ANÁLISE DE TRATAMENTO DA SEGURANÇA DA INFORMAÇÃO DE UMA INSTITUIÇÃO DE ENSINO PÚBLICO FEDERAL

ANÁLISIS DEL TRATAMIENTO DE SEGURIDAD DE LA INFORMACIÓN DE UNA INSTITUCIÓN FEDERAL DE EDUCACIÓN PÚBLICA

INFORMATION SECURITY TREATMENT ANALYSIS ON A FEDERAL PUBLIC EDUCATION INSTITUTION

Jackson Gomes Soares SOUZA[1]
Carlos Hideo ARIMA[2]
Francisco Rolfsen BELDA[3]

RESUMO: A Tecnologia da Informação (T.I.) e sua governança estão cada vez mais presentes no desenvolvimento das instituições educacionais, aprimorando estratégias e objetivos institucionais. O presente trabalho tem por objetivo verificar o tratamento dado à segurança da informação dentro da gestão de riscos na governança de T.I.. Trata-se de uma pesquisa exploratória quantitativa, com estudo de caso de uma instituição de ensino público federal desenvolvido por meio de questionários abertos e fechados para levantamento e análise de aspectos da gestão de riscos. A partir dos dados analisados, observou-se que os componentes verificados possuem aplicação na instituição, permitindo melhorias na implementação e manutenção de princípios, compreensão do ambiente de riscos no qual opera e oportunidades que este oferece.

PALAVRAS-CHAVE: Educação. Segurança da informação. Gestão de riscos. Governança de T.I.

***RESUMEN**: La Tecnología de la Información (T.I.) y su gobernanza están cada vez más presentes en el desarrollo de las instituciones educativas, mejorando las estrategias y los objetivos institucionales. Este trabajo tiene por objeto verificar el tratamiento que se da a la seguridad de la información compreendida em la gestíon de riesgos de la governanza de T.I.. Es una investigación mixta, con un estudio de caso de una institución educativa pública federal contemplando cuestionarios abiertos y cerrados para estudiar y analizar aspectos de la gestión de riesgos. A partir del análisis de los datos, se observó que los componentes verificados tienen aplicación en la institución, permitiendo mejorar la aplicación y el*

[1] Federal Institute of Education, Science and Technology of São Paulo (IFSP), Campinas - SP - Brazil. Professor of Computer Science. Doctoral student in School Education (UNESP). ORCID: https://orcid.org/0000-0003-4952-8618. E-mail: jackson@ifsp.edu.br
[2] Paula Souza State Center for Technological Education (CEETEPS), São Paulo - SP - Brazil. Professor of the Professional Master's Degree Program in Productive Systems and Researcher of the Post-Graduation Unit of Paula Souza State Center. Doctorate in Controllership and Accounting. ORCID: https://orcid.org/0000-0001-7922-0943. E-mail: charima@uol.com.br
[3] São Paulo State University (UNESP), Bauru - SP - Brazil. Professor in the Communication Department. Doctorate in Production Engineering (EESC-USP). ORCID: https://orcid.org/0000-0001-6350-7026. E-mail: belda@faac.unesp.br

mantenimiento de los principios, la comprensión de los riesgos que asume y las oportunidades que ofrece.

***PALABRAS CLAVE**: Educación. Seguridad de la Información. Gestión de riesgos. Gobernanza de T.I.*

***ABSTRACT**: Information Technology (I.T.) and its governance are increasingly present in educational institutions development by improving strategies and objectives. This study aims to verify how is information security processed through risk management within I.T. governance. As a mixed exploratory research, this study was developed in a federal public education institution through questionnaires for data survey and analysis regarding information security practices within I.T. governance. Data analysis suggests that the verified components are applicable to the institution, allowing improvements on principles implementation and maintenance by awareness of the risk environment and the opportunities it offers.*

***KEYWORDS**: Education. Information security. Risk management. I.T. governance.*

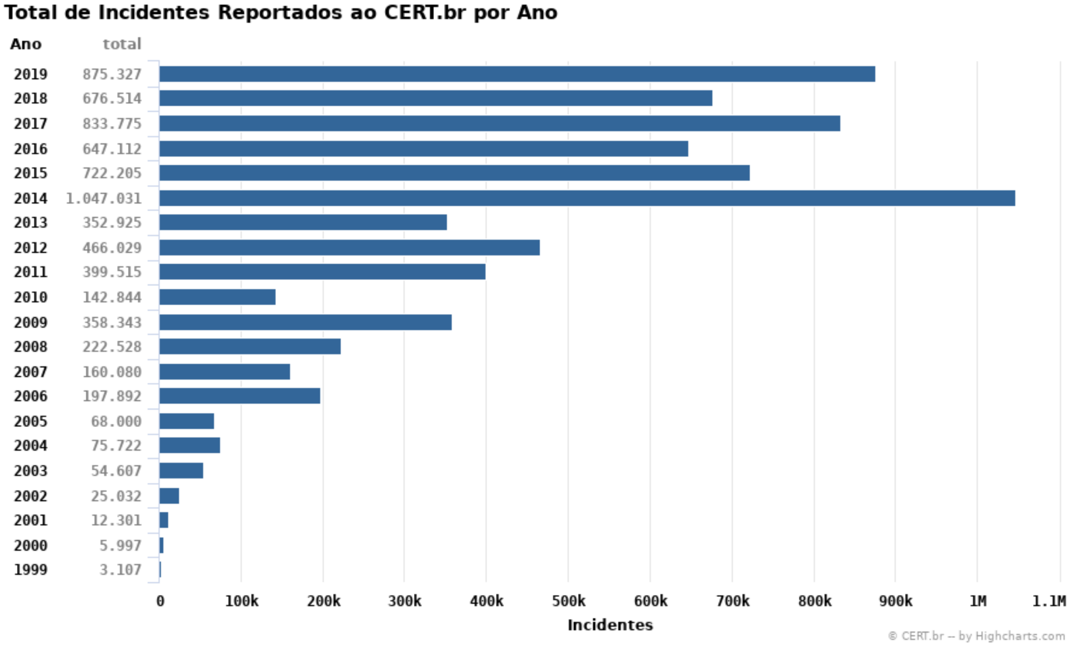
Introdução

Since the massification of their use, computational systems have brought several solutions and, among them, the possibility to improve processes and offer new opportunities in educational institutions. In addition, the interaction between humans and these systems bring concepts such as computational thinking, information security and privacy involved in this process.

According to Araújo (2012), actions for information security have been practiced since remote times. Singh (2001) presents several situations in human history when describing efforts to protect or find information. News about leaks of confidential information can be found in the reports of Ribeiro (2007) - information from contributors to the Brazilian IRS databases - or in O Globo (2012) - information from a CPI (Parliamentary Commission of Inquiry) conducted in the Federal Senate (ARAÚJO, 2012).

The Center of Studies, Response and Treatment of Security Incidents in Brazil maintains statistics on voluntary and spontaneous notifications of incidents occurring in networks reported to it. Figure 1 illustrates the attacks registered in the period 1999 to 2019 (CERT.BR, 2020).

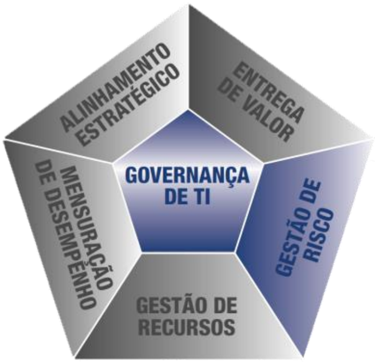
Figure 1 - Incidents reported per year



Source: CERT.BR (2020)

According to the IT Governance Institute - ITGI (2007), IT governance consists of leadership aspects, structure and processes, so that the Information Technology area supports and improves the organizational goals and strategies. Besides these characteristics, it integrates and institutionalizes good practices, enabling organizations to better use their information assets, maximizing benefits, capitalizing on opportunities and gaining competitive advantage. Figure 2 illustrates the areas of focus that contributes to the transparency of I.T. costs, value and risks, according to the *Control Objectives for Information and Related Technology* (COBIT) model, version 4.1.

Figure 2 - Areas of focus on I.T. governance



Source: ITGI (2007, p. 8)

The Information Technology (IT) governance of public educational institutions deals, within risk management, with the information security policy, working on several types of critical information directly related to the business, such as academic information from students or administrative staff that influence its continuity (BRAZIL, 2018). Thus, this research aims to analyze, by means of a case study, the treatment given to information security within the management of risks in I.T. governance and according to the managers of the rectory of the Federal Institute of Education, Science and Technology of São Paulo (IFSP).

Theoretical foundation

The production of new knowledge through the use of technologies is a reality that confronts traditional education and that, by introducing new computational tools, can generate controversy among educators who already have an established method to teach. Moreover, the I. T. implementation has generated new opportunities to produce knowledge in education, since it forces the human being to expand his exploratory potential, allowing an effective decision making at different educational levels. (PÚBLIO JÚNIOR, 2018).

In this environment, I.T. governance consists of aspects of organizational structure and processes that ensure that the I.T. area aggregates value, supports and improves objectives and strategies. Therefore, it is the field capable of enabling the organization the best way to use information assets in a secure way, preserving their confidentiality, integrity, authenticity and availability in order to maximize benefits, opportunities and competitive capacity.

In order to integrate the main assets or resources of corporate governance and I.T. governance, Weill and Ross (2004) propose the model contemplating the relations of the board of directors and the executive team as agents that articulate strategies, being also presented in the studies of Weill and Woodham (2002) that the governance of I.T. cannot be considered in an isolated way, since it is related to the governance of other assets of the company that, in turn, are linked to corporate governance. They also highlight five main decisions to be taken involving I.T. and contemplating principles, architecture, infrastructure, applications and investment prioritization.

Given these decisions and seeking to align decisions, Weill and Ross (2004) adapted a value creation model aimed at managers of public organizations, since the very concept of value in the public environment is extremely broad, and abilities, the concept of value and the environment in which these organizations operate create challenges for I.T. governance. The complexities and risks to be measured can address performance, transparency, investment in infrastructure, freedom of action, cost reduction and others.

Risk management can be seen as a holistic activity involving all aspects of the organization. The management process seeks to provide, in a solid way, the basis so that it is possible to determine the level of acceptance of risks, what opportunities they offer and how to obtain the information necessary for their proper treatment.

Information security, in turn, deals with the protection of information systems and unauthorized access, use, disclosure, interruption, modification or destruction, while also preserving confidentiality, integrity/authenticity and availability of information. The objective is to mitigate risks and protect information from threats that have a negative impact on business continuity and, ultimately, to maximize return on investments and business opportunities (DA VEIGA; MARTINS, 2015).

The approach in Table 1, initially proposed by Tudor (2000), contemplates an information security architecture to protect the assets of an organization (DA VEIGA; ELOFF, 2007).

Table 1 - Principles of Information Security Architecture

1. **Security organization and infrastructure**: Roles played by people and responsibilities are defined and support by executive management is established..
2. **Security policies, norms and procedures**: Policies, norms and procedures are developed.
3. **Security program**: An information security program is organized taking into account risk management.
4. **Training and awareness of the safety culture**: Users are trained and there is a reflection of awareness in the various activities developed. There is trust between users, management and third parties.
5. **Adequacy**: There is an internal and external control of information security.

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

Methodological procedures

The research carried out in this paper can be classified as quantitative and, according to the general objective, descriptive and exploratory, based on a logical process of inductive research that explores, describes and then generates theoretical perspectives (SAMPIERI; COLLADO; LUCIO, 2006).

As Yin (2001) points out, the case study is an empirical inquiry that investigates contemporary phenomena inserted in some real life context, allowing the use of evidence sources, such as direct observation and interviews, using protocols (LAKATOS, 2003).

The steps developed in this paper include reviewing the literature related to corporate governance, information technology governance, risk management and information security in order to establish the research object.

In addition, information security aspects within I.T. governance were quantitatively analyzed, data collected through case study protocol; tabulated, data collected and information security application examined at the Federal Institute of Education, Science and Technology of São Paulo.

Quantitative study

In order to verify the treatment given to information security, through risk management within the I.T. governance of the institution under study, risk management aspects involving the principles of security organization and infrastructure were analyzed (Dimension 1); security policies (Dimension 2), norms and procedures; security program (Dimension 3); training and awareness of security culture (Dimension 4); adequacy (Dimension 5).

These principles can be seen as dimensions of information security architecture, allowing questions to be raised in accordance with Frame 1, whose more detailed relationship between information security architecture and authors is presented in a previously published study (SOUZA *et al.,* 2019).

Frame 1 - Construction of the relationship between dimensions and closed questionings

Dimensions	Questionings
D1 **Security and infrastructure organization** **Questions:** **01 e 02**	In terms of information security, are the roles played by people defined?
	In terms of information security, are the people' responsibilities defined?
D2	Are information security policies developed?

Security policies, norms and procedures **Questions:** **03, 04 e 05**	Are information security norms developed?
	Are information security procedures developed?
D3 **Security Program** **Question:** **06**	Is an information security programme organised with risk management in mind?
D4 **Security culture training and awareness** **Questions:** **07 e 08**	Are users trained and aware of the importance of information security?
	Is there a positive reflection of this awareness?
D5 **Adequacy** **Question:** **09 e 10**	Is there internal control of information security through audits?
	Is there an external control of information security through audits?

Source: Elaborated by the authors

The collection instrument used at this stage was a closed-structured questionnaire composed of 10 questions - elaborated according to the information security architecture and authors described in Frame 1 - classified on a scale from 1 ("I completely disagree") to 6 ("I completely agree"), whose chart is shown in Figure 3.

The quantitative analyses are in item 4 and the data were collected through a digital questionnaire, applied with the help of the *Google Forms* platform and data sheets.

Results analysis

The data presentation used in this case study, as well as the results obtained, was due to the development of a descriptive structure, aiming at a better organization. The results were analyzed according to the data obtained from the questions applied during the first semester of 2016, contemplating the managers of the three I.T. areas of the institution - Systems; Infrastructure and Networks; and that of Support.

Profile of the interviewees

Frame 2 – Profile of the interviewees

Managers	Time management	Education	Age range
A	up to 2 years	Postgraduate (Extension)	40
B	up to 3 years	Postgraduate (Extension)	20
C	up to 3 years	Master's Degree	30
D	up to 1 years	Postgraduate (Extension)	20
E	up to 3 years	Postdoctoral	40

Fonte: Resultado da Pesquisa.

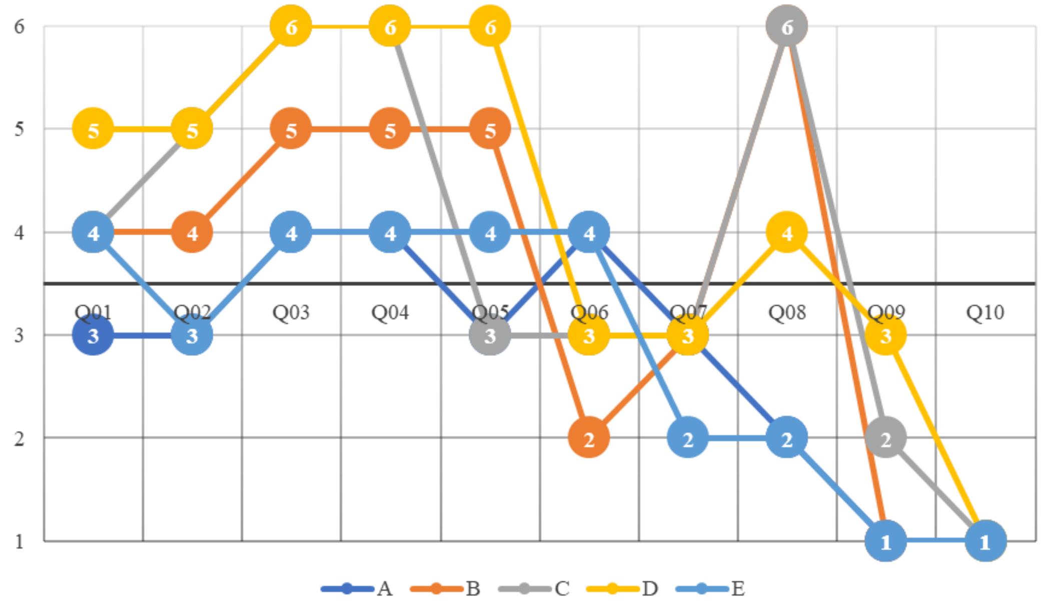
Quantitative data analysis

The data obtained is represented in Figure 3, and contains a total of 10 questions listed from Q01 to Q10, classified as 1 ("I strongly disagree") to 6 ("I strongly agree") and divided into 5 dimensions: security organization and infrastructure (Q01 and Q02), security policies, norms and procedures (Q03, Q04 and Q05), security program (Q06), security culture training and awareness (Q07 and Q08), and finally, adequacy (Q09 and Q10).

The answers regarding dimension D1, as far as safety and infrastructure organization are concerned (Q01 and Q02), show little variation and, according to the managers, people understand and play their roles, as far as safety is concerned, in a satisfactory way, as well as have their responsibilities defined, but there is room for improvement.

With regard to the D2 dimension of security policies, norms and procedures (Q03, Q04 and Q05), despite the small variation presented regarding security procedures, the responses indicate a greater agreement that these are developed, as well as an agreement that there are established policies and norms.

Figure 3 - Line chart contemplating the responses of managers



Source: Research Results

It is observed, on the other hand, that despite the same variation, the answers of the interviewees, regarding dimensions D3 (security program - Q06), D4 (training and awareness of the security culture - Q07 and Q08) and D5 (adequacy - Q09 and Q10), are presented with greater intensity in the disagreement range.

Nevertheless, as presented in Frames 3 and 4, the analysis of the answers per manager and per research question that present a high coefficient of variation indicates that they may have a relationship with the profile of the interviewees presented in Frame 2.

Frame 3 - Mean (M), standard deviation (D.P.) and coefficient of variation (C.V.) per manager

		M	**D.P.**	**C.V.**
Managers	**A**	2,8	1,1	40,55%
	B	3,6	1,8	49,34%
	C	3,9	1,8	45,95%
	D	4,2	1,7	40,16%
	E	2,9	1,3	44,37%

Source: Research Results

Frame 4 also contains the mean, standard deviation and coefficient of variation of responses per research question and highlights questions related to the safety program (D3), training and security culture awareness (D4) and adequacy (D5), which presented mean below 4 or very high coefficient of variation.

Frame 3 - Mean (M), standard deviation (D.P.) and coefficient of variation (C.V.) of the structured questionnaire

	Research questions									
	D1		**D2**			**D3**	**D4**		**D5**	
	01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**
M	4,0	4,0	5,0	5,0	4,2	3,2	2,8	4,0	1,6	1,0
D.P.	0,7	1,0	1,0	1,0	1,3	0,8	0,4	2,0	0,9	0,0
C.V.	17,7%	25,0%	20,0%	20,0%	31,0%	26,1%	16,0%	50,0%	55,9%	0,0%

Source: Research Results

Analyzing these results, it shows that:

- **Dimension 3** - Security programme: the answers to question 6, although converging, give an average of 3.2 regarding the organisation of the information security programme that takes risk management into account.
- **Dimension 4** - Training and awareness of security culture: the answers to question 07, although convergent, have an average of 2.8 and allow us to verify that the respondents disagree that there is an effective application of training and awareness of users regarding information security. The answers to question 08, on the other hand, present a standard deviation of 2.0 and a coefficient of variation of 50%, values that indicate divergences among respondents that there is a positive reflection of user awareness. Nevertheless, these values may be related to elements not addressed at this stage of the survey.
- **Dimension 5** - Adequacy: the answers to question 09, besides being divergent, have an average of 1.6, indicating low internal control through audits. Finally, regarding question 10, all respondents attributed the lowest possible value (1.0), indicating that they totally disagree with the application of an external control through audits.

The aforementioned points did not allow a clear understanding of the factors that influenced the responses obtained regarding the security program (D3), security culture training and awareness (D4) and adequacy (D5).

Final considerations

According to the results obtained, it is initially verified that the analyzed aspects of information security risk management, involving principles such as security and infrastructure organization, policies, security programs, training, awareness and adequacy, are convergent and refer to a concern on the part of the institution with the risk environment in which it operates.

According to managers, people tend to understand and play their roles, as well as have their responsibilities defined. The institution develops security procedures, as well as establishes internal policies and standards, which help to adequately identify and report risk and can thus be used as a basis for decision making.

Although security incidents and breaches are monitored and investigated - even in a punctual way - for improvements, managers tend to disagree that there is a security programme or information classification method that takes risk management into account and is considered to be based on legislation, tacit knowledge, experience and observations.

As for training and raising users' awareness of the information security culture, managers tend to disagree that users are trained and made aware of the importance of information security, diverging from each other that there is a positive reflection.No que se refere à adequação, os gestores tendem a discordar de que o controle interno por meio de auditorias é presente e discordam totalmente de que haja um controle externo de segurança da informação.

Finally, there is room for improvement applications - especially with regard to the safety program, information security awareness through training, risk assessments, technical controls and adequacy - which could help the institution to understand the risk environment in which it operates and the opportunities it offers.

REFERENCES

ARAÚJO, W. J. Leis, Decretos e normas sobre gestão da segurança da informação nos órgãos da administração pública federal. **Informação & Sociedade: Estudos**, João Pessoa, v. 22, p.

13-24, 2012. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/13675. Acesso em: 04 mar. 2020.

BRASIL. Ministério da Educação. **Portal da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo**. Brasília, DF: Senado Federal. Disponível em: http://ti.ifsp.edu.br/. Acesso em: 10 nov. 2018.

CERT.BR. **Total de incidentes reportados ao CERT.br por ano**. Brasília: Comitê Gestor da Internet no Brasil. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 04 mar. 2020.

DA VEIGA, A.; ELOFF J. H. P. An information security governance framework. **Information Systems Management**, África do Sul, 2007, p. 13.

DA VEIGA, A.; MARTINS, N. Information security culture and information protection culture: A validated assessment instrument. **Computer Law & Security Review**, v. 31, n. 2, p. 243-256, abr. 2015.

ITGI. **COBIT 4.1**: Objetivos de controle para informações e tecnologias correspondentes. Rolling Meadows: IT Governance Institute, 2007, p. 212.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. São Paulo: Atlas, 2003.

PÚBLIO JÚNIOR, C. O docente e o uso das tecnologias no processo de ensinar e aprender. **Revista Ibero-Americana de Estudos em Educação**, v. 13, n. 3, p. 1092-1105, jul./set. 2018. Disponível em: https://periodicos.fclar.unesp.br/iberoamericana/article/view/11190. Acesso em: 04 mar. 2020.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. P. B.. **Metodología de la Investigación**. 4. ed. Cidade do México: Mac Graw Hill, 2006, p. 736.

SINGH, S. **O livro dos códigos:** a ciência do sigilo o do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.

SOUZA, J. G. S., *et al*. Análise de políticas e segurança da informação na governança de tecnologia da informação de instituições públicas de ensino. *In*: XIV EIDE - ENCONTRO IBEROAMERICANO DE EDUCAÇÃO, 2019, Araraquara. **Anais**[...]. Araraquara: UNESP/FCLAr, 2019.

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

WEILL, P.; ROSS, J. W. **IT governance: how top performers manage IT decisions rights for superior results**. Boston: HBS Press, 2004.

WEILL, P.; WOODHAM, R. Don’t Just Lead, Govern: implementing effective IT governance. **Center For Information Systems Research**, Massachusetts, n. 326, abr. 2002.

How to reference this article

SOUZA, Jackson Gomes Soares; ARIMA, Carlos Hideo; BELDA, Francisco Rolfsen. Análise de tratamento da segurança da informação na gestão de riscos da governança de tecnologia da informação de uma instituição de ensino público federal. **Revista Ibero-Americana de Estudos em Educação**, Araraquara, v. 15, n. 3, p. 1309-1321, jul./set. 2020. e-ISSN: 1982-5587. DOI: https://doi.org/10.21723/riaee.v15i3.13584

Submitted on: 19/11/2019
Revisions required: 20/12/2019
Approved on: 29/01/2020
Published: 20/02/2020