Revista Científica y Tecnológica UPSE, Vol. IV, N°2 Pág. 99-104 Junio

13

Seguridades de las Tecnologías de la Información (TI) en el trabajo colaborativo y su aporte a la gobernanza de TI.

Gloria Valencia V., Wendy Wasbrum T., Flor Garcès M.

Recibido: febrero 2017

Aprobado: abril 2017

Seguridades de las Tecnologías de la Información (TI) en el trabajo colaborativo y su aporte a la gobernanza de TI.
Information Technology (IT) Security in Collaborative Work and its Contribution to IT Governance.

Gloria Valencia Vivas, Wendy Wasbrum Tinoco, Flor Garcès Mancero
Unidad Académica Especial Salinas
Departamento de Seguridad y Defensa
Universidad de las Fuerzas Armadas ESPE
Av. General Rumiñahui s/n, Sangolquí-Ecuador. P.O. BOX: 171-5-231B
Escuela de Postgrado
gmvalencia@espe.edu.ec

Resumen

El ataque de amenazas en las plataformas que se manejan a través del internet en las diferentes organizaciones es cada vez más frecuente, se derivan normalmente por motivos económicos, eludiendo las medidas de seguridad comunes. Es por ello, que en este trabajo de investigación, se hace una revisión de la literatura sobre los diferentes estudios que han surgido en los últimos años abordando factores como seguridad, vulnerabilidad y mejora, con el fin de proporcionar una base para futuras investigaciones a ser utilizados en la mejora de la calidad y la seguridad en las organizaciones para contribuir con la gobernanza de las TI. Se concluye que hay una ausencia de monitoreo efectiva y escasez de la seguridades en la TI, por abaratar costos, causando la baja efectividad en las seguridades.

Palabras Claves: *Seguridades de las TI, Plataformas en la nube, Vulnerabilidad de las TI, Trabajo colaborativo*

Abstract

The attack threats on platforms that are managed through the internet in different organizations is becoming more frequent, threats are usually derived for economic reasons, avoiding common security measures. That is why, in this research, a review of the literature on the various studies that have emerged in recent years addressing factors such as security, vulnerability and improved in order to provide a basis for further research to be done used in improving the quality safety organizations and contribute to the governance of IT. Finally we conclude there is an absence of effective monitoring and lack of assurance on IT to cut costs, causing low effectiveness in securities.

Keywords: *Assurances IT, cloud platforms, IT Vulnerability, collaborative work*

I. INTRODUCCIÓN

El Internet y las tecnologías de la información han influido de manera significativa en la vida humana, sin embargo la seguridad de la información sigue siendo una preocupación importante para los usuarios y las organizaciones, coincidiendo con (Kearney & Kruger, 2016) quienes manifiestan que la seguridad en la tecnología de la información en las organizaciones es a menudo amenazada por el comportamiento de riesgo de los usuarios a pesar de los programas de sensibilización y capacitación en seguridad de la información, el aspecto humano de la información la seguridad sigue siendo un componente crítico y desafiante de un entorno de información segura y protegida, por ello (DeNardis & Hackl, 2015) revela que un área emergente de investigación es el gobierno de Internet en el ámbito académico como rol intermediario de la información privada en la promulgación de la gobernabilidad a través de las opciones de diseño técnico y de políticas de usuario en las plataformas, abordando el gobierno en medios de comunicación social, más de la gobernabilidad de los medios sociales.

Se considera que la seguridad es uno de los temas más importantes para la estabilidad y el desarrollo de estos sistemas, por lo tanto, la mayoría de las organizaciones invierten en esta zona y están estableciendo Sistemas de Gestión de Seguridad de la Información (SGSI). Información Evaluación de Riesgos de Seguridad (ISRA) es un elemento esencial

del proceso de Sistema de gestión de seguridad (ISMS). Las organizaciones necesitan ISRA para identificar los riesgos de seguridad y para ayudarles a elegir las mejores garantías para reducirlos según (Shameli-Sendia & Cherietc, 2016). El objetivo principal de este estudio es realizar una revisión de literatura de las últimas investigaciones que tratan de

En este estudio se presentan las investigaciones más recientes que abordan seguridades de la TI. En la sección (1) se presenta la introducción indicando la necesidad de las seguridades de las TI, en las organizaciones En la sección (2) se esquemaiza la revisión de la literatura. En la sección (3) se presenta el método utilizado para la realización del estudio (4) se presenta la los resultados obtenido, y por último en la sección (5) se presentan las conclusiones.

II. REVISIÓN DE LA LITERATURA

Las seguridades de las TI, más conocida como la seguridad informática, está orientada a la protección de la infraestructura computacional y todo lo que deriva de ella, de manera especial en el trabajo colaborativo aplicado de forma sincrónica o asincrónica en en ámbito académico o laboral usando herramientas tecnológicas por lo que es necesario contar con seguridad de la información siguiendo estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información de la organización, la seguridades de las TI, deben ser consideradas en software, base de datos, archivos, ,metadatos, hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial.

A. Seguridad de la TI

La necesidad de cumplir con las Seguridades de las TI, (Chunghun, Choong C, & Kim, 2016) manifiestan que los esfuerzos de las organizaciones para proteger los activos de información están obligados cada vez más por las regulaciones gubernamentales y las normas debido a las crecientes amenazas y costo de falla de seguridad.

Estos esfuerzos consisten principalmente en la introducción de nuevos esquemas técnicos y de gestión de prevención y la vigilancia del cumplimiento de los empleados con las políticas de seguridad de la información y las obligaciones técnicas más estrictas.
Para contribuir con ello (Safaa, Solmsa, & Furnella, 2016) presentan un marco conceptual que muestra cómo debe darse el cumplimiento de la política de seguridad de la información que surge en las organizaciones, considerando dos secciones principales, en la primera parte se analizan los diferentes aspectos de la participación seguridad de la información, tales como el intercambio de conocimientos seguridad de la información, la colaboración, la intervención y la experiencia, la segunda parte discute el compromiso y las normas las Seguridades de las TI en el trabajo colaborativo y su aporte en la gobernanza de TI, abordando factores como seguridad, vulnerabilidad y mejora, con el fin de proporcionar una base para futuras investigaciones a ser utilizados en mejorar la calidad , la seguridad en las organizaciones y contribuir con la gobernanza de las TI.

Tomando en cuenta que el Internet es una enorme red y tiene un gran potencial para violaciones de la seguridad de la información, ya que los hackers utilizan varios métodos para romper la confidencialidad, integridad y disponibilidad de la información, los autores consideran que el intercambio de información en conocimientos de seguridad es un método eficaz para aumentar el nivel de conciencia en la seguridad de la información.

El estudio fue aplicado cuatro empresas diferentes que habían establecido de forma adecuada las políticas de seguridad de la información a través de una encuesta, donde todos los participantes tenían acceso a Internet y trabajaban con un sistema de web en diferentes departamentos, dando como resultados reveladores, que el intercambio de información sobre conocimientos de seguridad tiene fuertes efectos sobre la actitud de cada persona hacia el cumplimiento de las políticas de seguridad de la información en las organizaciones (ISOP).

Llegando a la conclusión que Internet se ha convertido en un conducto para los servicios, aplicaciones, contenido de información y oportunidades para individuos y organizaciones. Sin embargo, la evidencia anecdótica y empírica implica que el número y la gravedad de las violaciones de seguridad de la información es cada vez mayor por la falta de apoyo para el impacto de fijación en actitudes hacia el cumplimiento de ISOP.

Este estudio puede continuar con las investigaciones sobre las diferencias en el cumplimiento con la organización información de políticas de seguridad y los procedimientos basados en el género, la edad (adolescentes, jóvenes, adultos, etc.), el nivel de la educación, el estilo de trabajo, y así sucesivamente.

B. Seguridades de la información en las plataformas de medios sociales en la nube

Según el estudio de (Yanbo, Qingfei, & Shengnan, 2016) para una mejor comprensión de las seguridades de las TI, realiza un meta análisis con el fin de generar una mejor comprensión de la confianza, el riesgo, y sus efectos en diferentes tipos de comportamientos individuales hacia las plataformas de medios sociales (SMP). Este estudio sirve para contribuir al conocimiento generalizado con respecto a la influencia de la confianza y el riesgo en el comportamiento individual hacia las SMP, basándose en 43 estudios relacionados en los sistemas de información.

Los autores concluyen en los resultados, que tanto la confianza y el riesgo tuvieron efectos significativos en el comportamiento individual hacia las SMP. Teniendo como efecto más fuerte la confianza, ya que estudios sobre privacidad de la información se centraron principalmente en las preocupaciones sobre una posible pérdida de privacidad, como resultado de la divulgación de información a los demás en SMP.

Por lo que es necesario que los profesionales deben hacer un mayor esfuerzo en la incluir los mecanismos de confianza en sus plataformas. Ellos puede concentrarse en la inclusión de una declaración sobre la política de privacidad y condiciones de garantía, certificaciones y códigos formales de conducta por ejemplo sellar marcas, o el uso de los sistemas de cifrado y digitales firmas, junto al control de las actividades de los individuos, la captura y el análisis de su retroalimentación, y la gestión de las interacciones sociales en SMP.

Este meta análisis reflejó que hay una falta de estudios sobre el cambio de comportamiento y las percepciones de riesgo en las interacciones sociales; re-buscadores pueden prestar más atención a estos conceptos. Los autores dejan abierto el camino para un estudio futuro que incluya más pruebas en las múltiples disciplinas y una visión más completa con respecto a los factores que influyen en el comportamiento individual hacia las SMP.

C. Vulnerabilidades de las seguridades en la nube

Debido a la importancia de identificar los posibles ataques en las TI. (Santosh & Sunil, 2016) realizó el estudio de las diferentes vulnerabilidades de seguridad de plataformas en la nube, centrándose en tres ejes principales: la migración de máquinas virtuales en la nube, el análisis del contexto de seguridad en la migración de Máquina virtual (VM) y (VM) planificación de la migración con respecto a la seguridad, los requisitos de capacidad, los autores realizaron una investigación sistemática para detectar los posibles ataques a varias plataformas en la nube, lo que ayudará a los desarrolladores de seguridad a diseñar una plataforma segura, clasificando de una manera generalizada como se muestra en la tabla 1, las amenazas que pueden darse en las plataformas en la nube.

Tabla 1. Amenazas a las plataformas en la nube

PLAN	ATAQUE	PLATAFORMA
Plan de Control	Negación del servicio	Xen, Virtualbox, Hyper-v
	Publicidad de recurso falsos	
	Migración de VM dañada a host legítimo	
	Diversificación de VM	Xen, Virtualbox
Plan de Datos	Ataque intermediario por el hombre	Xen, Virtualbox
	Fuga de información	
Módulo de Migración	Vulnerabilidades del software	Xen
	Ataques repetitivos	
	Enmascaramiento	

(Santosh & Sunil, 2016)

En otro estudio analizado para fundamentar esta fase (Florian, Giuseppe, & Roman, 2016) crean una concientización sobre las amenazas potenciales y los incidentes actuales, lo cual es un requisito previo para la preparación efectiva y la asistencia de incidentes a gran escala, por lo que defienden la idea que la creación de centros nacionales de seguridad cibernética coordinados centralmente es emergente en todo el mundo.

También analizaron que los centros de seguridad cibernéticos eficaces son difíciles de establecer y, a menudo ni cuerpos ni las empresas gubernamentales y organizaciones de clientes están bien preparados para funcionar y el uso ellos.

Los autores llegan a determinar que aunque la configuración de tales sistemas a menudo reducen los aspectos técnicos, es un desafío significativo para los expertos legales, comités de normalización y científicos sociales, así como económicos.

D. Mejoras de seguridad de las plataformas en la nube

En este medio cambiante a nivel globalizado y sobre todo en lo tecnológico y con el fin de colaborar con la calidad de seguridad en las TI (Shameli-Sendia & Cherietc, 2016) proponen una taxonomía para enfoques de evaluación de riesgos de seguridad de información que generalmente se clasifican en cuatro categorías: La valoración, la perspectiva, la evaluación de recursos y la medición de riesgos, cuyo propósito es identificar todos los posibles riesgos para los activos y evaluar con precisión y mitigar los riesgos de manera apropiada, considerando que la relación entre la vulnerabilidad y la amenaza se define como un riesgo.

Mediante el estudio los autores creen que el análisis de riesgo de seguridad de la información debe ser más servicio o negocio orientado ya que es un proceso que

está directamente involucrado en los ingresos del negocio y luego en la evaluación de los riesgos.

La Taxonomía presentada en este trabajo es un paso hacia el logro de ISRA de alta calidad, descubrimos otros elementos importantes que deben ser considerados en la evaluación de riesgos, proporcionando a las organizaciones con una visión general de las diferentes técnicas utilizadas para evaluar los riesgos, llevando a una evaluación rigurosa y exitosa.

Los autores concluyen que este estudio de los métodos de evaluación de riesgo es importante, va a ayudar a explicar los principales problemas que surgen y poder conducir al desarrollo de más mecanismos integrales y eficaces de evaluación de riesgos. También puede ayudar a las organizaciones a encontrar el enfoque más apropiado para su evaluación de riesgos o incluso desarrollar su propia sobre la base de los enfoques disponibles.

III. MATERIALES Y MÉTODOS

Para desarrollar y mostrar los resultados del presente trabajo, se realizó mediante una revisión de literatura de la siguiente forma.

A. Búsqueda de la literatura

Para poder obtener los estudios que ayudaron a la revisión de la literatura se asistió a las diferentes bases de datos indexadas como ScienceDirect, IEEE y Google Scholar. Considerando estudios comprendidos entre año 2015 y 2016, con términos de búsqueda de Seguridad de las Tecnología de Información, Seguridad de la información en plataformas virtuales, Seguridad de la información y plataformas virtuales, seguridad de la información en el aprendizaje colaborativo, llegando a un total de 30 estudios de los cuales fueron seleccionado 8 para la elaboración de la revisión de la literatura. Para la organización de la búsqueda y llegar a los 8 estudios seleccionados, se utilizó una ficha creada por el investigador en una hoja de cálculo, donde se reflejaban los siguientes datos: (a) Base de datos,(b) Revista, (c) Titulo, (d) Objetivo de la investigación, (e)Método de estudio (f)Autor (g)Año.

B. Selección de los estudios

Para llegar hasta esta instancia se consideró los estudios que estaban ligados estrechamente con el tema del trabajo a realizar, tomando en cuenta los siguiente: (a) Búsqueda con los términos en las bases de datos, (b) Lectura de los títulos y abstracto, (c) Se procede al proceso de inclusión y exclusión, (d) Se realiza lectura de la introducción, método, discusión de resultados y conclusiones.

C. Extracción de Datos

Para la extracción de datos se utilizó una plantilla para facilitar el proceso de síntesis de los datos recogidos considerando lo siguiente: (a) Propuesta del autor, (b) Objetivo del estudio, (c) Resultados, (d) Conclusiones.

IV.APORTE A LA GOBERNANZA DE LA TI

Según, (DeNardis & Hackl, 2015) la mayoría de las organizaciones recientemete están invirtiendo en sistemas de seguridad de infomación(SGSI), gracias a los estudios realizados sobre políticas de seguridad que deben cumplir las organizaciones apegandose a las gobernazas de las TI.

V.RESULTADOS OBTENIDOS

Después de haber realizado todo el proceso metodológico para poder sustentar este estudio se obtuvo el siguiente resultado presentado en la tabla 2

Tabla 2. Resumen de resultados de estudios obtenidos

N°	TÍTULO	AUTOR Y AÑO	TEMA QUE ABORDA
E1	Understanding information security stress: Focusing on the type of information security compliance activity	L. Chunghun, L. Choong C y S. Kim 2016	Seguridad de las TI
E2	A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing	S. Florian, S. Giuseppe y F. Roman 2016	Seguridad de las TI
E3	Can perceptual differences account for enigmatic information security behaviour in an organisation?	W. Kearney y Kruger 2016	Seguridad de las TI
E4	Information security policy compliance	N. S. Safaa, R. V. Solmsa	Seguridad de las TI

	model in organizations	y S. Furnella 2016	
E5	Understanding the effects of trust and risk on individual behavior	W. Yanbo, M. Qi ngfei y H. Shengnan 2016	Vulnerabilidad de TI
E6	A Study on Security Vulnerability on Cloud Platforms,	K. M. Santosh y K. D. Sunil 2016	Vulnerabilidad de TI
E7	Taxonomy of information security risk assessment (ISRA)	A. A.-B. Shameli-Sendia y M. Cherietc 2016	Mejoras de TI
E8	Internet governance by social media platforms	L. DeNardis y A. Hackl 2015	Gobernanza de TI

Valencia, Wasbrum,Garcés (2017)

El estudio de (Chunghun, Choong C, & Kim, 2016), dan a conocer las reacciones negativas ante las seguridades de las TI, en las organizaciones analizando los diferentes aspectos de la participación de la seguridad de la información, en dos fases la primera fase, el intercambio de conocimientos seguridad de la información, la colaboración, la intervención y la experiencia, la segunda parte discute el archivo adjunto, el compromiso y las normas personales que son los otros elementos principales en SBT. Mientras que (Florian, Giuseppe, & Roman, 2016), Motivan y elaboran con más detalle los requisitos para un sistema de intercambio de información seguro. Sien embargo (Kearney & Kruger, 2016),manifiesta que la información en las organizaciones es a menudo son amenazadas por el comportamiento de riesgo de los usuarios a pesar de los programas de sensibilización y capacitación en seguridad de la información. (Safaa, Solmsa, & Furnella, 2016) conceptualizan los diferentes aspectos de la participación, tales como el intercambio de seguridad de la información del conocimiento, la colaboración, la intervención y la experiencia, así como el apego, el compromiso y las normas personales que son elementos importantes en la teoría de enlace social, mientras que (Yanbo, Qingfei, & Shengnan, 2016) en su estudio contribuye al conocimiento de la confianza y el riesgo en el comportamiento individual hacia las plataformas de medios sociales SMP. (Santosh & Sunil, 2016) clasifica los diversas vulnerabilidades de seguridad en diferentes plataformas en la nube lo ayuda a los desarrolladores de seguridad para diseñar una plataforma en la nube segura, centrándose en tres ejes principales: la migración de máquinas virtuales en la nube, el análisis del contexto de seguridad en la migración de VM y VM planificación de la migración con respecto a la seguridad, los requisitos de capacidad. (Shameli-Sendia & Cherietc, 2016). Discute las características clave de la evaluación de riesgos que deben ser incluidos en un sistema de gestión de seguridad de la información, como la esquemas técnicos y de gestión, prevención y la vigilancia del cumplimiento de las políticas de la segurdad de la información, finalmente (DeNardis & Hackl, 2015). Abordan temas de gobierno para los medios de comunicación social, más que de la gobernabilidad de los medios sociales enmarcados en Internet, estudios científicos y tecnológicos, sugiriendo que las arquitecturas técnicas de medios sociales y las políticas planteen nuevos desafíos a los derechos de comunicación.

VI. ANÁLISIS DE LOS RESULTADOS ENCONTRADOS

En la tabla 2, mostrada anteriormente se muestra los estudios revisados, que analizan las posibles causas de amenazas y proponen medidas de seguridad en las TI, encontrados en la revisión de la literatura.

En este contexto se puede apreciar que los estudios de (Florian, Giuseppe, & Roman, 2016), (Kearney & Kruger, 2016) y (Safaa, Solmsa, & Furnella, 2016) determinan que las organizaciones deben dar cumplimiento estricto a las políticas de seguridad de la información.

Los estudios de (Santosh & Sunil, 2016) y (Yanbo, Qingfei, & Shengnan, 2016) manifiestan que al cumplir y monitorear la seguridad de las TI, se contribuye a mejorar la calidad de la seguridad para desarrollar políticas y plataformas mas seguras.

Los estudios de (DeNardis & Hackl, 2015), (Florian, Giuseppe, & Roman, 2016), (Safaa, Solmsa, & Furnella, 2016), (Santosh & Sunil, 2016) y (Yanbo, Qingfei, & Shengnan, 2016), revelan que la seguridad de las TI, siguen siendo un componente crítico y desafiante de la información segura y protegida.

VII. CONCLUSIONES

Una vez culminada la investigación se llegó a las siguientes conclusiones:

1) La información obtenida en la revisión de la literatura ha reflejado las necesidades emergentes de las seguridades de las TI.
2) Al realizar el análisis de los estudios tratados revelan que existe ausencia de monitoreo efectivo y escasez de las seguridades de TI por las organizaciones.
3) Todos los autores que han sido plasmados en este estudio explican los principales problemas que surgen al no contar con buenas seguridades en las TI.

4) Los estudios tratados en esta investigación conducen al desarrollo de mecanismos más integrales y eficaces para las seguridades de TI.

REFERENCIAS

Chunghun, L., Choong C, L., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security, 59*, 60-70.

DeNardis, L., & Hackl, A. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770.

Florian, S., Giuseppe, S., & Roman, F. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security, 60*, 154-176.

Kearney, W., & Kruger, H. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security, 61*, 46-58 .

Safaa, N. S., Solmsa, R. V., & Furnella, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Santosh, K. M., & Sunil, K. D. (2016). A Study on Security Vulnerability on Cloud Platforms. *International Conference on Information Security & Privacy (ICISP2015)*. Nagpur, INDIA.

Shameli-Sendia, A. A.-B., & Cherietc, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security, 57*, 14-30.

Yanbo, W., Qingfei, M., & Shengnan, H. (2016). Understanding the effects of trust and risk on individual behavior. *Computers in Human Behavior, 56*, 34-44.