Revista Cubana de Ciencias Informáticas
Vol. 14, No. 3, Mes Julio-Septiembre, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 148-164

Tipo de artículo: Artículo de revisión
Temática: Seguridad informática
Recibido: 16/03/2020 | Aceptado: 27/05/2020

Factores que contribuyen en la pérdida de información en las organizaciones

Factors that contribute to the loss of information in organizations

Shonerly Bustamante Garcia[1*] https://orcid.org/0000-0002-8173-203X
Miguel Angel Valles Coral [1] https://orcid.org/0000-0002-8806-2892
Dany Levano Rodriguez[1] https://orcid.org/ 0000-0002-1783-1105

[1]Universidad Peruana Unión. {shonerly.bustamante, danlev} @upeu.edu.pe, mavalles@unsm.edu.pe

*Autor para la correspondencia. (shonerly.bustamante@upeu.edu.pe)

RESUMEN

Resguardar la información es garantizar su integridad, confidencialidad y disponibilidad, pero en algunos casos estas características se ven comprometidas. El objetivo de la revisión fue identificar los factores que contribuyen a la pérdida de información en las organizaciones. Para su desarrollo, se realizó una búsqueda de artículos científicos publicados en revistas indexadas a base de datos como Latindex, Scielo, Ebsco y Scopus entre los años 2016 y 2020. La revisión permitió identificar factores tales como los recursos humanos dados por empleados, ex empleados y personas ajenas a la organización; además de factores presupuestales; el poco

Revista Cubana de Ciencias Informáticas
Vol. 14, No. 3, Mes Julio-Septiembre, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 148-164

conocimiento en temas de seguridad de la información por parte de la organización; los desastres naturales y los agentes maliciosos. Se concluyó que estos factores afectan la imagen y la estabilidad de la organización, causando pérdidas económicas y de información, lo que puede incluso conducir a estas a cerrar sus operaciones.

Palabras clave: factores; seguridad; pérdida; información.

ABSTRACT

Safeguarding the information is to guarantee its integrity, confidentiality and availability, but in some cases these characteristics are compromised. The objective of the review was to identify the factors that contribute to the loss of information in organizations. For its development, we carried out a search for scientific articles published in journals indexed to databases such as Latindex, Scielo, Ebsco and Scopus between the years 2016 and 2020. The review allowed identifying factors such as human resources given by employees, former employees and people outside the organization; in addition to budget factors; the organization's little knowledge of information security issues; natural disasters and malicious agents. We concluded that these factors affect the image and the stability of the organization, causing economic and information losses, which can even lead them to close their operations.

Keywords: factors; security; lost; information.

Introducción

La información es un activo valioso para toda organización, que sirve como insumo para lograr niveles competitivos, sin embargo, por el deficiente conocimiento sobre cómo resguardarla, o por

la complejidad en la implantación de normas de seguridad, muchas organizaciones, en especial las pequeñas y medianas empresas ponen en jaque la continuidad de sus operaciones (Crespo, 2017); pues las dificultades para proteger su información, según (Díaz-Batista y Blanco-Fernández, 2018) se deben a recursos financieros insuficientes, y la formación básica del personal para desempeñar funciones complejas.

(Donalds y Osei-Bryson, 2018) señalan que los impactos financieros son considerables y están en aumento; el Foro Económico Mundial en el año 2018 dio a conocer que el 65% de las organizaciones australianas fueron víctimas de ataques informáticos, uno de cada diez reportó pérdidas superiores a $ 1 millón, y el 9% informó haber tenido su información confidencial comprometida (Wiley, McCormac y Calic, 2020).

Según el estudio de *International Information Systems Security Certification Consortium* (ISC2), señala que los frecuentes ataques que atentan contra la información, se deben básicamente a vulnerabilidades de software, malware, personal interno y hackers, los cuales acaparan alrededor del 69% del total de las incidencias de seguridad registradas (Miranda et al., 2016).

(Altamirano y Bayona, 2017) señalan que, en organizaciones de Norteamérica y Europa, el 39% de los empleados sufrieron trasgresiones de seguridad en el 2015, pues estos ataques provenían del interior de la organización, debido a la facilidad de los mismos empleados al conocer las debilidades de los sistemas informáticos y por los privilegios de accesibilidad a datos confidenciales.

Por su lado, (Sabillón y Cano, 2019) sostienen que los ataques informáticos en organizaciones británicas, estadounidenses y alemanas son considerables; el 57% han sufrido al menos uno y el 42% alrededor dos o más ataques en el 2016. De estas organizaciones un 62% recobraban sus funciones en menos de 24 horas; al 26% les tomaba menos de una hora, mientras que algunas entre dos o más días, ocasionando pérdidas económicas y hasta pérdida de información confidencial.

En América Latina, los principales ataques informáticos son dirigidos por malware destinados a robar información y los troyanos dirigidos a la estafa bancaria, pues se considera que el 92 % de las entidades financieras sufrieron un ciberataque en el 2015 (Aguilar-Antonio, 2019).

(Perdigón y Pérez, 2020) indican que los ataques informáticos son la principal amenaza de pérdida de información en entidades bancarias peruanas, pues en un reporte de Kaspersky Lab en el 2018, señala que en Perú la frecuencia de ataques aumentó en un 740%, con alrededor de 22 mil incidentes. Personal poco capacitado es otro de los causales de pérdida de información en organizaciones peruanas; (Fernández y Vargas, 2018) destacan este inconveniente en las comisarías al interior del país, donde los policías desconocen de estrategias para hacer frente a ataques informáticos de manera efectiva y garantizar el resguardo de la información.

En vista de lo anterior, la presente revisión tuvo como objetivo evaluar exhaustivamente los diferentes factores que contribuyen a la pérdida de información en las organizaciones, teniendo en cuenta evidencias empíricas en diversas partes del mundo, con la finalidad de recopilar información relevante, y generar un artículo con base científica que pueda ser de gran ayuda para que cualquier organización, tenga en cuenta y pueda implantar medidas enfocadas a estos factores, para evitar pérdidas económicas considerables o la manipulación de su información confidencial.

Metodología

Para lograr el objetivo planteado, y dar respuesta a nuestra pregunta ¿Cuáles son los factores que contribuyen a la pérdida de información en las organizaciones? se realizó una intensa revisión bibliográfica, la cual permitió identificar impactantes acontecimientos sobre pérdida de información y los factores que la originaron.

- **FASE 1:** Búsqueda de documentos

La búsqueda de documentos se realizó bajo el criterio de (Angraini, Alias y Okfalisa, 2019), quienes afirman que, para lograr un buen resultado, se tiene que realizar una revisión explícita e integral de una gran variedad de fuentes.

Revista Cubana de Ciencias Informáticas
Vol. 14, No. 3, Mes Julio-Septiembre, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 148-164

Bajo estas consideraciones, se seleccionó una base de datos como fuente principal de información, tal como Google Scholar; y para no limitar la búsqueda, el alcance se extendió a ScienceDirect. Para cada base de datos, se acondicionaron cadenas de búsqueda, con la finalidad de obtener precisión en cada consulta.

Tabla 1 - Fuentes de búsqueda.

Fuente	Palabras claves (Pc)	Cadenas de búsqueda	Notas
Google Scholar	Pc01: factores* Pc02: seguridad* Pc03: pérdida* Pc04: información* Pc05: ciberseguridad* Pc06: ataques* Pc07: organizaciones* Pc08: riesgo:	Título: ((factores*AND pérdida* AND información*) OR (ciberseguridad* AND organizaciones*) OR (riesgo* AND ataques* AND información*))	Búsqueda multidisciplinaria
Science Direct			Búsqueda multidisciplinaria

Respecto a la cadena de búsqueda, se generó mediante la combinación de las palabras claves definidas con la combinación de conectores lógicos “AND” y “OR”. Las palabras claves en base a nuestra pregunta de investigación establecida.

Dentro de los criterios de inclusión estuvieron las publicaciones realizadas entre los años 2016 hasta julio 2020, donde los tipos de documentos a considerar fueron los artículos científicos en el idioma español e inglés y publicados en revistas indexadas a Latindex, Scielo, Ebsco y Scopus.

- **FASE 2:** Lectura y análisis de los documentos

Los documentos utilizados están clasificados como artículos de revistas indexadas a las base de datos mencionadas, los cuales fueron importados a la plataforma de Mendeley Desktop, obteniéndose información relevante, tales como: título, autor(es), nombre de la revista científica,

año de publicación, volumen, número de páginas; para luego ser leídos, y subrayados las partes importantes realizando la técnica de paráfrasis para entender mejor, con lo cual se dio respuesta a la pregunta de 1a presente revisión.

Desarrollo de la revisión

Los resultados del desarrollo se organizaron en orden relacionado a los factores identificados durante la revisión, sin que necesariamente tenga relación con su ponderación.

El manejo de la información es determinante tanto para la excelencia como para la competitividad en las organizaciones, ya que su valor es fuente de conocimiento para la conducción y la toma de decisiones (Rodríguez, Mho y Ramírez, 2017).

(Szczepaniuk et al., 2020) afirman que, en toda organización, la información se encuentra en diversos formatos, no es estática, sino que se encuentra adosada a procedimientos que van sufriendo cambios, y fluye mediante medios físicos como electrónicos, para ambos medios existe posibilidad de que la información sea violentada en cualquier momento.

En los últimos 20 años, la proliferación de tecnologías de información ha brindado a personas y organizaciones nuevas oportunidades, tales como recopilar, almacenar y administrar información de manera eficiente, pero al mismo tiempo estos entornos tienen nuevos desafíos de seguridad; por lo cual merece ser gestionada de manera eficiente (Bongiovanni, 2019).

Para (Castellanos, Rodríguez y Martínez, 2017), el objetivo de la gestión de la información es ayudar a que las organizaciones puedan acceder y usar la información de manera adecuada; sin embargo, a pesar de mantener establecidos procesos de gestión de la información y niveles de seguridad, han

surgido una serie de riesgos en contra de la integridad de la información; por lo que se hace imprescindible identificar qué factores causan estos inconvenientes.

Factores que contribuyen a la pérdida de información

Recursos humanos. La información al ser considerada como activo preciado, merece ser tratada de manera cuidadosa, ya que presenta posibilidades a ser atacada por el personal trabajador en cualquier momento (Martelo, Tovar y Maza, 2018); lo peor es que, según (Meraz, 2018) los gerentes en ciertas oportunidades ignoran el uso inadecuado que se le da a la información, a esto se suma la independencia de cada trabajador en determinar el grado de privacidad. Es así, que el factor humano tiene un papel trascendental en cuanto al resguardo de información, ya que las personas son consideradas como el eslabón más débil dentro de una organización, pues causan graves pérdidas económicas y el robo de información (Altamirano y Bayona, 2017).

Empleados. (Amaro y Rodríguez, 2016) mencionan que en los años 60 se dieron los primeros ataques informáticos, donde empleados deshonestos o descontentos provocaron graves daños desde su propio lugar. IBM en su informe Índice de Inteligencia de Seguridad Cibernética en el año 2016, afirmó que el 60% de los ataques informáticos tienen un origen interno, considerando a los empleados descontentos como la principal causa, a fin de conseguir información para uso personal o simplemente desprestigiar a la organización (Schouteren, 2019).

Ex empleados. Los ataques que suceden en las organizaciones, muchas veces son causados por ex empleados disgustados, ya que cuentan con la capacidad de ingresar a los sistemas informáticos, debido a los accesos privilegiados con los que cuentan, con el objetivo de violentar la seguridad y realizar acciones indebidas, poniendo en jaque la continuidad de la organización (Sohrabi et al., 2018).

Personas ajenas a la organización. Muchos delitos informáticos son cometidos por personas desconocidas que no tienen ninguna relación con la organización, que se encargan de explotar

vulnerabilidades y logar acceder a un sistema informático (Lux, 2018), entre ellos están los hackers, lo cual (Roque y Juárez, 2018) definen como personas con alto nivel de conocimientos técnicos, que gracias al apoyo de una computadora logran ingresar a un equipo o red.

Presupuesto. (Zuña et al., 2019) indican que uno de los puntos débiles de las organizaciones es el bajo presupuesto que destinan a la seguridad de la información, pues algunas creen que es un gasto innecesario; ya que las organizaciones con limitado presupuesto, ponen en riesgo la información y tienden a tener considerables pérdidas económicas. Con restricciones presupuestales, las pequeñas y medianas empresas se encuentran en una desventaja significativa para hacer frente a ataques informáticos de forma efectiva, porque los costos que implica implantar medidas de seguridad superan sus posibilidades financieras (Benz y Chatterjee, 2020).

Conocimiento. El escaso conocimiento por parte del personal en una organización respeto a temas de seguridad, permiten mantener insuficientes controles y mecanismos de protección, para hacer frente a actividades maliciosas de manera efectiva (Castillejos, Torres y Lagunes, 2016), por lo que (Torres et al., 2017) enfatizan la importancia de la capacitación y sensibilización de los trabajadores en lo referente a seguridad, ya que esto incide en la calidad del servicio. En Ecuador, gran parte de organizaciones fueron víctimas de fraude, sabotaje y robo de información, debido al desconocimiento respecto a la manipulación, transmisión y resguardo de la información por parte del personal (Proaño y Gavilanes, 2018).

Desastres naturales. (Agwu, Labib y Hadleigh-Dunn, 2019) describió la inevitabilidad de los desastres en las organizaciones, lo cual provocan que las instalaciones y los servicios se vieran afectados; por consiguiente tienen pérdidas económicas y de información, además, señalan que la complejidad de las tecnologías y los procesos bien definidos, han evitado constantemente fallas catastróficas. (Sahi, Lai y Li, 2016) mencionan que entre los desastres naturales que atentan contra la información están los incendios, terremotos, inundaciones, huracanes y erupciones volcánicas.

Agentes maliciosos. Los agentes maliciosos dados por malware como virus, gusanos, troyanos y ransomware, que se encargan de acceder a los sistemas de información e interrumpir operaciones, con la intención de modificar su comportamiento original, realizando actividades como robo, alteración o destrucción de la información (Bander, Maarof y Syed, 2018). (Qamar, Karim y Chang, 2019) consideran que las amenazas de malware van dirigidos a dispositivos de red que ocasionan actividades dañinas, ataques de ingeniería social y causar el robo de información confidencial y en ciertos casos pérdidas económicas; por lo que obliga a las organizaciones a mejorar los niveles de seguridad (Gibert, Mateu y Planes, 2020).

En su mayoría la bibliografía consultada refiere que el factor recurso humano es el de mayor importancia, debido a que son quienes gestionan la infraestructura de tecnología que da soporte al almacenamiento de la información y contrariamente a lo que se piensa, las empresas suelen contratar a personas cuyas competencias son insuficientes para el trabajo de gestión de la seguridad a realizar. Así mismo, mencionan que buscar solución a este problema es difícil porque no solo se trata de contratar al personal más calificado, sino que además se necesita de tiempo de entrenamiento para acoplarse al equipo de trabajo y la tecnología utilizada.

Consideramos que los factores identificados, deben ser evaluados por la oficina de tecnologías de información de las organizaciones, a fin de tomar las medidas necesarias para evitar que el impacto y la prevalencia del acontecimiento no necesiten de soluciones difíciles de implantar.

Para la asignación de los niveles de impacto de cada factor, se tuvo como base los criterios de información de COBIT (Carvajal, Cardona y Valencia, 2019) y de la información recolectada, lo que nos permitió categorizar problemas y riesgos, y el resultado de los mismos dio lugar a identificar el nivel de impacto de cada factor en las diferentes áreas de las organizaciones, tal como a continuación de detalla:

Tabla 2 - Nivel de impacto de cada factor.

Revista Cubana de Ciencias Informáticas
Vol. 14, No. 3, Mes Julio-Septiembre, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 148-164

Impacto	Descripción
Alto	Afecta a la organización en: Eficacia, eficiencia, confidencialidad, integridad y disponibilidad de su información
Medio	Afecta a procesos parciales en las operaciones normales de las organizaciones.

Así mismo, teniendo en cuenta el trabajo de (Carvajal, Cardona y Valencia, 2019) en cuanto a la medición de frecuencia de COBIT y la revisión de información, determinamos la prevalencia de cada factor en las organizaciones. A continuación de describe en la tabla 3.

Tabla 3 - Prevalencia de los factores identificados.

Prevalencia	Descripción
Frecuente	Se presentaría frecuentemente afectando las operaciones de las organizaciones y a los cliente.
Poco frecuente	Se daría bajo ciertas condiciones.

Es por ello, que producto de la revisión y de los factores causantes de pérdidas de información identificados, se ha considerado definir el impacto que causarían dentro de las organizaciones, en un nivel que va desde alto a medio, así como la frecuencia y la solución requerida para cada factor, tal como a continuación se detalla en la Tabla 4.

Tabla 4 - Estimaciones de los factores en las organizaciones.

Factores	Impacto	Prevalencia	Solución
Recursos humanos	Alto	Frecuente	Difícil
Presupuesto	Medio	Poco frecuente	Difícil
Conocimiento	Medio	Frecuente	Fácil
Desastres naturales	Alto	Poco frecuente	Fácil
Agentes maliciosos	Alto	Frecuente	Fácil

A fin de realizar una evaluación sistemática, se ha elaborado la Tabla 4, en la que hacemos una estimación de los factores que se ven influenciados producto de un mal manejo de la seguridad de la información. En ese sentido, los recursos humanos es uno de los factores determinantes en la pérdida de información, que causan un alto impacto dentro de las organizaciones; considerando que las personas son una amenaza directa para la información (Kim, 2018); además, implantar soluciones desde el factor presupuesto es difícil, puesto que requiere de la asignación de dinero, que para los altos ejecutivos no es más que gastos innecesarios; a esto se suma la prevalencia frecuente del factor conocimiento por parte de los trabajadores, ya que según (Roba, Vento y García, 2016) la coyuntura actual de las organizaciones implica contratar personal con bajo conocimiento en seguridad; en tanto, otros de los factores que muestran un alto impacto son los desastres naturales y agentes maliciosos, dada la complejidad y magnitud de ocurrencia.

El Foro Económico Mundial (FEM) en el 2019, consideró que los ataques informáticos son amenazas críticas para las organizaciones y su economía, pues solo las pequeñas empresas son el objetivo de 65,000 ataques al día, con un costo promedio de 25,700 euros por año, es así que cada organización con acceso a internet debe entender que será víctima en algún momento (Nicholson, 2019).

En línea con la tabla 4, (Porras, Pastor y Alvarado, 2018) señalan que un 41% de las PYMES peruanas poseen probabilidades mínimas para la detección de ataques informáticos complejos, pues los principales motivos son en un 100% limitaciones presupuestarias, y un 89% debido a la falta de recursos especializados entre personas y tecnología.

Por lo tanto, garantizar niveles óptimos de seguridad de la información en las organizaciones depende de la implantación de un conjunto de medidas administrativas, operativas y técnicas, con un enfoque interdisciplinario (Aguilera, Pérez y Rivero, 2017); es decir, soluciones orientadas a los factores identificados, de forma que se garantice la confidencialidad, integridad y disponibilidad de la información.

Revista Cubana de Ciencias Informáticas
Vol. 14, No. 3, Mes Julio-Septiembre, 2020
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 148-164

Según (Peña y Anías, 2019), la definición de políticas de seguridad de la información en las organizaciones con un enfoque interdisciplinario entre personas y tecnología, trae mejoras considerables en el proceso del negocio, reduciendo costos y garantizando un adecuado resguardo de la información.

Conclusiones

Con el desarrollo de la revisión, se ha demostrado una deficiente gestión de la información, debido a la poca atención en el fortalecimiento de medidas preventivas para garantizar un adecuado resguardo de la misma, poniendo en evidencia factores que contribuyen a la pérdida de información en las organizaciones.

Pues estos factores repercuten gravemente en la inoperatividad de los procesos operativos, administrativos y técnicos de las organizaciones, los cuales traen consigo altas pérdidas económicas, que puede generar una crisis en la organización, y la manipulación de información, pues se estaría violando el activo más importante, afectando la imagen y estabilidad de la organización.

Por lo tanto, lograr entender los factores que contribuyen a la pérdida de información, es llegar a implantar medidas y/o controles de seguridad desde una perspectiva interdisciplinaria, es decir, generar soluciones enfocadas en las personas y los recursos tecnológicos con los que cuenta la organización, a fin de garantizar un adecuado resguardo de la información.

Referencias

AGUILAR-ANTONIO, J.-M., Hechos ciberfísicos : una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO, Revista Latinoamericana de Estudios

de Seguridad [en línea], 2019. vol. 4299, no. 25, pp. 24-40. [Consulta: 14 junio 2020]. Disponible en: doi.org/10.17141/urvio.25.2019.4007.

AGUILERA, O., PÉREZ, E. y RIVERO, R., La protección de la información. Una visión desde las entidades educativas cubanas. Ciencias de la Información [en línea], 2017. vol. 48, no. 3, pp. 41-47. [Consulta: 21 mayo 2020]. ISSN 0864-4659. Disponible en: https://www.redalyc.org/pdf/1814/181457243006.pdf.

AGWU, A., LABIB, A. y HADLEIGH-DUNN, S., Disaster prevention through a harmonized framework for high reliability organisations. Safety Science [en línea], 2019. vol. 111, pp. 1-15. [Consulta: 19 junio 2020]. ISSN 18791042. DOI 10.1016/j.ssci.2018.09.005. Disponible en: https://doi.org/10.1016/j.ssci.2018.09.005.

ALTAMIRANO, J. y BAYONA, S., Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao [en línea], 2017. no. 25, pp. 112-134. [Consulta: 29 mayo 2020]. ISSN 16469895. DOI 10.17013/risti.25.112-134. Disponible en: http://www.scielo.mec.pt/pdf/rist/n25/n25a09.pdf.

AMARO, J. y RODRÍGUEZ, C., Seguridad en internet. PAAKAT: Revista de Tecnología y Sociedad [en línea], 2016. vol. 6, no. 11, pp. 9. [Consulta: 9 junio 2020]. ISSN 2007-3607. Disponible en: http://www.scielo.org.mx/pdf/prts/v6n11/2007-1094-apertura-6-11-00006.pdf.

ANGRAINI, ALIAS, R. y OKFALISA, Information security policy compliance: Systematic literature review. Procedia Computer Science [en línea], 2019. vol. 161, pp. 1216-1224. [Consulta: 29 mayo 2020]. ISSN 18770509. DOI 10.1016/j.procs.2019.11.235. Disponible en: https://doi.org/10.1016/j.procs.2019.11.235.

BANDER, S., MAAROF, M. y SYED, M., Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers and Security [en línea], 2018. vol. 74, pp. 1-48. [Consulta: 22 junio 2020]. ISSN 01674048. DOI 10.1016/j.cose.2018.01.001. Disponible en: https://doi.org/10.1016/j.cose.2018.01.001.

BENZ, M. y CHATTERJEE, D., Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons [en línea], 2020. vol. 63, no. 4, pp. 1-10. [Consulta: 24 junio 2020]. ISSN 00076813. DOI 10.1016/j.bushor.2020.03.010. Disponible en:

https://doi.org/10.1016/j.bushor.2020.03.010.

BONGIOVANNI, I., The least secure places in the universe? A systematic literature review on information security management in higher education. Computers and Security [en línea], 2019. vol. 86, pp. 350-357. [Consulta: 9 junio 2020]. ISSN 01674048. DOI 10.1016/j.cose.2019.07.003. Disponible en: https://doi.org/10.1016/j.cose.2019.07.003.

CARVAJAL, D., CARDONA, A. y VALENCIA, F., Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. Entre ciencia e ingeniería [en línea], 2019. vol. 13, no. 25, pp. 68-76. [Consulta: 20 julio 2020]. ISSN 1909-8367. DOI 10.31908/19098367.4016. Disponible en: http://www.scielo.org.co/pdf/ecei/v13n25/1909-8367-ecei-13-25-00068.pdf.

CASTELLANOS, A., RODRÍGUEZ, Y. y MARTÍNEZ, A., Comportamiento de la producción científica en Gestión de Información, Gestión del Conocimiento e Inteligencia Organizacional en revistas brasileñas indizadas en la categoría LIS en WOS entre 2008-2014. Revista Publicando [en línea], 2017. vol. 4, no. 11(1), pp. 108-134. [Consulta: 28 mayo 2020]. Disponible en: https://revistapublicando.org/revista/index.php/crv/article/view/462/pdf_343.

CASTILLEJOS, B., TORRES, C. y LAGUNES, A., La seguridad en las competencias digitales de los millennials. Apertura [en línea], 2016. vol. 8, no. 2, pp. 54-69. [Consulta: 15 mayo 2020]. Disponible en: http://www.scielo.org.mx/pdf/apertura/v8n2/2007-1094-apertura-8-02-00054.pdf.

CRESPO, E., Una metodología para la gestión de riesgo aplicada a las MPYMES. Enfoque UTE [en línea], 2017. vol. 7, no. 1, pp. 107-121. [Consulta: 24 octubre 2019]. Disponible en: http://scielo.senescyt.gob.ec/pdf/enfoqueute/v8s1/1390-6542-enfoqueute-8-s1-00107.pdf.

DÍAZ-BATISTA, J. y BLANCO-FERNÁNDEZ, Y., Adopción y uso de las Tecnologías de la Información en organizaciones cubanas. Ingeniería Industrial [en línea], 2018. vol. 39, no. 2, pp. 273-282. [Consulta: 9 junio 2020]. ISSN 1815-5936. Disponible en: http://scielo.sld.cu/pdf/rii/v39n3/1815-5936-rii-39-03-273.pdf.

DONALDS, C. y OSEI-BRYSON, K.-M., Toward a cybercrime classification ontology: A knowledge-based approach. Computers in Human Behavior [en línea], 2018. vol. 92, pp. 1-38. [Consulta: 4 junio 2020]. ISSN 07475632. DOI 10.1016/j.chb.2018.11.039. Disponible en:

https://doi.org/10.1016/j.chb.2018.11.039.

FERNÁNDEZ, W. y VARGAS, C., ¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías. The Law, State and Telecommunications Review [en línea], 2018. vol. 10, no. 2, pp. 37-52. [Consulta: 4 junio 2020]. Disponible en: https://doi.org/10.26512/lstr.v10i2.21492.

GIBERT, D., MATEU, C. y PLANES, J., The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. Journal of Network and Computer Applications [en línea], 2020. vol. 153, pp. 1-22. [Consulta: 23 junio 2020]. ISSN 10958592. DOI 10.1016/j.jnca.2019.102526. Disponible en: https://doi.org/10.1016/j.jnca.2019.102526.

KIM, L., Concienciación en materia de ciberseguridad: protección de datos y de pacientes. Nursing (Ed. española) [en línea], 2018. vol. 35, no. 1, pp. 62-64. [Consulta: 6 junio 2020]. ISSN 02125382. DOI 10.1016/j.nursi.2018.02.017. Disponible en: http://dx.doi.org/10.1016/j.nursi.2018.02.017.

LUX, L., Elementos criminológicos para el análisis jurídico-penal de los delítos informáticos. Revista lus et Praxis [en línea], 2018. vol. 24, no. 1, pp. 159-206. [Consulta: 18 mayo 2020]. Disponible en: https://scielo.conicyt.cl/pdf/iusetp/v24n1/0718-0012-iusetp-24-01-00159.pdf.

MARTELO, R., TOVAR, L. y MAZA, D., Modelo básico de seguridad lógica . Caso de Estudio : el Laboratorio de Redes de la Universidad de Cartagena en Colombia. Informacion Tecnologica [en línea], 2018. vol. 29, no. 1, pp. 3-10. [Consulta: 7 mayo 2020]. Disponible en: http://dx.doi.org/10.4067/S0718-07642018000100003.

MERAZ, A., Empresa y privacidad : el cuidado de la información y los datos personales en medios digitales. IUS [en línea], 2018. vol. 12, no. 41, pp. 293-310. [Consulta: 10 junio 2020]. Disponible en: http://www.scielo.org.mx/pdf/rius/v12n41/1870-2147-rius-12-41-293.pdf.

MIRANDA, M., VALDÉS, O., PÉREZ, I., PORTELLES, R. y SÁNCHEZ, R., Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. Revista Cubana de Ciencias Informáticas [en línea], 2016. vol. 10, no. 2, pp. 14-26. [Consulta: 28 abril 2020]. ISSN 1994-1536. Disponible en: http://scielo.sld.cu/pdf/rcci/v10n2/rcci02216.pdf.

NICHOLSON, S., How ethical hacking can protect organisations from a greater threat. Computer Fraud and Security [en línea], 2019. vol. 2019, no. 5, pp. 15-19. [Consulta: 6 junio 2020]. ISSN 13613723. DOI 10.1016/S1361-3723(19)30054-5. Disponible en: http://dx.doi.org/10.1016/S1361-3723(19)30054-5.

PEÑA, M. y ANÍAS, C., Sistema para ejecutar políticas sobre infraestructuras de Tecnologías de la Información IT policies execution system. Revista chilena de ingeniería [en línea], 2019. vol. 27, no. 3, pp. 479-494. [Consulta: 7 julio 2020]. Disponible en: https://scielo.conicyt.cl/scielo.php?pid=S0718-33052019000300479&script=sci_arttext&tlng=e.

PERDIGÓN, R. y PÉREZ, M., Análisis holístico del impacto social de los negocios electrónicos en América Latina, de 2014 a 2019. Paakat: Revista de Tecnología y Sociedad [en línea], 2020. vol. 10, no. 18, pp. 1-23. [Consulta: 18 junio 2020]. Disponible en: http://dx.doi.org/10.32870/Pk.a10n18.459.

PORRAS, J., PASTOR, S. y ALVARADO, R., Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. Revista peruana de computación y sistemas [en línea], 2018. vol. 1, no. 1, pp. 47-56. [Consulta: 4 mayo 2020]. Disponible en: http://dx.doi.org/10.15381/rpcs.v1i1.14856.

PROAÑO, R. y GAVILANES, A., Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana. Revista Enfoque UTE [en línea], 2018. vol. 9, no. 1, pp. 90-101. [Consulta: 7 mayo 2020]. Disponible en: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-65422018000100090.

QAMAR, A., KARIM, A. y CHANG, V., Mobile malware attacks: Review, taxonomy & future directions. Future Generation Computer Systems [en línea], 2019. vol. 97, pp. 887-909. [Consulta: 23 junio 2020]. ISSN 0167739X. DOI 10.1016/j.future.2019.03.007. Disponible en: https://doi.org/10.1016/j.future.2019.03.007.

ROBA, L., VENTO, J. y GARCÍA, L., Metodología para la detección de vulnerabilidad en las redes de datos utilizando Kali-Linux. Revista Científica Avances [en línea], 2016. vol. 18, no. 5, pp. 334-344. [Consulta: 18 mayo 2020]. ISSN 0718-0764. Disponible en: http://www.ciget.pinar.cu/ojs/index.php/publicaciones/article/view/182.

RODRÍGUEZ, M., MHO, J. y RAMÍREZ, R., Infotecnología y gestión de la información en la carrera de economía. Transformación [en línea], 2017. vol. 13, no. 1, pp. 139-149. [Consulta: 1 junio 2020]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2077-29552017000100014.

ROQUE, R. y JUÁREZ, C., Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. PAAKAT: Revista de Tecnología y Sociedad [en línea], 2018. vol. 8, no. 14, pp. 13. [Consulta: 9 junio 2020]. ISSN 2007-3607. DOI 10.18381/pk.a8n14.318. Disponible en: http://www.scielo.org.mx/pdf/prts/v8n14/2007-3607-prts-8-14-00005.pdf.

SABILLÓN, R. y CANO, J., Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação [en línea], 2019. no. 32, pp. 33-48. [Consulta: 15 junio 2020]. DOI 10.17013/risti.32.33-48. Disponible en: http://www.scielo.mec.pt/pdf/rist/n32/n32a04.pdf.

SAHI, A., LAI, D. y LI, Y., Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan. Computers in Biology and Medicine [en línea], 2016. vol. 78, pp. 1-8. [Consulta: 20 junio 2020]. ISSN 18790534. DOI 10.1016/j.compbiomed.2016.09.003. Disponible en: http://dx.doi.org/10.1016/j.compbiomed.2016.09.003.

SCHOUTEREN, S., From wooden shoe to click of a button: the risk of disgruntled employees. Computer Fraud and Security [en línea], 2019. vol. 2019, no. 3, pp. 10-13. [Consulta: 15 noviembre 2019]. ISSN 13613723. DOI 10.1016/S1361-3723(19)30029-6. Disponible en: http://dx.doi.org/10.1016/S1361-3723(19)30029-6.

SOHRABI, N., MAPLE, C., WATSON, T. y VON, R., Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of Information Security and Applications [en línea], 2018. vol. 40, pp. 1-11. [Consulta: 18 junio 2020]. ISSN 22142126. DOI 10.1016/j.jisa.2017.11.001. Disponible en: https://doi.org/10.1016/j.jisa.2017.11.001.

SZCZEPANIUK, E., SZCZEPANIUK, H., ROKICKI, T. y KLEPACKI, B., Information security assessment in public administration. Computers and Security [en línea], 2020. vol. 90, pp. 1-11. [Consulta: 17 junio 2020]. ISSN 01674048. DOI 10.1016/j.cose.2019.101709. Disponible en:

https://doi.org/10.1016/j.cose.2019.101709.

TORRES, J., GALLO, J., HALLO, R., ABCARIUS, J., MURIEL, M. y FERNÁNDEZ, A., Gestión de la información como herramienta para la toma de decisiones en salud: escenarios más probables. Revista Cubana de Investigaciones Biomédicas [en línea], 2017. vol. 36, no. 3, pp. 1-10. [Consulta: 23 octubre 2019]. ISSN 0864-0300. Disponible en: http://scielo.sld.cu/pdf/ibi/v36n3/ibi10317.pdf.

WILEY, A., MCCORMAC, A. y CALIC, D., More than the individual: Examining the relationship between culture and Information Security Awareness. Computers and Security [en línea], 2020. vol. 88, pp. 1-8. [Consulta: 16 mayo 2020]. ISSN 01674048. DOI 10.1016/j.cose.2019.101640. Disponible en: https://doi.org/10.1016/j.cose.2019.101640.

ZUÑA, E., ARCE, Á., ROMERO, W. y SOLEDISPA, C., Análisis de la seguidad de la información en las pymes de la ciudad de Milagro. Revista Universidad y Sociedad [en línea], 2019. vol. 11, no. 4, pp. 487-492. [Consulta: 15 mayo 2020]. ISSN 2218-3620. Disponible en: http://scielo.sld.cu/pdf/rus/v11n4/2218-3620-rus-11-04-487.pdf.

Conflicto de interés

El artículo se encuentra público en el repositorio de la Universidad Peruana Unión como trabajo de bachiller del autor **Shonerly Bustamante Garcia.**

Los autores declaramos que no tenemos ningún tipo de conflicto de interés de este trabajo con ninguna organización académica y/o comercial.

Contribuciones de los autores

Shonerly Bustamante Garcia: Tesista de pregrado, autor de la tesis "Políticas basadas en la Norma ISO 27001:2013 y su influencia en la Gestión de Seguridad de la Información en una Municipalidad Distrital" a partir de la cual se realizó el artículo de revisión. **Miguel Angel Valles Coral:** Docente del curso de Investigación II, asesor metodológico, contribución en la conceptualización de la idea del estudio, redactor y revisor crítico del

documento. Se encargó de levantar las observaciones . **Danny Lévano Rodríguez:** Apoyo en diseño de la metodología para la selección e identificación de los artículos para su revisión y revisor temático del artículo.

Financiación

El trabajo se realizó sin ningún tipo de financiamiento por parte de ninguna institución académica y/o comercial.