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

[1] Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), Campinas - SP - Brasil. Docente do curso de Informática. Doutorando em Educação Escolar (UNESP). ORCID: https://orcid.org/0000-0003-4952-8618. E-mail: jackson@ifsp.edu.br

[2] Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS), São Paulo - SP - Brasil. Professor Doutor do Programa de Mestrado Profissional em Sistemas Produtivos e Pesquisador da Unidade de Pós-Graduação do Centro Paula Souza. ORCID: https://orcid.org/0000-0001-7922-0943. E-mail: charima@uol.com.br

[3] Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP), Bauru - SP - Brasil. Professor do Departamento de Comunicação Social. Doutor em Engenharia de Produção (EESC-USP). ORCID: https://orcid.org/0000-0001-6350-7026. E-mail: belda@faac.unesp.br

***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.*

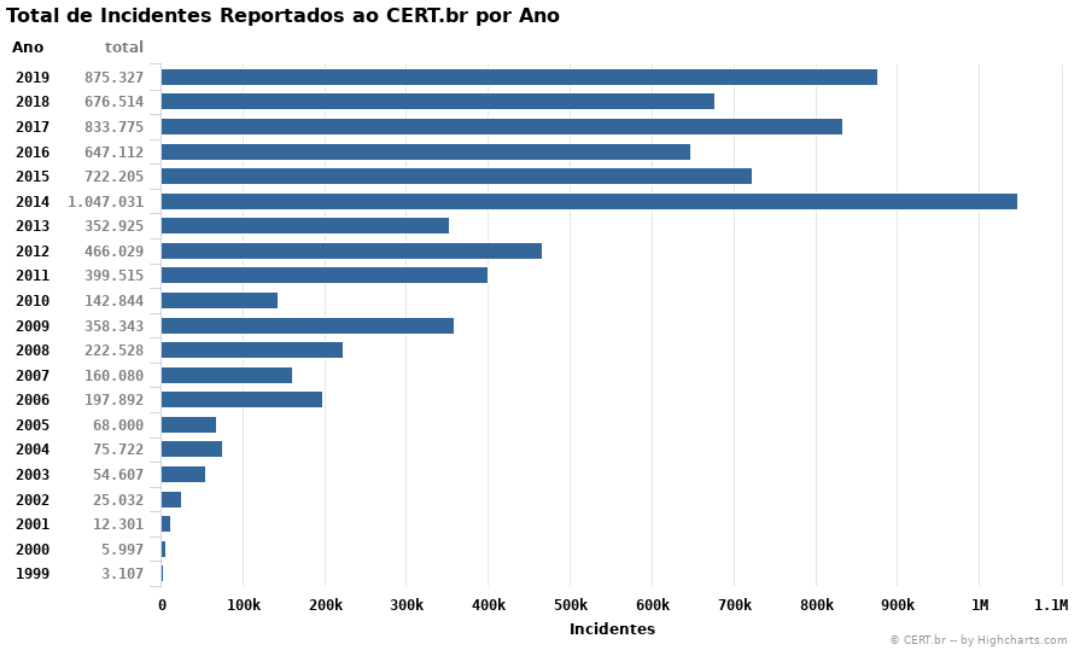
Introdução

Desde a massificação de sua utilização, os sistemas computacionais trouxeram diversas soluções e, entre elas, a possibilidade de aprimorar processos e oferecer novas oportunidades em instituições educacionais. Além disto, a interação entre humanos e estes sistemas trazem consigo conceitos como o pensamento computacional, a segurança da informação e a privacidade envolvidos neste processo.

Segundo Araújo (2012), ações para segurança da informação são praticadas desde tempos remotos. Singh (2001) apresenta várias situações na história da humanidade ao descrever esforços para proteger ou encontrar informações. Notícias sobre vazamento de informações sigilosas podem ser constatadas nos relatos de Ribeiro (2007) – informações de contribuintes da base dados da Receita Federal do Brasil – ou em O Globo (2012) – informações de uma CPI (Comissão Parlamentar de Inquérito) conduzida no Senado Federal (ARAÚJO, 2012).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil mantém estatísticas sobre notificações voluntárias e espontâneas de incidentes ocorridos em redes a ele reportados. A Figura 1 ilustra os ataques registrados no período 1999 a 2019 (CERT.BR, 2020).

Figura 1 – Incidentes reportados por ano



Fonte: CERT.BR (2020).

Segundo o Instituto de Governança de TI – ITGI (2007), a governança de T.I. consiste em aspectos de liderança, estrutura e processos, para que a área de tecnologia da informação suporte e aprimore os objetivos e estratégias organizacionais. Além dessas características, integra e institucionaliza boas práticas, habilitando as organizações para melhor utilizarem seus ativos de informação, maximizando benefícios, capitalizando oportunidades e adquirindo vantagem competitiva. A Figura 2 ilustra as áreas de foco que contribuem para que haja transparência dos custos, do valor e dos riscos de T.I., conforme o modelo de Objetivos de Controle para Informação e Tecnologias Relacionadas (*Control Objectives for Information and Related Technology – COBIT*), versão 4.1.

Figura 2 – Áreas de foco na governança de T.I.

Fonte: ITGI (2007, p. 8).

A governança de Tecnologia da Informação (T.I.) de instituições públicas de ensino trata, dentro da gestão de risco, da política de segurança da informação, trabalhando diversos tipos de informações críticas diretamente relacionadas ao negócio, como informações acadêmicas dos alunos ou administrativas que influenciam em sua continuidade (BRASIL, 2018). Deste modo, esta pesquisa tem como objetivo analisar, por meio de um estudo de caso, o tratamento dado à segurança da informação dentro da gestão de riscos na governança de T.I. e segundo os gestores da reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP).

Fundamentação teórica

A produção de novos conhecimentos por meio do uso de tecnologias é uma realidade que confronta a educação tradicional e que, ao introduzir novas ferramentas computacionais, pode gerar controvérsia entre educadores que já possuem um método estabelecido para ensinar. Ademais, a implementação da T.I. gerou novas oportunidades para produzir conhecimento na educação, visto forçar o ser humano a ampliar seu potencial exploratório, permitindo uma tomada de decisão efetiva em diferentes níveis educacionais. (PÚBLIO JÚNIOR, 2018).

Neste ambiente, a governança de T.I. consiste em aspectos de estrutura organizacional e processos que asseguram que a área de T.I. agregue valor, dê suporte e aprimore objetivos e estratégias. Portanto, é o campo capaz de habilitar a organização a melhor forma de utilizar ativos de informação de forma segura, preservando sua confidencialidade, integridade, autenticidade e disponibilidade, a fim de maximizar benefícios, oportunidades e capacidade competitiva.

De forma a integrar os principais ativos ou recursos de governança corporativa e governança de T.I., Weill e Ross (2004) propõem o modelo contemplando as relações da diretoria e a equipe executiva como agentes articuladores de estratégias, sendo também apresentado nos estudos de Weill e Woodham (2002) que a governança de T.I. não pode ser considerada de forma isolada, pois se relaciona com a governança de outros ativos da empresa que, por sua vez, estão interligados à governança corporativa. Destacam ainda cinco principais decisões a serem tomadas envolvendo T.I. e contemplando princípios, arquitetura, infraestrutura, aplicações e priorização de investimentos.

Diante dessas decisões e buscando alinhar decisões, Weill e Ross (2004) adaptaram um modelo de criação de valor voltado a gerentes de organizações públicas, uma vez que o

próprio conceito de valor no ambiente público é extremamente amplo, e as habilidades, o conceito de valor e o ambiente no qual atuam essas organizações criam desafios para a governança de T.I. As complexidades e riscos a serem mensuradas podem abordar performance, transparência, investimento em infraestrutura, liberdade de atuação, redução de custos e outros.

A gestão de risco pode ser vista como uma atividade holística que envolve todos os aspectos da organização. O processo de gestão busca fornecer, de forma sólida, a base para que seja possível determinar o nível de aceitação dos riscos, quais oportunidades estes oferecem e como obter informações necessárias para seu devido tratamento.

A segurança da informação, por sua vez, lida com a proteção dos sistemas de informação e do acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados, preservando, também, a confidencialidade, integridade/autenticidade e disponibilidade de informações. O objetivo é mitigar riscos e proteger a informação das ameaças que têm impacto negativo sobre a continuidade do negócio e, em última instância, maximizar o retorno sobre investimentos e oportunidades de negócios (DA VEIGA; MARTINS, 2015).

A abordagem da Tabela 1, proposta inicialmente por Tudor (2000), contempla uma arquitetura de segurança da informação para proteger os ativos de uma organização (DA VEIGA; ELOFF, 2007).

Tabela 1 – Princípios da Arquitetura de Segurança da Informação

1. **Organização de segurança e infraestrutura**: Papéis desempenhados pelas pessoas e responsabilidades são definidas e o suporte por parte da gerência executiva é estabelecido.
2. **Políticas de segurança, normas e procedimentos**: Políticas, normas e procedimentos são desenvolvidos.
3. **Programa de segurança**: Um programa de segurança da informação é organizado tendo em conta a gestão de riscos.
4. **Treinamento e conscientização da cultura de segurança**: Os usuários são treinados e há reflexo da conscientização nas diversas atividades desenvolvidas. Há confiança entre os usuários, a gerência e os terceiros.
5. **Adequação**: Existe um controle interno e externo da segurança da informação.

Fonte: Tudor (2000), adaptado por Da Veiga e Eloff (2007).

Procedimentos metodológicos

A pesquisa realizada neste trabalho pode ser classificada como quantitativa e, segundo o objetivo geral, descritiva e exploratória, baseada em um processo lógico de investigação indutivo que explora, descreve e, em seguida, gera perspectivas teóricas (SAMPIERI; COLLADO; LUCIO, 2006).

Conforme salienta Yin (2001), o estudo de caso é uma inquirição empírica que investiga fenômenos contemporâneos inseridos em algum contexto da vida real, permitindo a utilização de fontes de evidências, como a observação direta e entrevistas, utilizando protocolos (LAKATOS, 2003).

As etapas desenvolvidas neste estudo englobam revisar a literatura relacionada à governança corporativa, governança de tecnologia da informação, gestão de risco e segurança da informação no sentido de estabelecer o objeto de pesquisa.

Além disso, foram analisados quantitativamente aspectos da segurança da informação dentro da gestão de risco dentro na governança de T.I., levantados dados por meio de protocolo do estudo de caso; tabulados, analisados os dados coletados e examinada a aplicação de segurança da informação no Instituto Federal de Educação, Ciência e Tecnologia de São Paulo.

Estudo quantitativo

Para verificar o tratamento dado à segurança da informação, por meio da gestão de riscos dentro da governança de T.I. da instituição em estudo, foram analisados aspectos da gestão de risco que envolvem os princípios de organização de segurança e infraestrutura (Dimensão 1); políticas de segurança (Dimensão 2), normas e procedimentos; programa de segurança (Dimensão 3); treinamento e conscientização da cultura de segurança (Dimensão 4); adequação (Dimensão 5).

Estes princípios podem ser vistos como dimensões da arquitetura de segurança da informação, permitindo que sejam levantados questionamentos conforme Quadro 1, e cuja relação mais detalhada entre a arquitetura de segurança da informação e autores é apresentada em estudo anteriormente publicado (SOUZA *et al.*, 2019).

Quadro 1 – Constructo da relação entre as dimensões e questionamentos fechados

Dimensões	Questionamentos
D1 **Organização de segurança e infraestrutura** **Questões:** **01 e 02**	No que tange à segurança da informação, os papéis desempenhados pelas pessoas são definidos?
	No que tange à segurança da informação, as responsabilidades das pessoas são definidas?
D2 **Políticas de segurança, normas e procedimentos** **Questões:** **03, 04 e 05**	São desenvolvidas políticas de segurança da informação?
	São desenvolvidas normas de segurança da informação?
	São desenvolvidos procedimentos de segurança da informação?
D3 **Programa de segurança** **Questão:** **06**	Um programa de segurança da informação é organizado tendo em conta a gestão de riscos?
D4 **Treinamento e conscientização da cultura de segurança** **Questões:** **07 e 08**	Os usuários são treinados e conscientizados quanto à importância da segurança da informação?
	Há reflexo positivo dessa conscientização?
D5 **Adequação** **Questões:** **09 e 10**	Existe um controle interno da segurança da informação por meio de auditorias?
	Existe um controle externo da segurança da informação por meio de auditorias?

Fonte: Elaborado pelos autores.

O instrumento de coleta utilizado nesta etapa foi um questionário estruturado fechado, composto por 10 perguntas – elaboradas conforme a arquitetura de segurança da informação e autores descritos no Quadro 1 –, classificadas em uma escala de 1 (“discordo completamente”) a 6 (“concordo completamente”), cujo gráfico encontra-se na Figura 3.

As análises quantitativas encontram-se no item 4 e os dados foram coletados por meio de um questionário digital, aplicado com auxílio da plataforma *Google Forms* e planilhas de dados.

Análise de resultados

A apresentação de dados utilizada neste estudo de caso, assim como a dos resultados obtidos, deu-se pelo desenvolvimento de uma estrutura descritiva, objetivando melhor organização. Os resultados foram analisados conforme os dados obtidos dos questionamentos aplicados durante o primeiro semestre de 2016, contemplando os gestores das três áreas de T.I. da instituição – Sistemas; Infraestrutura e Redes; e a de Suporte.

Perfil dos entrevistados

Quadro 2 – Perfil dos entrevistados

Gestores	Tempo de gestão	Escolaridade	Faixa etária
A	até 2 anos	Pós-graduação (Extensão)	40
B	até 3 anos	Pós-graduação (Extensão)	20
C	até 3 anos	Mestrado	30
D	até 1 ano	Pós-graduação (Extensão)	20
E	até 3 anos	Pós-doutorado	40

Fonte: Resultado da Pesquisa.

Análise quantitativa de dados

Os dados obtidos estão representados na Figura 3, e contêm um total de 10 questões enumeradas de Q01 a Q10, classificadas de 1 (“discordo totalmente”) a 6 (“concordo totalmente”) e divididas em 5 dimensões: organização de segurança e infraestrutura (Q01 e Q02), políticas de segurança, normas e procedimentos (Q03, Q04 e Q05), programa de segurança (Q06), treinamento e conscientização da cultura de segurança (Q07 e Q08) e, por fim, adequação (Q09 e Q10).

As respostas referentes à dimensão D1, quanto à organização de segurança e infraestrutura (Q01 e Q02), apresentam poucas variações e, segundo os gestores, as pessoas entendem e desempenham seus papéis, no que diz respeito à segurança, de maneira

satisfatória, assim como têm suas responsabilidades definidas, havendo, porém, margem para melhorias.

No que se refere à dimensão D2, de políticas de segurança, normas e procedimentos (Q03, Q04 e Q05), apesar da pequena variação apresentada quanto aos procedimentos de segurança, as respostas indicam maior concordância de que estes são desenvolvidas, assim como concordam que há políticas e normas estabelecidas.

Figura 3 – Gráfico de linhas contemplando as respostas dos gestores

Fonte: Resultado da Pesquisa.

Observa-se, por outro lado, que apesar da mesma variação, as respostas dos entrevistados, no que diz respeito às dimensões D3 (programa de segurança – Q06), D4 (treinamento e conscientização da cultura de segurança – Q07 e Q08) e D5 (adequação – Q09 e Q10), apresentam-se com maior intensidade na faixa de discordância.

Não obstante, conforme apresentado nos Quadros 3 e 4, a análise das respostas por gestor e por questão de pesquisa que apresentam coeficiente de variação elevado indica que podem ter relação com o perfil dos entrevistados apresentado no Quadro 2.

Quadro 3 – Média (M), desvio padrão (D.P.) e coeficiente de variação (C.V.) por gestor

		M	D.P.	C.V.
Gestores	**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%

Fonte: Resultado da pesquisa

O Quadro 4 contém, ainda, a média, desvio padrão e coeficiente de variação das respostas por questão de pesquisa e destaca questões relativas ao programa de segurança (D3), treinamento e conscientização da cultura de segurança (D4) e adequação (D5), que apresentaram média inferior a 4 ou coeficiente de variação muito elevado.

Quadro 4 – Média (M), desvio padrão (D.P.) e coeficiente de variação (C.V.) do questionário estruturado

	Questões de pesquisa									
	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%

Fonte: Resultado da pesquisa

Analisando estes resultados, verifica-se que:

- **Dimensão 3** – Programa de segurança: as respostas da questão 6, apesar de convergentes, apresentam média de 3,2 quanto à organização do programa de segurança da informação que leve em conta a gestão de riscos.
- **Dimensão 4** – Treinamento e conscientização da cultura de segurança: as respostas da questão 07, apesar de convergentes, apresentam média de 2,8 e permitem verificar que os respondentes discordam de que haja uma aplicação

eficaz de treinamentos e conscientização dos usuários quanto à segurança da informação. Já as respostas da questão 08 apresentam desvio padrão de 2,0 e coeficiente de variação 50%, valores que indicam divergências entre os respondentes de que haja reflexo positivo da conscientização dos usuários. Apesar disso, esses valores podem estar relacionados a elementos não abordados nesta etapa da pesquisa.

- **Dimensão 5** – Adequação: as respostas da questão 09, além de estarem divergentes, apresentam média de 1,6, indicando um baixo controle interno por meio de auditorias. Por fim, quanto à questão 10, todos os respondentes atribuíram o menor valor possível (1,0), indicando que discordam totalmente de que haja aplicação de um controle externo por meio de auditorias.

Os pontos supracitados não permitiram uma clara compreensão dos fatores que influenciaram as respostas obtidas quanto ao programa de segurança (D3), ao treinamento e conscientização da cultura de segurança (D4) e à adequação (D5).

Considerações finais

Conforme os resultados obtidos, verifica-se inicialmente que os aspectos analisados da gestão de riscos de segurança da informação, envolvendo princípios como organização de segurança e infraestrutura, políticas, programas de segurança, treinamento, conscientização e adequação, são convergentes e remetem à uma preocupação, por parte da instituição, com o ambiente de risco em que esta opera.

Segundo os gestores, as pessoas tendem a compreenderem e desempenharem seus papéis, assim como terem suas responsabilidades definidas. A instituição desenvolve procedimentos de segurança, assim como estabelece políticas e normas internas, o que auxilia para que o risco seja adequadamente identificado e reportado, podendo, assim, ser utilizado como base na tomada de decisões.

Apesar das incidências e violações de segurança serem monitoradas e investigadas – mesmo que de forma pontual –, para que melhorias sejam aplicadas, os gestores tendem a discordar de que haja um programa de segurança ou um método de classificação das informações que leva em conta a gestão de riscos, sendo o mesmo considerado como algo baseado na legislação, conhecimentos tácitos, experiências e observações.

Quanto ao treinamento e conscientização de usuários acerca da cultura de segurança da informação, os gestores tendem a discordar de que usuários são treinados e conscientizados quanto à importância da segurança da informação, divergindo entre si de que haja um reflexo positivo.

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.

Verifica-se, por fim, que há margem para aplicações de melhorias – especialmente no que tange ao programa de segurança, conscientização de segurança da informação por meio de treinamentos, avaliação de riscos, controles técnicos e adequação – que poderiam auxiliar a instituição a compreender o ambiente de risco no qual opera e as oportunidades que este oferece.

REFERÊNCIAS

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.

Como referenciar este artigo

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

Submetido em: 19/11/2019
Revisões requeridas: 20/12/2019
Aprovado em: 29/01/2020
Publicado em: 20/02/2020