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

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

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 comprendida en la gestión de riesgos de la gobernanza 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 de la carrera de Informática. Estudiante de Doctorado en Educación 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. Profesor Doctor del Programa de Maestría Profesional en Sistemas Productivos e Investigador de la Unidad de Posgrado del 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. Profesor del Departamento de Comunicación Social. Doctor en Ingeniería de Producción (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.*

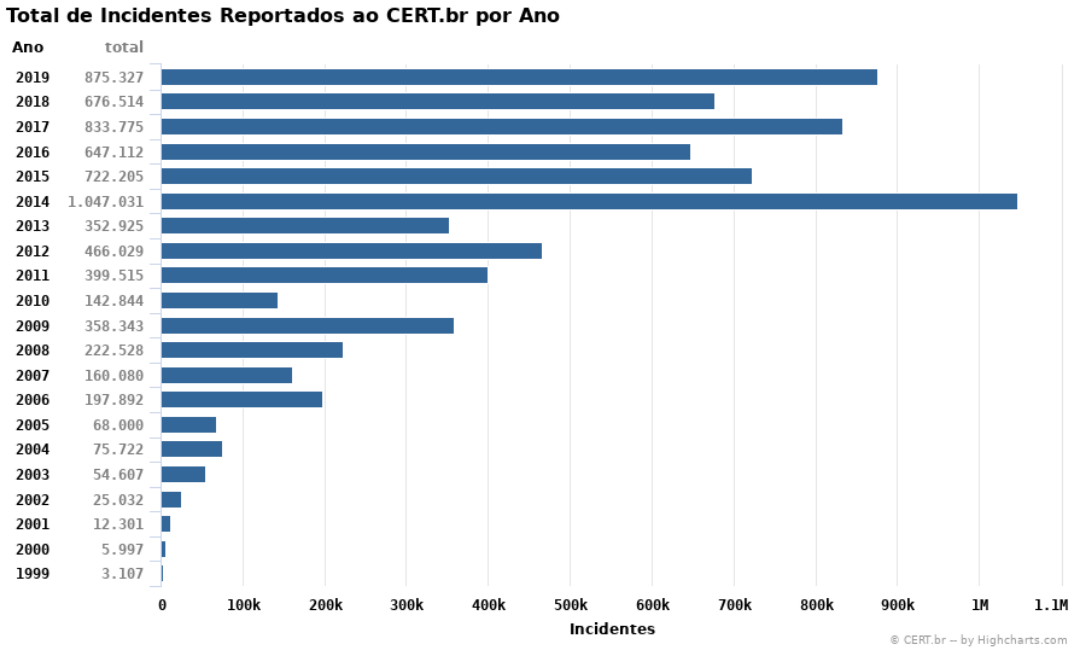
Introducción

Desde la masificación de su utilización, los sistemas computacionales han traído soluciones y, entre ellas, la posibilidad de primorear procesos y ofrecer nuevas oportunidades en instituciones educacionales. Además de eso, la interacción entre humanos y estos sistemas conllevan conceptos como el pensamiento computacional, la seguridad de la información y la privacidad involucrados en este proceso.

Según Araújo (2012), acciones para la seguridad de la información se practica desde hace mucho. Singh (2001) presenta varias situaciones en la historia de la humanidad al describir esfuerzos para proteger o encontrar informaciones. Noticias sobre fuga de informaciones sigilosas se pueden constatar en los relatos de Ribeiro (2007) – informaciones de contribuyentes de la base de datos de la Receta Federal de Brasil – o en O Globo (2012) – informaciones de una CPI (Comisión Parlamentaria de Investigación) conducida en el Senado Federal (ARAÚJO, 2012).

El Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil mantiene estadísticas sobre notificaciones voluntarias y espontáneas de incidentes ocurridos en redes reportadas a ellos. La Figura 1 ilustra los ataques registrados en el período 1999 a 2019 (CERT.BR, 2020).

Figura 1 – Incidentes reportados por año



Fuente: CERT.BR (2020).

Según el Instituto de Gobernanza de TI – ITGI (2007), la gobernanza de T.I. consiste en aspectos de liderazgo, estructura y procesos, para que el área de tecnología de la información soporte y perfeccione los objetivos y estrategias organizacionales. Además de esas características, integra e institucionaliza buenas prácticas, habilitando las organizaciones para mejor utilizar sus activos de información, maximizando beneficios, capitalizando oportunidades y adquiriendo ventaja competitiva. La Figura 2 ilustra las áreas de enfoque que contribuyen para que haya transparencia de los costes, del valor y de los riesgos de T. I., según el modelo de Objetivos de Control para Información y Tecnologías Relacionadas (*Control Objectives for Information and Related Technology – COBIT*), versión 4.1.

Figura 2 – Áreas de enfoque en la gobernanza de T.I.

Fuente: ITGI (2007, p. 8).

La gobernanza de Tecnología de la Información (T.I) de instituciones públicas de enseñanza trata, dentro de la gestión de riesgo, de la política de seguridad de la información, trabajando diversos tipos de informaciones críticas directamente relacionadas al negocio, como informaciones académicas de los alumnos o administrativas que influencian en su continuidad (BRASIL, 2018). De este modo, esta investigación tiene por objeto analizar, por medio de un estudio de caso, el tratamiento de datos a la seguridad de la información dentro de la gestión de los riesgos en la gobernanza de T.I. y segundo los gestores del rectorado del Instituto Federal de Educación, Ciencia y Tecnología de São Paulo (IFSP).

Fundamentação teórica

La producción de nuevos conocimientos por medio del uso de tecnologías es una realidad que confronta la educación tradicional y que, al introducir nuevas herramientas computacionales, puede generar controversia entre educadores que ya tienen un método establecido para enseñar. Además, la aplicación de la informática ha generado nuevas oportunidades para producir conocimientos en la educación, ya que obliga al ser humano a ampliar su potencial exploratorio, lo que permite una eficaz toma de decisiones en los diferentes niveles educativos. (PÚBLIO JÚNIOR, 2018).

En ese ambiente, la gobernanza de T.I. consiste en aspectos de estructura organizacional y procesos que aseguran que el área de T.I adicione valor, dé soporte y perfeccione objetivos y estrategias. Por lo tanto, es el campo capaz de habilitar la organización y mejor forma de utilizar activos de información de forma segura, preservando su confidencialidad, integridad, autenticidad y disponibilidad, con el fin de maximizar beneficios, oportunidades y capacidad competitiva.

De modo a integrar los principales activos o recursos de gobernanza corporativa y gobernanza de T.I., Weill e Ross (2004) proponen el modelo contemplando las relaciones de la dirección y el equipo ejecutivo como agentes articuladores de estrategias, siendo también presentado en los estudios de Weill y Woodham (2002) que la gobernanza de T.I. no se puede considerar de forma aislada, pues se relaciona con la gobernanza de otros activos de la empresa que, a su vez, están interrelacionados a la gobernanza corporativa. Destacan también cinco principales decisiones por toma involucrando T.I y contemplando principios, arquitectura, infraestructura, aplicaciones y priorización de investimentos.

Frente a esas decisiones y buscando alinear decisiones, Weill y Ross (2004) adaptaron un modelo de creación de valor direccionado a gerentes de organizaciones públicas, dado que

el propio concepto de valor en el ambiente público es extremadamente amplio, y las habilidades, el concepto de valor y el ambiente en el que actúan esas organizaciones crean retos para la gobernanza de T.I. Las complejidades y riesgos a ser mensurados pueden abordar performance, transparencia, investimento en infraestructura, libertad de actuación, reducción de costes y otros.

La gestión de riesgo se puede ver como una actividad holística que involucra todos los aspectos de la organización. El proceso de gestión busca fornecer, de forma sólida, la base para que sea posible determinar el nivel de aceptación de los riesgos, cuáles oportunidades ellos ofrecen y cómo obtener informaciones necesarias para su debido tratamiento.

La seguridad de la información, a su vez, lidia con la protección de los sistemas de información y del acceso, utilización, divulgación, interrupción, modificación o destruición no autorizados, preservando, también, la confidencialidad, integridad/autenticidad y disponibilidad de informaciones. El objetivo es mitigar riesgos y proteger la información de las amenazas que tienen impacto negativo sobre la continuidad del negocio y, en última instancia, maximizar el retorno sobre investimentos y oportunidades de negocios (DA VEIGA; MARTINS, 2015).

El abordaje de la Tabla 1, propuesta inicialmente por Tudor (2000), contempla una arquitectura de seguridad de la información para proteger los activos de una organización (DA VEIGA; ELOFF, 2007).

Tabla 1 – Principios de la Arquitectura de Seguridad de la Información

1. **Organización de seguridad e infraestructura**: Se definen los papeles y responsabilidad las personas desempeñan y se define el soporte por parte de la gerencia ejecutiva.
2. **Políticas de seguridad, normas y procedimientos**: Políticas, normas y procedimientos son desarrollados.
3. **Programa de seguridad**: Un programa de seguridad de la información es organizado teniendo en cuenta la gestión de riesgos.
4. **Entrenamiento y concientización de la cultura de seguridad**: Los usuarios son entrenados y hay reflejo de la concientización en las diversas actividades desarrolladas. Hay confianza entre los usuarios, la gerencia y los terceros.
5. **Adecuación**: Hay un control interno y externo de la seguridad de la información.

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

Procedimientos metodológicos

La investigación llevada a cabo en este trabajo se puede clasificar como cuantitativa y, según el objetivo general, descriptiva y exploratoria, basada en un proceso lógico de investigación inductivo que explora, describe y, a continuación, genera perspectivas teóricas (SAMPIERI; COLLADO; LUCIO, 2006).

Según señala Yin (2001), el estudio de caso es una investigación empírica que investiga fenómenos contemporáneos insertados en algún contexto de la vida real, permitiendo la utilización de fuentes de evidencias, como la observación directa y entrevistas, utilizando protocolos (LAKATOS, 2003).

Las etapas desarrolladas en este estudio abarcan revisar la literatura relacionada a la gobernanza corporativa, gobernanza de tecnología de la información, gestión de riesgo y seguridad de la información en el sentido de establecer el objeto de investigación.

Además de eso, se analizó cuantitativamente aspectos de la seguridad de la información dentro de la gestión de riesgo en la gobernanza de T.I., planteando datos por medio de protocolo de estudio de caso; tabulados, analizados los datos recopilados y examinada la aplicación de seguridad de la información en el Instituto Federal de Educación, Ciencia y Tecnología de São Paulo.

Estudio cuantitativo

Para verificar el tratamiento de los datos a la seguridad de la información, por medio de la gestión de riesgo dentro de gobernanza de T.I. de la institución en estudio, se han analizado aspectos de la gestión de riesgo que involucran los principios de organización de seguridad e infraestructura (Dimensión 1); políticas de seguridad (Dimensión 2), normas y procedimientos; programas de seguridad (Dimensión 3); entrenamiento y concientización de la cultura de seguridad (Dimensión 4); adecuación (Dimensión 5).

Estos principios se pueden ver como dimensiones de la arquitectura de seguridad de la información, permitiendo que sean levantados cuestionamientos conforme Cuadro 1, y cuya relación más detallada entre la arquitectura de seguridad de la información y autores se presenta en estudio anteriormente publicado (SOUZA *et al.*, 2019).

Cuadro 1 – Constructo de la relación entre las dimensiones y cuestionamientos cerrados

Dimensiones	Cuestionamientos
D1 Organización de seguridad e infraestructura Cuestiones: 01 e 02	En lo que respecta a la seguridad de la información, ¿se definen los roles que las personas desarrollan?
	En lo que respecta a la seguridad de la información, ¿se definen las responsabilidades de las personas?
D2 Políticas de seguridad, normas y procedimientos Cuestiones: 03, 04 e 05	¿Se desarrollan políticas de seguridad de la información?
	¿Se desarrollan normas de seguridad de la información?
	¿Se desarrollan procedimientos de seguridad de la información?
D3 Programa de seguridad Cuestión: 06	¿Se organiza a un programa de seguridad de la información, teniendo en cuenta la gestión de riesgos?
D4 Entrenamiento de concientización de la cultura de seguridad Cuestiones: 07 e 08	¿Los usuarios son entrenados y concientizados con relación a la importancia de la seguridad de la información?
	¿Hay reflejo positivo de esa concientización?
D5 Adecuación Cuestiones: 09 e 10	¿Hay un control interno de seguridad de la información por medio de auditorías?
	¿Existe un control externo de la seguridad de la información por medio de auditorías?

Fuente: Elaborado por los autores.

El instrumento de recopilación utilizado en esta etapa fue un cuestionario estructurado cerrado, compuesto por 10 preguntas – elaboradas según la arquitectura de seguridad de la información e autores descriptos en el Cuadro 1 –, clasificadas, en una escala de 1 (“no estoy acorde completamente”) a 6 (“estoy acorde completamente”), cuyo gráfico se encuentra en la Figura 3.

Los análisis cuantitativos se encuentran en el ítem 4 y los datos han sido recopilados por medio de un cuestionario digital, aplicado con auxilio de la plataforma *Google Forms* y las hojas de control de datos.

Análisis de resultados

La representación de datos utilizada en ese estudio de caso, así como a los resultados obtenidos, sucedió por el desarrollo de una estructura descriptiva, objetivando mejor organización. Los resultados han sido analizados según los datos obtenidos de los cuestionamientos aplicados durante el primer semestre de 2016, contemplando los gestores de las tres áreas de la T.I. de la institución – Sistemas; Infraestructura y Redes; y la de Soporte.

Perfil de los entrevistados

Cuadro 2 – Perfil de los entrevistados

Gestores	Tiempo de gestión	Escolaridad	Franja etaria
A	hasta 2 años	Posgrado (Extensión)	40
B	hasta 3 años	Posgrado (Extensión)	20
C	hasta 3 años	Maestría	30
D	hasta 1 año	Posgrado (Extensión)	20
E	hasta 3 años	Posgrado (Extensión)	40

Fuente: Resultado de la Investigación.

Análisis cuantitativo de datos

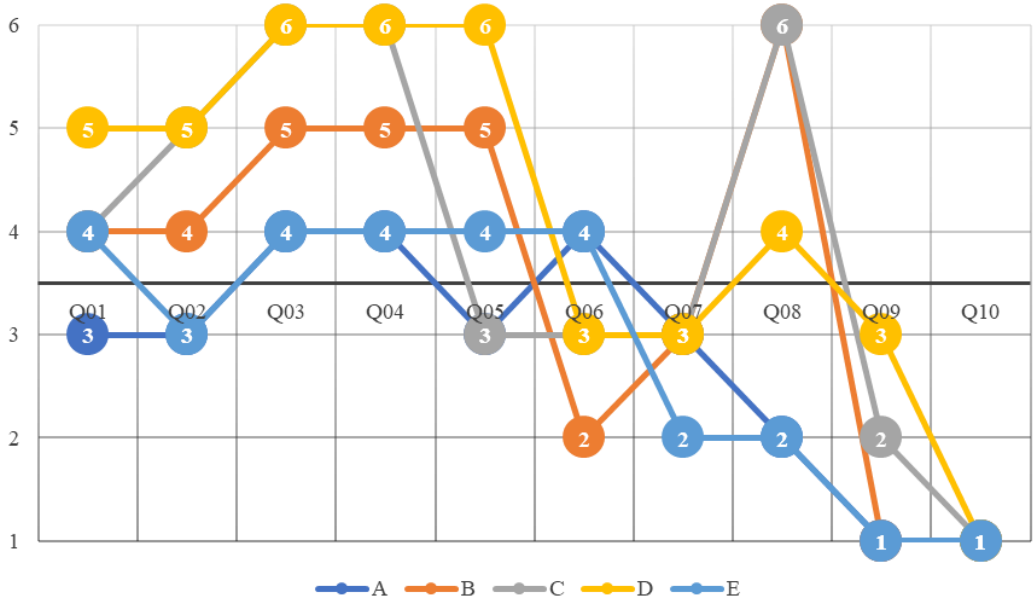
Los datos obtenidos están representados en la Figura 3 y contienen un total de 10 cuestiones enumeradas de Q01 a Q10, clasificadas de 1 (“estoy totalmente en desacuerdo”) a 6 (“estoy totalmente de acuerdo”) y dividas en 5 dimensiones: organización se seguridad e infraestructura (Q01 y Q02), políticas de seguridad, normas y procedimientos (Q03, Q04 e Q05), programas de seguridad (Q06), entrenamiento y concientización de la cultura de seguridad (Q07 e Q08) y, por fin, adecuación (Q09 e Q10).

Las respuestas referentes a la dimensión D1, con relación a la organización de seguridad e infraestructura (Q01 e Q02), presentan pocas variaciones y, según los gestores, de

modo satisfactorio, así como tienen sus responsabilidades definidas, habiendo, sin embargo, margen de mejoras.

En lo que respecta a la dimensión D2, de políticas de seguridad, normas y procedimientos (Q03, Q04 e Q05), a pesar de la pequeña variación presentada con relación a los procedimientos de seguridad, las respuestas señalan mayor concordancia que estos son desarrolladas, así como que están acorde que hay políticas y normas establecidas.

Figura 3 – Gráfico de líneas contemplando las respuestas de los gestores



Fuente: Resultado de la Investigación.

Por otro lado, se observa que, a pesar de la misma variación, las respuestas de los entrevistados, en lo que respecta a las dimensiones D3 (programa de seguridad – Q06), D4 (entrenamiento y concientización de la cultura de seguridad – Q07 y Q08) y D5 (adecuación – Q09 y Q10) se presentan con mayor intensidad en la franja de discordancia.

Sin embargo, conforme se ha presentado en los Cuadros 3 y 4, el análisis de las respuestas por gestor y por cuestión de investigación que presentan coeficiente de variación elevado señala que pueden tener relación con el perfil de los entrevistados presentado en el Cuadro 2.

Cuadro 3 – Promedio (P), desviación típica (D.T.) y coeficiente de variación (C.V.) por gestor

		P	D.T.	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%

Fuente: Resultado de la investigación

El Cuadro 4 contiene también el promedio, desviación típica y coeficiente de variación de las respuestas por cuestión de investigación y destaca cuestiones relativas al programa de seguridad (D3), entrenamiento y concientización de la cultura de seguridad (D4) y adecuación (D5), que presentaron promedio inferior a 4 o coeficiente de variación muy elevado.

Cuadro 4 – Promedio (M), desviación típica (D.P.) y coeficiente de variación (C.V.) del cuestionario estructurado

	Cuestiones de investigación									
	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%

Fuente: Resultado de la investigación

Analizando estos resultados, se verifica que:

- **Dimensión 3** –Programa de seguridad: las respuestas de la cuestión 6, a pesar de convergentes, presentan promedio de 3,2 con relación a la organización del programa de seguridad de la información que lleve en cuenta la gestión de riesgos.

- **Dimensión 4** – Entrenamiento y concientización de la seguridad: las respuestas de la cuestión 07, a pesar de convergentes, presentan promedio de 2,8 y permiten verificar que los respondientes están no están acordes que haya una aplicación eficaz de entrenamientos y concientización de los usuarios con relación a la seguridad de la información. Ya las respuestas de la cuestión 08 presentan desviación típica de 2,0 y coeficiente de variación 50%, valores que señalan divergencias entre los respondientes de que haya reflejo positivo de la concientización de los usuarios. A pesar de eso, esos valores pueden estar relacionados a elementos no abordados en esa etapa de la investigación. **Dimensión 5** – Adecuación: las respuestas de la cuestión 09, más allá de estar divergentes, presentan promedio de 1,6, señalando un bajo control interno por medio de auditorías. Por fin, con relación a la cuestión 10, todos los respondientes atribuyeron el menor valor posible (1,0) señalando que no están acordes totalmente de que haya aplicación de un control externo por medio de auditorías.

Los puntos citados anteriormente permitieron una clara comprensión de los factores que influenciaron las respuestas obtenidas con relación al programa de seguridad (D3), al entrenamiento y concientización de la cultura de seguridad (D4) y a la adecuación (D5).

Consideraciones finales

De conformidad con los datos obtenidos, se verifica inicialmente que los aspectos analizados de gestión de riesgo de seguridad de la información, involucrando principios como organización de seguridad e infraestructura, políticas, programas de seguridad, entrenamiento, concientización y adecuación, son convergentes y remeten a una preocupación, por parte de la institución, con el ambiente de riesgo en que esta trabaja.

Según los gestores, las personas tienden a comprender y desempeñar sus papeles, así como tener sus responsabilidades definidas. La institución desarrolla procedimientos de seguridad, así como establece políticas y normas internas, lo que auxilia para que el riesgo sea adecuadamente identificado y reportado, pudiendo, así, ser utilizado como base en la toma de decisiones.

A pesar de las incidencias y violaciones de seguridad ser monitoreadas e investigadas – aunque de forma puntual –, para que mejoras se apliquen, los gestores tienden a no estar

acordes que haya un programa de seguridad o un método de clasificación de las informaciones que tiene en cuenta la gestión de riesgos, siendo lo mismo considerado como algo basado en la legislación, conocimientos tácitos, experiencias y observaciones.

Con relación al entrenamiento y concientización de usuarios acerca de la cultura de seguridad de la información, los gestores tienden a no estar acordes que los usuarios son entrenados y concientizados con relación a la importancia de la seguridad de la información, divergiendo entre ellos de que haya un reflejo positivo.

En lo que respecta a la adecuación, los gestores tienden a no estar acordes que el control interno por medio de auditorías es presente y no están acordes totalmente de que haya un control externo de seguridad de la información.

Se verifica, por fin, que hay margen para aplicaciones de mejoras – especialmente en lo que respecta al programa de seguridad, concientización de seguridad de la información por medio de entrenamientos, evaluación de riesgos, controles técnicos y adecuación – que podrían auxiliar la institución a comprender el ambiente de riesgo en el cual opera y las oportunidades que este ofrece.

REFERENCIAS

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.

Cómo referenciar este artículo

SOUZA, Jackson Gomes Soares; ARIMA, Carlos Hideo; BELDA, Francisco Rolfsen. Análisis del tratamiento de seguridad de la información de una institución federal de educación pública. **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

Enviado el: 19/11/2019
Revisiones requeridas: 20/12/2019
Aprovado el: 29/01/2020
Publicado el: 20/02/2020