Revisión sistemática: vulnerabilidades de seguridad cibernética en los activos digitales

Systematic review: cybersecurity vulnerabilities in digital assets

Milton Edward Humpiri Flores
mehumpirif.doc@unaj.edu.pe - Universidad Nacional de Juliaca
https://orcid.org/0000-0001-5743-2064
Edgardo Martín Figueroa Donayre
em.figueroa@unaj.edu.pe - Universidad Nacional de Juliaca
https://orcid.org/0000-0001-7891-3334
Mía Lucía Guillen Guevara
mguillen@unaj.edu.pe - Universidad Nacional de Juliaca
https://orcid.org/0000-0001-8641-0833
Domingo Jesús Cabel Moscoso
jesus.cabel@unica.edu.pe - Universidad Nacional San Luis Gonzaga de Ica
https://orcid.org/0000-0001-9361-7744
Rogger Humpiri Flores
rogger.rhf@gmail.com - Universidad Nacional del Altiplano
https://orcid.org/0000-0003-4760-6467
Julio Cesar Huanca Marín
juliohuanca@unaj.edu.pe - Universidad Nacional de Juliaca
https://orcid.org/0000-0001-8714-2623

Recibido el 19/01/23 | Aceptado el 11/03/23
DOI: https://doi.org/10.47190/nric.v4i2.250

Resumen

Con la disrupción de nuevas tecnologías de información y comunicaciones, la seguridad que se consideraba protegida se ha visto comprometida por numerosos ataques, los cuales antes eran percibidos como irrelevantes, pero hoy en día resulta fundamental controlar los datos o minería de datos. Estos activos digitales son vulnerables a diversas amenazas y debemos preguntarnos: ¿Es crucial identificar estas vulnerabilidades y amenazas en los activos de información? El objetivo de la presente investigación fue de detectar aquellas vulnerabilidades y amenazas que afectan a los activos de información y proponer soluciones. Para llevar a cabo esta tarea, se realizó una búsqueda exhaustiva en bases de datos bibliográficos, tales como Scopus, Scielo, IEEE Xplore, IOPScience, ScienceDirect, ResearchGate, World Wide Science, Dialnet, Semantic Scholar y Google Academy, abarcando el periodo comprendido entre 2018 y 2022. Los resultados obtenidos se centran en la identificación de las vulnerabilidades y sus correspondientes amenazas, destacando el malware como principal amenaza y en cuanto a las soluciones, se sugiere el uso de la criptografía como mecanismo de protección de la información.

Palabras clave: Amenazas, criptografía, seguridad de la información, vulnerabilidades.

Como citar: Humpiri-Flores, M.E., Figueroa-Donayre, E.M., Guillen-Guevara, M.L., Cabel-Moscoso, D.J., Humpiri-Flores, R. & Huanca-Marín, J.C. (2023). Revisión sistemática: vulnerabilidades de seguridad cibernética en los activos digitales. ÑAWPARISUN – Revista de Investigación Científica de Ingenierías, 4(2), 93-100.

Abstract

With the disruption of new information and communication technologies, the security that was considered protected has been compromised by numerous attacks, which were previously perceived as irrelevant, but today it is essential to control data or data mining. These digital assets are vulnerable to various threats and we must ask ourselves: ¿Is it crucial to identify these vulnerabilities and threats in information assets? The objective of this research was to detect those vulnerabilities and threats that affect information assets and propose solutions. To carry out this task, an exhaustive search was carried out in bibliographic databases, such as Scopus, Scielo, IEEE Xplore, IOPScience, ScienceDirect, ResearchGate, World Wide Science, Dialnet, Semantic Scholar and Google Academy, covering the period between 2018 and 2022. The results obtained focus on the identification of vulnerabilities and their corresponding threats, highlighting malware as the main threat and in terms of solutions, the use of cryptography is suggested as an information protection mechanism.

Keywords: Threats, cryptography, information security, vulnerabilities.

INTRODUCCIÓN

La disrupción tecnológica ha permitido una mayor interacción global y ha mejorado la calidad de vida de las personas como los procesos empresariales (nacional y privado). Sin embargo, no todas las empresas comprenden la importancia de la gestión adecuada de la seguridad de la información, lo que resulta en diversas vulnerabilidades y amenazas pueden afectar la información almacenada. Maquera Quispe & Serpa Guillermo (2019), afirman que la información y los servicios de TI son activos importantes para la gestión empresarial de procesos. A medida que las empresas dependen más de estos activos, se producen amenazas que aprovechan las vulnerabilidades que las empresas no identifican a tiempo, como lo demuestra (Sohrabi Safa et al., 2016).

En términos de seguridad de la información, a menudo se piensa que solo es necesario tener un buen antivirus y una contraseña segura. Sin embargo, se necesitan normativas y estrategias que garanticen la privacidad y protección de los datos. La Gestión de Riesgos de los Sistemas de Información (GRSI), según Firdaus & Suprapto (2018), es responsable de identificar las diferentes vulnerabilidades y amenazas a los recursos de información utilizados por los gerentes de TI para lograr los objetivos planificados, reducir los riesgos y equiparar los gastos para obtener beneficios y proteger la información.

Teniendo en cuenta los problemas de seguridad de la información, se ha llevado a cabo una revisión sistemática utilizando la metodología PRISMA, que, según Urrútia & Bonfill (2010), ayuda a mejorar la transparencia y claridad en la publicación de revisiones sistemáticas. Por lo tanto, con el objetivo de proteger la información y analizar las vulnerabilidades y amenazas que la afectan, se ha logrado determinar una lista de las diversas vulnerabilidades y amenazas en los activos de digitales, así como soluciones.

MATERIALES Y MÉTODOS

Para llevar a cabo el presente estudio se usó la metodología PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses), descrita por (Urrútia & Bonfill, 2010).

Metodología PRISMA

Esta metodología promueve la utilización de un sistema fundamentado en la evaluación de distintos componentes clave del diseño y la implementación de estudios para proporcionar evidencias precisas y empíricas acerca de la relación entre ellos. Por lo tanto, es necesario llevar a cabo este artículo de manera explícita y con un enfoque investigativo que satisfaga los resultados del estudio. Para comenzar con este método, que consta de un total de 27 elementos, se inicia con el título que identifica la revisión, un resumen estructurado, una introducción que justifica y describe el objetivo, y una sección más extensa que aborda el proceso de selección de las diversas bases de datos bibliográficos, las fuentes de información, los criterios de elegibilidad y la selección de estudios, como se explican en los siguientes parrafos, se incluye la lista completa de citas únicas, después de eliminar las duplicadas, y se finaliza con la revisión individual, que incluye tanto la síntesis cualitativa (revisión sistemática) como la cuantitativa (metaanálisis), así como la discusión que resume la evidencia y los principales hallazgos. Finalmente, se presentan las conclusiones y las limitaciones encontradas en el estudio (Urrútia & Bonfill, 2010).

Recolección de información

Para la búsqueda se utilizó términos clave cuidadosamente seleccionados en función de su relación con la pregunta de investigación y posibles medidas de prevención, tales como "seguridad de la información", "amenazas", "gestión de riesgos", "information security" y "vulnerabilidades". Se seleccionaron bases de datos académicas populares y con gran cantidad de artículos debido a su uso común en revisiones sistemáticas. Las bases de datos seleccionadas incluyen Scopus, Scielo, IEEE Xplore, IOPScience, ScienceDirect, ResearchGate, World Wide Science, Dialnet, Semantic Scholar y Google Académico.

Términos de búsqueda

Scielo

("seguridad de información" AND "gestión de riesgos" OR "amenazas" OR "ISO 27001" OR "information security" AND "risk management" OR "ISO 27001" OR "threats")

Dialnet

("cryptography information")

World Wide Science

("cryptography")

ScienceDirect

("security of the information")

IOPScience

("seguridad de información" AND "risk")

ResearchGate

("seguridad de información" AND "riesgos" AND "amenazas"AND "ISO 27001" OR "criptografía")

Scopus

TITLE-ABS-KEY (("Security Risk ") OR ("cybersecurity") AND ("information"))

IEEE Xplore

("All Metadata": risk management) OR ("All Metadata": information security)

Semantic Scholar

("seguridad de información" OR "amenazas")

Google Academy

("gestión de riesgos " AND "seguridad de información" OR "amenazas" AND "ITIL" OR "information security" OR "risk")

Criterios de inclusión y exclusión

En relación al proceso de selección de artículos, se tomaron en cuenta dos criterios de inclusión: que se enfocaran en el ámbito de la seguridad de información en tecnología y sistemas, y que hubieran sido publicados dentro de los últimos cuatro años. Por otro lado, se estableció un criterio de exclusión para no considerar publicaciones que trataran sobre la seguridad de información en empresas que no se relacionen con el ámbito tecnológico, y aquellas que solo mencionaran las normas ISO sin ofrecer soluciones o aplicaciones.

La búsqueda y extracción de información se llevó a cabo por varios colaboradores del estudio de manera independiente, y cualquier discrepancia fue resuelta mediante consenso para asegurar la precisión de la revisión sistemática.

Tabla 1.
Proceso de selección de artículos

	Identificación	Filtrado Inicial	Idoneidad	Inclusión
N° de artículos	66	12	54	40

RESULTADOS

La búsqueda realizada en las bases de datos descritas, se identificaron aproximadamente 66 artículos sobre el tema de seguridad de información, distribuidos de la siguiente manera: Scopus con 17 artículos, ResearchGate con 13, seguido por Google Academy con 9 y Dialnet con 8 artículos. Además, ScienceDirect e IOPscience contienen 5 y 4 artículos respectivamente, mientras que Scielo, IEEE Xplore y World Wide Science tienen 3 artículos cada uno y, por último, Semantic Scholar solo cuenta con 1 artículo en este ámbito.

Tras aplicar los criterios de inclusión y exclusión previamente establecidos, se seleccionaron 40 artículos para realizar una revisión adecuada y precisar las definiciones de activo de información y/o seguridad de información, así como para identificar las vulnerabilidades y amenazas a las que se enfrentan estos activos, y encontrar soluciones para protegerlos.

En cuanto a los países que lideran las publicaciones en este tema, se destaca la importancia que tiene la seguridad de información para todos los países: Ecuador con 7 artículos, Perú con 6, Indonesia y Colombia con 5 cada uno, India con 4, China con 3 y otros países con 1 artículo.

Activos de información

Los activos son valiosos para las empresas (públicas y privadas) y su buena gestión es responsabilidad de los altos directivos y juntas, según Evans & Price (2020), estos activos incluyen activos financieros, físicos, humanos y de sobre todo información. Los activos de información son una parte importante en el mundo digital, según Maquera Quispe & Serpa Guillermo (2019), y son evaluados mediante diferentes escalas, basadas en las características del activo de información en una universidad.

Tabla 2.
Criterios para activos de información

Confidencialidad	Integridad	Disponibilidad	Valor
Información pública para personas internas o externas a la universidad	Información modificada sin permiso que se logra remediar de manera sencilla o que no tiene efecto en los procesos desarrollados por la universidad	Información no disponible pero que no afecta los procesos de la universidad	0
Información solo para toda la comunidad universitaria	Información modificada sin permiso que se puede remediar pero que tiene un efecto negativo en los procesos desarrollados por la universidad	Información que al no estar disponible durante 1 semana puede tener un efecto negativo en los procesos de la universidad	1
Información solo para una parte de la comunidad universitaria	Información modificada sin permiso que es difícil de remediar y que tiene un gran efecto negativo en los procesos desarrollados por la universidad	Información que al no estar disponible durante 1 día laboral puede detener los procesos realizados por la universidad	2
Información solo para una parte muy pequeña de la comunidad universitaria y que su difusión tendrá un efecto negativo a externos o a la propia universidad	Información modificada sin permiso que no se puede remediar y que detiene los procesos desarrollados por la universidad	Información que al no estar disponible durante 1 hora puede detener los procesos realizados por la universidad	3

Nota. Elaborado por Maquera Quispe & Serpa Guillermo (2019).

Alonge et al. (2020), sugieren que la clasificación de los activos de información enfrenta un problema debido a la falta de lineamientos genéricos. Dado que no existe una adaptación definida en la clasificación de los activos de información para todas las organizaciones, cada organización puede tener su propio esquema de clasificación. Prajanti & Ramli (2019), argumentan que los activos de información más relevantes para la organización deben priorizarse para mitigar los riesgos identificados. Angraini et al. (2019), apoyan esta idea, afirmando que es necesario un plan de riesgos para los activos de información para establecer un mejor plan de seguridad de la información. Por lo tanto, es importante detectar, clasificar y priorizar los activos de información.

Sin embargo, Kativu & Pottas (2019), no están de acuerdo y afirman que, aunque estas clasificaciones y priorizaciones de activos brindan una idea de seguridad completa, los controles que se pueden identificar no abordarán todo lo que la organización necesita para protegerse. Sin embargo, estos controles ayudan a reducir las vulnerabilidades de los activos de información.

Seguridad de Información

La importancia de cumplir con las características de los activos de información ha llevado a un mayor enfoque en la seguridad de estos, según Velepucha Sánchez et al. (2022), sostienen que la seguridad de la información debe ser un proceso continuo y que debe ser llevada a cabo por la dirección de control interno de la organización. Este proceso debe ser periódico y adaptado a las necesidades específicas de cada organización, utilizando un Sistema de Gestión de Seguridad de la Información (SGSI).Yupanqui & Oré (2017), complementan esta idea mencionando la norma ISO-27000, que tiene como objetivo general proteger los activos de información. También destacan la importancia de las políticas de seguridad, que comprometen la mejora de los SGSI y facilitan su desarrollo.

Vulnerabilidades de la información

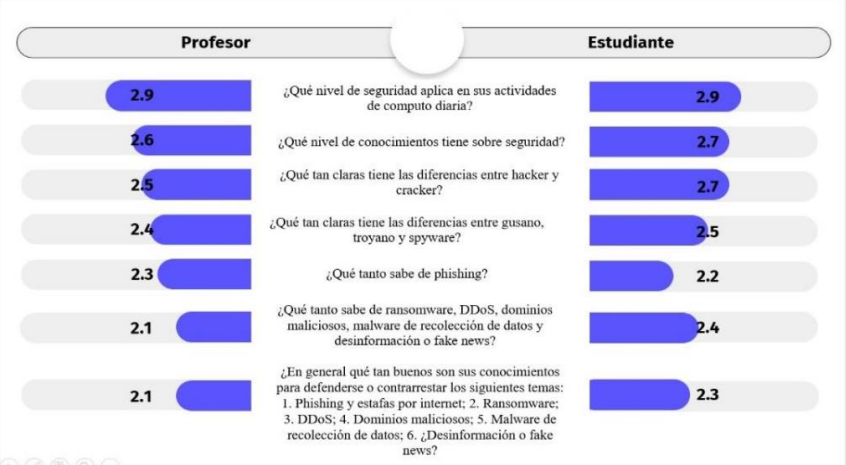
De acuerdo con Sánchez-Bautista & Ramírez-Chávez (2022), las vulnerabilidades se refieren a la inconsistencia de los sistemas, las cuales pueden ser aprovechadas por cibercriminales o atacantes para afectar negativamente los activos de información. Además, se identifican múltiples amenazas como problemas para los activos de información, las cuales explotan diferentes tipos de vulnerabilidades. En cuanto a la definición de vulnerabilidad y amenaza, Guerra et al. (2021), explican que la vulnerabilidad es el factor que permite la ejecución de la amenaza, lo que resulta en daños a los activos de la organización.

Tabla 3.
Vulnerabilidades encontradas

Vulnerabilidad	Cantidad
Conocimiento	10
Acceso	7
Parches	7
Software	6
Integridad	5
Servidores	3
Autorizaciones	2
Recursos	2
Backup	2
Fluido eléctrico	2
Otros (desastres naturales o provocados)	1

En adición a la Tabla 3, se destaca la vulnerabilidad más discutida en varios artículos revisados por Estrada-Esponda et al. (2021), quienes llevaron a cabo una encuesta para investigar las prácticas de seguridad en términos de información en una universidad. En la Figura 1, presentada por mismos autores, se muestran los resultados de la encuesta de seguridad, evaluados en una escala tipo Likert de 1 a 5, donde se obtuvo una calificación media satisfactoria de 4.

Figura 1.
Resultados sobre conocimientos de seguridad



El estudio concluye que tanto los profesores como los estudiantes tienen un bajo nivel de conocimiento sobre seguridad, según se evidencia en los resultados de la encuesta, en ambos casos, la calificación obtenida no supera la media satisfactoria, lo que representa un problema significativo, ya que esto podría convertirse en una vulnerabilidad común y ser aprovechada por un delincuente cibernético.

Amenazas de la información

De acuerdo con Sánchez-Bautista & Ramírez-Chávez (2022), los desarrolladores tienen la responsabilidad de incorporar tanto los requisitos de seguridad como los funcionales del sistema. Considerando el uso de los datos por parte de una organización, se identifican amenazas internas y externas, tales como ataques técnicos, naturales o humanos, documentados por ISO 27001 (Erb, 2007). Es crucial distinguir estas amenazas y evaluar su impacto para poder implementar medidas de prevención necesarias y evitar posibles ataques, señalan (Sánchez-Bautista & Ramírez-Chávez, 2022). En este sentido, la Tabla 4 proporciona una lista de las principales amenazas a la seguridad de la información.

Tabla 4.
Amenazas encontradas

Amenaza	Cantidad
Malware	14
Hackers	10
Acceso	5
Privacidad	3
Fuerza bruta	2
Phishing	2
Rootkit	1
Robo de datos	1
Denial of Service	1

Soluciones de seguridad

Después de haber examinado las diferentes amenazas y vulnerabilidades a los activos de información, se centrará en buscar soluciones para gestionarlas. La Tabla 5 resume las principales soluciones encontradas en los artículos revisados.

Tabla 5.
Soluciones encontradas

Solución	Cantidad
Criptografía	18
Acceso	4
Firewall	3
Detección de intrusos	2
Esteganografía	2
Antivirus	2
Software antimalware	2
Seguridad de protocolos	1
Backup	1
Licencia	1
Conexión segura (SSL)	1
Derecho de acceso	1
Pen Testing	1

La principal solución identificada es la criptografía, mencionada en 18 artículos, seguida por un sistema de control de acceso en 4 artículos y un firewall en 3 artículos. Además, sistemas de detección de intrusos (IDS), esteganografía y antivirus son mencionados en 2 artículos cada uno, mientras que otros métodos solo son mencionados en 1 artículo.

Según Nikita & Kaur (2014), la criptografía, cuyo término proviene del griego que significa "escritura oculta", es la ciencia que se encarga de los principios y métodos para transformar un texto en otro que no sea fácil de interpretar (cifrado), y ejecutar el proceso opuesto para obtener el mensaje original (descifrado).

La criptografía se divide en dos tipos: clave simétrica o privada y clave asimétrica o pública. Según Roa, (2015), la clave simétrica implica compartir una sola clave entre el emisor y el receptor para encriptar y desencriptar el mensaje. En cambio, con la clave asimétrica, se utilizan dos claves: una pública que se entrega a cualquier persona y una privada que se entrega solo a personas autorizadas. El emisor utiliza la clave pública del receptor para encriptar el mensaje, y solo el receptor, con su clave privada, puede desencriptar el mensaje (Maiorano, 2009).

Criptografía como solución idónea

Según los artículos revisados, se han identificado ciertos algoritmos criptográficos, tal como se muestra en la Figura 2, que serán utilizados por herramientas de código abierto como OpenSSL, TrueCrypt y DiskCryptor, los cuales estiman la velocidad de encriptación y desencriptación a través del uso de benchmark, tal como lo mencionan (Velasco et al., 2017).

Figura 2.
Algoritmos de criptografía

Solís et al. (2017), afirmó que una clave con mayor longitud proporciona una mayor seguridad en la información, ya que aumenta el tiempo de cifrado y descifrado, lo que dificulta que los ataques informáticos puedan descifrar la información, garantizando la confidencialidad, autenticidad y disponibilidad de la misma.

La criptografía es una de las principales soluciones para proteger los activos de información contra amenazas y vulnerabilidades, ya que asegura la privacidad y confidencialidad en la comunicación entre individuos, organizaciones y gobiernos. Si se implementa la criptografía de manera efectiva, se podrán proteger los canales de comunicación y, en última instancia, los activos de información.

CONCLUSIONES

La identificación de las vulnerabilidades es esencial para determinar las posibles brechas que un atacante podría explotar y los activos que una empresa o persona tiene. La falta de conocimiento sobre seguridad de la información puede ser muy perjudicial, especialmente para las empresas, debido a la información que manejan y a las consecuencias económicas y de reputación que podrían sufrir en caso de un ciberataque. La falta de control de acceso y las demoras en las actualizaciones de aplicaciones son factores que contribuyen al aumento de la probabilidad de sufrir una amenaza.

A pesar de que la tecnología siempre tendrá alguna vulnerabilidad, existen medidas que se pueden tomar para mitigar las amenazas, como la capacitación constante y el cumplimiento de normas como ISO 27000, la implementación de criptografía o sistemas de control de acceso, entre otras soluciones mencionadas en la revisión. El malware es la principal amenaza debido a las diversas formas de infección, pero también existen otras amenazas, como el phishing y las filtraciones de datos, en las que las personas son el principal objetivo de los ataques. Con un estudio adecuado, se pueden evitar estas amenazas y mejorar la seguridad de la información.

La revisión sistemática muestra las principales vulnerabilidades y riesgos de los activos de información y se mencionan algunas soluciones para gestionar la seguridad de estos activos. Se hace especial énfasis en la criptografía como el principal método para proteger las comunicaciones.

REFERENCIAS BIBLIOGRÁFICAS

Alonge, C. Y., Arogundade, O. T., Adesemowo, K., Ibrahalu, F. T., Adeniran, O. J., & Mustapha, A. M. (2020, March 1). Information Asset Classification and Labelling Model Using Fuzzy Approach for Effective Security Risk Assessment. 2020 International Conference in Mathematics, Computer Engineering and Computer Science, ICMCECS 2020. https://doi.org/10.1109/ICMCECS47690.2020.240911

Angraini, Megawati, & Haris, L. (2019). Risk Assessment on Information Asset an academic Application Using ISO 27001. 2018 6th International Conference on Cyber and IT Service Management, CITSM 2018. https://doi.org/10.1109/CITSM.2018.8674294

Erb, M. (2007). Gestión de Riesgo en la Seguridad Informática. Markus Erb. https://protejete.wordpress.com/gdr_principal/

Estrada-Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. Revista Logos, Ciencia & Tecnología, 13(3), 98-110. https://doi.org/10.22335/rlct.v13i3.1446

Evans, N., & Price, J. (2020). Development of a holistic model for the management of an enterprise's information assets. International Journal of Information Management, 54, 102193. https://doi.org/10.1016/j.ijinfomgt.2020.102193

Firdaus, N. Z., & Suprapto. (2018). Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT . Petrokimia Gresik). Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 2(1), 1–10. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/702

Guerra, E., Neira, H., Díaz, J. L., Patiño, J., Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Development of an information security management system based on analysis methodology and risk identification in university libraries. Información Tecnológica, 32(5), 145–156. https://doi.org/10.4067/S0718-07642021000500145

Kativu, K., & Pottas, D. (2019). Leveraging intrinsic resources for the protection of health information assets. South African Computer Journal, 31(2), 150â€“161-150â€“161. https://doi.org/10.18489/SACJ.V31I2.536

Maiorano, A. (2009). Criptografía : Técnicas de desarrollo para profesionales. https://www.alphaeditorialcloud.com/library/publication/criptografia-tecnicas-de-desarrollo-para-profesionales

Maquera Quispe, H. G., & Serpa Guillermo, P. N. (2019). Gestión de activos basado en ISO/IEC 27002 para garantizar seguridad de la información. Ciencia & Desarrollo, 0(21), 100–112. https://doi.org/10.33326/26176033.2017.21.736

Nikita, & Kaur, R. (2014). A Survey on Secret Key Encryption Technique. IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET), 2(5), 7–14. http://www.impactjournals.us/journals.php?id=77&jtype=2&page=1

Prajanti, A. D., & Ramli, K. (2019). A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods. 34th International Technical Conference on Circuits/Systems, Computers and Communications, ITC-CSCC 2019. https://doi.org/10.1109/ITC-CSCC.2019.8793421

Roa Buendía, J. F. (2015). Seguridad informática. www.mhe.es/cf/informatica

Sánchez-Bautista, G., & Ramírez-Chávez, L. (2022). Amenazas de seguridad a considerar en el desarrollo de software. XIKUA Boletín Científico de La Escuela Superior de Tlahuelilpan, 10(19), 31–37. https://doi.org/10.29057/xikua.v10i19.8118

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers and Security, 56, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Solís, F., Pinto, D., & Solís, S. (2017). Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema Android utilizando el método de encriptación RSA. Enfoque UTE, 8(1), 160–171. https://doi.org/10.29019/enfoqueute.v8n1.123

Urrútia, G., & Bonfill, X. (2010). Declaración PRISMA: una propuesta para mejorar la publicación de revisiones sistemáticas y metaanálisis. Medicina Clinica, 135(11), 507–511. https://doi.org/10.1016/j.medcli.2010.01.015

Velasco, P. M., Jiménez, M. S., Chafla, G. X., Maritza Velasco Sánchez, P., Soledad Jiménez Jiménez, M., & Xavier Chafla Altamirano, G. (2017). Análisis de los mecanismos de encriptación para la seguridad de la información en redes de comunicaciones. SATHIRI, 12(1), 91–103. https://doi.org/10.32645/13906925.38

Velepucha Sánchez, M. A., Morales Carrillo, J., & Pazmiño Campuzano, M. F. (2022). Análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO. Informática y Sistemas: Revista de Tecnologías de La Informática y Las Comunicaciones, 6(1), 63–78. https://doi.org/10.33936/isrtic.v6i1.4473

Yupanqui, J. R. A., & Oré, S. B. (2017). Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 2017(25), 112–134. https://doi.org/10.17013/risti.25.112-134