governance, among which are the visibility of the directory on the state of security, an agile approach to decision making and information risks, as well as efficient and effective investments in terms of information security complying with external requirements (legal, regulatory or contractual).

ISO/IEC 27014:2013 presents six principles: establish information security throughout the organization, adopt a risk-based approach, establish the direction of investment decisions, ensure compliance with internal and external requirements, foster a positive security environment and performance of opinion in relation to business results, through which corporate governance can design and implement its information security governance framework, listing the responsibilities they must take into account [13].

Unlike ISO/IEC 38500:2015, which presents a model of evaluate-direct-monitoring and lets the governance committee creates its particular governance framework; ISO/IEC 27014:2013 shows a proportionate framework for the management of information security defined in five areas with a flow of communication, among them, focused on monitoring, evaluation, communication, direction and, finally, assurance; that is, evaluate - direct - monitor - communicate - secure (see Fig. 2).

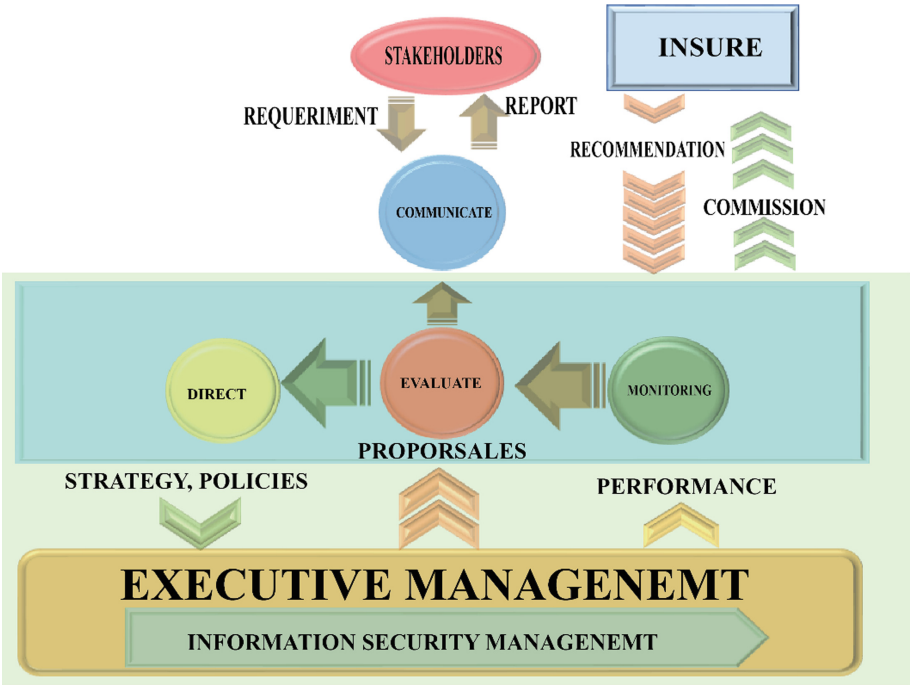

Fig. 2. Information security model [13]

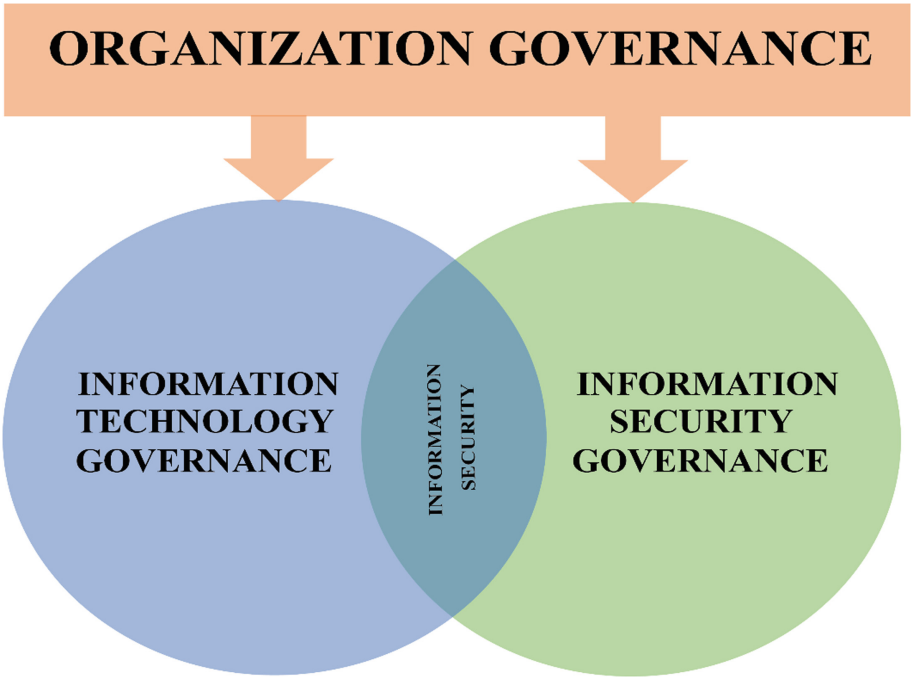

Fig. 3. Information security and IT government [13]

Figure 3 presents something very important that consists of some relationship between IT governance and information security governance, which is ultimately the reason for this study.

3 Methods and Materials

For the purpose of this research, ISO/IEC 38500:2015 [10] and ISO/IEC 27014:2013 [13] standards were taken into account. Then, difficulties were identified, and a comparison of objectives, policies, models and processes was made; using the harmonization process of [14–16].

For the mapping of standards, the following steps were executed [16]:

1. Selection of elements to compare from both standards.
2. Standards mapping design, in the following terms:

    a. Obtaining the elements identified in the first step;
    b. Definition of a comparison scale, to show the degree of similarity between the two standards; and
    c. Definition of the comparison template through which it was determined whether the scale values represent the ratio of ISO/IEC 27014:2013 in ISO/IEC 38500:2015.

3. Execution of the mapping of standards through a process of valuation of the main elements and components of the standards. Where the rows are made up of the elements of ISO/IEC 38500:2015 and in the columns are the elements of ISO/IEC 27014:2013.

4 Results

4.1 Selection of Elements to Be Compared

The following elements were considered for the comparative analysis:

- Government Objectives
- Principles of governance
- Models of government
- Governance activities

Each one of the objective elements, principles and models allowed to know the scopes, areas of applicability of each one of the norms, for example, as much the principles of the government of security of the information as of technologies of the information are oriented to guarantee the attainment of the objectives raised by the organizational government; as for the model of governance the two norms establish a model of two levels with processes of government by segregation of functions.

The governance activities of each of the standards studied are determined by evaluation, management, and monitoring, as common elements; however, communication is explicit in ISO/IEC 38500:2015 while in ISO/IEC 27014:2013 communication and assurance towards the fulfillment of organizational objectives is an essential part of the model.

4.2 Standards Mapping Design

Once the elements in each of the standards have been identified, the level of relationship that exists between them was determined using a similarity scale, using the Holmes matrix as a tool for comparison, analysis and prioritization of each of the criteria, as presented in Table 1 to establish the importance of the elements of both standards [17].

Table 1. Holmes weighting scale

Scale	Verbal scale
0.5	Value of the main diagonal of the matrix considering the comparison with itself
1	Whether the criterion is more important than the other criteria
0	Whether the criterion is less important than the other criteria

With the parameters or criteria established and defined, Holmes' matrix allowed the decision making based on the criteria and value judgments according to the scale determined based on the quantification with respect to each element determined in Table 2.

Table 2. Definition of criteria

Criteria	Definition
Effectiveness	Refers to information generated that is relevant and pertinent to the business, allowing to achieve strategic goals and improvements to business processes
Efficiency	Efficiency is about delivering or providing quality information to services faster by allowing IT departments to look for ways to achieve it, with strategies that contribute to this goal
Confidentiality	It relates to the characteristic of protection, privacy and access to information and to the policies and actions necessary to guarantee it

(*continued*)

Table 2. (*continued*)

Criteria	Definition
Integrity	Refers to the integrity of the data that are processed to generate information, these must be accurate, valid and consistent with mechanisms that prevent unauthorized removal, modification and disposal [18]
Availability	It refers to the information that must be available at the time it is required by any business unit, as well as the IT services that the business requirements need
Reliability	[19] work it as the provision of appropriate information that IT services provide to be considered in decision-making
Strategic alignment	They are the strategies of IT governance as well as information security support the business strategy
Meeting the needs of stakeholders	It is understood as the information needs that each one of the interested parties seeks to obtain for decision making, evaluating the benefit and associated risks
Cover the organization in a comprehensive manner	All the processes and functions necessary for the governance and administration of the entire organization, including IT services, are contemplated
Organizational structures	Defines its responsibilities to IT governance and information security in order to ensure the stated objectives
Risk management	It is considered as the adequate management of the risks associated with the use and generation of information by IT and each business unit of the organization
Measuring performance	It is the value generated by IT and information security governance strategies in the execution and control of projects, performances focused on cost-benefit
Resource management	It is defined as the adequate management that each of the available resources of the organization must have in order to guarantee the fulfillment of the organizational strategies

The comparison was made considering a superior triangular matrix that is completed with the opposites to the scale as corresponds to the analysis obtaining at the end of a type L matrix. Subsequently, the sum was made for each of the criteria or parameters to quantitatively determine the importance of the criterion or parameter in order from highest to lowest.

Once the results were obtained, the Pareto rule was applied to make visible the choice of criteria or parameters under which the analysis of the two government standards was carried out (see Table 3).

Table 3. Application of the Pareto rule

Parameters	Importance	Accumulated importance	% Sum	% Sum accumulated
Confidentiality	11,5	11,50	12%	12%
Integrity	10,5	22,00	11%	22%
Availability	10,5	32,50	11%	33%
Strategic alignment	10,5	43,00	11%	44%
Value delivery	9,5	52,50	10%	54%
Effectiveness	7,5	60,00	8%	61%
Meeting the needs of stakeholders	7,5	67,50	8%	69%
Reliability	6,5	74,00	7%	76%
Efficiency	5,5	79,50	6%	81%
Cover the organization in a comprehensive manner	4,5	84,00	5%	86%
Measuring performance	4,5	88,50	5%	90%
Risk management	3,5	92,00	4%	94%
Resource management	3,5	95,50	4%	97%
Organizational structures	2,5	98,00	3%	100%

Figure 4 shows the result of applying the Pareto rule, the focal criteria are: confidentiality, integrity, availability and strategic alignment. This means that the four criteria or parameters are of major importance for assessing the relationship between the standards studied.

According to the above figure, the four focal criteria constitute the minimum desirable elements in an information security governance model. Holmes' matrix helped determine the categorical and numerical values for each of the criteria (see Table 4), from which a relational valuation matrix was defined, as shown in Table 5.

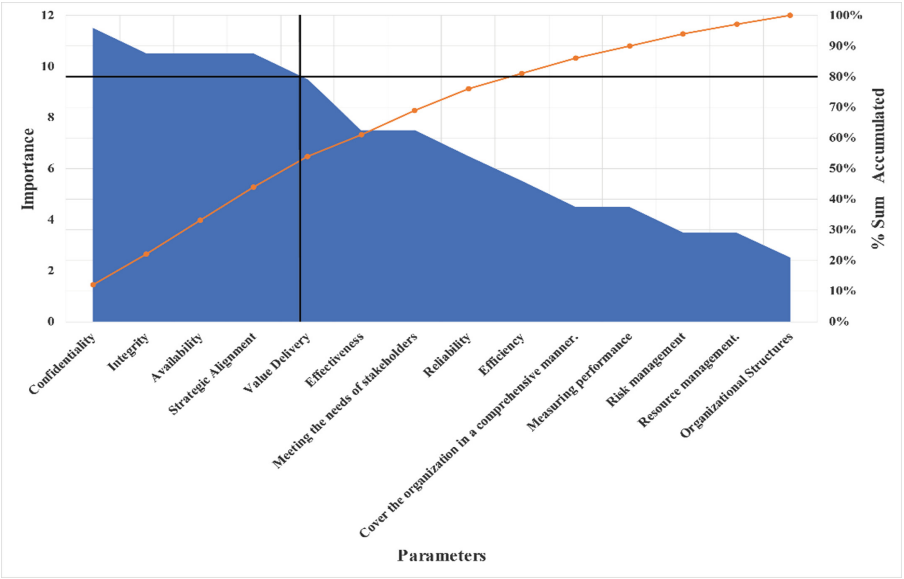

Fig. 4. Pareto diagram

Table 4. Matrix of Holmes selected criteria

Criteria	Confidentiality	Integrity	Availability	Strategic alignment	SUM	Weighting factor
Confidentiality	0,5	1	1	1	4	0,44
Integrity	0	0,5	1	0	2	0,19
Availability	0	0	0,5	1	2	0,19
Strategic alignment	0	1	0	1	2	0,19

Table 5. Relational valuation scale

CRITERIA	1-NR	2 -PR	3-MR	4 – FR
Confidentiality	Does not facilitate the confidentiality of information	Facilitates a little the confidentiality of the information	Mildly facilitates the confidentiality of information	Completely facilitates the confidentiality of information
Integrity	Does not take into account any element of information integrity	It takes into account some elements that guarantee the integrity of the information	It takes into account most of the elements that guarantee the integrity of the information	Takes into account all the elements that guarantee the integrity of the information
Availability	Does not comply with information availability policies	Complies with some information availability policies	Complies with most information availability policies	Complies with all information availability policies
Strategic Alignment	Does not facilitate strategic alignment	Facilitates in a few aspects the strategic alignment	Facilitates in several aspects the strategic alignment	Completely facilitates strategic alignment

4.3 Execution of the Comparison

Confidentiality Criteria
The strongly related element between the two standards represents a two-tier system: management body and corporate governance. In the same way the principles, mitigate the risk of directors not complying with their obligations, strategy, performance, human behavior, responsibility, compliance, procurement, IT governance, balance the risks and promote the opportunities derived from the use of IT, establish and sustain a suitable environment and monitor, as to the activities of greatest relative importance are: evaluate, manage, add value to the board of directors and stakeholders, monitor, provide alignment between information security strategies and objectives with business strategies and objectives to ensure that information and risks are being adequately addressed, through assertive communication.

Integrity Criteria
The mapping under integrity determined that in a two-tier system that brings together the bodies of management and corporate governance should be focused on performance, accountability, strategy trying to mitigate the risk of directors who failed to meet their obligations, on procurement and especially on human behavior to seek compliance in IT governance, balancing the risks and encouraging opportunities arising from the use of IT to establish and sustain a fit environment, ensuring compliance with obligations relating to the acceptable use of IT with a monitoring of activities.

Availability Criteria
It is established that to guarantee the availability of information, the model must have a two-tier system that combines management and corporate governance bodies focused on performance, responsibility, strategy trying to mitigate the risk of directors who did not comply with their obligations, on acquisition and above all on human behavior to seek compliance in IT governance, balancing the risks and promoting the opportunities derived from the use of IT to establish and sustain a suitable environment ensuring compliance with obligations related to the acceptable use of IT with a monitoring of activities.

Strategic Alignment Criteria
The best results in terms of ISO 38500:2015 is obtained by having a two-tier system that brings together management and corporate governance bodies focused on performance, responsibility and strategy; seeking to mitigate the risk of directors who did not comply with their obligations, in procurement and especially in human behavior to seek compliance in IT governance, balancing risks and promoting opportunities arising from the use of IT, to establish and sustain a suitable environment ensuring compliance with obligations relating to the acceptable use of IT with a monitoring of activities.

To perform a strategic alignment as seen from ISO/IEC 27014:2013 must be assessed, managed and monitored; it will add value to the board of directors and stakeholders by ensuring that risk-based information is being properly treated and thus ensuring information integrity to provide alignment between information security strategies and objectives with business strategies and objectives by means of efficient communication that are marked as being of greatest relative importance.

To achieve an integration mapping between ISO/IEC 38500:2015 and ISO/IEC 27014:2013 and have agreement with the results for each of its elements, a consolidated matrix was established in which both standards present evidence of a strong and moderate relationship between model, objectives, activities and principles of the two standards, which allows confirming that the information security governance is not totally misaligned from the IT governance, as shown in Table 6.

Table 6. ISO/IEC 27014:2013 related to ISO/IEC 38500:2015

		ISO/IEC 27014:2013														
		Model	Aims and Objectives			Activities						Principles				
	ISO/IEC 38500:2015	Two-level system (Executive management and corporate governance)	Provide alignment between information security objectives and strategies and business objectives and strategies	Adding value to the board of directors and stakeholders	Ensure that information risks are being adequately addressed	*Evaluate*	*Direct*	*Monitor*	*Communicate*	*Insure*	Establish Information Security Across the Organization	Adopt a risk-based approach	Set the direction of investment decisions	Ensure compliance with internal and external requirements	Fostering a positive security environment	Performance of opinion in relation to business results
Model	Two-tier system (management body and corporate governance)	FR		MR	MR	FR	FR	FR	FR	FR	FR	PR	MR	MR	PR	FR
Objectives	Balance risks and promote opportunities arising from the use of IT.	FR								MR		PR	MR	MR	PR	FR
	Mitigate the risk of directors failing to meet their obligations	PR	MR			FR	FR	FR	MR	MR	MR	FR	MR			PR
	Ensure compliance with obligations relating to acceptable use of IT.	FR	MR	FR							MR					
	Ensure that the use of IT contributes positively to the organization's performance		FR	MR					MR	MR	FR	MR	FR	MR	MR	FR
Activities	*Evaluate*	FR	PR	PR		FR	PR			PR		PR		PR		FR
	Direct	FR	MR	MR		MR	FR			MR	FR		MR	MR		
	Monitor	MR	MR	FR	FR	MR	MR	FR	PR		PR	FR	MR		PR	
Principles	Liability		FR	MR		FR	FR	FR			MR	MR	MR	MR	MR	MR
	Strategy		MR	FR	MR	FR	FR	FR	MR			MR	MR	MR	MR	
	Acquisition			MR	MR	FR	FR	FR			PR	MR		MR	MR	
	Performance	PR	MR		FR	FR	FR	FR			MR	PR	MR	FR	MR	MR
	Conformity		FR	FR	MR	FR	FR	FR	MR	MR	MR	MR	PR	PR	MR	MR
	Human Behavior		FR	FR	FR	FR	FR	FR		MR	MR	PR	MR	MR	PR	MR
	ISO/IEC 38501:2015															
Establishing and sustaining an enabling environment		MR		FR	MR	FR	FR	PR	FR	FR		MR	MR			FR
Governing IT		FR	FR	PR	FR	MR	MR	MR	FR	FR	MR	FR	PR	PR	PR	PR
Continuous Review			MR	MR	MR	FR	FR	FR								

Model

ISO/IEC 27014:2013 shows a strong relationship with ISO/IEC 38500:2015 from the sectional point of view: management and governance. In addition, they share a strong relationship with activities and elements.

It can also be observed that the ISO/IEC 27014:2013 standard is strongly related to the balancing of risks and the promotion of opportunities derived from IT in the fulfillment of obligations for the acceptable use of IT and government properties corresponding to the ISO/IEC 38500:2015 standard.

On the other hand, the establishment of information security policies will make it possible to correctly measure performance in relation to business results.

Principles
At the time of mapping, we found that ISO/IEC 27014:2013 has a strong relationship with five of the six principles of ISO/IEC 38500:2015: responsibility, strategy, performance, compliance, and human behavior; which enable information security to be established throughout the organization by adopting a risk-based approach to measuring performance in relation to business results.

Finally, the principles of responsibility, strategy, performance, human behavior, compliance, performance, and risk analysis are strongly related in the two standards. Each one of them with its descriptions and conceptualizations that allow describing the activities related to the security, integrity, and reliability of the information.

Activities
The activities of evaluating, directing, monitoring, communicating and assuring the ISO/IEC 27014:2013 standard are strongly related to the IT governance model (management and corporate governance), in addition three of them (evaluating, directing, monitoring) are strongly related to the objective of the ISO/IEC 38500:2015 standard to mitigate the risk of directors not complying with their obligations.

On the other hand, there is a moderately strong relationship with the six principles of the ISO/IEC 38500:2015 governance model, directly with responsibility, strategy, human behavior, compliance, and performance.

Objectives
The objective to add value to the board of directors and stakeholders, to provide alignment between the information security objectives, strategies and business of ISO/IEC 27014:2013, is strongly related to the objective of ensuring compliance with the obligations relating to the acceptable use of IT, to ensure that the use of IT contributes positively to the performance of the ISO/IEC 38500:2015 standard organization.

In addition, a moderate relationship is established by providing alignment between information and security objectives, mitigating the risks that directors have by failing to comply with their obligations and ensuring compliance with obligations relating to the acceptable use of IT at the level of integrity, reliability, and availability of information within the organization.

5 Discussions and Conclusions

A model of information security governance for higher education institutions would be strongly based on both standards in an integrated manner. The ISO/IEC 38500:2015 standard is mainly present at the first level of the model in terms of principles (responsibility, performance, strategy, and human behavior), with two substantial elements (risk analysis and compliance) of the ISO 27014:2013 standard that include the actions of directing, evaluating, monitoring, communicating, and ensuring.

In this study, a harmonization process has been carried out using a mapping for the comparison of both standards, identifying the related elements, following the guidelines

of [16] and [3], and with the help of Pareto's rule it has been possible to summarize in Table 6 the correspondence that exists between the two standards in order to define MoGSIIES levels.

The governance of information security is a specific part of IT governance, although it can be seen separately the two affect the strategic processes of organizations.

Another important aspect that has been carried out is the understanding of the importance of government information security on IT governance and being aware that the responsibility for making decisions rests with a strategic steering committee of the institution.

This study has contributed to the knowledge and collaboration of decision-makers in the strategic steering committee for information security in institutions, overcoming the visibility barrier that an organizational government suffers. Future work will focus on strengthening the model through substantives components and factorial analysis of components with the participation of actors from Ecuador's higher education institutions.

References

1. Gashgari, G., Walters, R., Wills, G.: A proposed best-practice framework for information security governance. In: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, (IoTBDS), pp. 295–301 (2017). https://doi.org/10.5220/0006303102950301
2. Carcary, M., Renaud, K., McLaughlin, S., O'Brien, C.: A framework for information security governance and management. IT Prof. **18**(2), 22–30 (2016). https://doi.org/10.1109/MITP.2016.27
3. Tenorio Chacón, O.: Government information security, myth or reality. In: ISACA (ed.) IX Congress ISACA Costa Rica, pp. 1–21 (2016). http://m.isaca.org/chapters12/costa-rica/events/Documents/PresentacionescongresoIsaca2016/13.GovernmentInformationSecurity.pdf
4. Luqman Ayodele, P.: Information Security Governance: an action plan for a non-profit organization based in the Nordics (Thesis, Laurea University of Applied Sciences) (2018). https://www.theseus.fi/bitstream/handle/10024/147149/Information_Security.pdf?sequence=1
5. Da Veiga, A., Eloff, J.H.P.: An information security governance framework. Inf. Syst. Manag. **24**(4), 361–372 (2007). https://doi.org/10.1080/10580530701586136
6. Clark, T.L., Sitko, T.D.: Information security governance: standardizing the practice of information Security. Res. Bull. **2008**(17), 1–11 (2008)
7. CGI Group: IT Security Governance—A holistic approach. CGI Group INC, pp. 1–8 (2016)
8. Bowen, P., Hash, J., Wilson, M.: Information Security Handbook: A Guide for Managers. NIST Special Publication 800-100, (October), 137 (2006). https://doi.org/10.6028/NIST.SP.800-100
9. De Oliveira Alves, G.A., Rust da Costa Carmo, L.F., Ribeiro Dustra de Almeida, A.C.: Enterprice security governance a practical guide to implement and control Information Security Governance (ISG). In: IEEE/IFIP Business Driven IT Management, pp. 71–80 (2006). https://doi.org/10.1109/BDIM.2006.1649213
10. INEN-ISO/IEC: Information Technology-IT Governance for the Organization (ISO/IEC 38500:2015, IDT), pp. 1–5. INEN, Quito (2019)
11. Quintanilla, M.Y.: Reference model of information technology governance for university institutions. Interfaces **9**(9), 87–116 (2016)

12. Merchán, V., Rodríguez, R.N.: Analysis of information technology government models and their relationship with the Ibero-American Model of Excellence. In: R. of U. with C. in I. (RedUNCI) (ed.) XXI Congreso Argentino de Ciencias de la Computación, vol. 1, p. 10 (2015). http://sedici.unlp.edu.ar/handle/10915/50028
13. NTE INEN-ISO/IECN: Information Technologies-Security Techniques-Information Security Government (ISO/IEC 27014:2013, IDT), pp. 1–5. INEN, Quito (2016)
14. Baldassarre, M.T., Caivano, D., Pino, F.J., Piattini, M., Visaggio, G.: Harmonization of ISO/IEC 9001: 2000 and CMMI-DEV: from a theoretical comparison to a real case application. Softw. Qual. J **20**(2), 309–335 (2012)
15. Pardo, C., Pino, F.J., Garcia, F., Baldassarre, M.T., Piattini, M.: From chaos to the systematic harmonization of multiple reference models: a harmonization framework applied in two case studies. J. Syst. Softw. **86**, 125–143 (2013)
16. Serrano, A., Gomez, B., Juiz, C.: Why the governance of projects, programs and portfolios (PPP) cannot be separated from the governance of IT standard. In: 2017 National Information Technology Conference, NITC 2017, September 2017, pp. 106–111 (2018). https://doi.org/10.1109/NITC.2017.8285661
17. Albán, P., Saavedra, R.: Proposal for a Strategic Control Plan and System, Applying the Balanced Scorecard Methodology, in the company Kilikos Flowers Cia. Ltda, dedicated to the production and commercialization of roses, located in the Canton Pedro Moncayo. National Polytechnic School (2009)
18. Gelbstein, E.: Data integrity: the most neglected aspect of information security. ISACA J. **6**(1), 6 (2011)
19. Fernández, A., Llorenz, F.: IT governance for universities. In: Conferencia de Rectores de las Universidades Españolas (ed.) Igarss 2014 (CRUE) (2014). https://doi.org/10.1007/s13398-014-0173-7.2