JISTEM - Journal of Information Systems and Technology Management
Revista de Gestão da Tecnologia e Sistemas de Informação
Vol. 12, No. 2, May/Aug., 2015 pp. *289-316*
ISSN online: 1807-1775
DOI: 10.4301/S1807-17752015000200006

ADOPTION OF INFORMATION SECURITY MEASURES IN PUBLIC RESEARCH INSTITUTES

ADOÇÃO DE MEDIDAS DE SEGURANÇA DA INFORMAÇÃO EM INSTITUTOS DE PESQUISA PÚBLICOS

Antonio Eduardo de Albuquerque Junior
Ernani Marques dos Santos
Universidade Federal da Bahia, Bahia, Brasil

ABSTRACT

There are several Information Security measures recommended by international standards and literature, but the adoption by the organizations should be designated by specific needs identified by Information Security Governance structure of each organization, although it may be influenced by forces of the institutional environment in which organizations are inserted. In public research institutes, measures may be adopted as a result of pressure from Government and other agencies that regulate their activities, or by the influence of Information Security professionals, or simply adopting the same measures of leading organizations in the organizational field. This study aimed to investigate whether in public research institutes the adoption of Information Security measures is influenced by organizational factors relating to Information Security Governance, and by external factors relating to its institutional environment. The results show that these organizations are subject to institutional influences more than organizational influences.

Keywords: information security, governance, adoption, measures, research institutes

RESUMO

As organizações dispõem de uma série de medidas de Segurança da Informação recomendadas por normas internacionais e pela literatura, mas a adoção deve ser balizada pelas necessidades específicas identificadas pela Governança da Segurança da Informação de cada organização, embora possa ser influenciada por pressões do ambiente institucional em que as organizações estão inseridas. Em institutos de pesquisa públicos, as medidas podem ser adotadas como resultado de pressões exercidas pelo Governo e outros órgãos que regulam suas atividades, ou por influência de profissionais de Segurança da Informação, ou simplesmente por serem adotadas por outras

---

Manuscript first received/*Recebido em:* 30/12/2014 Manuscript accepted/*Aprovado em*: 15/06/2015

Address for correspondence / Endereço para correspondência

Antonio Eduardo de Albuquerque Junior, Mestre em Administração, estudante de Doutorado da Escola de Administração, Universidade Federal da Bahia, Av. Reitor Miguel Calmon, Salvador, Bahia, Brasil
E-mail: eduardo.albuquerque@bahia.fiocruz.br

Ernani Marques dos Santos, Doutor em Administração, Professor do Núcleo de Pós-Graduação em Administração, Escola de Administração, Universidade Federal da Bahia, Av. Reitor Miguel Calmon, Salvador, Bahia, Brasil, E-mail: emarques@ufba.br

organizações de destaque nesse campo. Este trabalho teve o objetivo de investigar se nos institutos de pesquisa públicos a adoção de medidas de Segurança da Informação é influenciada por fatores organizacionais, relativos à Governança da Segurança da Informação, e por fatores externos, relativos ao ambiente institucional em que estão inseridos. Os resultados mostram que essas organizações estão mais sujeitas à influência de fatores institucionais do que de fatores organizacionais.

Palavras-chave: segurança da informação, governança, adoção, medidas, institutos de pesquisa

1. INTRODUCTION

Some organizations have information as important or strategic assets and, therefore, they need to protect it. Among these organizations, Alexandria (2009) highlights that research institutes need to protect not only the information, but also knowledge, which is the main product of their activities. Pimenta and Sousa Neto (2010) consider information as a competitive advantage for these organizations. Similarly, Caminha, Leal, Marques Junior and Nascimento (2006) argue that information is a raw material, a product and one of its most valuable assets, such as technical management, data analysis, designs and patents. Albuquerque Junior, Santos and Albuquerque (2014) argue that research institutes have information as an important element of their activities and need to protect intellectual property. For these reasons, research institutes need to adopt measures to protect their information.

According to Dzazali and Zolait (2012), public organizations also face the challenge of protecting their information, considering they are environments where there are increasing complexity, interconnections, uncertainties and dependence on technology. These organizations also have to carry out their respective missions and comply with standards and guidelines from central agencies of the government. These organizations also need to ensure confidentiality of citizens' data and the availability and integrity of information that need to be accessible to the society, as well as continuity of public services, many of which are mediated by technology.

Because leading with sensitive information related to scientific research and its activities as public organizations, in addition to providing access to public information, disseminating research results, sharing data with partners and respecting regulations, public research institutes need to protect their information to ensure the continuity of their activities.

In these organizations, the Internet is a primary need and is actually a common fact researchers have remote access to technological resources (Bernaschi, d'Aiutolo, & Rughetti, 1999). In this context, technology that facilitates exchange and access to information also exposes these organizations to new threats that may hinder or even derail the fulfillment of their objectives (Alexandria, 2009). With the increasing of risk of the incidents that may compromise information, there was an increase of their impact for organizations (Fachini, 2009). Incidents may jeopardize not only information, but also related people and transactions (Marciano, 2006). As a result, organizations need to protect not only information, but also other assets involved in its processing, storage and transmission (Fontes, 2006).

To protect information and other associated assets, organizations have a set of Information Security measures recommended by international standards and models widely accepted by professionals and organizations around the world. According to the

Brazilian Association of Technical Standards [ABNT] (2005), Information Security is achieved through different controls, including organizational structures, policies, procedures and technology. These controls, or Information Security measures, as Sêmola (2014) prefers, are defined by this author as the practices, procedures and mechanisms to protect information and its assets against threats that exploit vulnerabilities, reducing them or limiting the probability or the impact of their exploitation, minimizing or avoiding risks.

Despite the need to adopt Information Security measures in research institutes, Perkel (2010) points out that there are problems in protecting information in these organizations, because Information Technology (IT) professionals attempt to protect information and knowledge, as researchers, students and research project teams have specific needs and demand freedom to develop their activities. Thus, Sêmola (2014) points out that each organization has its own characteristics that lead to particular Information Security needs. ABNT (2005), through NBR ISO/IEC 27002 (the Brazilian standard that is identical to international ISO/IEC 27002), expressed the same understanding by proposing that organizations need to conduct a risk analysis and assessment to identify vulnerabilities, threats, probability of occurrence and potential impact, allowing them to select which measures are necessary to their own reality.

However, the adoption of Information Security measures may not be result of strategic decisions by an Information Security Governance structure. Adoption may be a result of the regulation by the Government and other agencies responsible for regulating and controlling public research institutes activities, or the recognition of its importance for IT managers and professionals, because these measures are recommended by international standards widely adopted, and are associated with a training and certification market that may lead organizations to hire consulting services, professionals and managers with a homogeneous understanding about Information Security measure's needs. Also, measures adopted by leading organizations in academia or public sector may be imitated by public research institutes because of uncertainties about Information Security risks to which they are exposed (Albuquerque Junior & Santos, 2014). Thus, these organizations may adopt measures that do not meet the needs identified after a risk analysis, but that are responses to external forces to which they are subject.

Kam, Katerattanakul, Gogolin and Hong (2013) note that external pressures influence Information Security in academic organizations and that this influence may be understood from the perspective of Institutional Theory, approach suggested by Björck (2004) and Albuquerque Junior and Santos (2014) for research on Information Security.

As information is an extremely important asset for public research institutes and as the protection of information is a necessity or even an obligation, and in the characteristics of these organizations, this research aimed to investigate whether the adoption of Information Security measures by these organizations is influenced by organizational and institutional factors proposed by Albuquerque Junior and Santos (2014). To achieve this objective, the measures adopted by public research institutes were identified, and then it was examined whether the research model's factors influenced the adoption.

The organizational factors are related to Information Security Governance and include the formalization of roles and responsibilities, strategies and objectives of Information Security, risk assessment and management processes, resource analysis for the protection of information, internal control related to compliance with laws and

regulations, communication with other organizations, the engagement of leaders and managers, the organizational structures of Information Security, the Information Security Policy and the compliance with it, and the processes, procedures, internal rules and standards of Information Security. Institutional factors covered by the research are the laws, regulations and agreements requiring the adoption of security measures by organizations, the use of Information Security standards as models to be implemented, professionals with training or knowledge on Information Security and their participation in networks for knowledge and exchange of experience, and the use of successful experiences of other public or research organizations as models to be copied.

The article has seven sections, including this introduction and the references used. The second section presents the theoretical framework, with the theory of Information Security, security measures and Institutional Theory, the theoretical approach used in the research. The third section covers Information Security at public research institutes, the context of this research. The fourth section presents the methodological procedures used in the research. The fifth section shows the research results and analysis. Finally, in the sixth section the article shows the final considerations, limitations and future research suggestions.

2. THEORETICAL FRAMEWORK

According to Beal (2005) and Donner and Oliveira (2008), Information Security is the process for information assets protection against any threats to their availability, integrity and confidentiality. Sêmola (2014) argues that Information Security is a knowledge area with a focus on protecting information against unavailability and unauthorized access and change. According to Cooper (2009), it is the practice of ensuring confidentiality, integrity and availability of information resources. Based on the concepts presented in different texts and articles, Silva and Stein (2007) postulate that Information Security is the protection of information against the unauthorized access and use, the denial of service for those who are authorized to do it, with the protection of its confidentiality and integrity.

Marciano (2006) notes that different authors question the concepts commonly found in the literature. Although there is disagreement about the concept, it is clear that, to protect the integrity, confidentiality and availability of information is necessary to adopt Information Security measures. Fontes (2006), for example, argues that Information Security is the set of actions, policies, procedures, standards and guidelines that aims to protect the information. The NBR ISO/IEC 27002 (ABNT, 2005), which defines Information Security as the protection of confidentiality, integrity and availability of information, points out that it is obtained by adopting appropriate controls to the organizations' requirements. This standard specifies policies, processes, organizational structures, procedures, and hardware and software functions as examples of these controls.

ABNT (2005) defines Information Security measures (or controls, as described in the standard) as ways to manage risk. According to Sêmola (2014), these measures have the potential to prevent threats that exploit vulnerabilities, and to reduce vulnerabilities by limiting the probability of exploitation or the impact on the organization, minimizing or even avoiding the related risks.

It is important to mention that many incidents originate in human behavior. People are regarded as the greatest weakness of Information Security (Mitnick &

Simon, 2003; Silva & Stein, 2007; Sêmola, 2014). For this reason, information protection should not be only a technical issue, but also social, for which there is no purely technological solution known (Marciano & Lima-Marques, 2006). Therefore, measures should address not only technological and physical issues but also administrative, to change human behavior in the organization. Björck (2005) proposes to classify Information Security measures as they aim to affect in the organization:

a) Administrative measures: aim to change people's behavior; affect the organization and its members. They may be formal (rules present in an Information Security Policy) or informal (training and education to promote knowledge on Information Security). They are related to standards, organizational structure and Information Security processes.

b) Technical measures: aim to affect the technology used to process and store information, ensuring access only to those who are legitimately authorized. They operate in computer systems and may reinforce administrative measures.

c) Physical measures: designed to protect information and its assets by physical mechanisms that affect the physical environment. They are related to security of property, such as doors, locks and perimeters, and measures against environmental events such as floods and fire.

Björck (2005), Belasco and Wan (2006) and ABNT (2005) suggest various administrative, technical and physical measures. Although some of them are widely adopted, such as the use of firewall, antivirus, anti-spam, logical access control, proxy, the existence of Information Security Policy, incident treatment team, backup routines, the use of uninterruptible power supply (UPS) and a safe box to store media, Sêmola (2014) warns that each organization has its own characteristics, and that this leads to particular needs of Information Security. Dresner (2011) agrees and adds that the simple adoption of measures proposed by standards and models does not guarantee the mitigation of risks. Likewise, ABNT (2005) explains that the organization should select in the standard the most appropriate measures, considering its own requirements. In order to avoid the adoption of inappropriate measures to the needs and characteristics of the organization, decisions about adoption should be guided by the risks identified in an analysis and risk assessment process aligned to organizational plans, strategies and objectives. Therefore, they are decisions that must be taken by a governance structure.

2.1. INFORMATION SECURITY GOVERNANCE

"Information Security Governance consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, procedures, processes, technologies and compliance enforcement mechanisms" (Von Solms, 2005, p. 444). It is part of IT Governance and of Corporate Governance, and addresses privacy, vulnerabilities and tools, metrics and effectiveness assessment, and an Information Security strategy for the organization (Da Veiga & Eloff, 2007), being responsible for strategic decisions of Information Security. In alignment with other components of Corporate Governance, a poor Information Security Governance can result in negative impacts on the strategies of an organization (Tyukala, 2007).

Allen (2005) postulates that the Information Security Governance shall disclose and disseminate responsibilities, actions, behaviors and beliefs to protect information

and associated assets. Moulton and Coles (2003) conceptualize Information Security Governance as the creation and maintenance of the necessary control environment to manage the risks related to information and its processes and support systems, which may include the definition of responsibilities, strategies and objectives, risk assessment and management, rational management of resources, compliance with laws, regulations, policies and rules, and communication and relationship actions.

Von Solms and Von Solms (2006b) argue that the protection of the information and of the continuity of the organizational operations depends on a model supplied by Information Security Governance. According to Williams (2001), Information Security Governance is responsible for aligning Information Security requirements to the business. This alignment calls for an organizational model to be established and, as noted by Britto (2011), should include people, technology and processes for a program of Information Security.

Different models of Information Security Governance can be identified in the literature. The model proposed by Von Solms and von Solms (2006a) prescribes directives, policies, organizational norms, procedures and Information Security measures. The National Institute of Standards and Technology [NIST] (2006) proposes a model that combines superior determination with policies and strategies, defining organizational structure, architecture, roles and responsibilities.

Da Veiga and Eloff (2007) propose a model with organizational structures and processes focused on the commitment of leaders, definition of strategies, risks assessment, metrics and measures of effectiveness, targeting investments, certification and compliance with legislation and other regulations, policies, procedures, standards and guidelines, audits and monitoring, awareness and education, privacy protection, management of information assets, systems development, incident management and technical operations, environment protection and operations continuity.

To make strategic decisions on Information Security, Sêmola (2014) proposes an Information Security Corporate Committee that should be formed by representatives of different strategic areas and with different views. Decisions of this Governance structure should be guided by a plan aligned to the guidelines and strategies, organizing activities related to the adoption of appropriate measures to the risks to which the organization is exposed. The author also proposes sub-committees, a team to treat Information Security incidents and a manager to lead the Corporate Committee.

As noted by Koh, Ruighaver, Maynard and Ahmad (2005), Information Security Governance makes decisions, directs actions, establishes norms and principles, and prioritizes investments. The models show that decisions on the adoption of Information Security measures should be the responsibility of the Information Security Governance structure, and that the measures are not only technical, but also social, to the members of the organization.

Information Security Governance is considered the fourth wave of development of the Information Security (Von Solms, 2006). Initially, it was considered a purely technical issue, but there was a movement that led Information Security to the management frameworks, when managers realized that the issue was not only technical. Later, there was its institutionalization, characterized by a standardization influenced by norms widely adopted, by the demand for certification and compliance, by the concern for the creation of an Information Security culture and internal risks in organizations, and by use of metrics to evaluate its effectiveness (Von Solms, 2000). With the Information Security Governance, there is an understanding that it also requires

strategic decisions with a greater emphasis on Corporate Governance, and legal and regulatory support, however, without leaving aside technical, management and institutional issues (Von Solms, 2006).

Although there is in the literature the understanding that decisions on the adoption of measures should be made by Information Security Governance structure and that the measures must meet the principles, requirements and risks of the organization, external factors can influence the decisions about the adoption of Information Security measures. Posthumus and Von Solms (2004) proposed a governance model that integrates internal and external factors to Information Security actions. The internal dimension consists of "Business Issues" and "IT Infrastructure" domains, and the external dimension consists of "Legal/Regulatory" and "Standards/Best Practices" domains. Thus, even while focusing on Information Security Governance, the authors raise the importance of external factors, such as laws and regulations published by the Government to guide actions and the internal structure of organizations, and Information Security standards and models, such as NBR ISO/IEC 27002 (ABNT, 2005), which propose internationally accepted good practices to be adopted.

Therefore, Information Security is associated with laws and regulations, and international standards that prescribe practices perceived as necessary. This may influence the implantation, definition or establishment of roles and responsibilities, strategies, processes, organizational structures, policies, technologies and other Information Security measures (Albuquerque Junior & Santos, 2014). Thus, the measures may be adopted not because the Governance structure decides about it based on principles, risks and organizational strategies, but because organizations suffer external pressures to adopt them, which may lead to the adoption of inadequate measures. However, it is unknown the factors that influence the adoption of Information Security measures, what can prove or refute that assumption.

Information Security is not only technical, but also social, and most of the incidents originate in people and in a social context, like organizations. Therefore, information security should be treated based on theories that help to understand it from a social perspective, as proposed by Dhillon and Backhouse (2001), Björck (2004, 2005), Marciano and Lima-Marques (2006) Albrechtsen (2008) and Coles-Kemp (2009). Besides, the adoption of Information Security measures must be addressed by a theory that considers the influence of external factors, which is consistent with the Institutional Theory (Kam, Katerattanakul, Gogolin, & Hong, 2013), a theoretical approach that is common in studies of social sciences and suggested for studies on Information Security by different authors, such as Björck (2004), Kam et al. (2013) and Albuquerque Junior and Santos (2014).

2.2. INSTITUTIONAL THEORY AND INFORMATION SECURITY

Institutional Theory is widely used in organizational studies, including Information Systems studies. According to Quinello (2007), it is a theoretical approach that assumes that organizations suffer environmental influence where they operate, and they also influence this environment. The author notes two schools in the Institutional Theory developed: the Old Institutional School and the New Institutional School, or Neo-Institutional school. The first has a focus on the organization, and the second has the organizational field as unit of analysis.

Despite the distinction, DiMaggio and Powell (1983) explain that both schools are based on the relationship between the organization and the environment. In addition, Peci (2006) notes that both schools are skeptical about the rationality of the decisions of the actors in organizations. But Quinello (2007) argues that in the Old Institutional School, there is an understanding that leaders try to get legitimacy for their power or personal interests through the influence of the external environment and internal alliances and agreements, while at Neo-Institutional school understands that organizations try to establish legitimacy in their field as a requirement for their survival, and this is by adopting institutions seen as necessary for survival in the organizational field.

In the context of Institutional Theory, "institutions" are rules, practices, procedures, policies and programs incorporated by organizations that are part of the institutional environment. Within the institutional environment, organizations begin to act according to those institutions that are considered appropriate and able to make them efficient and successful. Consequently, they can legitimate them for the other components of the same field (Meyer & Rowan, 1977). Thus, organizations are influenced by existing institutions in the environment in which they operate, incorporating structures, rules, practices, procedures, policies and programs already institutionalized.

The institutional environment is composed of different organizations, as key suppliers, consumers, regulatory agencies, and other organizations that produce similar services or products and is a recognized area of institutional life called "organizational field" (DiMaggio & Powell, 1983). Therefore, organizational field is a set of organizations with a common meaning system and whose members interact with each other more frequently than with external organizations (Scott, 1992). The use of the organizational field as a unit of analysis has the advantage of allowing studying all relevant actors, rather than focus on only one organization (Lopes, 2012).

According to DiMaggio and Powell (1983), within the organizational field, given the uncertainties and risks common to its members, innovations initially adopted by an organization become adopted by others until they become a rule, where innovation is no longer a way of differentiation and becomes an institution, a means for legitimization and survival. As a consequence, the members of a field become similar to each other, and the mechanisms by which this happens are three:

i) coercive isomorphism – a relationship of power and dependency between organizations of the same field can lead to pressure to adopt structures, rules, practices, procedures, policies and programs;

ii) mimetic isomorphism – the most prestigious organizations, most successful or most legitimate within the organizational field can lead others to imitate them in their structures, rules, practices, procedures, policies and programs, given the uncertainties in activities that develop;

iii) normative isomorphism – the professionalization within the organizational field can lead organizations to select professionals who work in other organizations of the same field, or professionals trained in the same tools or technologies or trained in the same schools, and can also lead professionals in the same field to share and exchange information, experiences and opinions on their networks, helping in the dissemination of models and innovations.

Coercive isomorphism is the mechanism that may explain how the regulatory power of the government and other control and regulation organizations can influence the structure, rules, practices, procedures, policies and programs in an organizational field, making them similar. This mechanism may also explain how some organizations can influence by imposing compliance requirements with a model or standard for conducting common business or projects. The mimetic isomorphism may explain how a prominent organization can be a model for other organizations in the same field to make changes in their structures, and rules, practices, procedures, policies and programs. And the normative isomorphism may explain how professionals working in an organizational field and international standards can cause organizations to adopt structures, rules, practices, procedures, policies and programs perceived as necessary for the survival of organizations.

Information Security is related to government regulations, international standards and practices seen as necessary, which make organizations deploy, define or establish roles and responsibilities, strategies, processes, organizational structures, policies, technologies and other measures. As postulated by Institutional Theory, these measures are not adopted because Information Security Governance structure rationally decides about it, but because the organization is exposed to external pressure, which may be coercive, mimetic or normative. For this reason, Kam et al. (2013) argue for Institutional Theory as a theoretical approach to research phenomena related to Information Security. Nevertheless, Björck (2004) notes that the institutional approach is rarely used in Information Security studies, despite being common in Information Systems and IT researches.

Albuquerque Junior and Santos (2014) cited studies that show the influence of external forces in Information Security. Holgate, Williams and Hardy (2012) note that Information Security Governance arrangements are influenced by institutional forces and that there is isomorphism in organizations of same field. Hu, Hart and Cooke (2007) conclude that institutional coercive and normative forces are effective to stimulate investments in Information Security technology and the development of Information Security Policies. Lopes (2012) proposed a model of Information Security Policy that may be adopted as standard by coercion or normative pressure. For Hsu, Lee and Straub (2012), organizations are subject to mimetic and coercive influences for adoption and assimilation of Information Security management. According to Luesebrink (2011), Information Security management structures are influenced by normative and coercive mechanisms of institutional change. Kam et al. (2013) observed that regulatory and normative external pressures influence compliance with Information Security Policies. Finally, Spears, Barki and Barton (2013) concluded that external factors encourage the adoption of measures in a regulatory context, and that ensuring Information Security is supported more in its symbolic representation, and less in the effectiveness of the measures.

Although the possibility of identifying articles and theses that examine Information Security by the perspective of Institutional Theory, empirical research that aims to identify the factors that influence the adoption of Information Security measures was not found. However, an analysis model based on Institutional Theory was proposed (Albuquerque Junior & Santos, 2014). The model consists of an Organizational Dimension, which allows the identification of internal factors associated to Information Security Governance, and an Institutional Dimension, which allows to identify factors associated with the institutional environment. Both Organizational and Institutional

factors can influence the adoption of Information Security measures, and the purpose or consequence of adoption may be legitimacy or operations continuity.

To achieve this research, the model proposed by Albuquerque Junior and Santos (2014) (see Figure 1) was used. According to the model, the Organizational Dimension has as component the Information Security Governance, and the Institutional Dimension has as components: a) Government, Regulatory Organizations, and Funding Organizations for Research; b) The Professionalization of IT and Information Security; c) Other Organizations of the Organizational Field. The factors identified in the Organizational Dimension can influence the adoption of Information Security measures as rational decisions by the Information Security Governance structure, based on identified risks to the organization. Factors identified in the Institutional Dimension can lead to the adoption of measures as a response to coercive forces originated in the Government, regulatory organizations, and other organizations that fund research, or as a response to normative pressures from the community of IT and Information Security professionals and managers, or by the imitation of the measures adopted by other organizations of the same organizational field. The adoption of Information Security measures may ensure both operations continuity and legitimacy in the field, and the legitimacy ensures the survival of the organization, or the operations continuity.

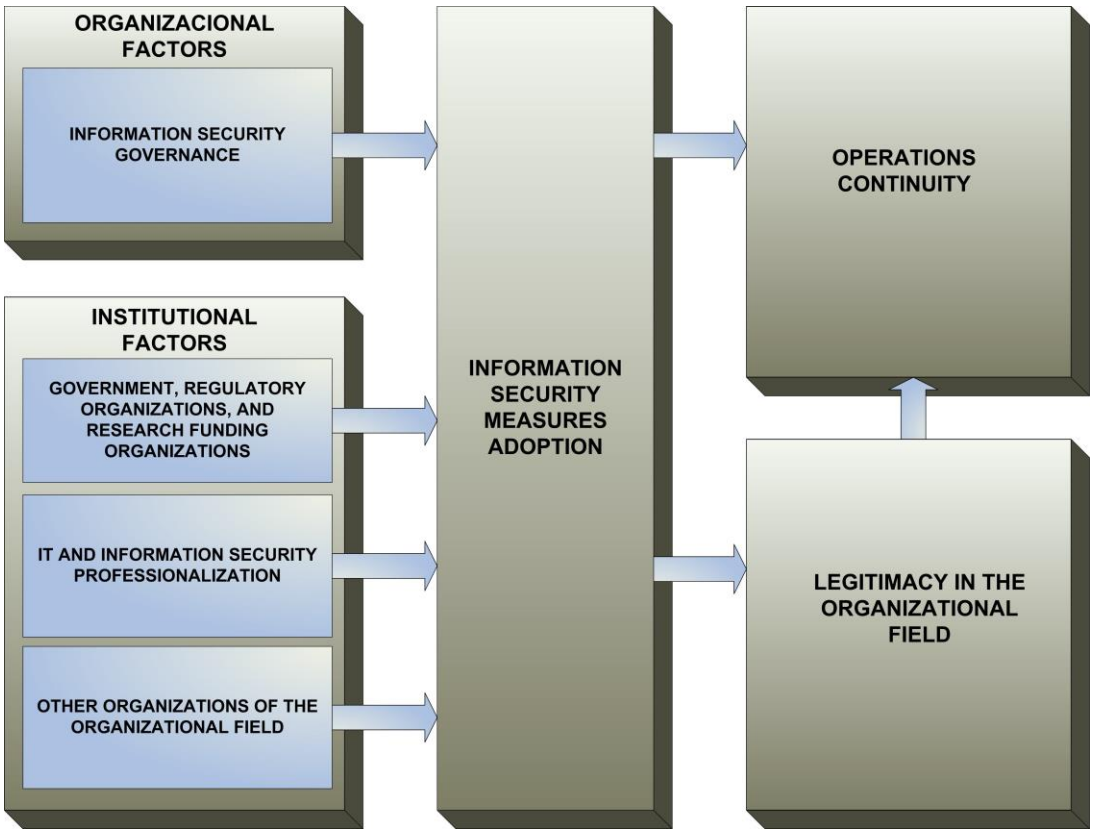

Figure 1 – Analysis model (Albuquerque Junior & Santos, 2014).

Thus, as shown in Table 1, the existence of risk assessment procedures, the compliance of Information Security with laws and regulations, the commitment of managers and leaders to Information Security, the existence of organizational structures, processes, procedures, internal regulations and standards, and a formal Information

Security Policy are indicators of the Organizational Dimension, which allow the identification of the factors that influence the adoption of Information Security measures, and that are related to decisions of the Information Security Governance structure.

Organizational Dimension	
Component	Indicators
Information Security Governance	IG01 – Formal definition of rules and responsibilities on Information Security for managers and other members of the organization
	IG02 – Strategies and objectives of Information Security defined and documented
	IG03 – Risk evaluation and management processes
	IG04 – Processes of analysis of resources management to Information Security
	IG05 – Control mechanisms for Information Security compliance with laws and agreements
	IG06 – Communication processes on Information Security with funding organizations and partners
	IG07 – Directives, actions and formal declaration of commitment by leaders and managers to Information Security
	IG08 – Information Security organizational structures
	IG09 – Information Security awareness processes
	IG10 – Formal and published Information Security Policy
	IG11 – Documented Information Security organizational procedures
	IG12 – Documented Information Security internal regulations and standards
	IG13 – Control mechanisms for organizational actions compliance with Information Security
Institutional Dimension	
Components	Indicators
Government, Regulatory Organizations, and Funding Organizations for Research	IC01 – Laws, decrees, norms, resolutions and other regulations published by the Government
	IC02 – Existence of agreements signed with other organizations that develop or fund research requiring the adoption of Information Security measures
Professionalization of IT and Information Security	IN01 – Use of international norms and standards as Information Security models
	IN02 – Use of criteria that require training or specific knowledge on Information Security for hiring professionals
	IN03 – Participation of IT and Information Security professionals in information and knowledge sharing networks for Information Security
Other Organizations of the Organizational Field	IM01 – Use of experiences of successful public organizations in the organizational field as models
	IM02 – Use of experiences of successful research organizations in the organizational field as models

Table 1 – Dimensions, components and indicators of the analysis model.
Adapted from: Albuquerque Junior and Santos (2014).

In the Institutional Dimension, Government, regulatory organizations, and funding organizations for research may influence through laws, decrees and other regulations that require the adoption of measures, and the professionalization of IT and Information Security may influence through the use of international norms and standards as models, or by the selection of professionals following criteria that require

training or expertise in Information Security, and measures adopted by other successful organizations in the organizational field may serve as role models, which may cause organizations to copy them, adopting the same Information Security measures.

Despite the possibility of being adapted to investigate the factors influencing the adoption of Information Security measures in any organization or organizational field, the analysis model of Albuquerque Junior and Santos (2014) was proposed to public research institutes, organizations that have an important role for scientific and technological development. As shown in the next section, these organizations need to protect information, because they are public organizations and because they develop scientific research.

3. INFORMATION SECURITY IN PUBLIC RESEARCH INSTITUTES

With the growth of automated actions and the provision of electronic services by the Government, public organizations have been experiencing increasing dependence on IT resources to carry out their daily operations, deliver products and provide services to meet social demands (NIST, 2006). According to Dzazali and Zolait (2012), public organizations have experienced increasing complexity, interconnections, uncertainties and dependence on technology, and they need to accomplish their missions and comply with regulations and guidelines from the Government's central agencies. Nevertheless, Grant (2007) found that around 80% of public servants have behaviors that put organizations' information at risk, while this percentage is just over 50% in private organizations.

There is a need to address Information Security as a priority in Brazilian public organizations to minimize losses and unauthorized access to sensitive information aboutGovernment and citizens, as observed by Cepik, Canabarro, Possamai and Sebben (2014). According to Britto (2011), protection of critical information should be established in Public Administration, since much of it may be vulnerable to interruptions of essential services and functions, data loss and fraud that may affect the society. Araújo (2012) notes that information leakage incidents and confidentiality breaches in public organizations are recurring, but also that the Federal Government has tried to combat this situation by regulations, decrees and laws for the management of Information Security, which is also observed by Castro (2010), Britto (2011), and Albuquerque Junior and Santos (2013). Nevertheless, Costa and Almeida (2011) show that there is noncompliance with these laws and regulations, which lead to risks of Information Security. Britto (2011) argues that public organizations must protect their critical information, because many of them may be vulnerable to data loss, fraud and disruption of essential functions and services, which may affect the society.

Information Security has been the subject of audits of the Brazilian Federal Court of Accounts (TCU), according to Cepik, Canabarro and Possamai (2014), which reinforces its importance to the Brazilian federal public administration. According to Alexandria (2009), TCU exposed the worrying situation in which the Brazilian public administration about Information Security is, especially in Information Security Governance and Management. Britto (2011) found that Brazilian Government organizations deal with lack of qualified professionals in Information Security and lack of support from managers. The author also noted that their Information Security plans and programs are not aligned with their organizational goals and strategies.

Among the public organizations, Alexandria and Quoniam (2010) highlight the public research institutes as organizations that need to protect information and the knowledge they produce. This need to protect information in the scientific research environment is justified by the arguments of Caminha et al. (2006), who state that research institutes have information as raw material and product, and also by the arguments of Burd (2006), who explains that academic organizations are vulnerable to incidents due to a combination of factors, including:

a) a lot of private and research data;

b) relatively open computer networks with high capacity, constant changes in IT end users , risk activities and decentralized structure;

c) extensive links with government, military, private and academic organizations.

Luesebrink (2011) points out that academic organizations are engaged in facilitating access to information and has a culture that encourages experimentation, tolerance and individual autonomy, and Perkel (2010) argues that these organizations tend to be open environments and that many researchers prefer to have freedom and control over the information they use than submit to the Information Security controls. Rezgui and Marks (2008) observe that IT infrastructure of academic organizations not only meet the needs of staff and students, but also of visitors and researchers who are physically elsewhere and share large amounts of data, which the authors argue may lead to incidents with information and systems. In this context, Alexandria and Quoniam (2010) argue that the need to ensure information confidentiality in research institutes, which are organizations that try to share the knowledge resulting from their research, as opposed to the need to ensure Information Security. But even if not all the information in research institutes is confidential, the authors state that is necessary to ensure their integrity and availability.

The impact of Information Security incidents in scientific research organizations are observed by Burd (2006), who cite as consequences the damage to private data and intellectual property, financial losses, and threats to critical infrastructure, public safety and national security. Alexandria (2009) also points out many incidents in a research institute and their consequences, which include business interruption, unavailability of services and systems, and non-compliance with laws. Perkel (2010) includes website defacement, theft of personal information and passwords, stealing of computing resources, intellectual property, proprietary compounds, instrument designs, patient data and personal communications, and lawsuits, public embarrassment and loss of grants. According to Rezgui and Marks (2008), the compromise of information and systems can undermine the credibility and viability of academic organizations. Given these impacts, protecting information in a public research institute is crucial to comply with legal and ethical obligations, as well as protecting the image of the organization, and ensuring the continuity of its activities.

Alexandria (2012) researched how Information Security management in Brazilian public research institutes is structured and concluded that there is little maturity in these organizations. Luesebrink (2011) analyzed Information Security Governance in public academic organizations in the United States through the lens of Institutional Theory, evaluating the impact of regulatory initiatives on the Information Security management structures. The author noted that management structures of Information Security are influenced by normative and coercive mechanisms of institutional change. Kam et al. (2013) studied how academic organizations in the

United States are influenced by institutional expectations to comply with Information Security Policies and the influence of these expectations in the awareness of their members. The authors concluded that external pressures influence significantly compliance of these organizations with Information Security Policies, particularly coercive and normative pressures.

The coercive influences may come from the fact that public research institutes are subject to both regulations about protection of information in public organizations and in research environment. As Brazilian examples, Federal Law No. 8,159/1991 requires the protection of supporting documents to scientific development, and Resolution No. 466/2012 of the National Health Council establishes rules for ethical conduct in human research, guaranteeing the confidentiality of human subject information. Moreover, Castro (2010), Britto (2011), Araújo (2012), and Albuquerque Junior and Santos (2013) present laws, decrees and other regulations that require public organizations to adopt Information Security measures. It is also possible that funding organizations impose on research institutes an obligation to adequately protect sensitive information and maintain compliance with laws about Information Security, as noted by Perkel (2010) in the United States.

Hu et al. (2007) point out influences of normative isomorphism, which takes place through the participation of managers in professional conferences, where there is an extensive exchange of experiences on Information Security. In addition, the standards of International Organization for Standardization (ISO) are well accepted worldwide due to the fact that they are institutionalized in different organizational fields, as noted by Posada (2009) and Papadimitriou and Westerheijden (2010). The same can be said about Information Security standards, like NBR ISO/IEC 27002 (ABNT, 2005), which is used as a model by organizations in many fields, and has an extensive training and certification structure. Von Solms (2000) argues that Information Security is institutionalized, with the standardization of international best practices, certification processes, metrics for evaluation and the development of an Information Security culture in organizations.

Hu et al. (2007) had difficulties in identifying mimetic isomorphism in Information Security initiatives in a multinational organization, but argue that may be difficult to differentiate mimetic of normative influences, as noted by Mizruchi and Fein (1999). According to Hu et al. (2007), it is easier to find news about Information Security failures than successes, which may explain the difficulty in identifying and consequently imitating successes. These authors point out that different studies showing mimetism in adoption of Information Technology, which reinforces the possibility of Information Security measures being imitated by research institutes. Hsu et al. (2012) observed Information Security mimetism in Korean organizations, although articles about the same phenomenon in research institutes were not identified.

Public research institutes should adopt or implement policies, regulations, processes, organizational structures, services and technology, guided by their Information Security Governance structure, but these organizations may be subject to coercive, normative and mimetic forces of the institutional environment, which may influence the adoption of Information Security measures (Albuquerque Junior & Santos, 2014). Luesebrink (2011) and Kam et al. (2013) studied Information Security in academic organizations from the perspective of Institutional Theory, and reinforce the adequacy of this theoretical approach to the theme and context of this research. Nevertheless, there is no research on the bibliography that aims to identify the factors influencing the adoption of Information Security measures in these

organizations. Public research institutes have information as an important element for their activities, they have characteristics that favor the occurrence of incidents, and the impact of incidents on these organizations make them appropriate for this research.

4. METHODOLOGY

In order to identify the factors influencing the adoption of Information Security measures, a document analysis and a survey were conducted, based on the research indicators and according to the technical procedures and the methods used to collect information shown in Table 2.

Indicators	Technical Procedures	Methods Used for Data Collection
IG01	Document analysis	Consultation in Information Security Policies and Information Security Management Systems
IG02	Document analysis	Consultation in Information Security Policies, Information Security Plans, and IT Master Plans
IG03	Survey	Question in electronic form
IG04	Document analysis	Consultation in Information Security Plans or IT Master Plans
IG05	Survey	Question in electronic form
IG06	Document analysis	Consultation in agreements and cooperation documents
IG07	Document analysis	Consultation in Information Security Policies, Information Security Plans, and IT Master Plans
IG08	Survey	Question in electronic form
IG09	Survey	Question in electronic form
IG10	Survey	Question in electronic form
IG11	Survey	Question in electronic form
IG12	Survey	Question in electronic form
IG13	Survey	Question in electronic form
IC01	Survey	Question in electronic form
IC02	Document analysis	Consultation in agreements and cooperation documents
IN01	Survey	Question in electronic form
IN02	Survey	Question in electronic form
IN03	Survey	Question in electronic form
IM01	Survey	Question in electronic form
IM02	Survey	Question in electronic form

Table 2 – Technical procedures and methods for data collection.

The document analysis consisted of consultations in Information Security Policies, Information Security Management Systems, and IT and Information Security plans, which are documents that formalize Information Security Governance structures, or the Information Security strategic alignment in organizations. To locate the documents, searches were conducted on the websites of 22 research institutes and on the Google search engine. The searches included the acronym of each research institute with terms related to the documents to be analyzed, like "information security policy", "information security management system", and "isms".

To perform the survey, questions were elaborated based on the indicators, and were included in an electronic form on FormSUS (http://formsus.datasus.gov.br), a system made by the Informatics Department of the Unified Health System (DATASUS) in Brazil. In the first part of the form, the participants should inform what kind of public organization the research institutes are, such as foundation, mixed-capital or public

company. The participants should also inform the level of government the organizations belongs to, their position and function, the organizations' research areas, the organizations which regulate the activities of the research institutes, and what Information Security measures their companies adopt. The second part of the form had 14 questions, one for each indicator of the analysis model, except those investigated through document analysis. The questions were designed to determine if research institutes are subject to the influence of the indicators of the analysis model on the adoption of Information Security measures. Table 3 shows the questions.

#	Questions
1	The institute is an autarchy, public foundation, mixed-capital company or public company?
2	Is the research institute subordinate to which level of government?
3	What is your position in the research institute?
4	What is the role you play in the research institute?
5	What is the area of expertise of the research institute?
6	What are the organizations that regulate the activities developed by the research institute?
7	What are the Information Security measures adopted by the research institute?
8	IG03 – Do decisions on the adoption of Information Security measures by the research institute consider risk assessment and management processes?
9	IG05 – When adopting Information Security measures, are internal mechanisms of control of compliance with the laws considered?
10	IG08 – Do the Information Security Committee, Office or Manager of the research institute participate in decisions on the adoption of Information Security measures?
11	IG09 – Is the adoption of Information Security measures in the research institute preceded by awareness processes for users?
12	IG10 – Do decisions on the adoption of Information Security measures consider the Information Security Policy of the research institute?
13	IG11 – Does the adoption of Information Security measures by the research institute consider existing Information Security procedures?
14	IG12 – Does the adoption of Information Security measures consider internal Information Security regulations and standards adopted by the research institute?
15	IG13 – Have decisions on the adoption of Information Security measures been considering control mechanisms of compliance in with the Information Security Policy?
16	IC01 – Were Information Security measures of the research institute adopted based on laws, decrees or other resolutions published by the Government or other organizations that control its activities?
17	IN01 – Does the research institute adopt Information Security measures based on models of guidelines, international norms and standards widely accepted?
18	IN02 – Does the organization select professionals to participate in decisions concerning the adoption of measures requiring specific knowledge or training about Information Security?
19	IN03 – Do professionals working with Information Security at the research institute exchange information and experiences about the adoption of Information Security measures with professionals from other organizations?
20	IM01 – When making decisions on the adoption of Information Security measures in the research institute, are the experiences of successful public organizations used as a model?
21	IM02 – When making decisions on the adoption of Information Security measures in the research institute, are the experiences of successful research organizations used as a model?

Table 3 – The survey questions.

Most of the questions accept only one answer, but some of them allow the respondent to select two or more options, such as the questions about organizations that regulate research institutes activities, Information Security measures adopted, and models, norms and international standards that guide the adoption of Information

Security measures. Other questions allowed respondents to type information into a text field, in addition to options that could be selected. This allowed the identification of additional information about the operation field, Information Security measures adopted, organizations that regulate activities developed by the research institutes, and the models, norms and standards that guide the adoption of Information Security measures, whose options available in the form were not sufficient to reflect the reality of the organizations.

Possible respondents and contact addresses were identified on the websites of 22 public research institutes, 11 of them belonging to the Federal Government, and 11 belonging to different sub-national states. Of these, three research institutes are located in Paraná and two in São Paulo, while the others are of Amapá, Bahia, Espírito Santo, Paraíba, Pernambuco and Sergipe. Potential respondents were preferably those that are responsible for Information Security in their organizations, or when it was not possible to identify them, the ones responsible for the IT department.

The link for the survey was sent by e-mail to every possible respondent with explanations about the research. While some of these organizations are composed of several independent institutes and research centers, and sometimes located in different cities, only respondents who work in the headquarters of their organizations received the e-mail. When it was not possible to identify the individual e-mail address or even the name of the possible respondents, the form was sent to IT or Information Security e-mail address. In two cases, the impossibility to identify an e-mail to send the message forced us to use existing forms on the research institutes websites to contact the IT or Information Security department.

5. DATA PRESENTATION AND ANALYSIS

The form was sent to 22 research institutes, and 11 responded to the survey. Eight of those who responded are federal and three are state-level organizations. Ten research institutes are autarchy or public foundations, and only one of them is a public company. Two institutes conduct research on energy, one on healthcare, one on space technology, one on economic and social development, one on agriculture and livestock, one on mineral exploration, and one on worker´s safety. Three respondents did not inform the research area of their organizations. Only one form was answered by the Information Security coordinator or manager, while four of them were answered by professionals that are not Information Security managers, and six were answered by IT managers. Six respondents reported being analysts, three are technologists, one is as technician and one is a researcher of their research institutes.

The Information Security measures that respondents reported being adopted in their research institutes were classified as technical, administrative and physical, as proposed by Björck (2005). On administrative measures, the results show that nine research institutes documented and formalized internal regulations of Information Security, while seven of them have internal processes and six have Information Security procedures. All 11 research institutes have professionals working with Information Security, nine of them have an incident treatment team, and five of them have an Information Security Office in their organizational structures. Seven institutes have published Information Security Policies, and another seven of them have Information Security Committees.

The fact that nine research institutes have Information Security regulations and seven have Information Security Policies means that two of them have internal regulations that were created without the guidance of a formalized Policy. Information Security regulations must comply with the organizational Policy, which must have been formally approved and must be aligned with organizational objectives and strategies. Although the Information Security Committee is responsible for assessing and approving the Information Security Policy, the results show that one of the institutes has a documented Policy, but does not have a Committee, and that other one has a Committee but does not have a Information Security Policy document. Besides being a need for properly direct Information Security actions, a Committee and an Information Security Policy are obligations created by the Brazilian Federal Government for its organizations. As eight federal institutes responded to the survey, half of them violate the obligation to have a corporate Committee and three do not fulfill the obligation to create an Information Security Policy.

It is important to point out that all of the 11 research institutes have experts in Information Security, even though not all of them have a team specialized in Information Security incidents, which may influence in prioritizing solutions to incidents that have occurred. Also, five institutes have an Information Security Office, which may mean that Information Security has a less technical focus on these institutes, unlike when it is a technical IT staff responsibility.

As for the technical measures adopted by research institutes, all respondents reported that their organizations have a backup solution, ten have a firewall to protect the network against unauthorized access from the Internet, and ten of them have computing assets with redundant parts. Nine institutes have an anti-spam system, eight have a proxy to control internal access to the Internet, eight have a corporate antivirus system, and eight of them have a tape library to automate data backup. The less common technical measures are data encryption, adopted by five research institutes, intrusion detection system (IDS), used in four, and intrusion prevention system (IPS), adopted by three organizations.

Although some measures are widely adopted, the use of a firewall and network antivirus do not happen in all research institutes, which means that they may be exposed to viruses and other malicious codes and unauthorized access. The results highlight the use of tape libraries, despite the high cost of acquisition and use. Data encryption, which increases the confidentiality of information stored or transmitted through the Internet, is used in less than half of the research institutes, which may jeopardize sensitive information, whose secrecy must be guaranteed. Also, modern measures, such as IDS or IPS, are uncommon in these organizations, possibly because of the complexity involved in its use.

The physical measures adopted by research institutes include: use of UPS for protection against failure in the power supply, in 11 research institutes; access restriction to rooms where information are processed and stored, which occurs in 10 institutes; use of fire and water resistant safe boxes to store media and information, adopted by seven institutes; equipment redundancy, measure that facilitates disaster recovery and that is adopted by six institutes; and the backup site, which allows the replication of entire IT infrastructure to a remote place, that is adopted by one research institute. None of the research institutes has a safe room.

The use of fire and water resistant safe boxes protects the media against fires and floods, facilitating the restoration of information and recovery of organizational

operations. As four public research institutes do not adopt these measures, they are vulnerable to such incidents. The backup site and the safe room, both to ensure the continuity of the organization's operations even in the event of disasters, are unusual or not adopted, perhaps because of the high cost involved.

With regard to organizations which regulate public research institutes activities, most of them are subject to regulations issued by federal organizations. Ten respondents said their organizations must comply with TCU regulations, eight of them from a federal level. Nine research institutes are regulated by the System of Administration of Information Technology Resources (SISP), an organization of the Brazilian Federal Government (eight of them are federal research institutes). The Ministry of Planning, Budget and Management (MPOG) regulates activities of the eight organizations, all of them of a federal level. With this, respondents of federal research institutes stated that they are subject to regulations of Federal Government organizations, which regulate activities of Federal organizations in general. The three state-level research institutes are regulated and monitored by the Audit Courts of their respective states.

MPOG, through the SISP, disciplines Information Security in Federal public organizations, and the compliance of federal research institutes with these regulations is TCU's deliberations target. At the state level, these roles are played by state departments and the Audit Courts of the states. In addition, state institutes can receive research grants from federal organizations that fund research activities, such as Coordination for the Improvement of Higher Education Personnel (CAPES) and National Council for Scientific and Technological Development (CNPq), and other federal entities such as Ministry of Science, Technology and Innovation, and the Ministry of Health. With this, these state research institutes are also subject to supervision and regulation of the TCU.

The organizations that promote research activities also regulate the activities of research institutes. Four respondents stated that their organizations are regulated by the Ministry of Science, Technology and Innovation, three federal-level and one state-level research institutes, and three federal institutes are regulated by CAPES. Two federal institutes are regulated by the National Commission on Ethics in Research (CONEP), organization that regulates research involving human subjects. It is worth noting that one of the respondents of the two federal institutes stated that his organization develops healthcare research, and the other did not inform the research area of his organization.

The CONEP regulates research involving human subjects, especially clinical research of drugs and vaccines. Research involving human subjects requires the authorization of a Research Ethics Committee, and registration in the CONEP. Without meeting these requirements, these research institutes cannot get funding resources for research, and will have difficulty publishing the results of their research in scientific journals.

Three institutes have their activities regulated and supervised by the National Health Surveillance Agency (ANVISA), two of them are federal and conduct research on healthcare and energy areas, and the third is a state-level agriculture and livestock research institute. Two federal institutes are regulated by the National Health Council (CNS) and another two federal institutions are regulated by the Ministry of Health. In such cases, one of the answers came from an institute of healthcare-related research, and the other respondent did not inform the institute’s research area.

The CNS is a department that monitors and decides about public healthcare policies and healthcare budget, and the ANVISA acts in the sanitary control of various products and services such as medicines for people and animals, food, cosmetics,

personal and environmental hygiene products, medical equipment and supplies, radioactive products used in diagnostics and therapies, and any material and product that may bring risk to human health. The CNS and the ANVISA report to the Ministry of Health, and regulate activities in sectors that may affect public health, including research involving people, animals and plants.

Two federal research institutes are regulated by the Ministry of Education (MEC), while a federal and a state-level institute are regulated by the Ministry of Mines and Energy (MME) and the Ministry of Labor and Employment (MTE).

The regulations by the MME and the MTE are related to the area in developing scientific research, noting that there are institutes working in the areas of job security, energy and mineral research. The MEC regulates teaching activities, as some research institutes offer professional technical and graduation courses, , which are regulated by the CAPES.

The results presented up to this point show that research institutes are subject to coercive pressure from government organizations because they develop research and education activities and they are public organizations.

Of the 13 indicators of organizational dimension, the ones selected as of the most influential in the adoption of Information Security measures are: "IG12 – Documented Information Security internal regulations and standards", with nine responses; "IG09 – Information Security awareness processes", with seven responses; "IG10 – Formal and published Information Security Policy", also with seven responses; "IG11 – Documented Information Security organizational procedures" with six responses. Other indicators were selected by less than half of the respondents.

In the search for documents, three Information Security Policies were found, and two documents that formalize organizational Information Security Management Systems, and seven IT Master Plans, all from federal research institutes, but no Information Security plan was located. Although the respondent of state-level institutes responded that their organizations have Information Security Policies, the documents were not found in searches on their websites or on Google. Also IT Master Plans and Information Security Management Systems were not identified for state research institutes. Seven respondents stated that their institutions have Information Security Policy, but three documents were located.

In the three Information Security Policies located, it was found formally defined Information Security roles and responsibilities, complemented by the documents that formalize the Information Security Management System in two cases. In three research institutes, strategies and Information Security goals are formalized in the IT Master Plan, Information Security Policy and Information Security Management System. Five research institutes formalized Information Security resource analysis and management processes in their IT Master Plans. Three research institutes have formalized in their respective Policies the commitment of managers with Information Security. The "IG06 – Communication processes on Information Security with funding organizations and partners" indicator was not identified in the analyzed documents. Due to the small number of documents available for analysis, it is not possible to state how many research institutes adopt these measures, but the analysis of the documents shows that in some of the institutes the roles and responsibilities are defined and managers support the Information Security. The documents also show that there are resource analysis and management processes, and Information Security strategies and objectives defined, which indicates maturity of the Information Security Governance in some organizations.

Of the 11 research institutes, four of them have risk assessment and management processes and two of them have internal mechanisms to monitor Information Security compliance with laws and regulations. Four research institutes have an Information Security Committee, a team for incident treatment, and Information Security Office in their organizational structure, which are important items for Information Security. Although only three Information Security Policies documents were identified, seven participants responded that there are Policies in their organizations, which are consistent with the answers about the Information Security measures adopted. The existence of risk assessment and management processes, Information Security Policy, incident treatment team, Information Security Committee and Office indicate that Information Security Governance structure influences the adoption of Information Security measures in these organizations.

Fifteen agreements and cooperation documents of different research institutes were located, but could not be identified in these documents, evidence that organizations maintain Information Security communication processes with partners, which does not confirm indicator "IG06 – Communication processes on Information Security with funding organizations and partners".

Formalized and documented Information Security operational procedures have influence on six research institutes, and internal regulations and standards of Information Security influence nine institutes, but only two of them have internal monitoring mechanisms of compliance of Information Security activities with the Information Security Policy document. None of the participants responded that the research institute has continuous awareness processes for Information Security.

For the Institutional Dimension, coercive, normative and mimetic influences were identified. Six of the seven indicators of this dimension were mentioned by more than half of the respondents as influencing the adoption of Information Security measures: "IC01 – Laws, decrees, norms, resolutions and other regulations published by the Government" and " IN03 – Participation of IT and Information Security professionals in information and knowledge sharing networks for Information Security", both of them mentioned by respondents from nine research institutes; "IM01 – Use of experiences of successful public organizations in the organizational field as models" and "IN01 – Use of international norms and standards as Information Security models", both appointed by eight respondents; and "IM02 – Use of experiences of successful research organizations in the organizational field as models" mentioned by six respondents.

Coercive influence of laws, decrees, normative instructions and other resolutions of the Government dealing with the adoption of Information Security measures was identified, since nine participants answered that their organizations adopted Information Security measures under the influence of these indicators. The document analysis did not show whether organizations are influenced by agreements signed with other research institutes and organizations that fund research, as none of the documents contained elements that obligate the adoption of Information Security measures. Although it was not possible to verify one of the survey indicators, the coercive influence of the Government on decisions regarding Information Security measures adoption was confirmed.

Participants from eight research institutes responded that their organizations adopt Information Security measures based on internationally accepted models, norms and standards, citing as examples the ISO/IEC 27002 (seven respondents), ISO/IEC

27001 (five respondents) and ISO/IEC 27005 (two respondents). Nine participants responded that their organizations' IT and Information Security professionals participate in information and knowledge networks on this subject. However, only four respondents reported that their organizations select professionals according to Information Security training or expertise criteria. Although few participants responded positively on this last indicator, it is possible to say that there are normative influences in adopting Information Security measures due to the number of positive responses for the other two indicators.

There is also mimetism in Information Security adoption. Eight participants responded that their research institutes use experiences of other public organizations as a model for adoption of Information Security measures. The experiences of other scientific research organizations are also used as a model by six public research institutes, which indicates that the influence of public organizations are more common than scientific research organizations' experiences. This can be due to uncertainty about compliance with Government regulations about Information Security in Public Administration, which is associated with the Government´s coercive influence.

Although the Institutional Dimension has fewer indicators than Organizational Dimension, six institutional indicators have influence over most of the research institutes that participated in the study, whereas four indicators of Organizational Dimension have influence on adoption of Information Security measures. In addition, three indicators have influence over nine research institutes, but two of them are Institutional Dimension's indicators. These results point out that the adoption of Information Security measures in these organizations is more influenced by external factors than Information Security Governance factors. The results also indicate that the main factors influencing the adoption of these measures are laws, decrees, resolutions and other regulations issued by the Government (coercive factor of Institutional Dimension), the participation of IT and Information Security professionals in networks of knowledge and information sharing (normative factor of Institutional Dimension), Information Security internal regulations and standards (Information Security Governance factor), the use of international Information Security norms and standards of as models (normative factor of Institutional Dimension), and the use of experiences of successful public organizations in the organizational field as models (mimetic factor of Institutional Dimension).

6. CONCLUSIONS

This study investigated whether the adoption of Information Security measures in public research institutes is influenced by organizational and institutional factors proposed by Albuquerque Junior and Santos (2014). Research showed that the institutional environment influences the adoption of Information Security measures in most public research institutes that participated in the survey. This influence is mainly through laws, decrees and other regulations published by the Government, and through participation of IT and Information Security professionals in networks for the exchange of experiences and information. The institutes are subject to regulations published by different federal and state-level organizations that regulate their activities as members of the public administration and as scientific research organizations. Imitation of the measures adopted by other public organizations and the use of international Information Security norms and standards as models, factors that belongs to Institutional Dimension, also influence the adoption of Information Security measures in most research institutes.

Information Security Governance also influences the adoption of measures, but the main indicator of influence of Organizational Dimension is the definition and adoption of internal regulations and standards of Information Security. Although there are influences from both internal and institutional environment, the Institutional Dimension factors have more influence on research institutes than Organizational Dimension factors. Among the most mentioned factors, four are institutional, which show the importance of the external environment in decisions on the adoption of Information Security measures, despite the need to adopt appropriate measures for the risks identified for the organizations.

The research also showed that the most adopted Information Security measures by research institutes are mainly technical or physical, such as backup routines, use of UPS, anti-spam and equipment with redundant parts. Among the administrative measures, internal Information Security regulations and incident treatment team are the most adopted. It is worth noting that all institutes have Information Security professionals in their staff, even though they do not always have in their organizational structure an Information Security Committee or Office.

Decisions on adoption of Information Security measures are not based on needs identified in risk assessments and analysis, or based on the organizational objectives set by Information Security Governance, as proposed by the theory on this subject, but to fulfill obligations created by the Government or other organizations that regulate research and public organizations activities, or to imitate experiences of other public organizations, or even to follow models and standards that are institutionalized in IT and Information Security professional areas, including ISO/IEC 27002, ISO/IEC 27001 and ISO/IEC 27005, as proposed by Institutional Theory.

The main limitations of the research are the small number of organizations that participated in the survey and answered the questionnaire, and also the fact that few documents were analyzed, which weakens the results. In addition, despite having identified the organizational and institutional factors influencing the adoption of Information Security measures in public research institutes, the research did not investigate what motivates the adoption of these measures: the protection of information, or the legitimacy that the adoption of Information Security measures brings to the research institute in the organizational field. Given these limitations, it is suggested to research why these organizations adopt Information Security measures. Understanding the motivation may contribute to the implementation and maintenance of effective structures to the information and knowledge protection in the scientific research environment. It is also suggested a similar survey, but expanding the number of organizations by including other research institutes and universities that develop scientific research, which can increase knowledge about Information Security in academic organizations.

REFERENCES

Albrechtsen, E. (2008). *Friend or foe? Information security management of employees*. Doctoral thesis, Norwegian University of Science and Technology, Trondheim, Norway.

Albuquerque Junior, A. E., & Santos, E. M. (2013). Adoção de normas de segurança da informação em institutos de pesquisas no setor público: uma proposta de análise explorando as possibilidades da Teoria Institucional. *Proceedings of International Conference on Information Resources Management*, Natal, RN, Brazil, 6.

Albuquerque Junior, A. E., & Santos, E. M. (2014). Adoção de medidas de Segurança da Informação: um modelo de análise para institutos de pesquisa públicos. *Revista Brasileira de Administração Científica*, 5(2).

Albuquerque Junior, A. E., Santos, E. M., & Albuquerque, E. S. (2014). Segurança da Informação em um instituto de pesquisa: uma análise utilizando a norma ISO/IEC 27002:2005. *Revista Formadores*, 7(2), 71-89.

Alexandria, J. C. S. (2009). *Gestão de Segurança da Informação – uma proposta para potencializar a efetividade da Segurança da Informação em ambiente de pesquisa científica*. Doctoral thesis, University of São Paulo, São Paulo, SP, Brazil.

Alexandria, J. C. S. (2012). A Picture of Information Security in public institutions of scientific research in Brazil. *Proceedings of International Conference on Information Systems and Technology Management*, São Paulo, SP, Brazil, 9, 4209-4215.

Alexandria, J. C. S., & Quoniam, L. M. (2010). Proposta para a estruturação da Gestão da Segurança da Informação em um ambiente de pesquisa científica. *Proceedings of International Conference on Information Systems and Technology Management*, São Paulo, SP, Brazil, 7, 2175-2197.

Allen, J. H. (2005). *Governing for Enterprise Security – Technical Note CMU/SEI-2005-TN-023*. Pittsburgh: Carnegie Mellon University.

Araújo, W. J. (2012). Leis, decretos e normas sobre Gestão da Segurança da Informação nos órgãos da Administração Pública Federal. *Informação & Sociedade: Estudos*, 22(special issue), 13-24.

Associação Brasileira de Normas Técnicas (2005). *NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação*. Rio de Janeiro: ABNT.

Beal, A. (2005). *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. São Paulo: Atlas.

Belasco, K., & Wan, S.-P. (2006). Online retail banking: security concerns, breaches, and controls. In Bidgoli, H. (Org.). *Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management* (pp. 37-48). New Jersey: John Wiley & Sons, v.1.

Bernaschi, M., D'Aiutolo, E., & Rughetti, P. (1999). Enforcing network security: a real case study in a research organization. *Computers & Security*, 18(6), 533-543.

Björck, F. (2004). Institutional Theory: A new perspective for research into IS/IT security in organisations. *Proceedings of Hawaii International Conference on System Sciences*, Big Island, HI, United States of America, 37.

Björck, F. (2005). *Discovering Information Security Management*. Doctoral thesis, Stockholm University, Stockholm, Sweden.

Britto, T. D. (2011). *Levantamento e Diagnóstico de Maturidade da Governança da Segurança de Informação na Administração Direta Federal Brasileira*. Master's thesis, Catholic University of Brasília, Brasília, DF, Brazil.

Burd, S. A. (2006). *The Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy and Practice*. Rockville: NCJRS.

Caminha, J., Leal, R. T., Marques Junior, R. O. P. C., & Nascimento, M. G. (2006). Implantação da Gestão da Segurança da Informação em um instituto de pesquisa tecnológica. *Proceedings of Congresso da Associação Brasileira das Instituições de Pesquisa Tecnológica e Inovação*, Campinas, SP, Brazil, 4.

Cepik, M., Canabarro, D. R., & Possamai, A. J. (2014). A institucionalização do SISP e a era digital no Brasil. In Cepik, M., & Canabarro, D. R. (Orgs.). *Governança de TI: Transformando a Administração Pública no Brasil* (pp. 37-74). Porto Alegre: UFRGS.

Cepik, M., Canabarro, D. R., Possamai, A. J., & Sebben, F. D. (2014). Alinhando TI e políticas públicas: quatro temas prioritários. In Cepik, M., & Canabarro, D. R. (Orgs.). *Governança de TI: Transformando a Administração Pública no Brasil* (pp. 157-204). Porto Alegre: UFRGS.

Castro, R. A. A. (2010). *Segurança e garantia da informação: um estudo de caso em organização pública*. Master's thesis, Catholic University of Brasília, Brasília, DF, Brazil.

Coles-Kemp, L. (2009). Information Security Management: an entangled research challenge. *Information Security Technical Report*, 14(4), 181-185.

Cooper, M. H. (2009). Information security training: what will you communicate? *Proceedings of Annual ACM SIGUCCS Fall Conference*, St. Louis, MO, United States of America, 37, 217-222.

Costa, R. G., & Almeida, H. A. (2011). IT outsourcing services: security issues. *Proceedings of International Conference on Information Systems and Technology Management*, São Paulo, SP, Brazil, 8, 3626-3648.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160.

Donner, M. L., & Oliveira, L. R. (2008). Análise de satisfação com a segurança no uso de internet banking em relação aos atuais recursos disponíveis no canal eletrônico. *Proceedings of Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, Rio de Janeiro, RJ, Brazil, 32.

Dresner, D. G. (2011). *A Study of Standards and the Mitigation of Risk in Information Systems*. Doctoral thesis, The University of Manchester, Manchester, United Kingdom.

Dzazali, S., & Zolait, A. H. (2012). Assessment of information security maturity – An exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology*, 14(1), 23-57.

Fontes, E. L. G. (2006). *Segurança da Informação: o usuário faz a diferença*. São Paulo: Saraiva.

Grant, I. (2007). Public sector staff 'ignore IT security'. *ComputerWeekly.com*, 12. Retrieved from http://www.computerweekly.com/news/2240084242/Public-sector-staff-ignore-IT-security

Holgate, J. A., Williams, S. P., & Hardy, C. A. (2012). Information Security Governance: investigating diversity in critical infrastructure organizations. *Proceedings of Bled eConference*, Bled, Slovenia, 25.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on Information Systems Security – a neo-institutional perspective. *The Journal of Strategic Information Systems*, 16(2), 153-172.

Kam, H.-J., Katerattanakul, P., Gogolin, G., & Hong, S. (2013). Information Security Police compliance in higher education: a neo-institutional perspective. *Proceedings of Pacific Asia Conference on Information Systems*, Jeju Island, South Korea, 17.

Koh, K., Ruighaver, A. B., Maynard, S. B., & Ahmad, A. (2005). Security Governance: its impact on security culture. *Proceedings of Australian Information Security Management Conference*, Perth, WA, Australia, 3, 47-57.

Luesebrink, M. (2011). *The institutionalization of Information Security Governance structures in academic institutions: a case study*. Doctoral thesis, Florida State University, Tallahassee, FL, United States of America.

Lopes, I. M. (2012). *Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal*. Doctoral thesis, University of Minho, Braga, Portugal.

Marciano, J. L. P. (2006). *Segurança da Informação – uma abordagem social*. Doctoral thesis, University of Brasília, Brasília, DF, Brazil.

Marciano, J. L. P., & Lima-Marques, M. (2006). O enfoque social da segurança da informação. *Ciência da Informação*, 35(3), 89-98.

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: formal structure as myth and ceremony. *The American Journal of Sociology*, 83(2), 340-363.

Mitnick, K. D., & Simon, W. L. (2003). *Mitnick – A arte de enganar – ataques de hackers: controlando o fator humano na Segurança da Informação*. São Paulo: Makron Books.

Mizruchi, M.S., Fein, L.C. (1999). The social construction of organizational knowledge: a study of the uses of coercive, mimetic, and normative isomorphism. *Administrative Science Quarterly*, 44(4), 653–683.

Moulton, R., & Coles, R. S. (2003). Applying Information Security Governance. *Computers & Security*, 22(7), 580-584.

National Institute of Standards and Technology (2006). *Information security handbook: a guide for managers*. Gaithersburg: NIST.

Papadimitriou, A., & Westerheijden, D. F. (2010). Adoption of ISO-oriented quality management system in Greek universities: reactions to isomorphic pressures. *The TQM Journal*, 22(3), 229-241.

Peci, A. (2006). A Nova Teoria Institucional em Estudos Organizacionais: uma abordagem critica. *Cadernos EBAPE.BR*, 4(1).

Perkel, J. (2010). Cybersecurity: how safe are your data? *Nature*, 464, 1260-1261.

Pimenta, R. C. Q., Sousa Neto, M. V. (2010). Gestão da Informação: um estudo de caso em um instituto de pesquisa tecnológica. *Prisma.com*, (9).

Posada, L. M. L. (2009). Instituciones e isomorfismo: implicaciones en la incertidumbre organizacional. *Revista Mundo Económico y Empresarial*, 7(7), 42-49.

Posthumus, S., & Von Solms, R. (2004). A framework for the Governance of Information Security. *Computers & Security*, 23(8), 638-646.

Quinello, R. (2007). *A Teoria Institucional aplicada à Administração: entenda como o mundo invisível impacta na gestão dos negócios*. São Paulo: Novatec Editora.

Rezgui, Y., & Marks, A. (2008). Information Security awareness in higher education: an exploratory study. *Computers & Security*, 27(7-8), 241-253.

Scott, W. R. (1992). *Organizations: rational, natural, and open systems*. New Jersey: Prentice-Hall.

Silva, D. R. P., Stein, L. M. (2007). Segurança da Informação: uma reflexão sobre o componente humano. *Ciências & Cognição*, 10, 43-56.

Spears, J. L., Barki, H., & Barton, R. R. (2013). Theorizing the concept and role of assurance in Information Systems Security. *Information & Management*, 50(7), 598–605.

Tyukala, M. (2007). *Governing Information Security using organisational Information Security profiles*. Master's thesis, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.

Da Veiga, A., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management*, 24(4), 361-372.

Von Solms, B. (2000). Information Security – The Third Wave? *Computers & Security*, 19(7), 615-620.

Von Solms, B. (2005). Information Security Governance – compliance management vs operational management. *Computers & Security*, 24(6), 443-447.

Von Solms, B. (2006). Information Security: The Fourth Wave. *Computers & Security*, 25(3), 165-168.

Von Solms, R., & Von Solms, S. H. (2006a). Information Security Governance: a model based on the direct–control cycle. *Computers & Security*, 25(6), 408-412.

Von Solms, R., & Von Solms, S. H. (2006b). Information Security Governance: due care. *Computers & Security*, 25(7), 494-497.

Williams, P. (2001). Information Security Governance. *Information Security Technical Report*, 6(3), 60-70.

