ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of
DEVELOPMENT RESEARCH

International Journal of Development Research
Vol. 06, Issue, 09, pp.9561-9567, September, 2016

Full Length Research Article

INFORMATION SECURITY RISK MANAGEMENT IN A PUBLIC INSTITUTION: A CASE STUDY

[1,2,*]Jackson Gomes Soares Souza, [2]Dr. Carlos Hideo Arima , [2]Dr. Getulio Akabane, [2]Dr. Napoleão Verardi Galegale, [2]Renata Maria Nogueira de Oliveira and [3]João Marcos de Oliveira Machado

[1]Instituto Federal de São Paulo, Brazil
[2]Centro Paula Souza, Brazil
[3]Instituto Federal do Triângulo Mineiro, Brazil

ARTICLE INFO

Article History:
Received 18th June, 2016
Received in revised form
20th July, 2016
Accepted 25th August, 2016
Published online 30th September, 2016

Key Words:
Corporate Governance,
I.T. Governance,
Risk Management,
Information Security.

ABSTRACT

Information is a key asset to organizations, so they must apply security measures, policies, procedures, guidelines and also take advantage of good opportunities to leverage business success. This case study aims to verify how information security risk management is presented, according to I.T. manager's perceptions, in a Brazilian federal public institution. The results demonstrate the relevance of policies, standards, procedures and their implementation as well as roles played by people and their responsibilities aiming greater control of information security risks.

INTRODUCTION

Information is a necessary resource, from its creation to the moment it is destroyed to develop organization's business cycle. Information Technology (I.T.) plays a significant role in this process, advancing and diffusing in social, public, corporate environments and should be treated as a strategic asset (Nobre *et al.,* 2010; ISACA, 2012).Corporate governance holistically integrates components by involving principles, processes, information, services, infrastructure, human resources, internal and external stakeholders responsible for managing these components and providing the structure in which the organization's objectives are established, as well as determining and monitoring means to achieve them (OECD, 2004).Good corporate governance enables organizations to work efficiently and productively, ensuring management responsibility and transparency in both private and public organizations. Therefore, I.T. must be considered by organizations as an important asset, acting as a complex solution's driver, thus it's governance is a critical success factor to support business objectives (Akabane, 2012; Hardy, 2006; ITGI, 2003; Van Grembergen *et al.,* 2004).According to I.T. Governance Institute– ITGI –, information technology governance is a corporate governance component and consists of leadership, organizational structures and processes to ensure that I.T. supports and enhances organization's objectives and strategies by enabling it to take full advantage of information while maximizing opportunities and competitiveness (ITGI, 2007).To ITGI, successful organizations recognize information technology benefits using it to drive stakeholder's values and manage risks such as increasing regulatory demands and critical dependence of business processes. Performance measurement is essential for I.T. governance, thus identify critical processes and controls are essential for executives to raise processes at a desired capacity level. Information Security Governance Frameworks like COSO (Committee of Sponsoring Organizations of the Tread way Commission), COBIT (Control Objectives for Information and related Technology) and ISO 27001 have been widely used as guides to assess internal control, while risk management is one

****Corresponding author: Jackson Gomes Soares Souza,***
Instituto Federal de São Paulo, Brazil.

of the focus areas that contribute to ensure transparency of costs and I.T. value (ISACA, 2012; Fazlida and Jamaliah, 2015). I.T. processes deal with information security and risk management by identifying and measuring risk acceptance. Managers and others involved in security must be aware of opportunities and to control uncertainties that could impact business objectives. In addition, information security is a strategic agenda in the Brazilian public sector, having a wide range of legal provisions and standards addressing its application oninstitutions bound to the Federal Government in which compliance is mandatory. Also, recent studies addressed by Araujo (2012) demonstrates the relevance of the subject and how it is still not much explored in this area.A bibliometric query in Sopus basisof the last 5 years (term: Information Security) shows that scientific productions are having a significant increase by approximately 17,000 issues. However, when regarding management of information security risks, especially in the public sector (terms: Information Security Risk Management and Public Sector), only 16 articles were found, where none of which refers to the Brazilian federal public sector. Therefore, the relevance of this study is justified by difficulties addressed on some organizations to evaluate risks and opportunities in their activities, especially regarding information assets, information technology security and potential vulnerabilities that can be mitigated by verifying how information security risk management is presented on I.T. governance.

I.T. governance and information security risk management

I.T. Governance

I.T. broad definition includes information systems, hardware and software, telecommunications, automation and multimedia features used by organizations to provide data, information and knowledge; and organizations are increasingly using I.T. to achieve business objectives and goals, seeking greater organizational effectiveness and competitive advantage (Laurindo *et al.,* 2001; Luftman, 2003).Whether in public or private companies, I.T. is increasingly being considered as an important asset, acting as a driving force to provides complex solutions, thus it's governance is a critical success factor (Hardy, 2006).As a consequence, organizations and their executives strive to maintain high quality information to uphold business decisions, in order to deliver business value from investments in I.T., reaching strategic objectives through efficiency (ISACA, 2012).Judge and Toomey (2015) approach deploys the relevance in responsibility, strategy, acquisition, performance, human behavior and conformance allied to planning, leadership and control. All these principles are a framework based on ISO/IEC 38500 standard, guiding I.T. governance activities and supporting leaders on the construction and implementation of I.T. capabilities, while aiming for greater effectiveness on business goals according to director's perspective. Therefore, I.T. is a strategic business enabler, helping organizations to expand their scope in order to speed up businessobjectivesalignment as well as products and services improvement (Lunardi *et al.,* 2014). Weill and Woodham (2002) study demonstrate how I.T. governance cannot be seen asa single event, once it holistically bounds toother company assets and corporate governance, highlighting four I.T. key decisions: principles, infrastructure strategies, and architecture and investment prioritization. In addition, according to Weill and Ross (2004), these decisions excel how complex is creating value through I.T., especially on public not-for-profit driven corporations, where value concept is extremely wide. Therefore, aligning I.T. governance and organization's goals, requires technology to be seen as akey strategic tool to support stakeholder's interests through manager's actions.

Risk management

Risk is intrinsic to all human activity. Defining what will happen in the future and choosing among alternatives is a key factor to contemporary societies. Risk management guides us through various decisions, requiring attention to possible failures or errors regarding information and the complex technology involved in its processes (Bernstein, 1996).Also, according to the author, the act of taking risks is based in opportunities developed from deviations, and if everyone evaluates risk exactly the same way, facts considered to be negative could not be turned into real opportunities. Risk governance standards currently tend to be high-level, having scope for its application in different situations in companies, while potential challenges in risk assessment offers opportunity to detect problems in their internal processes (Akabane, 2012; Bromiley *et al.,* 2015).To OECD (2014), public institutions must apply similar governance practices as those by private companies, being crucial that there is a risk control both by manager's direct action as well as delegations from board directors, which can be used in any opportunity to formulate strategic and leadership policies. Governance aims to create value through benefits achievement, resources and risks optimization, while an effective I.T. governance manages and constantly evaluates activities and I.T. risks in order to keep them at an acceptable level (ITGI, 2007; ISACA, 2012).

ISO 31000:2009 standard provides principles and guidelines for risk management and can be applied in both public and private sectors to assess risk, regardless of its nature. According to the standard, success of risk management relies on the management structure which will provide foundations and arrangements to incorporate this processes throughout the organization, helping to effectively manage risk through its implementation at different organizational contexts and levels, ensuring they are properly identified and reported to be used as a decision making knowledge basis. Hardy (2006) states that a small gap, theft, error, violation of system or virus attack in I.T. can result in serious damage to organization's revenue and reputation. As a consequence, managers, stakeholders, employees and customers must be concerned with information security, while board directors must ensure organizational information assets protection.ISO/IEC 27005:2011 standard provides guidelines for Information Security Risk Management and can be applied by organizations willing for a satisfactory implementation of information security based on a risk management approach and can be used iteratively to assess or treat risk. Its iterative approach enables a detailed evaluation through with each repetition, reducing time and effort required to identify controls, ensuring that high probability and impact risks are properly assessed. Therefore, risk management can be seen as a holistic activity through organization aspects, which management process provides

background to set and operate risk acceptance levels, opportunities, and proper treatment.

Information security

Prevention of data loss, damage, destruction or unauthorized access to information processed by organizations is a continuous evolution while information security has increasingly drawn the attention of researchers, professionals, journalists, legislators and citizens. Governments and organizations are increasingly investing in their information assets security helping decision-making and improving operations continuity (Da Veiga and Martins, 2015; NIST, 2010; Purdy, 2010; Jourdan *et al.,* 2010).Technology is usually a visible artefact in organizations, and such evidence is a result of the implementation of information security components such as risk and security policy (Schein, 1985).Information systems are subject to threats that could both provide opportunities or negative impacts to the organization's operations, including its mission, proceedings, image, reputation, assets, individuals, as well as compromising the confidentiality, integrity, authenticity and availability of information being processed, stored or transmitted by these systems (NIST, 2010).Information security is the protection of information systems as well as access, use, disclosure, disruption, modification or destruction of unauthorized information. It preserves confidentiality (information is accessible only by authorized personnel), integrity, authenticity (accuracy and completeness of information), and availability (must be accessible by authorized persons) of information. The goal is to protect information from threats that could affect business continuity and ultimately maximize return on investments and business opportunities (Da Veiga and Martins, 2015; ISO/IEC 27002, 2013).

Electronic information used by companies constantly increases, while its management, ease of access, adequacy, reliability and compliance tends to be even more complex in order to meet organizational objectives. In addition, organizations are concerned about exposure caused by incidents that could compromise their activities (Posthumus and Von Solms, 2004).Influenced by needs, goals, security requirements, processes, size and structure, organizations tend to specify and strategically implement an Information Security Management System (ISMS) that meets organization's objectives. In its latest update, ISO/IEC 27001:2013 standardizes definitions and structures of different ISO standards in order to provide an even more effective risk management by including requirements to assess and treat information security risks (ISO/IEC 27001, 2013). Nevertheless, a continuous improvement approach through a process of creating, implementing, operating, monitoring, reviewing, maintaining and improving the organization's ISMS adopts the Plan-Do-Check-Act (PDCA) cycle while taking into account security requirements of information and actions required to meet stakeholder's expectations. The model reflects, among others, the principles of governance of information systems and networks, risk analysis, specification, implementation, administration and security revaluation (Da Veiga and Eloff, 2007; ISO/IEC 27001, 2005; ISACA, 2012). Information privacy and security are concepts related to protection and both should be considered when dealing with risk information. The dimension of privacy aligns organization's specific needs to verify principles that are in line with its preferences in different contexts. In addition, a good planning and information security implementation requires not only cooperation across the organization, but also by managers (Da Veiga and Martins, 2015; Montesdioca and Maçada, 2015).Various information security approaches could be applied regarding the implementation of security controls (components) and threats to information assets such as ISO/IEC 27002:2005, which is recognized as an essential standard for information security and defines a set of controls needed for most situations involving I.T. (Da Veiga and Eloff, 2007).Another approach presented by Eloff and Eloff (2005) is called PROTECT, which is an acronym for Policies, Risks, Objectives, Technology, Execute, Compliance and Team. Tudor (2000) proposed a comprehensive and flexible approach of an Information Security Architecture to protect organizational assets. His approach highlights five fundamental principles, listed in Table 1, which are used to understand the risk environment in which organizations operate in order to evaluate and implement controls to mitigate those risks, also having focus on the country's laws to ensure that confidential information is secured. These principles cover aspects of processes and technology to address security needs of organizations, and the first principle refers to security organization and infrastructure with defined roles and responsibilities, as well as management support.

Table 1. Information security architecture principles

- Security organization and infrastructure: Roles and responsibilities are defined and executive sponsorship is established.
- Security policies, standards, and procedures: Policies, standards and procedures are developed.
- Security program: A security program is compiled taking risk management into account.
- Security culture awareness and training: Users are trained and awareness is raised through various activities. Trust among users, management, and third parties are established.
- Monitoring compliance: Internal and external monitoring of information security is conducted.

Source: Da Veiga and Eloff (2007), adapted from Tudor (2000)

The second principle refers to security policies, standards and procedures, addressing its development and implementation relevance once security control requirements in security policies cannot be implemented by itself and should consider as much as possible risk backgrounds. As a third principle, risk assessments should be performed on all platforms, databases, applications, and networks, as well as a procedures should be established aiming to provide adequate resources to address risks and implement controls. For controls to operate effectively, users need to be aware of their responsibilities and be encouraged to participate in training programs. The fourth principle aims to establish an environment of trust among users, management and third parties, enable transactions and protect privacy, while the fifth and last principle focuses on compliance verification allied to internal and external audits to monitor program's effectiveness of security.

Information security in Brazilian public sector

Most institutions, private or public, are raising awareness on applying security protection countermeasures, policies, procedures and guidelines (Jourdan *et al.,* 2010). This is due to

the fact that security incidents can cause adverse consequences for organizations, which may affect information assets, organizational reputation, customer confidence, employee productivity and even legal risks (Dzazali *et al.,* 2009; Shedden *et al.,* 2011).Not only regulatory requirements are increasing, but also the governance responsibilities in increasingly oversee information security since this provides a strong link between the governing body, the executive management and those responsible for the implementation and operation of an information security system management that supports organizational goals (ISO/IEC 27001, 2013).A survey of Brazilian legislation related to Information Security and Communications made by Vieira and Fraga (2014) lists federal, state and municipal regulations. As shown in Table 2, there are many laws, decrees, regulatory instructions and projects related to the topic.

Table 2. Information security related regulation

Regulation	Quantity
Federal legal provisions	83
Federal law	48
State law	6
Municipal law	2
Technical standards	8
Law projects	13
Total	160

Source: Vieira and Fraga (2014)

In addition, Araujo's (2012) research also presents a legislation review pointing the existence of two normative instructions and 14 supplementary rules which contents must necessarily be observed and followed by all Brazilian federal public agencies. Regulatory bodies and control of public administration such as the Ministry of Planning, the General Comptroller and the Audit Court also heavily supervises public organizations and public archives (Albuquerque and Santos, 2014).

MATERIALS AND METHODS

This exploratory research is based on an induction process, then generates and describes theoretical approaches (Sampieri, Collado, Lucio, 2006). Consisting on a single case study, it aims to determine how information security risk management is presented in a Brazilian public federal institution according toI.T. managers perception. The methodological relevance of a research can be justified by proper scientific background and the best approach addressing research questions. In addition, a single case study allows further deeper research development and is often used in lengthwise research (Miguel, 2007).According to Yin (2009), a case study is an empirical inquiry that investigates contemporary phenomena inserted in a real life context and allows the use of evidence from sources such as direct observation and interviews. Also, the case studies generally have three main steps: definition and planning; preparation, data gathering and analysis; information analysis and conclusion, as shown below:

Definition and planning

- **Case choice:** Information obtained through a bibliometric study shows a small number of researches about information security risk management in the context of Brazilians public federal education institutions. In addition, authors ease of access with I.T. governance directors helped data gathering while facing time, financial, material and people constraints (Mattar, 1996).
- **Selection of respondents:** The respondents were selected by being skilled I.T. directors having frequent contact with the subject.

Data gathering and analysis

- **Query application:** based on the ISA raised in this research and the selection of respondents, an online questionnaire was used to collect answers. Seeking a diverse sample, questions were applied to directors responsible for different I.T. areas.
- **Preliminary report:** a preliminary case report was prepared with the information obtained from the questionnaire for detailed analysis.

Information analysis and conclusion

- **Information analysis:** a detailed analysis of the responses was performed from the preliminary report.
- **Conclusions:** observations through a detailed analysis of the results.

The proposed questionnaire was based on the study addressed in Section 2 and intended to verify aspects such as: security organization and infrastructure; security policies, standards, and procedures; security program; security culture awareness and training; monitoring compliance.

Data analysis and discussion

As shown in Table 3, respondent's profile demonstrates that two of them works for less than two years as anI.T. director, while having a considerable age difference and the same education level. Others are working for more than two years while having different education levels and age groups.

Table 3. Respondents profile

Managers	Time	Education Level	Age group
M1	up to 2 years	Graduate	40 to 50 years
M2	up to 3 years	Master	20 to 30 years
M3	up to 3 years	Ph. D	40 to 50 years
M4	up to 1 year	Graduate	20 to 30 years
M5	up to 3 years	Graduate	20 to 30 years

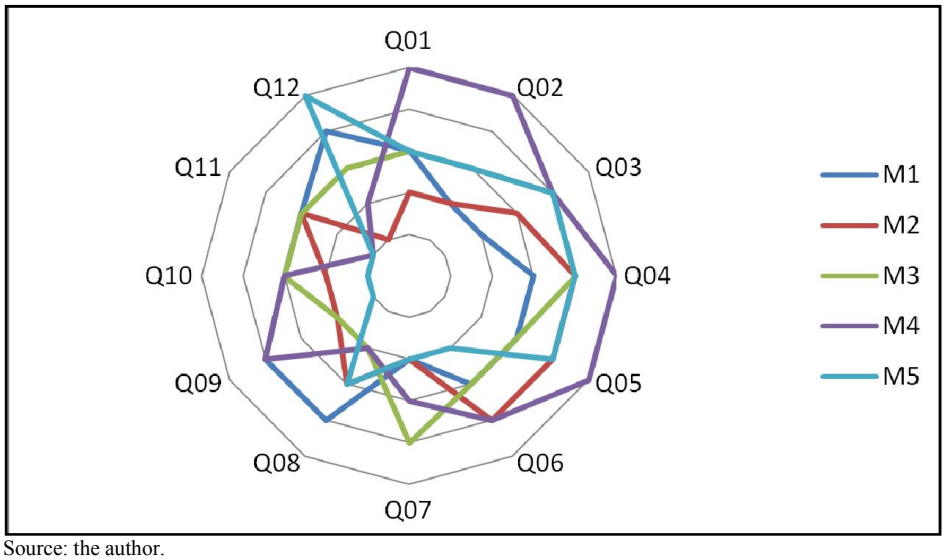
Source: the author.

Answers shown in Table 4 are a set of5 dimensions (D1 to D5), each one containing questions ranked according to Likert's scale from 1 (completely disagree) to 5 (completely agree), in a total of 12 questions. Questions 01, 02 and 03 refers to security organization and infrastructure (D1); 04, 05 and 06 refers to security policies, standards (D2); 07 refers to security program (D3); 08, 09 and 10 refers to security culture awareness and training (D4) and, finally, 11 and 12 refers to the monitoring compliance (D5).

Table 4. Questionnaire answers

Managers	D1			D2			D3	D4			D5	
	Q01	Q02	Q03	Q04	Q05	Q06	Q07	Q08	Q09	Q10	Q11	Q12
M1	3	2	2	3	3	3	2	4	4	3	3	4
M2	2	2	3	4	4	4	2	3	2	2	3	1
M3	3	3	4	4	3	3	4	2	2	3	3	3
M4	5	5	4	5	5	4	3	2	4	3	1	2
M5	3	3	4	4	4	2	2	3	1	1	1	5
TOTAL	16	15	17	20	19	16	13	14	13	12	11	15

Source: the author.



Source: the author.

Figure 1. Questionnaire responses radar graph

The analysis regarding security organization and infrastructure (D1) displays a considerable neutral range, while the remaining ones differs specially about the roles played by people as well as responsibilities while some disagreement is noticeable among the respondents. On the other hand, as shown in Image 1, three respondents agreed that executive sponsorship is well established. Internal studies are recommended in order to improve responsibilities and clarify roles played by people in this context. In security policies, standards, and procedures (D2), respondents seem to somewhat agree that policies and standards are developed, but procedures responses demonstrate certain neutrality and low agreement, having room for improvement. Due to its relevance, it is recommended that a special attention is given to the implementation of safety control requirements along with policies development and implementation of standards and procedures in order to reduce risks to the institution. Analyzing the organization of a security program that takes risk management into account(D3), a significant disagreement is noticeable among the respondents, which may suggest special attention to the risk assessment regarding platforms, databases and network applications by implementing controls and provide adequate financial resources while acting toprevent negative risks. Regarding security culture awareness and training (D4), responses indicates low confidence among users, management and third parties, pointing out the need for users training in order to improve awareness and responsibilities, as well encourage their participation in training programs aiming privacy protection.

Monitoring compliance (D5) dimension responses suggests that internal information security audits should be carried out aiming effectiveness of the institution's security program, while external audits would improve and validate its effectiveness.

Conclusions

The verified information security components are described as principles bytheir implementation and maintenance, such as information security policies, risk assessment, technical controls, and information security awareness. The main contribution of this work both in practical and theoretical perspective lies in verifying how information security principles regarding risk management are implemented in a public federal educational institution from Brazil according the perception of I.T. managers. These principles can be used to understand the risk environment in which organizations operate in order to evaluate and implement controls to mitigate such risks (Da Veiga and Eloff, 2007).Nevertheless, limitations of this study refers to the application of data collection techniques, as well as time constraints and lack of financial resources. These results were based on non-probabilistic sampling and respondent's selection was not random, thus not allowing generalizations (Kish, 1965; Oliveira, 2001). Further research addressing larger samples and studies regarding information security risk management in public federal institutions are highly suggested.

REFERENCES

Akabane, G. K. 2012. *Gestão estratégica da tecnologia da informação: conceitos, metodologias, planejamento e avaliações*. Atlas. São Paulo, Brazil.

Albuquerque, A. E. Jr.,Santos, E. M. 2014. Análise das Publicações Brasileiras sobre Segurança da Informação sob a Ótica Social em Periódicos Científicos entre 2004 e 2013. *XXXVIII Encontro da ANPAD*, Rio de Janeiro, Brazil.

Araujo,W. J. 2012. Leis, decretos e normas sobre gestão da segurança da informação nos órgãos da administração pública federal. *Informação and Sociedade: Estudos*, João Pessoa, Brazil.

Bernstein, P. L. 1996. *Against The Gods: The Remarkable Story of Risk*. New York: John Wiley and Sons.

Bromiley, Philip; Mcshane, Michael; Nair, Anil; Rustambekov, Elzotbek. 2015. Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning*, v. 48, n. 1, p.265-276.

Da Veiga, A., Martins, N. 2015. Information security culture and information protection culture: A validated assessment instrument. *Computer Law and Security Review*.

DaVeiga, A.,Eloff, J. H. P. 2007. An information security governance framework. *Information Systems Management*. South Africa.

Dzazali, S., Sulaiman, A., Zolait, A. H. 2009. Information security landscape and maturity level: case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*.

Eloff, J. H. P.,Eloff, M. 2005. Integrated Information Security Architecture. *Computer Fraud and Security*.

Fazlida, M. R., Jamaliah, S. 2015. Information Security: Risk, Governance and Implementation Setback, *Procedia Economics and Finance*.

Hardy, G. 2006. Using I.T. governance and COBIT to deliver value with I.T. and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, v. 11, n. 1, p.55-61.

ISACA, 2012. COBIT 5: A business framework for the governance and management of enterprise I.T..*Information Systems Audit and Control Association*. Rolling Meadows, IL, United States.

ISO. ISO 31000. 2009. Risk Management: Principles and guidelines. International Organization for Standardization.

ISO/IEC 27001. 2005. Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization.

ISO/IEC 27001. 2013. Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization.

ISO/IEC 27002. 2013. Information technology – Security techniques – Code of practice for information security management. International Organization for Standardization.

ITGI. 2003. *Board Briefing on I.T. Governance*, 2nd Ed. I.T. Governance Institute. Rolling Meadows, IL, United States.

ITGI. 2007. *COBIT 4.1: Control Objectives for Information and Related Technology*. I.T. Governance Institute. Rolling Meadows, IL, United States.

Jourdan, Z.,Rainer, R. K., Marshall, T. E., Ford, F.N. 2010. An investigation of organizational information security risk analysis. *Journal of Service Science*, Alabama.

Juiz, C., Toomey, M. 2015. To govern IT, or not to govern IT? Communications of the ACM, [s.l.], v. 58, n. 2, p.58-64.

Kish, L. 1965. Survey sampling. *John Wiley and Sons*, Inc.

Laurindo, F. J. B., Shimizu, T., Carvalho, M. M., Rabechini JR., R. 2001. O papel da Tecnologia da Informação (TI) na Estratégia das Organizações. *Gestão and Produção*.

Luftman, J. N. 2003. Assessing I.T.-Business alignment. *Information Systems Management*.

Mattar, F. 1996. *Marketing research*. Atlas.

Miguel, P. A. C. 2007. Estudo de caso na engenharia de produção: estruturação e recomendações para sua condução. Produção, São Paulo, v. 17, n. 1, p.216-229.

Montesdioca,G. P. Z.,Maçada, A. C. G. 2015. Measuring user satisfaction with information security practices, *Computers and Security*.

NIST. 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. 800-37 ed. Gaithersburg, National Institute of Standards and Technology.

Nobre, A. C. S., Ramos, A. S. M.,Nascimento, T. C. 2010. Fatores que influenciam a aceitação de práticas avançadas de gestão de segurança da informação: um estudo com gestores públicos estaduais no Brasil. *Encontro da associação nacional de pós-graduação e pesquisa em administração proceedings*, Rio de Janeiro, Brazil.

OECD, 2004. *Principles of Corporate Governance*. Organisation for Economic Co-operation and Development. OECD Publishing.

OECD, 2014. *Risk Management and Corporate Governance*. Organisation for Economic Co-operation and Development. OECD Publishing.

Oliveira, T. M. V. 2001. Amostragem não Probabilística: Adequação de Situações para uso e Limitações de amostras por Conveniência, Julgamento e Quotas. *Revista Administração On Line*. FECAP.

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

Sampieri, R. H., Collado, C. F., Lucio, M. P. B. 2006. *Metodología de la Investigación*. 4th ed. Mexico, MX. Mac Graw Hill.

Schein, E. H. 1985. *Organizational culture and leadership*. São Francisco: Jossey-Bass.

Shedden, P., Scheepers, R., Smith, W., Ahmad, A. 2011. Incorporating a knowledge perspective into security risk assessments. *Journal of Information and Knowledge Management Systems*.

Tudor, J. K. 2000. *Information Security Architecture – An integrated approach to security in an organization*. Boca Raton, FL: Auerbach.

Van Grembergen, W., De Haes, S., Guldentops, E. 2004. *Structures, Processes and Relational Mechanisms for I.T. Governance*. Idea Group Publishing.

Vieira, T. M.,Fraga,J. 2014. *Quadro da legislação relacionada à segurança da informação e comunicações*. http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm. Cited 25 Oct 2015.

Weill, P., Ross, J. 2004. *I.T. governance: how top performers manage I.T. decisions rights for superior results*. Boston: HBS Press.

Weill, P., Woodham, R. 2002. Don't Just Lead, Govern: Implementing Effective IT Governance. *Center For Information Systems Research*, Massachusetts, v. 326, n. 1, 20p.

YIN, Robert. K. 2009. *Case Study Research: Design and Methods* (4th ed., pp. 1-240. Thousand Parks, CA: Sage.

****