Information Technology Governance Model, Based on Risk Management and Information Security for Colombian Public Universities: Case on Study University of La Guajira

L R Viecco¹ and J G Arevalo¹, ²
¹University De La Guajira, Riohacha, La Guajira – Colombia.
²ENAPROT, Investigation Group of the Universidad De La Guajira.

E-mail: lviecco@uniguajira.edu.co

Abstract. Nowadays Universities require the implementation of practices in (IT) information technology governance issues where it involves structures, processes, mechanisms and measurement indicators for the good performance of Information Technology. In order to make a strategic alignment that defines the generation of value, and that is why this research shows the design of an IT governance. Based on model risk management and information security for Colombian public universities, for which its strategic alignment, its strategy is analysed business. Its institutional educational project in order to consolidate a model adjusted to the particular needs of each academic faculty.

1. Introduction

Technologies are now a reality in all processes of organizations, allow to store, manipulate, transport and manage information in universities and represents a valuable asset. It is increasingly common for companies to manage your information through electronic means, relying on various information technologies to comply with the processing objectives of information demanded by business processes today [1].

Undoubtedly, the support of Information Technology (IT) in the academic sector represents many benefits in the short and long term. Many of the largest universities in the world make extensive use of information technology to achieve their institutional objectives. IT support has allowed organizations around the world to be more competitive, but it has also created new scenarios of threats and risks, many of which are inherent to electronic or digital systems. Since the emergence of the first digital and electronic computing systems, there have been risks that have threatened three main attributes of high-quality information management: availability, integrity and confidentiality. Right now, information security has become crucial for any University and represents the protection of one of their most important assets: information. This important asset is stored and managed through the institutions hardware and software systems, which represent their base platform for information management. Unfortunately, there are serious risks that can threaten the continuity of their operations, and due to the fact that these risks can be characterized with having a high probability of occurrence and a potential for generating catastrophic damage; it necessitates that the organization adequately mitigate risks through a defined plan.

The threats and computer risks are of various kinds and day out they increase in number and probability of occurrence, such as the loss of data intentionally or not, information theft, loss of information caused by computer viruses, loss of information due to natural disasters such as electrical storms, earthquakes, fires etc. Due to the great variety of threats and risks to the security of information, the management of information security is a task that demands the commitment of the top management of the organization and for each of the management levels. The panorama of risks and computer threats information technologies have brought, has been the subject of studies by various agencies and companies of the largest in the world. Such Organizations as ISACA of the United
States, which is mostly integrated by computer auditors, the government of England, companies such as IBM, General Electric, American Telephone and Telegraph AT&T, and many others, have carried out research for decades. With the aim of collecting recommendations and best practices regarding the use and IT management, and its value for the achievement of business objectives, generating as results of their research, documents that formalize the methodologies of governance and management of information technology as best practices in organizations. [2].

The concept of IT governance was a subject of debate since the 90’s, and many definitions have been introduced by academics and professionals in the field. It has been noted that the various definitions differ in some aspects; however, most all of them share a commonality relating to the integration between companies and IT, usually known as strategic alignment and is considered one of the main elements of IT governance. The definitions also explicitly state that IT governance is an integral part of the company’s operations and incorporates processes and structures for decision making and best use of IT performance. It has also been observed that there is a clear difference between IT governance and IT management. IT governance is much broader and focuses on present and future demands for IT and the business while the latter maintains a management approach providing services, IT products, and operations. [3]

IT governance is a framework for an organization’s leadership, organizational structures, business processes, standards, and compliance with these standards, which ensure that the IT of the organization supports and allows for the achievement of their strategies and objectives. In the future, IT governance will be even more important than corporate governance today. Information and IT are critical to business survival, and organizations that do not” direct and control” their IT with a competitive advantage should expect to be left as roadkill on the information superhighway [4].

As previously discussed, the main purpose of IT governance is to align the strategic IT objectives with the purpose of the organization [5]; It may seem that this is only a matter of strategic planning and that the responsibility of this falls only the institutional managers, but in reality, this is not the case. Generally, in all organizations the IT areas are subject to different impositions, which can develop into impediments that can threaten the proper functioning of the organizational processes. Problems can also arise from succumbing to regulatory pressures and focusing too heavily on quick responses and not sustainable solutions, which can easily lead to losing alignment with the organization and leading them to dedicate themselves to solving lots of small, specific problems instead of focusing on the bigger picture [6]. According to the author, “it is intended to put the government and risk management of information technology in context, as an integral part of government and information technology management.” Based on this concept, organizations will not only contemplate management, control, operation, and administration systems, but also involve within their systems the risks that may exist in an organizational and technological structure from the dynamism that yields under the regulatory criteria [7]. The success stories and recommendations collected over the research on information technology management have concluded that companies must elevate IT management to top upper management applying the top-down methodology. This implies that IT business decisions must depart of filter down from the organization’s board of directors, thus elevating IT professionals to corporate governance and in this way, it is therefore, making it common to hear today the term, government of information technologies, applied to within the business world.

The governance of IT, ultimately involves the alignment of IT with business strategy, involving all processes of the organization, to promote better use of technology and organizational structures in order to achieve the organization’s objectives. The Colombian national government, aware of the need to continue advancing the construction of an inclusive and equitable that demonstrates adherence to the global standards of quality of life, has been promoting, through the ministry of IT. Important initiatives related to the government of the same and its management, including the launch of its IT4+ model demonstrating a great contribution to the advancement of a sector that is so vital to the further development of the nation. In short, it is crucial that a company use IT to streamline their processes, achieve a competitive advantage, and manage their most important asset: information.
However, it will be necessary to have IT governance in order to align the objectives of information technology with the business strategy.

2. Literature Review
Nowadays, higher education institutions, both public and private, have been stimulating a technological transformation with the incorporation of information technologies as a key element for generating value and seeking competitive advantages through focusing on achieving strategic alignment in order to determine which technological models should be implemented. Once this is determined, this is where IT governance comes into play and as a practice, has been strengthening itself through existing reference frameworks elevating technologies from a tactical level to a strategic level. Due to its constant innovations and the complexity of its planning process and execution, and producing positive reactions in top management a result of achieving favourable outcomes. When talking about governance, we are focusing on its primary objective, the creation of value, which allows us to enhance the resources and minimize the risks of IT, therefore obtaining benefits through the development of optimal processes.

When you reach this point in the process, you can address a governance model based on good practices to improve the efficiency and effectiveness of the fundamental resource of any organization: information and these in turn day by day are constantly updated, becoming an asset of great importance in them. As is well known, information and communications technology (ICT) used in the university are usually conceptually different, depending on whether they are focused on teaching, research, or community service. There are often important differences in ICT trainings among students as well as some manifestations of heterogeneity among the student’s training experiences depending on the area of the university that is taken into consideration [8].

In many universities, the relationship between IT and the business is totally disconnected; it is even more frequent that the IT infrastructure does not support the concept of an agile organization. The proliferation of information technologies, the increase in complexity, and the increase in costs are common features of many IT infrastructures. It is necessary to know the framework of concepts on which the research is based, so the following sections include a discussion of relevant findings from the literature review:

2.1 Strategy
They are the means by which long term objectives are achieved. Business strategies include geographic expansion, diversification, acquisition, product development, market penetration, cost reduction, disposal, liquidation and joint ventures. Strategies are potential actions that require decisions on the part of the management and resources of the company. In addition, the strategies affect the long-term finances of a company, at least for five years, thus guiding the future. The strategies produce effects on the functions and divisions of the company, and require that both external factors and internal factors facing the company be taken into account [9].

2.2 Strategic Management
Strategic management is defined as the art and science of formulating, implementing and evaluating decisions through functions that allow a company to achieve its objectives. According to this definition, the strategic direction focuses on the integration of management, marketing, finance, accounting, production, operations, research and development, and computer information systems to achieve the success of the company. The term strategic direction is used in this text as a synonym for the term strategic planning. The latter term is used more often in the business world, while the former is used in the academic environment.
2.3 Corporate governance
It is the set of mechanisms used to manage the relationship between stakeholders and determine and control strategic direction and performance at its core, corporate governance is concerned with identifying ways to ensure that strategic decisions are taken effectively. As a means of Corporations use it to establish order between the owner parties and their high-level managers whose interests may conflict. In modern corporations, especially the United States and the United Kingdom, a primary objective of companies is to ensure that the interests of senior managers are aligned with the interests of shareholders. Corporate governance implies supervision in areas where owners, managers and members of the board of directors may have conflicts of interest [10].

2.4 Business Governance
Corporate governance is the set of responsibilities and practices exercised by the Board and executive management, with the aim of providing strategic direction, ensuring that plans and objectives are achieved, assessing that risks are managed proactively and ensuring that Company resources are used responsibly. Corporate governance deals with the separation of ownership and control of an organization, while corporate governance focuses on the direction and control of the company, and IT governance focuses on the direction and control of IT [11].

2.5 University Government
It is a set of responsibilities and practices exercised by the higher university council and executive management in order to provide strategic direction, ensure compliance with objectives, establish an adequate management of risks, verify the responsible and efficient use of resources University. Compliance is a pattern of systematic behaviour of stakeholders, administrators and staff of the university, who are focused on achieving sustainable social and financial results. This behaviour must be directed towards the achievement of the four main assets of the organization: Infrastructure, customers and interested third parties, internal personnel, processes and the creation of value [12].

2.6 IT Government
Governance formalizes and clarifies oversight, accountability and decision rights for a wide range of IT strategy, resources and control activities. It is a collection of policies, practices and processes of management, planning and performance review; controls and metrics of performance on investments, plans, budgets, commitments, services, important changes, security, privacy, business continuity and compliance with laws and organizational policies [13]. An IT Government provides structures, processes, resources, and information to align with the company’s strategic objectives. As well as integrating and institutionalizing internationally recognized good practices in Organizational Planning, acquiring and implementing, delivering service and support, monitor the performance of IT [14]. There is no doubt that more and more organizations depend on Information Technology as the engine to generate value in the business. The implementation and administration of an IT government according to its line of business would generate a competitive advantage in the market. IT plays a role not only tactical or operational but also strategic, enabling new models, products and business services that ensure the leadership, growth and sustainability of the organization in the long term, transforming even its industries.

In the process of implementing GTI in any type of organization, it is necessary to take into account five fundamental areas as the main dimensions of the business, which in turn frame its development and its generation of value for its shareholders [15]. These Areas are listed below: Strategic Alignment: Focuses on securing the link of business and IT plans; in defining, maintaining and validating the IT value proposition and in aligning IT operations with the operations of the company. Delivery of Value: It refers to executing the value proposition throughout the delivery cycle, ensuring that IT delivers the agreed benefits aligned with the strategy, concentrating on cost optimization, and demonstrating the intrinsic value of IT. Resource Management: It refers to the optimal investment and the proper management of critical IT resources such as applications,
information, infrastructure and data. **Performance Measurement**: Follows and supervises the implementation strategy, the completion of projects, the performance of processes and the delivery of service. If there is no way to measure and evaluate IT activities, it is not possible to govern them or ensure alignment, delivery of value, risk management and effective use of resources.

3. **IT Governance Framework**

There is a growing concern in the top management of the entities about the activities of the IT function. The role that IT plays in organizations is vital, not only to maintain competitiveness, but to guarantee daily operations. This situation has led to the emergence of standards, models, methodologies and practices such as ISO / IEC 38500 own IT Government, COBIT 5, model GTI4U among others; aimed at ensuring better governance or a more optimal performance of IT in organizations. Although frameworks and guides such as COBIT and ITIL have been widely adopted, there is no absolute standard for Government IT [16]. Following is a description of each of the reference frames:

3.1 **Joint Information Systems Committee (JISC)**

The first initiative to design an IT governance model that serves as a reference for an entire university system was the Joint Information Systems Committee (JISC) for the universities of the United Kingdom. The JISC designed a reference model, and a self-assessment toolkit, which have become a starting point that helps universities in the process of identifying and defining the role of IT within the planning and governance of your organization. This framework was designed to be very flexible and can be used by different types of universities: large or small, old or modern and to take into account the different cultures that prevail in the institutional governance of universities. The reference model for IT governance of the JISC is based on five perspectives: government, administration, resources, organization and services.

3.2. **ISO 38500:2015**

The ISO / IEC 38500 standard, standardized and published by the ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission), is the first internationally recognized standard in IT Governance. It was published in June 2008 based on the Australian standard AS8015: 2005, provides a set of definitions related to the corporate governance of IT. Principles on which a task model is based and a task model focused on informing and guiding to all personnel involved in the design and implementation of the management policy system, processes and structures that support IT governance [17]. It is an international standard for corporate governance of information and communication technology. It is a “principled, high-level consultative standard”, provides “broad guidance on the role of the governing body and encourages organizations to use appropriate standards to support their governance of IT.” ISO / IEC 38500 does not replace, in other words, those norms and frameworks (such as COBIT™, ITIL, ISO 27001, etc.) that an organization has already implemented for the better governance of its IT, what it does do is provide a coherent framework to ensure that the council appropriately participates in the effective governance of IT[18].

The objective of this standard is to provide principles, definitions, and a model for governing bodies when using, evaluating, directing and monitoring the use of information technology (IT) in their organizations. This International Standard provides principles, definitions and a model for good governance of IT, to help those at the highest level of organizations to understand and comply with their legal, regulatory and ethical obligations related to the use of IT. Your organizations [19].

ISO 38500 establishes 6 principles for Corporate Governance of IT which are effective, efficient and acceptable, ensuring that organizations that follow these principles will help to balance risks and foster opportunities for the use of IT. They also express the desired behaviour that guides the decision making in the organization. According to the ISO / IEC (2015) these principles are: Responsibility, Strategy, Acquisitions, Performance, Conformity and Human behaviour. ISO 38500 divides IT governance activities into three main tasks: Evaluate the current and future use of IT, Direct the
Preparation and execution of plans and policies to ensure that the use of IT satisfies the objectives of the organization and Monitor the fulfilment of the policies and the performance in relation to the planned thing.

3.3 COBIT 5.0
It is the system that helps organizations create value to optimize risk levels within the organization, allowing information technologies to be managed holistically at all levels of the organization [20]. Provides of a comprehensive framework that helps companies achieve their goals for the governance and management of corporate IT. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire company, encompassing the entire business from start to finish and the functional areas of IT responsibility.

COBIT 5 describes a set of good practices for Senior Management and administration. This set establishes a set of controls on information technologies and organizes them around a logical framework of the processes related to IT. COBIT is not an isolated framework, but is aligned with other existing standards, such as the older COBIT versions, some standards such as: ISO 38500, essentially complementing the principles of (Evaluate, Direct and Monitor) (Isaca, 2015); ISO 15504 aligning with it in the concept to process capacity [21].

The process reference model of COBIT 5 divides the governance and management processes of business IT into two main process domains:

Government: Contains five government processes; within each process, evaluation, guidance and supervision (EDM) practices are defined.

Management: It contains five processes of government; within each process, evaluation, guidance and supervision (EDM) practices are defined.

The names of these domains have been chosen according to these designations of main areas, but contain more verbs to describe them: Align, Plan and Organize (Align, Plan and Organize, APO), Build, Acquire and Implement (Build, Acquire and Implement, BAI), Deliver, give Service and Support (Deliver, Service and Support, DSS) and Supervise, Evaluate and Evaluate (Monitor, Evaluate and Assess, MEA).

3.4 Model GTI4U
The GTI4U Model has been proposed by a group of Spanish researchers and developed by Fernandez (2009) and modified in the year (2011). This model is based on the ISO 38500 standard and has been developed to be implemented in the university environment and is also used to evaluate the overall level of maturity of the Spanish university system (SUE) [22]. The GTI4U Model is composed of three levels, which are mentioned below:

The first level: Includes all the elements of the ISO 38500 standard: IT governance model, principles, good practices and dictionary of terms and this in turn establishes that IT must be governed through three proposed actions such as assess, direct and monitor. Likewise adopts its principles of responsibility, strategy, acquisition, performance, compliance, and human factor. The principles express what are the behaviours that must be adopted when making decisions, and each of them establishes what should happen, but does not indicate how, where or who should implement these principles. These aspects will depend on the nature of the organization.

The second Level: It is composed of a Maturity Model (MM) using benchmarking tools for each principle, which will be used to establish at what level of IT governance maturity is the organization, MM usually establish several levels or states which each it has its level of demand, from a level of non-existent (0) to an optimized level (5), which helps the organization to self-evaluate and one level can’t surpass the other but has complied with the requirements in its entirety.

The third Level: It includes the indicators that will serve to measure the extent to which the criteria presented in the standard are met and if good practices of the IT Government are being satisfactorily carried out. At this level, a broad catalogue of government indicators has been designed,
divided into three groups: Maturity Model (CMM), Government Evidence Indicators (IEG) and Government Quantitative Indicators (ICG).

4. Results
The Colombian public universities in some particular cases, their technologies have been used for the support of their estates, which avoids doing the activities manually and that they are efficient in each established process. Resulting in an important organizational development supported by the exponential change of the technological development that has been experienced over time and the latter has increased the need for IT governance. Such university faculties obtaining as results two important variables to be addressed, such as the generation of value according to organizational objectives and the mitigation of the risks associated with IT services, allowing to achieve a correct strategic alignment. There are models on which they have been based to implement the IT Government in Universities such as: COBIT, JISC (Committee of Joint Information Systems) in the United Kingdom, MGTIU (Model of Government IT for Universities) in Spain, and the ISO standard / IEC 38500: 2015 (International Organization for Standardization), the latter as it focuses for public entities, it is necessary to know more details and integrate its model that proposes to govern IT through three fundamental actions such as Evaluate, Direct and Monitor.

The Responsibilities in the development of an IT Government planning in the universities should fall on the highest directives of the universities such as the Superior Council, Rectors, Vice-Rectors, Deans. For that reason, it is important to convince them technically of the convenience of adopting a Good governance of IT that focuses on establishing strategies and that these are aligned with those of the Universities. Determine the responsibilities of strategic IT planning where the current level is identified and clearly show where we want to go, proposing prioritized projects and these in turn must be monitored by an evaluation and monitoring of the performance of the processes through appropriate indicators.

According to the above, an IT Governance model is presented below, which is adapted to Colombian public universities where it is intended to provide guidance for managers, area managers and institutional support personnel on the acquisition and use of technology information. In this regard, the following model of IT governance is proposed, which brings together the guidelines for implementation in higher education institutions, which highlights the main processes for institutional improvements such as information security and risk management, which are identified in figure 1.

5. Macroprocesses of the Model and Government of IT
The following defined processes are presented below:

5.1 IT Strategic Planning
It focuses on determining an IT governance framework that ensures the strategic alignment of IT with institutional objectives by integrating its policies, processes and projects. The following are the Processes and Define Activities:

5.1.1 IT Strategic Management: Defined by the following activities:

PET1.1: Establish the current situation of the organization; identify its strategic direction to establish itself as an input for the construction of a good IT governance scheme.

PET1.2: Define the IT strategic plan where the desired level of the organization is defined and the definition of projects aimed at achieving the stated objectives, and define, in cooperation with relevant stakeholders, how IT will contribute to the strategic objectives of the company (goals) as well as the related costs and risks.

PET1.3: Analyse and know the initial situation of the organization in relation to IT governance, through the use of maturity models.
5.1.2 Organizational Structure of IT: Defined by the following activities:

PET2.1: Understand the business culture of decision making and determine an optimal model in decision making for IT.

PET2.2: Define the policies, guidelines and guidelines that are part of the IT Governance strategy, in accordance with institutional policies.

PET2.3: Conformation of an IT committee where functions are attributed with respect to aspects related to IT that have participation in all ICT decision activities and make sure to provide to the senior management performance reports on the performance of IT plans, policies and activities.

PET2.4: Define the roles and responsibilities in the IT structure, which have controls in IT decision making.

5.1.3 Evaluate and Supervise the IT Governance Model: Defined by the following activities:

PET3.1: Determine the relevance of IT and its role with respect to the business.

PET3.2: Periodically assess whether the mechanisms for IT governance agreed upon (structures, principles, processes, etc.) are established and operating effectively.

PET3.3: Supervise routine and regular mechanisms to ensure that the use of IT complies with relevant obligations (regulatory, legislation, common laws, contractual), standards and guidelines.
PET3.4: Evaluate the effectiveness of government design and identify actions to rectify any deviations.

PET3.5: Evaluate the effectiveness of the integration and alignment of IT strategies with institutional objectives to ensure that this contributes value.

5.2 Information Security Management

The objective of this process is to try to determine good practices through an ISMS in order to protect information assets in any of its states in the face of a series of risks or gaps that violate its fundamental principles of confidentiality, integrity and availability of information, through the implementation of processes and projects that allow managing and reducing the risks to which it is exposed and maximizing the return on investments in business opportunities. The following are the Processes and Define Activities:

5.2.1. Establish the SGSI: Defined by the following activities:

GSI1.1: Define the organizational understanding and its context, analysing the current situation of the entity in relation to the management of information security.

GSI1.2: Determine the scope of the SGSI.

GSI1.3: Define a diagnosis of the level of compliance of the entity in relation to the control objectives and controls established in Annex A of the ISO 27001 standard, and the action plans aimed at closing the gaps found.

GSI1.4: Determine the Maturity Level in which the entity is located for its information security model.

GSI1.5: Determine the needs and requirements of the stakeholders of the entity in relation to the Information Security Management System.

GSI1.6: Define and document information security policy that covers a defined scope and that is in the public domain for all officials of the institution.

GSI1.7: Establish the organizational structure, roles and responsibilities regarding Information Security.

GSI1.8: Define the Methodology of Analysis, Evaluation and treatment of Risks.

GSI1.9: Obtain authorization and support from senior management in the implementation of the SGSI.

5.2.2 Asset Management: Defined by the following activities:

GSI2.1: Assets associated with information and information processing facilities should be identified and an inventory of these assets should be developed and maintained.

GSI2.2: Each information asset must have its owner, who is responsible for the use throughout the life cycle.

GSI2.3: Rules for the acceptable use of information and assets associated with information and information processing facilities should be identified, documented and implemented.

GSI2.4: The assets of the organization that are under their charge must be returned, once the employment contract is finished, the delivery must be formalized.

GSI2.5: The information must be classified according to the legal requirements, value, criticality and susceptibility to disclosure or authorized modification.

GSI2.6: A set of procedures should be developed and implemented for the labeling of the information according to the information classification scheme adopted by the organization.

GSI2.7: Procedures for asset management should be developed and implemented according to the information classification scheme adopted by the organization.
GSI2.8: Procedures for the management of removable media should be implemented as these could store confidential information.

GSI2.9: Media containing information must be protected against unauthorized access, misuse or corruption during transport.

5.2.3 Communications Security Management: Defined by the following activities:

GSI3.1: Networks must be managed and controlled to protect information in systems and applications.

GSI3.2: The security mechanisms, service levels and management requirements of all network services must be identified.

GSI3.3: Groups of information services, users and information systems must be separated from the networks.

GSI3.4: Policies, procedures and formal transfer controls should be in place to protect the transfer of information through the use of all types of communication facilities.

GSI3.5: The information included in electronic messaging must be adequately protected.

GSI3.6: The requirements for confidentiality or non-disclosure agreements that reflect the needs of the organization to protect information must be identified, regularly reviewed and documented.

5.2.4 Access Control Management: Defined by the following activities:

GSI4.1: An access control policy must be established, documented and reviewed based on business requirements and information security.

GSI4.2: Users should only be allowed access to the network and to the network services for which they have been specifically authorized.

GSI4.3: A formal process of registration and cancellation of user registration must be implemented to enable the allocation of access rights.

GSI4.4: A formal user access provision process must be implemented to assign or revoke access rights for all types of users for all systems and services.

GSI4.5: The allocation and use of privileged access rights must be restricted and controlled.

GSI4.6: The allocation of secret authentication information must be controlled through a formal management process.

GSI4.7: The access rights of all employees and users external to the information and information processing facilities must be withdrawn upon termination of employment, contract or agreement, or adjusted when they are made changes.

GSI4.8: Users must be required to comply with the organization’s practices for the use of secret authentication information.

GSI4.9: Access to information and system functions of applications must be restricted in accordance with the access control policy.

GSI4.10: The use of utility programs that may have the ability to override the system and controls of applications should be strictly restricted and controlled.

GSI4.11: Access to program source codes must be restricted.

GSI4.12: A policy on the use of cryptographic controls for the protection of information should be developed and implemented.
GSI4.13: A policy on the use, protection and time of life of the cryptographic keys must be developed and implemented throughout its life cycle.

5.2.5 Supplier Management: Defined by the following activities.

GSI5.1: Information security requirements should be agreed upon and documented to mitigate the risks associated with provider access to the assets of the organization.

GSI5.2: All relevant information security requirements must be established and agreed upon with each provider that can access, process, store, communicate or provide IT infrastructure components for the organization's information.

GSI5.3: Agreements with suppliers should include requirements to address the information security risks associated with the supply chain of information and communication technology products and services.

GSI5.4: Organizations must regularly monitor, review and audit the provision of services by providers.

GSI5.5: Changes in the supply of services by suppliers must be managed, including the maintenance and improvement of existing information security policies, procedures and controls, taking into account the criticality of information, systems and business processes involved and the re-evaluation of risks.

5.2.6 Continuity Management: Defined by the following activities.

GSI6.1: The organization must determine its requirements for information security and the continuity of information security management in adverse situations, for example, during a crisis or disaster.

GSI6.2: The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the level of continuity required for the security of information during an adverse situation.

GSI6.3: The organization must verify at regular intervals the information security continuity controls established and implemented, in order to ensure that they are valid and effective during adverse situations.

5.2.7 Management of Acquisition, Development and Maintenance of Systems: Defined by the following activities.

GSI7.1: Requirements related to information security should be included in the requirements for new information systems or for improvements to existing information systems.

GSI7.2: The information involved in the services of the applications that pass over public networks must be protected from fraudulent activities, contractual disputes and unauthorized disclosure and modification.

GSI7.3: The rules for the development of software and systems should be established and applied to the developments within the organization.

GSI7.4: System changes within the development life cycle must be controlled through the use of formal change control procedures.

GSI7.5: Modifications to software packages should be discouraged, which should be limited to the necessary changes, and all changes should be strictly controlled.

GSI7.6: Principles for the construction of secure systems should be established, documented and maintained, and applied to any information systems implementation activity.
GSI7.7: Organizations must establish and adequately protect secure development environments for system development and integration activities that comprise the entire systems development life cycle.

GSI7.8: The organization should supervise and monitor the development activity of externally contracted systems.

GSI7.9: During the development, tests of security functionality must be carried out.

GSI7.10: Security tests must be performed based on the security requirements of the organization.

5.2.8 Cryptography Management: Defined by the following activities.

GSI8.1: A policy on the use of cryptographic controls for the protection of information should be developed and implemented.

GSI8.2: A policy on the use, protection and time of life of the cryptographic keys must be developed and implemented throughout its life cycle.

GSI8.3: Key management must be used to support the use of cryptography techniques in the organization.

5.2.9 Process Monitoring, Evaluation and Control Management: Defined by the following activities.

GSI9.1: Internal audits must be implemented at defined times.

GSI9.2: Periodic reviews of the ISMS should be carried out by Management to ensure that the scope is still adequate and that improvements have been identified in the ISMS process.

GSI9.3: The internal control office must ensure strict compliance with the improvement plans of the processes.

GSI9.4: Establish the methods to track, measure, analyze and evaluate the security processes and controls of the ISMS.

GSI9.5: Define an internal audit plan to measure the state of information security based on the ISO 27001: 2013 standard.

GSI9.6: Determine a continuous monitoring plan for the processes that lead the technology areas based on information security to identify compliance or otherwise implement corrective actions necessary for its good performance.

GSI9.7: Determine and document the causes of nonconformities with the ISMS and implement corrective actions identifying the vulnerability.

5.3 Risk Management of IT

Its function is to determine the risk management applied to Colombian public universities and four processes are proposed such as an establishment of the context of the risks, then a risk assessment, then a treatment of risks, then a stage of monitoring, which will try to mitigate the risk of a possible materialization. The following are the Processes and Define Activities:

5.3.1 Establishment of Context Defined by the following activities:

GRTI1.1: Understand the organization and its context. The organization must articulate its objectives and define the internal and external criteria and the evaluation factors to be considered in IT risk management.

GRTI1.2: Define the scope and appropriate depth of risk analysis activities, taking into account all the risk factors and the business criticality of the assets.
GRTI1.3: Establish and maintain policies for classification and analysis related to IT risks, with capacity for multiple types of events, multiple categories of IT risk and multiple risk factors.

GRTI1.4: Define and communicate the roles and responsibilities of IT risk management.

GRTI1.5: Define resources for risk management.

GRTI1.6: Establish mechanisms for internal communication and reporting.

5.3.2 Risk Assessment: Defined by the following activities.

GRTI2.1: The organization must identify the sources of risks, the areas of impacts, the events and the causes and potential consequences. The identification should include risks regardless of whether or not their origin is under the control of the organization, even though the origin of the risk or its cause may not be evident.

GRTI2.2: The organization must apply tools and techniques to identify risk, which are appropriate to its objectives and capabilities and the risks faced.

GRTI2.3: Factors that affect consequences and probability must be identified because the risk analysis involves the consideration of the causes and sources of the risk, its positive and negative consequences and the probability of that such consequences may occur.

5.3.3 Risk Treatment: Defined by the following activities:

GRTI3.1: Design and implementation plan that includes priorities in the treatment of risks.

GRTI3.2: Establish priorities in the implementation of risk treatment measures.

GRTI3.3: Apply security controls of Annex A of ISO 27001: 2013 to reduce the risk.

GRTI3.4: Allocate the necessary resources to carry out the implementation plan.

GRTI3.5: Give applicability to the most appropriate response plan in the event of occurrence of risk incidents and achieve the minimization of the impact that may be generated.

5.3.4 Monitoring and Revision: Defined by the following activities:

GRTI4.1: Measure the performance of risk management in relation to performance indicators, which are periodically reviewed for their suitability.

GRTI4.2: Periodically review if the risk management framework, the policy and verify whether the plan is still adequate, taking into account the internal and external context of the organization.

GRTI4.3: Evaluate the effectiveness of the risk management framework.

6. Roles and Responsibilities of the G&G Model for Colombian Public Universities

The following structure is proposed that defines roles and responsibilities according to the Macroprocesses and defined processes which have specific functions and we relate them below:

6.1 CEO - Rector

The highest executive (Chief Executive Officer - CEO), is responsible for making IT governance work in the organization, this in turn must have the organization committed to the vision of the business in terms of information, IT ensuring that executives and business users understand through a realistic internal communication strategy that is what is expected of IT, its contribution to the business in the future and that is expected from IT users. Finally, it has the following functions:

- Establish the current situation of the organization, identify its strategic direction that allow establishing itself as an input for the construction of a good governance scheme of you.
- Define the IT strategic plan where the desired level of the organization is defined and the
definition of projects aimed at achieving the stated objectives. Define in cooperation with relevant stakeholders, how IT will contribute to the strategic objectives of the company (goals) as well as the related costs and risks.

- Define the policies, guidelines and guidelines that are part of the IT Governance strategy, in accordance with institutional policies.
- Determine the relevance of IT and its role with respect to the business.
- Supervise routine and regular mechanisms to ensure that the use of IT complies with relevant obligations (regulatory, legislation, common laws, contractual), standards and guidelines.
- Periodically assess whether the mechanisms for IT governance agreed upon (structures, principles, processes, etc.) are established and operating effectively.

6.2 CIO- IT General Manager
The role of the general director of IT (Chief Information Officer - CIO) is strengthened, becoming strategic and fundamental support of the business strategy as responsible for the management of information in the company, among the functions in charge are established the following:

- Analyze and know the initial situation of the organization in relation to IT governance, through the use of maturity models.
- Define the roles and responsibilities in the IT structure, which have responsibilities in IT decision making.
- Evaluate periodically if the mechanisms for IT governance agreed upon (structures, principles, processes, etc.) are established and operating effectively.
- Evaluate the effectiveness of government design and identify actions to rectify any deviations.
- Evaluate the effectiveness of integrating and aligning IT strategies with institutional objectives to ensure that this adds value.

6.3 Information Security Leader
Its objective is to lead implementation projects in the information security management system in the entity and its defined functions are as follows:

- Define the organizational understanding and its context, analyzing the current situation of the entity in relation to information security management.
- Determine the Maturity Level in which the entity is located for its information security model.
- Determine the needs and requirements of the interested parties of the entity in relation to the Information Security Management System.
- Define and document information security policy that covers a defined scope and that is in public domain for all officials of the institution.
- Define an internal audit plan to measure the state of information security based on the ISO 27001: 2013 standard.
- Determine and document the causes of nonconformities with the ISMS and implement corrective actions identifying the vulnerability.
- Design a system that allows continuous improvement of the ISMS through a systematic process.
- A formal process of registration and cancellation of user registration must be implemented to enable the allocation of access rights.
- All relevant information security requirements should be established and agreed upon with each provider that can access, process, store, communicate or provide IT infrastructure components for the organization’s information.
- All relevant information security requirements should be established and agreed upon with each provider that can access, process, store, communicate or provide IT infrastructure components for the organization’s information.
6.4 **Risk Management Leader**
It is responsible for establishing all the risk management margins and is in charge of the following functions:

- Define the scope and appropriate depth of the risk analysis activities, taking into account all the risk factors and the criticality of the business assets.
- Establish and maintain policies for classification and analysis related to IT risks, with capacity for multiple types of events, multiple categories of IT risk and multiple risk factors.
- Establish mechanisms for internal communication and reporting.
- Design and implementation plan that includes priorities in the treatment of risks.
- Establish priorities in the implementation of risk treatment measures.
- Give applicability to the most appropriate response plan in the event of the occurrence of risk incidents and achieve the minimization of the impact that may be generated.
- Measure the performance of risk management in relation to performance indicators, which are reviewed periodically in terms of their suitability.
- Evaluate the effectiveness of the risk management framework.

6.5 **IT Infrastructure Leader**
It is in charge of proposing and managing the IT infrastructure and the operations that are given in it and is in charge of the following functions:

- The rules for the development of software and systems must be established and applied, to the developments within the organization.
- Establish and adequately protect secure development environments for system development and integration activities that encompass the entire systems development life cycle.
- Control changes in the organization, business processes, facilities and information processing systems that affect information security.
- Plan and obtain the homogeneity of equipment and base software in order to maximize the availability of information services.

6.6 **Internal Control Leader**
Its functions are the following:

- Define the policies, guidelines and guidelines that are part of the IT Governance strategy, in accordance with institutional policies.
- Evaluate periodically if the mechanisms for IT governance agreed upon (structures, principles, processes, etc.) are established and operating effectively.
- Verify that the planning, management, operation and support of the technological infrastructure, guarantee the availability, quality and operation of the electronic computer services, ready to fulfill the mission of the entity

7. **RACI Matrix**
Taking into account the roles defined in the government and management model for public universities, the matrix of responsibilities of each of the roles in the different macroprocesses is defined with their processes. Using the responsibility allocation matrix (RACI), they are named by the four letters with which the type of relationship with a process that each agent has is encoded:

- **R**: Responsible / Responsible. He is the one in charge of doing the task or activity.
- **A**: Accountable / Person in charge. It is the person who is responsible for the task being done. It is not the same as the R, since it does not have to be the one who performs the task,
you can delegate it to others. However, if he is the one who must ensure that the task is done, and done well.

- **C**: Consulted / Consult. The resources with this role are the people with whom one must consult data or decisions regarding the activity or process that is defined.
- **I**: Informed / Inform. These people are informed of the decisions that are made, results that occur, states of service, degrees of execution.

**Table 1. RACI Matrix**

| MACROPROCESS | PROCESS ID | PROCESS                                      | CEO - DIRECTOR UNIVERSITY | CEO - DIRECTOR GENERAL OF IT | RISK MANAGEMENT LEADER | INFORMATION SECURITY LEADER | IT INFRASTRUCTURE LEADER | INTERNAL CONTROL LEADER |
|--------------|------------|----------------------------------------------|---------------------------|-----------------------------|------------------------|-----------------------------|--------------------------|-------------------------|
| **IT STRATEGIC PLANNING** | PET1 | IT STRATEGIC ADDRESS | A-I | R-I | C | C | C | C |
|               | PET2 | ORGANIZATIONAL STRUCTURE OF GOVERNANCE | A-I | R-I | C | C | C | C |
|               | PET3 | EVALUATE AND SUPERVISE THE IT GOVERNANCE MODEL | A-I | R-I | C | C | C | C |
| **INFORMATION SECURITY MANAGEMENT** | GSI1 | ESTABLISH THE INFORMATION SECURITY MANAGEMENT SYSTEM | I | A-I | R-I | R | C | C |
|               | GSI2 | ASSENT MANAGEMENT | I | A-I | C | R | C | C |
|               | GSI3 | COMMUNICATIONS SECURITY MANAGEMENT | I | A-I | C | R | C | C |
|               | GSI4 | ACCESS CONTROL MANAGEMENT | I | A-I | C | R | C | C |
|               | GSI5 | SUPPLIER MANAGEMENT | I | A-I | C | R | R | C |
|               | GSI6 | CONTINUITY MANAGEMENT | I | A-I | R-I | R | C | C |
|               | GSI7 | MANAGEMENT OF ACQUISITION, DEVELOPMENT AND MAINTENANCE OF SYSTEMS | I | A-I | R-I | R | C | C |
|               | GSI8 | OPERATIONS SECURITY MANAGEMENT | I | A-I | C | R | C | C |
|               | GSI9 | CRYPTOGRAPHY MANAGEMENT | I | A-I | C | R | R | C |
|               | GSI10 | FOCUS-UP MANAGEMENT, EVALUATION AND PROCESS CONTROL | I | A-I | R-I | R | C | C-I |
| **IT RISK MANAGEMENT** | GRT1 | ESTABLISHMENT OF THE CONTEXT | I | A-I | R | C | C | C |
|               | GRT2 | RISK ASSESSMENT | I | A-I | R | C | C | C |
|               | GRT3 | RISK TREATMENT | I | A-I | R | C | C | C |
|               | GRT4 | MONITORING AND REVIEW | I | A-I | R | C | C | C |

**8. Conclusions**

IT governance implemented with a top down management system allows upper management to have direct control of IT investments, so that they are able to contribute directly to the fulfilment of institutional goals. This method is achieved through the distribution of roles and responsibilities that support decision making, as well as the implementation of rules and procedures that allow for strategic monitoring of IT decisions, ensuring the strategic alignment of IT with the institutional plans.

As it has been demonstrated evidenced throughout the article, it is clear and undeniable that information is the most important asset of an organization, that is why the importance of beginning starting from with this premise is vital when one is applying the framework to for public universities. The power to have Having an IT governance Model of Government and IT Management model of IT where, in which an Information Security Management System (ISMS) is established and a Risk Management strategy is established focusing on the needs of the business and based on standards and good practices. Such as ISO/IEC 27001:2013 and ISO/IEC 31000, allows enables the directing,
aligning, and monitoring of policies, processes and structures that support the corporate governance of information technologies in alignment with the institutional government within the framework of strategic, mission, and support processes.

The proposed model has characteristics of Colombian Public Universities, however to the extent that private universities want to adopt them, they will have to align it with their specific institutional needs and characteristics. At the time of design, senior management is taken into account who is the visible head of the organization and a general manager of IT who ensures that IT objectives are aligned with the strategy of the particular university and a good agreement of its resources. Manage security information, risk management and in addition to the performance of the aforementioned to generate added value to the company.

It is important to encourage public universities in the need to implement the IT Governance and Management model that in order to generates maturity in IT processes, where there are including its strategic, tactical and operational components. It is clear to determine that today’s organizations are aware of the need to govern IT, taking into account especially considering that there are critical mission processes and operations which would indicate that the model would achieve the goal of minimizing risks and strengthening the security of the organization. Knowledge in this particular case. It is for this reason that it is important to implement the model it because it clearly establishes strategic guidelines to successfully carry out the processes involved for continuous improvement, which would mean that Therefore, in order to achieve success in public universities. It is necessary to have knowledge is needed of standards and norms with clear methodologies and good IT governance that leads, organizes, and defines the guidelines to follow, and maintains with a view a vision for to sustaining their processes under an organizational culture.

Finally, from the results of the article, some recommendations have been determined on aspects that one should to take into account when implementing these IT governance model in public universities:

- It is important that the board of directors and senior management are involved in matters of governance related to the Government in order to ensure the commitment and alignment of between the IT area strategies with and the strategies defined by the University. This should be done in such a way that it will be able to generate obtains the maximum value through from the investments made.
- Those implementing the model should carry out trainings and maintain awareness of the importance of implementing good quality IT governance in Universities. Where highly relevant standards are present involved, such as information security to mitigate risks of attacks of all kinds.
- The figure of the CIO should be created in order to have a direct communication with the Superior Council and the upper management. Develop responsible decision making regarding the acquisition of the technology and understand that this is of great help in working towards achievement of the decided objectives.
- The Information Security Management System and risk management must be implemented to protect the most valuable asset of the organizations, the information, and for this, it is necessary to have professionals specialized in the aforementioned areas.

References

[1] Berciano J 2016 La importancia y la necesidad de proteger la información sensible. Obtenido de: RedSeguridad.com:http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/la-importancia-y-la-necesidad-de- proteger-la-informacion-sensible.

[2] Isaca 2016 Incident Management and Response. Obtendo de http://www.isaca.org/Knowledge-

[3] Janahi L, Griffiths M, Al-Ammal H 2015, A conceptual Model for IT Governance in Public

17
Sectors.

[4] Calder A 2008, *ISO/IEC 38500 The IT governance standard*.

[5] Webb P and Pollard C 2006, Attempting to Define IT Governance: Wisdom or Folly. Proceedings of the 39th Hawaii Ridley G, International Conference on System Science, IEEE Computer Society.

[6] Weill P and Ross J 2004, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business School Press.

[7] Butler B 2016, The cloud computing subnet. Obtained from the cloud computing industry.: https://www.networkworld.com/article/3016926/cloud-computing/ibm-will-manage-atandt-s-hosted-and-cloud-services-as-part-of-partnership.html

[8] Fernández V E 2008, UNITIL: Gobierno y Gestión de TIC basado en ITIL.

[9] Fred D R 2003, *Conceptos de Administración Estratégica*.

[10] Hitt M A, Ireland D and Hoskisson R 2007, Strategic Management: Competitiveness and Globalization (Concepts and Cases) Seventh Edition

[11] ISACA, IT Governance Developing a Successful Governance Strategy, 2005.

[12] Gómez V H, Tejada R A and Giraldo L M 2011, Un modelo preliminar de gobierno de tecnologías de información para universidades colombianas

[13] Selig G J PMP COP 2008, Implementing IT Governance A Practical Guide to Global Best Practices in IT Management.

[14] Isaca 2015, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL: ISACA

[15] Muñoz I and Ulloa G 2011, Gobierno de TI. Revista S&T, 9(17), 23-53. Cali: Universidad Icesi.

[16] Bayona S, Ayala M 2017, IT governance: Progress and challenges on public administration.

[17] De la Cámara Delgado Ms, Sáenz F J, Calvo J & Fernández V 2002, Project Management and IT Governance. Integrating PRINCE2 and ISO 38500.

[18] Calder A 2008, ISO/IEC 38500 The IT governance standard.

[19] International Organization for Standardization (ISO) / International Electro technical Commission (IEC), 2015.

[20] ISACA. COBIT 5 for Information Security. Illinois, Michigan, Estados Unidos de América: ISACA, 2012. p. 220.

[21] De Haes, S, Van Greembergen, W and Debreceny, R S 2013, COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal of Information Systems., 27(1), p307-324.

[22] Norma ISO 27000, Sistema de Gestión de Seguridad de la Información 2013.