It governance model for state entities, as support for compliance with the information security and privacy component in the framework of the digital government policy

C Ávila¹, E J Chinchilla¹, and T Velásquez Pérez¹
¹ Grupo de Investigación en Tecnología y Desarrollo en Ingeniería, Universidad Francisco de Paula Santander Seccional Ocaña, Colombia

E-mail: cavilam@ufpso.edu.co, ejsantiagoch@ufpso.edu.co

Abstract. This article proposes an information technology governance model that facilitates the direction, control and fulfillment of the objectives of the implementation and maintenance of the information security and privacy program proposed by the Ministry of Information Technology and Government Communications Colombian to state organizations in the framework of the digital government policy. Based on the identification of the regulations of the Colombia state for the implementation of the information security and privacy model, the analysis of the existing information technology governance frameworks that converge on the governance and management objectives of the information security and privacy model is continued and finally the model is structured of governance. contributes to the technological development of the Colombia society through the construction of an innovative tool that facilitates the direction, control and rapid adoption of the management system of information security and privacy defined by the Colombia State, which results in the assurance and privacy of information of all Colombian that is in the hands of state entities, reducing frauds, the exposure of our personal information among other risks.

1. Introduction

Government information technology (IT) government, is a concept that "with the promise of making visible the value they generate, has been taking shape to be better interpreted, implemented and applied, globally"[1]. There are currently many definitions [2], frames it in a structure of relationships to direct and control the role of IT technology within an organization in order to achieve the objectives with the aggregation of value and the balance of risk, compared to IT return and its processes. Part of the IT government lies in designing, applying and evaluating a set of criteria to govern the respective function optimally [3], explains it as a set of rules, principles, policies, or organizational charts that define or limit the scope of the area managers.

In parallel [4], IT governance is defined as a set of institutionalized practices or activities that minimize uncertainty and acquire better performance in terms of the outsourcing relationship between IT service providers and subcontractors. In relation [5], refers that the IT governance institute (ITGI) established five domains of coverage, strategic alignment of IT with the business, value delivery, risk management, resource management and performance measurement. “The IT government is the responsibility of the executives of the board of directors and contemplates leadership, structures and operational processes to ensure that the company’s IT supports the organizational strategies and objectives”. 
In this sense, information is the most important asset an organization has, therefore, its duty is to protect it. Your security depends on ensuring compliance with your confidentiality, integrity and availability, pillars or fundamental principles of information [6]. At present, an organization is clear that in order to remain current and improve market expansion, internet interconnectivity, business automation and online processes are relevant. This trend of “techno-dependence” as well as brings benefits, also implies risks for the information asset, as a consequence of the vulnerabilities in the software and hardware of technological products. Thus, the immersion in the network of networks, as well as expanding the business, also exposes a greater number of threats to the information asset, because it expands the area to be controlled. Therefore, the implementation of mechanisms to safeguard IT is currently a necessity for organizations [6].

In accordance with the new technological trends and with the objective of guiding the public entities of national and territorial order in the improvement of the standards of information security, the Colombia government through the Ministry of Information Technology and Communications (MinTIC), in the framework of the open government strategy (GEL), designed the information security and privacy model (MSPI), based on the references of ISO/IEC 27001 version 2013, the National Information Solutions Cooperative (NISC) cybersecurity framework, the legal basis of the law on protection of personal data [7], transparency and access to public information [8] among others, relevant in the management of the security of the assets of information [9]

In the context of international backgrounds [10], they proposed a model for cloud governance as a holistic framework that addresses IT governance, through a pattern that designs requirements management, for information security, the cycle of life, risk management and compliance, from the framework of IT governance. While in Colombia, MinTIC, designs a MSPI for online government strategy 2.0, with a sustainable approach that goes from preparing the entity to begin implementation, defining gaps, until alignment with the information security management system (ISMS) [11].

In this area, Escuela Colombiana de Ingeniería Julio Garavito presents a methodology for measuring the effectiveness of the MSPI Management indicators [12]. On the other hand [13], propose a model of integration of MECI and COBIT, for public entities; covering the relationship matrix for the components of the internal control standard model and the COBIT control objectives, in order to align the controls applicable to IT with the processes stipulated for these entities. In addition to this, it develops a maturity model that allows to know at what stage of IT governance application the organization is.

On the other hand [14], refers to the design of a proposed IT government framework for the Ministry of Higher Education, Science Technology and Innovation (SENESCYT), based on best practices, whose purpose is to develop a proposal that makes use of best practices of generating optimal value from IT, in search of maintaining the balance between the institutional strategic goals and the generation of benefits. Similarly, at the Universidad de Los Llanos, an IT governance model is applied as a case, in support of administrative processes, which proposes to sensitize and raise awareness among senior managers of the educational institution the need for the effective use of technologies [15].

The great use of technological tools in fulfillment of the missionary object, obliges most organizations to implement new patterns framed in standards that allow to manage the security of their information. The MSPI, designed by MinTIC, is aligned with the IT architecture reference framework and transversally supports the components of the GEL strategy: ICT for services, ICT for open government and ICT for management [9]. Although MinTIC has been available as a guide, at the time of implementation there are difficulties in carrying out the stages; among them and possibly the main one is the lack of trained professionals with experience in implementing ISMS within public entities [11]. In addition, senior management does not assume the role of leader and sponsor that corresponds to it, so it leads that the project is affected in its development, taking into account that it is not given the required importance [11].

This allows us to deduce that the MSPI is a management-oriented model, denoting the absence of direct control that helps to exercise direction and complements the management of new technologies in public administration. In addition, the IT area is highlighted and especially in the state entities, the need for control instruments related to key IT processes, which allow senior management to monitor, prevent
failures, observe trends and find possibilities for improvement [13]. In relation [16], they highlight the importance that IT managers have in order to achieve the alignment, synchronization and convergence of technology and business, as well as the ability to manage them. “Organizations are increasingly dependent on IT for decision making in order to sustain business growth” [5].

2. Methodology
The development of the proposed characterization of an IT governance model for state entities, in support of compliance with the MSPI component in the framework of the digital government strategy, was carried out under the research approach quantitative with a positivist paradigm with descriptive study scope, supported by field activities that facilitate the collection and analysis of the information obtained regarding the different models of IT governance, which could facilitate the characterization of the model required for the effective adoption of the MSPI by the government sector entities. Taking into account the methodological support that arises from the documentary analysis as the basis of the epistemic structure to generate an approach to the phenomenon of study.

3. Results
The development of the proposed IT governance model for state entities, in support of compliance with the information security and privacy component in the framework of the digital government policy, is a process in which a series of activities.

3.1. Identification of the regulatory framework of the Colombian state for the implementation of the security and privacy model
The national government has established the guidelines for the government strategy in decrees 1151 of 2008, 2573 of 2014, 1078 of 2015 and the digital government policy in 1008 of 2018. In the objective the digital government policy aims to take advantage of the technology by the state, citizens and interest groups, so that they acquire the specific competences and capacities for the fulfillment of needs, as well as the solution of public problems [17]. The scope of application is maintained. Regulated principles prevail in article 3 of law [18] and article 3 of law [19], as well as that of the innovation sector, competitiveness ICT, proactivity and information security are added. The structure of the gel strategy to that of digital policy, changes from four to two components (ICT for the state and ICT for the Society). It adds a series of enabling elements that allow entities, regardless of their resources and capacity, to carry out the implementation according to their needs and characteristics. As responsible for implementation institutional development is established in the state. The assignment of roles and responsibilities is made to the actors involved in the implementation of the digital government policy.

An institutional scheme is developed aligned with decree [20], in which the instances of direction and coordination of the planning and management system are adjusted and the institutional, departmental, district and municipal management and performance committees are created [21]. The monitoring and evaluation are in charge of the entities that report the achievement of the policy's proposals based on the fierce projects and initiatives that make use of icts and the progress in implementation is measured based on the goals reported in each term [15].

3.2. Existing IT governance frameworks that converge on governance and management objectives
The corresponding mapping between the principles of ISO/IEC 38500 and its alignment with the processes, catalysts and other elements of the COBIT 5 reference framework is presented (Figure 1).

3.3. Design of the governance model that facilitates the evaluation, direction and control of the security and privacy program of the information assets of the entities of the Colombian state
The structure of the proposed model aligns the phases of the MSPI, oriented mainly to the management of information asset security, with the IT goals and processes of the COBIT 5 management domain, in order to facilitate the application of the main governance processes proposed by ISACA to the MSPI. The model consists of 3 stages that include government and management activities throughout the
subsequent commissioning monitoring of the security and privacy management system proposed by the Colombia state (see Figure 2). The stages of the proposed model are:

- GAP analysis
- Model adoption
- Monitoring and maintenance

The stages are aligned with the government and IT management domains, the COBIT 5.0 IT goals and those required for the MSPI production start-up.

Figure 1. Existing IT governance frameworks that converge on governance and management objectives.
3.4. Alignment of the processes and activities of the proposed governance model

In order to identify the relevance of the governance processes proposed by COBIT 5.0 that facilitate the proposed model management, evaluation and monitoring of the implementation of the MSPI; the alignment of the processes of the selected government standard is carried out, with the activities required for the adoption of the information security and privacy model defined by the digital government policy to state organizations.

3.5. Implementation plan

The implementation of the IT government model in support of the MSPI for the entities of the Colombian state, begins with the creation of the appropriate environment for the application of the model, which allows the initiative to be guaranteed by stakeholders. The base implementation guide for the proposed model is that proposed by the IT [22], in which seven (7) phases are established.

3.5.1. Phase 1: Obtain the commitment of senior management. The objective of this phase is to obtain the endorsement and support of the top management of the organization for the implementation of the IT governance model in support of the MSPI. As well as dissemination among stakeholders (interested parties).

3.5.2. Phase 2: Determine the current status. The objective of this phase is to know through a diagnosis what is the current state of the level of maturity of IT governance in the organization and what the desired one to achieve is.

3.5.3. Phase 3: Establish the desired future state. Determine the maturity status of the IT government desired for the organization, according to the diagnosis made in the previous phase.

3.5.4. Phase 4: Identify the gaps. According to the diagnosis made in the previous two phases, through the levers, the current and desired level of IT maturity in the organization is obtained, the identification of gaps to be closed is performed to give continuity to the implementation of the model.

3.5.5. Phase 5: Define the implementation plan. The objective of this phase is to determine the implementation plan or program to follow to achieve the proposed objectives.

3.5.6. Phase 6: Develop the Implementation Plan. In this phase the implementation development established in the previous phase begins.

3.5.7. Phase 7: Monitor and control the performance of the implementation. Establish a periodic review program for each of the projects, which allows the validation of compliance with the proposed objectives.
4. Conclusions

After identifying the regulatory framework of the Colombia state for the implementation of the MSPI, it is identified that existing IT governance frameworks can support the achievement of governance and management objectives by integrating the model with the government domains and the strategic level with the IT goals of the domain guide, evaluate and monitor, and the diagnostic phase.

The management domain integrates the tactical and operational levels with the IT goals that are included in the four COBIT 5 domains associated with IT management and the planning, performance evaluation, implementation and continuous improvement phases. The model includes the stage of gap analysis associated with the government domain and the adoption of the model and monitoring and maintenance associated with management.

An implementation plan is included that includes the phase of obtaining senior management commitment, determining the current status, establishing the desired future status, identifying the gaps, defining the implementation plan, developing the plan and monitoring the implementation performance.

References

[1] León Lozano A 2015 Revista de Sistemas 97 4
[2] Verhoef C 2007 Quantifying the effects of IT-governance rules Sci Comput Program. 67 247
[3] Rahimi F, Møller C and Hvam L 2016 Int. J. Inf. Manage. 36 142
[4] Kim Y J, Lee J M, Koo C and Nam K 2013 Int. J. Inf. Manage. 33 850
[5] Aguilar Alonso I, Carrillo Verdún J, Tovar Caro E 2017 Int. J. Inf. Manage. 37 1461
[6] Chinchilla E J S, et al. 2017 Riesgos de ciberseguridad en las empresas Tecnología y Desarrollo 15 1
[7] Congreso de la República 2012 Ley estatutaria 1581 (Colombia: Congreso de la República)
[8] Congreso de la República 2014 Ley 1712 de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones (Colombia: Congreso de la República)
[9] Mintic 2016 Modelo de seguridad y privacidad de la información (Colombia: Ministerio de Tecnologías de la Información y las Comunicaciones)
[10] Brandis K, Dzombeta S and Haufe K 2014 Futur. Gener. Comput. Syst. 32 274
[11] Ocampo García D 2011 Modelo de seguridad de la información para las entidades públicas del estado Colombiano (Universidad Piloto de Colombia)
[12] Useche Samudio C 2016 Metodología para la medición de la efectividad de los indicadores de gestión del modelo de seguridad y privacidad de la información (Bogotá: Escuela Colombiana de ingeniería Julio Garavito)
[13] Andres J, Medina C, Edinson J and García M 2011 Modelo de integración entre meci y un marco de referencia para gobierno de TI aplicado a entidades territoriales municipales en Colombia (Santiago de Cali: Universidad ICESI)
[14] Espinoza Aguirre C and Pillo Guanoluisa D 2018 IT governance model for public institutions with a focus on higher education (Caceres:13a Conferencia Ibérica sobre Sistemas y Tecnologías de la Información)
[15] Vargas Alvarado S M 2017 Modelo de gobierno de TI como apoyo a los procesos administrativos caso universidad de los llanos (Manizales: Universidad Nacional de Colombia)
[16] Chen Y C, Wu J H 2011 Inf. Manag. 48 145
[17] Carlos J, Silva N, Fernandez L 1151 Manual para la implementación de la estrategia de gobierno en línea (Colombia: Gobierno digital)
[18] Congreso de la República 1998 Ley 489 sobre la organización y funcionamiento de las entidades del orden nacional (Colombia: Congreso de la República)
[19] Congreso de la República 2011 Ley 1437 código de procedimiento administrativo y de lo contencioso administrativo (Colombia: Congreso de la República)
[20] Congreso de la República 2017 Decreto 1499 del cual se modifica el Decreto 1083 de 2015, decreto único reglamentario del sector función pública, en lo relacionado con el sistema de gestión establecido en el artículo 133 de la Ley 1753 de 2015 (Colombia: Congreso de la República)
[21] Mendoza Silva L, Vega Gallegos G 2018 Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa Sisc (Colombia: Universidad del Pacífico)
[22] Governance Institute 2007 It governance using Cobit ® and val it Tm : Student book, 2nd edition to higher education (United States of America: Governance Institute)