

---

**SCIENTIFIC PRODUCTION ON INFORMATION SECURITY FROM THE SOCIAL PERSPECTIVE  
ON PORTUGUESE SPEAKING SCIENTIFIC JOURNALS BETWEEN 2004 AND 2013**

**Antonio Eduardo de Albuquerque Junior**

*Universidade Federal da Bahia  
Salvador – BA – Brazil*

E-mail: [eduardo.albuquerque@bahia.fiocruz.br](mailto:eduardo.albuquerque@bahia.fiocruz.br)

**Ernani Marques dos Santos**

*Universidade Federal da Bahia  
Salvador – BA – Brazil*

E-mail: [emarques@ufba.br](mailto:emarques@ufba.br)

**Ivo Pedro Gonzalez Junior**

*Universidade Federal da Bahia  
Salvador – BA – Brazil*

E-mail: [ivojunior@gmail.com](mailto:ivojunior@gmail.com)

**ABSTRACT**

---

*The value of information for organizations, the importance of protecting organizational information, the technological advances, the exposure to technological threats, and the risks associated to human behavior indicate the importance of studying Information Security under social approaches. This article aims to analyze the production on Information Security published on scientific journals of Administration, Information Systems and Information Science in the last ten years. This study is characterized as descriptive and exploratory, with a qualitative and quantitative approach. After filtering, 20 papers published in 10 journals were selected. The study shows that Information Security has not been sufficiently explored from social approaches. The results show many papers in health institutions, IT companies, public archives and public organizations.*

---

**Keywords:** *Information Security; Social approach; Bibliometrics*

**1. INTRODUCTION**

The importance of protecting information and the exposure of organizations to new technological threats (Alexandria, 2009) has led to the development of scientific research on Information Security, but Coles-Kemp (2009) points out that many studies have focused on technological and mathematical aspects, and that little amount of research has been produced on social aspects of Information Security. Luo, Brody, Seazzu and Burd (2011) state that the promotion of Information Security tends to have a focus on technological suggestions, although Silva and Stein (2007) argue that studies on Information Security should not only focus on technology. Frangopoulos, Eloff and Venter (2008) understand that organizations have technologies for protecting information and develop policies, standards and procedures technically complete, but incomplete by not properly treat human relations.

The need for more studies on Information Security from a social perspective is also observed by Dhillon and Backhouse (2001) and Björck (2004; 2005). Albuquerque Junior and Santos (2013; 2014) analyzed the production on Information Security under a social approaches in scientific conferences in Brazil. In both studies, the authors note that Information Security has had little representation in comparison to the overall number of papers and that few studies were based on social sciences theoretical approaches.

The present paper reveals the result of a research that analyzed Brazilian publications on Information Security in the last ten years. The objectives are to identify the number of authors who sign each article, the context in which each researches was conducted, models or theories used by the authors, the most common references and the way they were published. With this study, the intention is to encourage the development of research on

Information Security using social theoretical approaches, contributing to the development of the theme in the field of Administration.

## 2. THEORETICAL FRAMEWORK

Nobre, Ramos e Nascimento (2010) argue that the information may be one of the most valuable assets of an organization, but Alexandria (2009) notes that the advantages that new technologies bring on exchange and storage of information have exposed organizations to new threats. Therefore, it is necessary to properly protect information, since the occurrence of incidents may represent financial losses and damage to the organizations' image, according to Posthumus and von Solms (2004).

This situation leads to increase Information Security, which is defined by Silva and Stein (2007) as the protection of information against unauthorized use or access, and against the denial of access to authorized persons, ensuring its confidentiality and integrity. Sêmola (2014) highlights that Information Security is a knowledge area dedicated to protect the information against unavailability, unauthorized access and unauthorized changes.

The Brazilian Association of Technical Standards (Associação Brasileira de Normas Técnicas – ABNT, in Portuguese) recommends that organizations guide Information Security actions through formalized and documented policies (ABNT, 2005) and considers technological resources, infrastructure, processes, procedures and organizational structure. Marciano and Lima-Marques (2006) include the human resources needed for the promotion of Information Security. The Information Security Policy is a wide and formal document that should be evaluated and monitored constantly, and requires knowledge of social aspects, training and education activities of the organization's members (Karyda, Kiountouzis & Kokolakis, 2005). Nevertheless, Lorens (2007) points out that organizations generally plan or create Information Security standards without considering the human factor, which frustrate its development or regulation, making an inefficient or impracticable result (Lorens, 2007).

The audit and consulting company PriceWaterhouseCoopers (2013) realized a survey with 575 managers from Brazilian companies and found that 37% of Information Security incidents had been originated from organizations' employees, 36% comes from former employees and 16% are caused by third party service providers. Wilson (2009) cites a survey with more than 400 professionals of Information Technology (IT), realized by the journal "InformationWeek", which showed that 52% of participants were more focused on preventing attacks from organization's employees than caused by external agents, and 59% of virus infections and other malicious programs that occurred during the period of a year had been caused by the employees themselves.

The man is considered by Sasse, Brostoff and Weirich (2001) as the greatest weakness of Information Security. For these authors, organizations are more vulnerable than ever and human behavior enables or facilitates the occurrence of incidents of Information Security. Mitnick and Simon (2003) consider the man as the weakest element of Information Security, which makes the organization vulnerable to social engineering attacks in which social relationships with members of the organizations are exploited by the attacker in order to have access to sensitive information. Van Der Leeden (2010) highlights that IT users are the major causes of Information Security incidents and show little awareness about it. Alexandria (2009) observed that employees understand Information Security as an issue related to systems and institutional information, and that IT users don't have responsibility about it.

Even though the human component is important and related to Information Security attacks and incidents, it has been neglected (Luo et al., 2011) and it is a common mistake not to consider the social and human aspects associated with Information Security (Alexandria, 2009; Von Solms & Von Solms, 2004). Information security is not restricted to computer systems or digital information, but it is associated with any form of information protection and should encompass the systems, services and processes involved, argue Silva and Stein (2007). Accordingly to those authors, many efforts have been made to improve Information Security systems, but little effort has been made to develop human capabilities and limitations.

Technical solutions are necessary but insufficient to address Information Security challenges for complex socio-technical environments in constantly changing like the organizations (Holgate, Williams, & Hardy, 2012). The human behavior is complex and involves variables that cannot be controlled. Moreover, there is no way to

eradicate the risks related to human behavior (Silva & Stein, 2007). The idiosyncratic nature of people is not provided in most of the Information Security's rules and procedures, especially in a social context like organizations, making them unprepared for social engineering attacks (Frangopoulos et al., 2008)

To better understand and minimize the risks associated with social factors, it is necessary to analyze how Information Security had been addressed. Nevertheless, some authors have pointed out that Information Security is not being studied under a social perspective. Dhillon and Backhouse (2001) emphasize that the studies have been mainly directed to problems and technological solutions, with little regard for social, organizational and human factors. Björck (2004) argues that safe systems have been created, but the failures that arise from the social behavior lead to the need to study social aspects of Information Security. The author states that there is a gap of appropriate social sciences' theories used on Information Security researches.

Coles-Kemp (2009) argues that Information Security has traditionally been studied in a technological or mathematics approach, despite its hybrid nature, with technical and social dimensions. She also points that there are few relevant social and organizational theories applied to Information Security, which can lead to a gap in this area's knowledge. For Silva and Stein (2007), although it is necessary to develop research on social aspects of Information Security, little has been done to identify the causes that lead people to unsafe behavior. Coles-Kemp (2009) admits that Information Security should continue to be studied using technological or mathematical approaches, but points out that it should be studied from a social perspective too.

In two studies realized on scientific conferences proceedings (Albuquerque Junior & Santos, 2013; 2014), few papers were identified compared to total published: only 0.23%. Both articles show that ISO/IEC 27002 standard was the most mentioned text on conferences papers, and many researches was based on Information Security standards, in particular ISO/IEC 27002, while common theoretical approaches in social sciences studies have been little used.

### 3. METHODOLOGICAL PROCEDURES

This study is characterized as descriptive, exploratory, with qualitative and quantitative approach. Relevant national journals for researchers of Administration field in Brazil were identified. Eight articles on scientific production in the Administration field provided the journals' names: Barbosa Neto and Colauto (2010), Souza, Ribeiro, Machado Júnior and Corrêa (2011), Sobral and Mansur (2013), Mascarenhas and Barbosa (2013), Leal, Almeida and Bortolon (2013), Paiva and Brito (2013), Mazzon and Hernandez (2013), and Mota and Marques (2013).

Some other national and international journals that publish articles on Administration, Information Systems and Information Science in Portuguese in Webqualis system (<http://qualis.capes.gov.br/webqualis/principal.seam>), provided by *Coordenação de Aperfeiçoamento de Pessoal de Nível Superior* (CAPES), a Brazilian public agency that evaluates scientific journals and post-graduate programs. The journals identified have Qualis B3 or higher on Administration (on a scale consisting of C, B5, B4, B3, B2, B1, A2 e A1), according to CAPES evaluation, but only journals that publish articles in Portuguese, English or Spanish and on Administration, Information Science and Information Systems fields were considered. Thus, 43 journals were identified (see Table 1).

Therefore, searches were made for articles published the last 10 years on Information Security on the journals' websites using terms and keywords normally associated with Information Security: "security", "information", "privacy", "confidentiality", "availability", "integrity", "risk", "security + information", "risk + information", "confidentiality + information", "availability + information" and "integrity + information". Searches were made for articles with those terms Portuguese, English and Spanish. Abstracts of articles resulting from the searches were read to confirm that address the Information Security. So, 59 articles published in 12 different journals were fully read, which allowed the exclusion which had focus on technology. Thus, by having social focus, only 20 papers published in journals 10 were selected for analysis.

These 20 articles were read again to identify the total of authors, the context in which each research was conducted, the model or theoretical approach, the methodological approach, the research method, the most used references, the most used types of references, the most referenced authors and the most referenced scientific journals. The next section shows detailed results of the analysis of those 20 articles.

**Table 1** – Journals identified.

Journals' Names	Qualis
Brazilian Administration Review (BAR)	A2
Brazilian Business Review (BBR)	
<i>Organizações &amp; Sociedade (O&amp;S)</i>	
<i>Gestão &amp; Produção</i>	
<i>Revista de Administração de Empresas (RAE)</i>	
<i>Revista de Administração Contemporânea (RAC)</i>	
<i>Revista de Administração da Universidade de São Paulo (RAUSP)</i>	
<i>Revista de Administração Pública (RAP)</i>	
<i>Revista Brasileira de Economia (RBE)</i>	
<i>Revista Contabilidade &amp; Finanças</i>	
IEEE Latin America Transactions	
FACES: <i>Revista de Administração (FACES)</i>	B1
Journal of Information Systems and Technology Management (JISTEM)	
<i>Economia Aplicada</i>	
<i>Produção</i>	
<i>Cadernos EBAPE</i>	
<i>Revista Brasileira de Finanças (RBFIn)</i>	
<i>Base</i>	
<i>Revista Universo Contábil</i>	
<i>Revista de Ciências da Administração</i>	
<i>Revista de Administração Mackenzie (RAM)</i>	
<i>Revista Eletrônica de Administração (READ)</i>	
<i>Revista Brasileira de Gestão de Negócios (RBGN)</i>	
<i>Exacta</i>	
<i>Informação &amp; Sociedade</i>	
<i>Perspectivas em Ciência da Informação</i>	
<i>Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI)</i>	
<i>Brazilian Journal of Information Science</i>	
<i>Ciência da Informação</i>	
<i>Revista de Gestão (REGE)</i>	B2
<i>Gestão &amp; Planejamento (G&amp;P)</i>	
<i>Sistemas &amp; Gestão (S&amp;G)</i>	
<i>Revista Digital de Biblioteconomia e Ciência da Informação</i>	
<i>Revista Gestão e Tecnologia</i>	
<i>Revista Eletrônica de Sistemas de Informação (RESI)</i>	B3
<i>Revista da Micro e Pequena Empresa</i>	
<i>Revista de Gestão e Projetos</i>	
<i>Reuna</i>	
<i>Revista de Economia e Administração</i>	
<i>Informação &amp; Informação</i>	
<i>Navus Revista de Gestão e Tecnologia</i>	
<i>Revista Eletrônica de Comunicação, Informação &amp; Inovação em Saúde (RECIIS)</i>	
<i>Revista GEINTEC: Gestão, Inovação e Tecnologias (GEINTEC)</i>	

Source: data gathered by the authors on Barbosa Neto and Colauto (2010), Souza, Ribeiro, Machado Júnior and Corrêa (2011), Sobral and Mansur (2013), Mascarenhas and Barbosa (2013), Leal, Almeida and Bortolon (2013), Paiva and Brito (2013), Mazzon and Hernandez (2013), Mota and Marques (2013) and in Webqualis.

#### 4. DATA PRESENTATION AND ANALYSIS

As shown in Table 2, IEEE Latin America Transactions journal concentrates 34 articles on Information Security, which account for over 57% of production from 2004 to 2013, but 31 of them have a focus on technology, because this journal publishes also articles produced by researchers of Computer Science, Computer

Engineering and other areas studying Information Security technological aspects. The same applies to the *Revista Ibérica de Sistemas e Tecnologias de Informação* (RISTI).

**Table 2** – Quantities of articles published from 2004 to 2013 by journals.

Journal	Qualis	Articles on Information Security	Articles with social approach
IEEE Latin America Transactions	A2	34	3
<i>Ciência da Informação</i>	B1	1	1
<i>Exacta</i>	B1	1	-
<i>Informação &amp; Sociedade</i>	B1	3	3
JISTEM	B1	3	3
<i>Perspectivas em Ciência da Informação</i>	B1	2	2
RISTI	B1	1	-
<i>Revista Gestão e Tecnologia</i>	B2	1	1
<i>Reuna</i>	B3	2	2
RECIIS	B3	2	1
RESI	B3	8	3
GEINTEC	B3	1	1
TOTAL	-	59	20

Source: data gathered by the authors.

IEEE Latin America Transactions is the unique journal with three articles published qualified with Qualis A2. Another three magazines have published three articles each one on social aspects of Information Security: (a) *Informação & Sociedade* and (b) JISTEM, both qualified with Qualis B1; (c) RESI, qualified with Qualis B3. The magazine *Perspectivas em Ciência da Informação* has published two articles qualified with Qualis B1. Reuna, a journal with Qualis B3, published two articles. Another four magazines have published only one article: *Ciência da Informação*, Qualis B1; *Revista Gestão e Tecnologia*, Qualis B2; RECIIS and GEINTEC, both Qualis B3.

The layer B1 has nine papers on a total of 20 articles published. This fact demonstrates that the subject is interesting for journals qualified by CAPES in the superior layer (A2 and B2), but it needs a control check because magazines in layer A1 were not identified in this study.

The Table 3 shows the distribution of papers issued regarding Information Security from 2004 to 2013. The number of articles grows in the timeline, as well those concerning Information Security tout court as those with a social approach. Articles on this subject with a social approach in 2004 and 2008 were not found. The major number of publications was in 2013.

Table 4 shows the articles names, journals, authors and year of publication. Three authors have published more than an article: Sfredo and Flores published together (2009, 2012) in the magazine *Perspectivas em Ciência da Informação*; Araújo published with Amaral in 2010, and alone in 2012, both articles issued in *Informação & Sociedade* journal.

**Table 3** – Articles about Information Security with social approach issued from 2004 to 2013.

Year	Articles on Information Security	Articles With Social Approach
2004	3	-
2005	1	1
2006	3	1
2007	4	1
2008	6	-
2009	5	2
2010	8	3
2011	10	3
2012	10	3
2013	9	6
TOTAL	59	20

Source: data gathered by the authors.

**Table 4** – The articles on Information Security with social approach.

Title	Author / Year	Journal
<i>Uma Metodologia para Implantação de um Sistema de Gestão de Segurança da Informação</i>	Martins and Santos (2005)	JISTEM
<i>O enfoque social da segurança da informação</i>	Marciano and Lima-Marques (2006)	<i>Ciência da Informação</i>
<i>Gestão da Segurança da Informação: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas</i>	Silva Netto and Silveira (2007)	JISTEM
<i>Gerenciamento de Segurança Segundo ITIL: Um Estudo de Caso em uma Organização Industrial de Grande Porte</i>	Breternitz, Navarro Neto and Navarro (2009)	RESI
<i>O controle de acesso na percepção dos profissionais de arquivo: uma questão de segurança das informações institucionais</i>	Sfreddo and Flores (2009)	<i>Perspectivas em Ciência da Informação</i>
<i>Proposição de um Modelo Dinâmico de Gestão de Segurança da Informação para Ambientes Industriais</i>	Roque, Nunes and Silva (2010)	RESI
<i>Gestão da Segurança do Conhecimento: uma proposta de modelo</i>	Araújo and Amaral (2010)	<i>Informação &amp; Sociedade</i>
<i>Uma Proposta de Ontologia de Domínio para Segurança da Informação em Organizações: descrição do estágio terminológico</i>	Almeida, Souza and Coelho (2010)	<i>Informação &amp; Sociedade</i>
<i>Aligning Information Security with the Image of the Organization and Prioritization Based on Fuzzy Logic for the Industrial Automation Sector</i>	Knorst, Vanti, Andrade and Johann (2011)	JISTEM
<i>Privacidade de Informações de Pacientes de Instituições de Saúde: A Percepção de Profissionais da Área de Saúde</i>	Luciano, Bragança and Testa (2011)	<i>Reuna</i>
<i>Adoção de Práticas de Gestão de Segurança da Informação: Um Estudo com Gestores Públicos</i>	Nobre, Ramos and Nascimento (2011)	<i>Reuna</i>
<i>Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais</i>	Sfreddo and Flores (2012)	<i>Perspectivas em Ciência da Informação</i>
<i>Leis, Decretos e Normas sobre Gestão da Segurança da Informação nos Órgãos da Administração Pública Federal</i>	Araújo (2012)	<i>Informação &amp; Sociedade</i>
<i>LOPD Compliance and ISO 27001 Legal Requirements in the Health Sector</i>	Sánchez, Olmo, Álvarez, Medina and Piattini (2012)	IEEE Latin America Transactions
<i>Safety and Security in Critical Applications and in Information Systems – a Comparative Study</i>	Almeida Junior, Camargo Junior and Cugnasca (2013)	IEEE Latin America Transactions
<i>A percepção da importância de controles de segurança da informação em hospitais públicos brasileiros</i>	Albuquerque Junior and Santos (2013)	RECIIS
<i>The Need for Formal Education on Information Security</i>	Pacheco (2013)	IEEE Latin America Transactions
<i>Modos de Controle em uma Empresa de Segurança Cibernética</i>	Chiesa, Zíngano and Grisci (2013)	<i>Revista Gestão e Tecnologia</i>
<i>Modelo de Avaliação da Maturidade da Segurança da Informação</i>	Rigon and Westphall (2013)	RESI
<i>Gestão da Segurança da Informação: Caracterização da Incubadora Tecnológica de Santa Maria</i>	Potrich, Vieira and Nunes (2013)	GEINTEC

Source: data gathered by the authors.

The articles on Information Security with a social approach have at most five authors. Eight articles have been signed by two authors, another eight by three authors, and 18 articles have at most three authors. It seems indicate that there is a little collaboration among researchers studying this topic in applied social sciences, it

should be verified with an analysis of the contribution social networks. The distribution number of authors / number of articles is given in Table 5.

**Table 5** – Number of authors and articles.

Number of Authors	Number of Articles
1	2
2	8
3	8
4	1
5	1

Source: data gathered by the authors.

Three studies have been realized in health institutions, two in TI companies, two in public archives, and two in public organizations (see Table 6). The fact that health institutions have been the most studied highlight the importance of privacy in health institutions. This organizations are regulated and controlled by different organs, they must guarantee the privacy of the patients and at the same time let them available to professionals who work there as well as for the patient himself. Public organizations and public archives are also firmly regulated and controlled by Brazilian Government through laws, decrees and other rules that compel these organization to adopt practices of Information Security, as noted Araújo (2012).

**Table 6** – Number of articles and context of researches realization on Information Security.

Context of Researchh	Number
Health institutions (public and private)	3
TI Companies (public and private)	2
Public Archives	2
Others public organizations (Administration)	2
Industries	1
Industrial automation branch	1
Industrial waste treatment companies	1
Small enterprises	1
Technological Research and Development Institutions	1
Automobile industry	1
Not identified	1
Not applicable	4

Source: data gathered by the authors.

Studies realized in banks and e-commerce organizations were not identified. This organizations are IT-dependents and Information Security incidents can have a negative impact for their images. Even if their managers are not interested in revealing their controls, weakness and Information Security incidents, they may have mature Information Security processes that may guide other organizations in the same way. Only one study has been realized in a Research & Development institution, which has the responsibility to protect patents, projects, processing, as well as the knowledge developed in its activities, and that is submitted to the regulation of the National Committee on Ethics in Research (Comissão Nacional de Ética em Pesquisa – CONEP, in Portuguese), that rules the realization of researches related to human beings, including the protection of the privacy of the participant.

When analyzed the models or theories used in the researches, six works based on the standard ISO/IEC 27002 was noted. This standard presents an ensemble of Information Security controls, adopted by organizations all over the world. It emphasizes its importance also to the researches who study this subject in Brazil. Other standards by International Organization for Standardization (ISO) are also present with the models most used, as the ISO/IEC 27001, that establishes an Information Security Management System. The ISO 15489-1 standard, concerning the management of documents and information records, has been used in two studies. And ISO/IEC 27005, concerning the management of Information Security risks, has been used in one of the papers analyzed. The models and theories employed are given in Table 7

**Table 7** – Number of articles following model or theory employed.

Number	Model or Theory Used
6	ISO/IEC 27002
4	ISO/IEC 27001
2	Requirements for Computerized Archival Document Management (e-ARQ)
2	ISO 15489-1
2	Control Objectives for Information and Related Technology (COBIT)
1	ISO/IEC 27005
1	Information Technology Infrastructure Library (ITIL)
1	Technology Acceptance Model (TAM)
1	Balanced Scorecard
7	Others
8	Not identified or not applicable

Source: data gathered by the authors.

Two IT Governance models have been identified: Control Objectives for Information and Related Technology - COBIT, model employed in two researches, and Information Technology Infrastructure Library - ITIL, employed in one research. Those three papers concern more the IT governess although they give also orientations for the Information Security. Two articles have employed the Requirements Model for Informatics Systems to Manage Documents Archives (e-ARQ), or *Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos*, in Portuguese, standard create by the Brazilian Federal Government, an obligation for national public administration organizations.

One article was based on Technology Acceptance Model (TAM), a socio-technological model for study the acceptance and the use of technology in the organizations, a very common theory in academic studies on Information Systems. An article was based on Balanced Scorecard, a strategic management model, very common in Administration studies. Some other social sciences theory, like Actor-Network Theory or Institutional Theory, was not identified in the papers analyzed.

On a total of 20, 14 articles have qualitative approach, three of them have quantitative approach, and another three have qualitative and quantitative approach. It confirms the findings of others researches in scientific production on Information Systems, e.g. Teixeira Junior (2002), Rossoni and Hocayen-da-Silva (2007), Zimmer, Ferreira and Hoppen (2007) and Mota and Marques (2013).

The Table 8 shows that the case study is the method more often employed. Seven articles study a case and three of them study multiple cases, following the tendency highlighted in articles by Rossoni and Hocayen-da-Silva (2007), as well as Zimmer, Ferreira and Hoppen (2007). However it is not the tendency observed by Teixeira Junior (2002), who has noted a dominance of surveys in articles issued from 1999 to 2001.

**Table 8** – Number of articles and method of research.

Number	Method of Research
7	Case
5	Bibliography search
4	Survey
3	Multiple cases
1	Documental Analysis

Source: data gathered by the authors.

The Table 9 shows that there is no scientific article, thesis or dissertation among the ten most mentioned references. Five books, three technical standards and two legal regulations are the most used references. The Information Security standards are the most common. The ISO/IEC 27002 is the most referred text, it appears in 11 of the analyzed articles. It seems to confirm the importance of technical standards for the researchers and indicates the gap of scientific articles that could make reference to academic studies developed on that topic in Brazil.



**Table 9** – Categories of references more times employed in those articles and number of mentions.

Reference	Category	Number
ISO/IEC 27002 (ABNT, 2005)	Technical standard	11
ISO/IEC 27001 (ABNT, 2006)	Technical standard	6
Sêmola (2003)	Book	6
ISO/IEC 27005 (ABNT, 2008)	Technical standard	3
Beal (2005)	Book	3
Fontes (2006)	Book	3
Moreira (2001)	Book	3
Decree nr. 3.505 (2000)	Legal regulation	3
Decree nr. 4.553 (2002)	Legal regulation	3
Yin (2005)	Book	3

Source: data gathered by the authors.

Books are the most referred type of work in the analyzed articles. In 508 references, 151 (29.72%) are books. Second in the ranking, 24.80% (or 126) makes reference to articles published in scientific journals. In the third place, 79 papers of scientific conferences proceedings, that are 15.55% of total. In fourth, with 7.68% (or 39 mentions), are technical standards. Only 3.54% (or 18 articles) made reference to dissertations and 2.36% (or 12 articles), to thesis. Thus, a little number of scientific articles on Information Security are employed as basis to the researches. The Table 10 shows the most referred categories employed.

**Table 10** – Categories of references and number of times they were employed.

Category of Reference	Number
Books	151
Articles issued in scientific journals	126
Articles issued in scientific conferences annals	79
Technical standards	39
Websites	27
Chapters of a book	19
Laws and legal regulation	18
Dissertations	18
Thesis	12
Others	19
TOTAL	508

Source: data gathered by the authors.

Our analysis showed the authors individually most referred are Marcos Sêmola and Viswanath Venkatesh, each one mentioned in six articles (see Table 11). The six mentions to Venkatesh are related to six different articles. The six Sêmolas's references are related to the first edition of his book *Gestão da Segurança da Informação: uma visão executiva*, published in 2003.

The Table 12 shows the 21 journals that have been referred at least twice. You can note that 14 of the magazines the most referred do not have a Qualis for the Administration field. Among those which have a Qualis appreciation, three have A2, another three have B1, and one has B5. Seven journals are Brazilian and 14 are international. Among the eight most referred at least three times, two are Brazilian and have a Qualis evaluation for Administration. The journal most referred, *Computers & Security*, do not have a Qualis for Administration, perhaps because this magazine has not published a Brazilian paper in the field. The same happens with the two magazines in the second place, each one having five mentions: *Information & Management* and *IEEE Security & Privacy*. the unique international journal with Qualis in the Management field is *IEEE Latin America Transactions*, which accepts papers in Portuguese language. The other journals having Qualis are all Brazilian. It reveals that most of Brazilian papers are written in Portuguese and addressed to the Brazilian public. It needs a control check like this with international journals. The Brazilian journals most referred are *JISTEM* and *Ciência da Informação*, both having a Qualis B1 in Administration field, but only the first one is specialized in Information Systems.

**Table 11** – The most referred authors.

Author	Number
Marcos Sêmola	6
Viswanath Venkatesh	6
Anatalia S. M. Ramos	5
Carmem L. I. Grisci	5
Daniel Villafranca	5
Luis E. Sánchez	5
Mario Piattini	5
Edison L. G. Fontes	4
Eduardo Fernández-Medina	4
Fred D. Davis	4
José Claudio C. Terra	4
Abner da Silva Netto	3
Adriana Beal	3
Andreas Ekelhart	3
Barry J. Babin	3
Edgar R. Weippl	3
Gurpreet Dhillon	3
James Backhouse	3
Joseph F. Hair, Jr.	3
Nicola Guarino	3
Robert K. Yin	3
Stefan Fenz	3
Thomas H. Davenport	3
Chun Wei Choo	3
Rafael Espin	3
Nilton S. Moreira	3
Rossouw Von Solms	3
Adolfo Vanti	3

Source: data gathered by the authors.

**Table 12** – The most referred scientific journals.

Journals	Qualis	Number
Computers & Security	-	9
Information & Management	-	5
IEEE Security & Privacy	-	5
JISTEM	B1	4
<i>Ciência da Informação</i>	B1	4
Information Management & Computer Security	-	4
MIS Quarterly	-	3
Communications of the ACM	-	3
RAE	A2	2
RAC	A2	2
IEEE Latin America Transactions	A2	2
<i>Perspectivas em Ciência da Informação</i>	B1	2
<i>Parcerias Estratégicas</i>	B5	2
The Journal of Information and Knowledge Management Systems	-	2
Management Science	-	2
Information Systems Research	-	2
IEEE Software	-	2
Decision Sciences	-	2
<i>Arquivística.net</i>	-	2
Information Systems Control Journal	-	2
Journal of the American Society for Information Science and Technology	-	2

Source: data gathered by the authors.

## 5. CONCLUSION

Most articles have a maximum of three authors and are about Information Security in health institutions, IT companies, public archives, and public organizations, but no articles in banks, research institutions or e-commerce were found. The most common approach is qualitative and the method is case study, which confirms the tendency recently observed in other studies on Information Systems. We did not identify scientific articles among the most mentioned references. The books are the category most referred in the analyzed articles. Many authors and journals referred are not Brazilian. The journals most referred do not have a Qualis evaluation by CAPES for Administration field.

A little number of analyzed journals has published articles on Information Security with a social approach, but the number of studies is increasing. This paper also confirmed the importance of technical standards, the most used models to analyze Information Security phenomena and the most mentioned references in the articles. Social theories, which are employed in many social sciences studies, have not been identified in the analyzed articles. It confirms the statement of several authors who recommends studies on basis of such theories.

This work permitted to analyze the Brazilian scientific production on Information Security with a social approach from 2004 to 2013. The analysis is restricted to the Brazilian production, which is a limitation of this study. Consequently, is recommended a research on the scientific production about Information Security with international journals. It can orientate new studies and therefore to promote the development of more researches on this topic, mainly through a social point of view.

## REFERENCES

- Albuquerque Junior, A. E., & Santos, E. M. (2013). Produção Científica sobre Segurança da Informação em Anais de Eventos da ANPAD. *Proceedings of Encontro de Administração da Informação da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, Bento Gonçalves, RS, Brazil, 4.
- Albuquerque Junior, A. E., & Santos, E. M. (2014). Produção Científica sobre Segurança da Informação em Eventos Científicos Brasileiros. *Proceedings of International Conference on Information Systems and Technology Management*, São Paulo, SP, Brazil, 11.
- 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, Universidade de São Paulo, São Paulo, SP, Brazil.
- Almeida Junior, J. R., Camargo Junior, J. B. & Cugnasca, P. S. (2013). Safety and Security in Critical Applications and in Information Systems – a Comparative Study. *IEEE Latin America Transactions*, 11(4), 1127-1133.
- Almeida, M. B., Souza, R. R., & Coelho, K. C. (2010). Uma Proposta de Ontologia de Domínio para Segurança da Informação em Organizações: descrição do estágio terminológico. *Informação & Sociedade*, 20(1), 155-168.
- Ang, W. H., Lee, Y., Madnick, S., Mistress, D., Siegel, M., Strong, D. M., Wang, Y. R., & Yao, Y. (2006). House of Security: Locale Roles and Resources for Ensuring Information Security. *Proceedings of Americas Conference on Information Systems*, Acapulco, México, 12.
- Araújo, W. J., & Amaral, S. A. (2010). Gestão da Segurança do Conhecimento: uma proposta de modelo. *Informação & Sociedade*, 20(2), 91-103.
- Araújo, W. J. (2012). Leis, Decretos e Normas sobre Gestão da Segurança da Informação nos Órgãos da Administração Pública Federal. *Informação & Sociedade*, 22, 13-24.
- Associação Brasileira de Normas Técnicas (2005). *NBR ISO/IEC 27002: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação*. Rio de Janeiro: ABNT.
- Associação Brasileira de Normas Técnicas (2006). *NBR ISO/IEC 27001: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos*. Rio de Janeiro: ABNT.
- Associação Brasileira de Normas Técnicas (2008). *NBR ISO/IEC 27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação*. Rio de Janeiro: ABNT.
- Barbosa Neto, J. E., & Colauto, R. D. (2010). Teoria institucional: Estudo bibliométrico em anais de congressos e periódicos científicos. *ConTexto*, 10(18), 63-74.
- Beal, A. (2005). *Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações*. São Paulo: Atlas.
- 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, EUA, 37.
- Björck, F. (2005). *Discovering Information Security Management*. Doctoral thesis, Stockholm University, Stockholm, Sweden.

- Breternitz, V. J., Navarro Neto, F., & Navarro, A. F. (2009). Gerenciamento de Segurança Segundo ITIL: Um Estudo de Caso em uma Organização Industrial de Grande Porte. *RESI*, 8(2).
- Chiesa, C. D., Zingano, E. D., & Grisci, C. L. I. (2013). Modos de Controle em uma Empresa de Segurança Cibernética. *Revista Gestão e Tecnologia*, 13(1), 230-257.
- Coles-Kemp, L. (2009). Information Security Management: An entangled research challenge. *Information Security Technical Report*, 14(4), 181-185.
- Decreto n. 3.505, de 13 de junho de 2000 (2000). Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, DF, 2000.
- Decreto n. 4.553, de 27 de dezembro de 2002 (2002). Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Brasília, DF, 2002.
- Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.
- Dwivedi, Y. K., Wade, M. R., & Schneberger, S. L. (2012). *Information Systems Theory – Explaining and Predicting Our Digital Society*. Nova York: Springer.
- Ellwanger, C., Nunes, R. C., & Rocha, R. A. (2008). O Endomarketing como Ferramenta de Gestão para a Implementação de Políticas de Segurança da Informação. *Proceedings of Encontro Nacional de Engenharia de Produção*, Rio de Janeiro, RJ, Brazil, 28.
- Fontes, E. L. G. (2006). *Segurança da Informação: O Usuário Faz a Diferença*. São Paulo: Saraiva.
- Frangopoulos, E. D., Eloff, M. M., & Venter, L. M. (2008). Social Aspects of Information Security. *Proceedings of Information Security South Africa*, Johannesburg, South Africa, 7.
- 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.
- Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*, 24(3), 246-260.
- Knorst, A. M., Vanti, A. A., Andrade, A. E. A., & Johann, S. L. (2011). Aligning Information Security with the Image of the Organization and Prioritization Based on Fuzzy Logic for the Industrial Automation Sector. *JISTEM*, 8(3), 555-580.
- Leal, R. P. C., Almeida, V. S., & Bortolon, P. M. (2013). Produção científica brasileira em Finanças no período 2000-2010. *RAE*, 53(1), 46-55.
- Lorens, E. M. (2007). *Aspectos normativos da Segurança da Informação: um modelo de cadeia de regulamentação*. Master dissertation, Universidade de Brasília, Brasília, DF, Brazil.
- Luciano, E. M., Bragança, C. E. B. A., & Testa, M. G. (2011). Privacidade de Informações de Pacientes de Instituições de Saúde: A Percepção de Profissionais da Área de Saúde. *Reuna*, 16(2), 89-102.
- Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal*, 24(3), 1-8.
- Mandarini, M. (2004). *Segurança Corporativa Estratégica*. São Paulo: Usina do Livro.
- Marciano, J. L. P., & Lima-Marques, M. (2006). O enfoque social da segurança da informação. *Ciência da Informação*, 35(3), 89-98.
- Martins, A. B., & Santos, C. A. S. (2005). Uma Metodologia para Implantação de um Sistema de Gestão de Segurança da Informação. *JISTEM*, 2(2), 121-136.
- Mascarenhas, A. O., & Barbosa, A. C. Q. (2013). Produção científica brasileira em Gestão de Pessoas no período 2000-2010. *RAE*, 53(1), 35-45.
- Mazzon, J. A., & Hernandez, J. M. C. (2013). Produção científica brasileira em Marketing no Período 2000-2009. *RAE*, 53(1), 67-80.
- 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.
- Moreira, N. S. (2001). *Segurança Mínima: Uma visão corporativa da Segurança de Informações*. Rio de Janeiro: Axcel Books.
- Morgan, G. (1996). *Imagens da Organização*. São Paulo: Atlas.
- Mota, A. F., & Marques, E. V. (2013). Governança da Tecnologia da Informação: Um estudo bibliométrico no período de 2007 a 2012. *Proceedings of Encontro de Administração da Informação da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, Bento Gonçalves, RS, Brazil, 4.
- 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. *Proceedings of Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, Rio de Janeiro, RJ, Brazil, 34.
- Nobre, A. C. S., Ramos, A. S. M., & Nascimento, T. C. (2011). Adoção de Práticas de Gestão de Segurança da Informação: Um Estudo com Gestores Públicos. *Reuna*, 16(4), 95-113.

- Pacheco, F. (2013). The Need for Formal Education on Information Security. *IEEE Latin America Transactions*, 11(1), 668-670.
- Paiva, E. L., & Brito, L. A. L. (2013). Produção científica brasileira em Gestão de Operações no período 2000-2010. *RAE*, 53(1), 56-66.
- Potrich, A. C. G., Vieira, K. M., & Nunes, R. C. (2013). Gestão da Segurança da Informação: Caracterização da Incubadora Tecnológica de Santa Maria. *GEINTEC*, 3(2), 167-185.
- Posthumus, S., & Von Solms, R. (2004). A Framework for the Governance of Information Security. *Computers & Security*, 23(8), 638-646.
- PriceWaterhouseCoopers (2013). *Pesquisa Global de Segurança da Informação 2013*. Recuperado em 01 de abril, 2014, de [http://www.pwc.com.br/pt\\_BR/br/estudos-pesquisas/assets/pesquisa-seguranca-informacao-13.pdf](http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets/pesquisa-seguranca-informacao-13.pdf)
- Rigon, E. A., & Westphall, C. M. (2013). Modelo de Avaliação da Maturidade da Segurança da Informação. *RESI*, 12(1).
- Roque, A. S., Nunes, R. C., & Silva, A. D. (2010). Proposição de um Modelo Dinâmico de Gestão de Segurança da Informação para Ambientes Industriais. *RESI*, 9(2).
- Rossoni, L., & Hocayen-da-Silva, A. J. (2007). Administração da Informação: A Produção Científica Brasileira entre 2001 e 2006. *Proceedings of Encontro de Administração da Informação da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, Florianópolis, SC, Brazil, 1.
- Sánchez, L. E., Olmo, A. S., Álvarez, E., Medina, E. F., & Piattini, M. (2012). LOPD Compliance and ISO 27001 Legal Requirements in the Health Sector. *IEEE Latin America Transactions*, 10(3), 1824-1837.
- Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3), 122-131.
- Sêmola, M. (2003). *Gestão da Segurança da Informação: uma visão executiva*. Rio de Janeiro: Campus.
- Sêmola, M. (2014). *Gestão da Segurança da Informação: uma visão executiva* (2a ed.). Rio de Janeiro: Campus.
- Sfreddo, J. A., & Flores, D. (2009). O controle de acesso na percepção dos profissionais de arquivo: uma questão de segurança das informações institucionais. *Perspectivas em Ciência da Informação*, 19(2), 121-140.
- Sfreddo, J. A., & Flores, D. (2012). Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais. *Perspectivas em Ciência da Informação*, 17(2), 158-178.
- Silva, D. R. P., Stein, L. M. (2007). Segurança da Informação: uma reflexão sobre o componente humano. *Ciências & Cognição*, 10, 43-56.
- Silva Netto, A., & Silveira, M. A. P. (2007). Gestão da Segurança da Informação: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas. *JISTEM*, 4(3), 375-397.
- Sobral, F. J. B. A., & Mansur, J. A. (2013). Produção científica brasileira em Comportamento Organizacional no período 2000-2010. *RAE*, 53(1), 21-34.
- Souza, M. T. S., Ribeiro, H. C. M., Machado Júnior, C., & Corrêa, R. (2011). Perfil e Evolução da Pesquisa em Sustentabilidade Ambiental: uma Análise Bibliométrica. *Proceedings of Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, Rio de Janeiro, RJ, Brazil, 35.
- Teixeira Junior, F. (2002). Análise dos métodos de pesquisa utilizados em artigos de Administração da Informação: Levantamento de artigos publicados nos ENANPADs de 1999 a 2001. *Proceedings of Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, Salvador, BA, Brazil, 26.
- Van Der Leeden, K. (2010). *Security without risk? Investigating information security among Dutch universities*. Master dissertation, University of Twente, Enschede, Holland.
- Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371-376.
- Wilson, T. (2009). Security Pros Shift Attention From External Hacks to Internal Threats. *DarkReading*, 09 mar. 2009. Recuperado em 01 de abril, 2014, de <http://www.darkreading.com/vulnerability/reports-security-pros-shift-attention-fr/215801195>
- Yin, R. K. (2005). *Estudo de Caso: Planejamento e Métodos*. Porto Alegre: Bookman.
- Zimmer, M. V., Ferreira, L., & Hoppen, N. (2007). Validação e Confiabilidade em Pesquisas na Área de Sistemas de Informação: uma Análise dos Artigos Publicados no Enanpad entre 1998 e 2006. *Proceedings of Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, Rio de Janeiro, RJ, Brazil, 31.