Artículos de Revisión

Vulnerabilidades y amenazas en los activos de información: una revisión sistemática

Vulnerabilities and threats in information assets: a systematic review

Guevara-Vega, Evellyn Milles Duval; Delgado-Deza, Jose Ricardo; Mendoza-de-los-Santos, Alberto Carlos

Evellyn Milles Duval Guevara-Vega
emguevarav@unitru.edu.pe
Universidad Nacional de Trujillo, Perú

Jose Ricardo Delgado-Deza
Universidad Nacional de Trujillo, Perú

Alberto Carlos Mendoza-de-los-Santos
Universidad Nacional de Trujillo, Perú

Revista Científica de Sistemas e Informática
Universidad Nacional de San Martín, Perú
ISSN-e: 2709-992X
Periodicidad: Semestral
vol. 3, núm. 1, e461, 2023
rcsi@unsm.edu.pe

Recepción: 15/11/2022
Aprobación: 11/01/2023
Publicación: 20/01/2023

URL: http://portal.amelica.org/ameli/journal/535/5354040004/

DOI: https://doi.org/10.51252/rcsi.v3i1.461

Autor de correspondencia: emguevarav@unitru.edu.pe

Cómo citar este artículo:: Guevara-Vega, E. M. D., Delgado-Deza, J. R. & Mendoza-de-los-Santos, A. C. (2023). Vulnerabilidades y amenazas en los activos de información: una revisión sistemática. Revista Científica de Sistemas e Informática, 3(1), e461. https://doi.org/10.51252/rcsi.v3i1.461

Resumen: Con el avance del tiempo y la tecnología, la seguridad que antes se protegía se vio afectada por múltiples ataques, que en un cierto sentido se creía sin tanta importancia pero que, en la actualidad, es necesario que los datos estén controlados. Estos activos se verán implicados por vulnerabilidades y amenazas, que para poder defenderse será necesaria la pregunta de esta revisión sistemática: ¿Es importante identificar las vulnerabilidades y amenazas en los activos de información? Por lo tanto, nuestro objetivo de investigación es localizar aquellas vulnerabilidades y amenazas que afectan a los activos de información junto con soluciones. Esta búsqueda se logró gracias a las revisiones de artículos publicados en base de datos bibliográficos como: Scopus, Scielo, IEEE Xplore, IOPScience, ScienceDirect, ResearchGate, World Wide Science, Dialnet, Semantic Scholar y Google Academy comprendida entre los años 2017 a 2022. Como resultados se obtendrán aquellas vulnerabilidades junto con sus amenazas, destacando el malware como principal amenazador del activo y en soluciones la criptografía que buscará mejorar la seguridad de información.

Palabras clave: activo de la información, amenazas, criptografía, seguridad de la información, vulnerabilidades.

Abstract: With the advancement of time and technology, the security that was previously protected has been affected by multiple attacks, which in a certain sense were thought to be minor but, nowadays, it is necessary for the data to be controlled. These assets will be implicated by vulnerabilities and threats, which in order to defend themselves will require the question of this systematic review: Is it important to identify vulnerabilities and threats in information assets? Therefore, our research objective is to locate those vulnerabilities and threats that affect information assets along with solutions. This search was achieved thanks to the reviews of articles published in bibliographic databases such as: Scopus, Scielo, IEEE Xplore, IOPScience, ScienceDirect, ResearchGate, World Wide Science, Dialnet, Semantic Scholar and Google Academy between the years 2017 to 2022. As a result, those vulnerabilities will be obtained along with their threats, highlighting malware as the main threat to the asset and cryptography solutions that will seek to improve information security.

Keywords: information assets, threats, cryptography, information security, vulnerabilities.

1. INTRODUCCIÓN

El avance de la tecnología ha permitido una mayor interacción entre personas de todo el mundo mejorando la calidad de vida de personas y procesos en empresas, sin embargo, no todas entienden la importancia de tener una buena gestión de seguridad de información, trayendo consigo diversos tipos de vulnerabilidades y amenazas que perjudican la data que tenemos almacenada. Maquera Quispe & Serpa Guillermo (2019) afirman lo anterior aludiendo que las empresas tienen como activos para la gestión de los procesos a la información y servicios de TI, entonces, al aumentar la dependencia hacia los activos se producen amenazas que aprovechan aquellas vulnerabilidades que la empresa no identifica a tiempo.

Como lo demuestran Sohrabi Safa et al. (2016), cuando se trata de seguridad de información se suele pensar que solo es cuestión de un usuario (nombre) y una contraseña segura, pero se necesita de normativas, estrategias que permitan la privacidad y protección de datos. La GRSI: Gestión de Riesgos de los Sistemas de Información es la encargada de la identificación de las distintas vulnerabilidades y amenazas hacia los recursos de información que son utilizados por los gerentes de TI para lograr los objetivos planeados, reducir los riesgos y equiparar los gastos para conseguir beneficios y protección de la información (Firdaus & Suprapto, 2017).

Ante estos problemas en la seguridad de la información, se ha realizado la siguiente revisión sistemática, haciendo uso de la metodología PRISMA, que para Urrútia & Bonfill (2010), esta metodología ha sido ideado como un instrumento que ayuda a mejorar la transparencia y la claridad en la publicación de las diversas revisiones sistemáticas.

Por ello, con la perspectiva de proteger nuestra información, pero analizando aquellas vulnerabilidades y/o amenazas que la afectan, se logró determinar una lista de cada una de las diversas vulnerabilidades y amenazas en los activos de información, además de brindar soluciones para que el activo siga intacto.

2. MATERIALES Y MÉTODOS

2.1. Tipo de estudio

Este artículo tuvo como base la metodología PRISMA, descrita por Urrútia & Bonfill (2010), contemplando como pregunta de investigación a: ¿Es importante identificar las vulnerabilidades y amenazas en los activos de la información?

2.2. Fundamentación de la Metodología

Esta metodología fomenta según Urrútia & Bonfill (2010) que un sistema justificado en la evaluación de distintos componentes claves de diseño y ejecución de estudios nos delatara evidencias precisas y empíricas acerca de la relación entre ellos. Por lo que es necesario realizar este artículo con un método que sea de manera explícita, buscando el indagar para satisfacer los resultados del estudio.

Notas de autor

emguevarav@unitru.edu.pe

Para empezar con este método, que en total son 27 ítems, inicia por el título que identifica a la revisión, un resumen estructurado, introducción que contiene tanto la justificación y el objetivo, la siguiente parte es más extensa y abarca el proceso selectivo de las diversas bases de datos bibliográficos como lo son las fuentes de información, búsqueda, los criterios de elegibilidad, y la selección de estudios que se explican en los puntos 2.3 y 2.4 (es decir, las citas halladas en las búsquedas de las distintas bases de datos o fuentes), se sigue con la totalidad de citas únicas donde se eliminaron a los duplicados y finalizando con la revisión individual adjuntado en la síntesis cualitativa (revisión sistemática) cuantitativa (metaanálisis), así como la discusión que resume la evidencia y principales hallazgos, y por último las conclusiones con las limitaciones encontradas (Urrútia & Bonfill, 2010).

2.3. Proceso de recolección de información

Se dio inicio al proceso de búsqueda empleando descriptores, estos fueron seleccionados por la relación con respecto a la pregunta de investigación y posibles formas de prevención: “seguridad de información”, “amenazas”, “gestión de riesgos”, “information security”, “vulnerabilities”.

Las bases de datos para esta revisión sistemática fueron elegidas debido a que son bases de datos académicas muy usadas en las diversas revisiones sistemáticas, así como también por sus grandes cantidades de artículos. Como base de datos seleccionados tenemos a Scopus, Scielo, IEEE Xplore, IOPScience, ScienceDirect, ResearchGate, World Wide Science, Dialnet, Semantic Scholar y Google Academy. En la Tabla 1, se mostrarán las bases de datos seleccionadas con sus respectivos términos de búsqueda.

TABLA 1.
Términos de búsqueda

Base de datos	Términos de búsqueda
Scopus	TITLE-ABS-KEY (("Security Risk ") OR ("cybersecurity") AND ("information"))
Scielo	("seguridad de información" AND "gestión de riesgos" OR "amenazas" OR "ISO 27001" OR "information security" AND "risk management" OR "ISO 27001" OR "threats")
IEEE Xplore	("All Metadata": risk management) OR ("All Metadata": information security)
IOPScience	("seguridad de información" AND "risk")
ScienceDirect	("security of the information")
ResearchGate	("seguridad de información" AND "riesgos" AND "amenazas" AND "ISO 27001" OR "criptografía")
World Wide Science	("cryptography")
Dialnet	("cryptography information")
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")

Con respecto a los términos de búsqueda se han usado diferentes términos en cada base de datos bibliográficos para obtener una mayor variedad de artículos, debido a que se consideró que la inclusión de los mismos términos de búsqueda traería consigo obtener una variedad de artículos repetidos y limitaría el alcance que busca esta revisión.

2.4. Criterios de inclusión y exclusión

Para lograr desarrollar este estudio, se revisaron artículos que han sido publicados en bases de datos científicas referenciados en la Tabla 1, en idiomas, inglés y español, comprendidos entre los años 2017 al año 2022 (últimos 5 años).

Con respecto al criterio de inclusión los artículos escogidos fueron de acuerdo al contexto de la seguridad de información en el ámbito de tecnología y sistemas; también que pertenezcan a los últimos 5 años asignados. Como criterio de exclusión se dispuso no abordar dichas publicaciones que tienen como temas de seguridad de información en empresas que no abarquen el ámbito tecnológico, y tampoco aquellas que toman a las normas ISO sin recalcar en soluciones o aplicativos.

El registro de búsqueda y extracción de información fue tratado por los colaboradores del estudio de manera independiente, donde las desigualdades fueron observadas y resueltas en consenso por los mismos para poder realizar una revisión sistemática.

En la Figura 1 se realizó un diagrama resumen del flujo del proceso de selección de artículos.

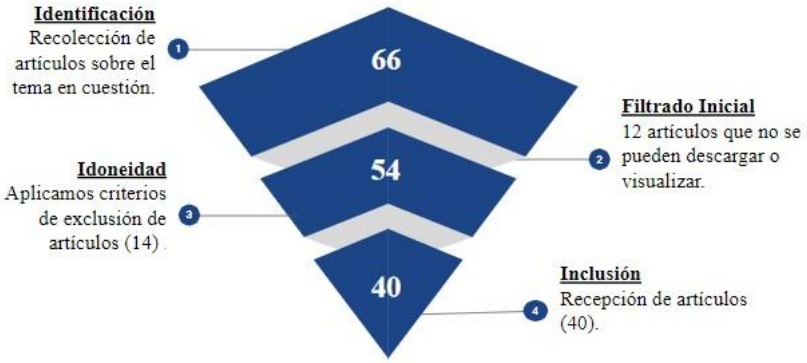

FIGURA 1.
Flujo de proceso de selección de artículos

3. RESULTADOS Y DISCUSIÓN

Por la búsqueda de artículos en las distintas bases de datos se determinaron un total de, aproximadamente, 66 artículos publicados; ordenados así: Scopus 17 artículos, ResearchGate con 13 artículos, Google Academy con 9 seguida de Dialnet con 8 artículos, ScienceDirect e IOPscience con 5 y 4 artículos respectivamente; Scielo, IEEE Xplore y World Wide Science con 3 artículos cada uno y por último Semantic Scholar con 1 artículo. A partir de este número total, se aplicaron criterios de inclusión y de exclusión, explicados anteriormente, hasta obtener 40 artículos, lo que permitió hacer una recopilación apropiada para dar con los resultados del tema.

Tomando en cuenta estos artículos seleccionados, se procedió a precisar las definiciones sobre activo de información y/o seguridad de información, así como también a identificar las vulnerabilidades y amenazas que sufren los activos, incluyendo soluciones para seguir protegiéndolos.

Con respecto a los países que lideran las publicaciones, se demuestra que es importante para todos los países el tema de seguridad de información identificando aquellas vulnerabilidades, amenazas y revisando soluciones para que el activo no se pierda; principalmente Ecuador con 7 artículos, Perú con 6 artículos,

Indonesia y Colombia con 5 artículos cada uno, India con 4 artículos, seguida de China con 3 y otros con 1 artículo, véase la Figura 2.

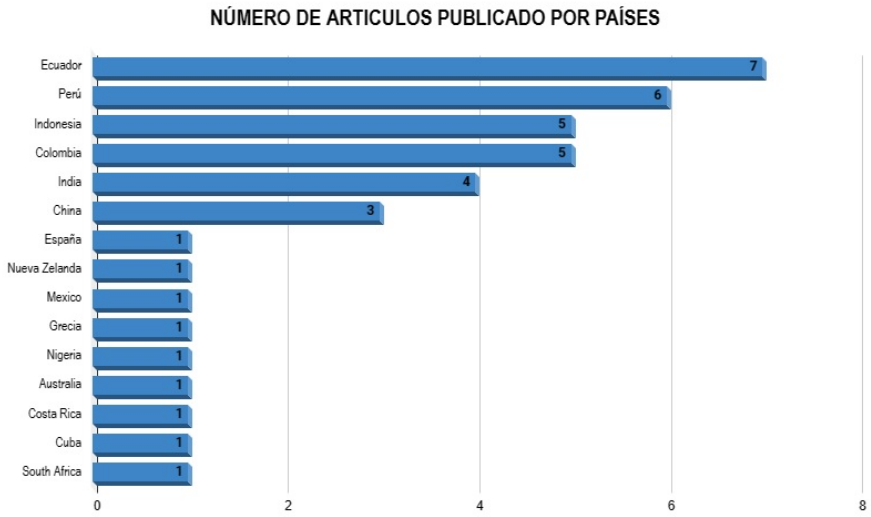

FIGURA 2.
Número de artículos publicados según cada país

3.1. Activos de Información

En general, los activos se han caracterizado por generar valor para las empresas, siendo estos de mucha importancia. Para Evans & Price (2020), la responsabilidad del buen manejo de los activos recae en los altos directivos y juntas, además los activos radican en activos financieros, físicos, humanos y de información.

Como una parte importante de este mundo digital son los activos de información, según Maquera Quispe & Serpa Guillermo (2019), estos activos poseen gran relevancia, siendo evaluados mediante diferentes escalas según las características que se presentan en la Tabla 2, los cuales son un resumen sobre la aplicación de criterios proveniente de cada característica 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

Fuente: Elaborado por Maquera Quispe & Serpa Guillermo (2019).

Por otro lado, los activos de información, según Alonge et al. (2020), la clasificación enfrenta un problema como lo es la falta de directrices genéricas, debido a que no hay una adaptación en la clasificación de activos de información definida para todas las organizaciones, es por ello que cada organización puede tener su esquema de clasificación propio, y para Prajanti & Ramli (2019), se deben priorizar los activos de información más relevantes para la organización debido a que serán los más importantes para mitigar, todo esto en caso de identificar algún riesgo.

De igual forma Angraini et al. (2018), ratifican la idea anterior mencionando que se necesita de un plan de riesgos de sus activos de información para poder establecer un mejor plan para la seguridad de la información, es por ello que resulta importante detectar, clasificar y priorizar los activos de información.

A pesar de que todas estas clasificaciones y priorizaciones en los activos brindan una idea de seguridad completa, Kativu & Pottas (2019) difieren, porque los controles que se logren identificar no terminarán abordando todo lo que necesita la organización para protegerse, pero sí ayudan a reducir las vulnerabilidades de los activos de información.

3.2. Seguridad de Información

Con los problemas actuales sobre los activos de información y la importancia que cumplan con estas características es donde se presta atención hacia la seguridad de este activo, Velepucha Sánchez et al. (2022) mencionan que la seguridad de información debe ser un proceso constante y su ejecución debe ser hecha por la dirección de control interno que pertenezca a la organización, siendo periódico, además de contar con un SGSI que se adapte a lo que requiera cada organización, otro autor como Yupanqui & Oré (2017) complementan la idea anterior mencionando a ISO-27000 que tienen como propósito general proteger los activos de información, y sobre las políticas de seguridad que compromete la mejora de los SGSI facilitando su desarrollo.

3.3. Vulnerabilidades del activo de información

Sánchez-Bautista & Ramírez-Chávez (2022) mencionan que, las vulnerabilidades vienen a ser la inconsistencia de los sistemas, donde estas pueden servir para un cibercriminal o atacante con la intención de afectar negativamente los activos de información.

Asimismo, como problemas para los activos de información, encontramos múltiples amenazas que se aprovechan de los diversos tipos de vulnerabilidades, Guerra et al. (2021) menciona la diferencia entre vulnerabilidad y amenaza, siendo la vulnerabilidad el factor que permite la ejecución de la amenaza, que trae como consecuencia un daño a los activos de la organización.

Por ejemplo, en la Figura 3, presentamos la identificación de las principales vulnerabilidades en las diferentes literaturas científicas analizadas:

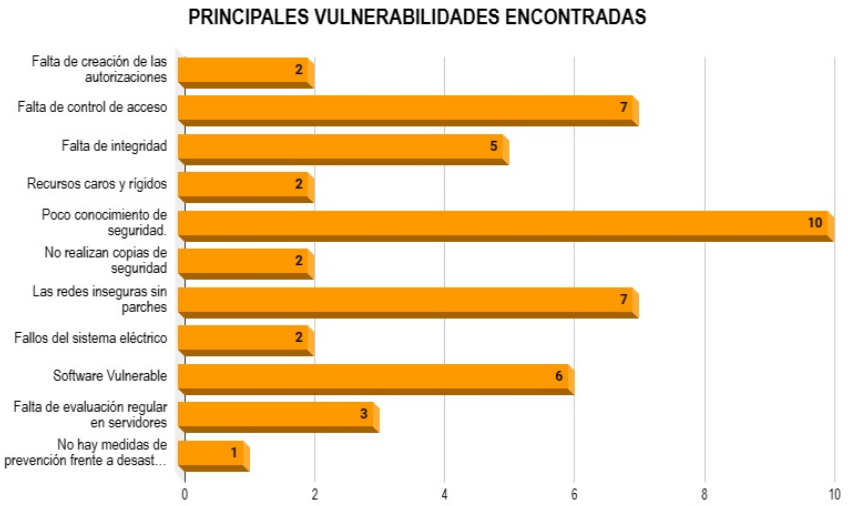

FIGURA 3.
Principales vulnerabilidades encontradas

En este gráfico podemos visualizar que la principal vulnerabilidad encontrada es acerca del poco conocimiento de seguridad con un total de 10 menciones, mostrando al ser humano como un eslabón débil ante posibles amenazas debido a su propio desconocimiento sobre seguridad de información. Siguiendo con el gráfico se encuentra tanto la falta de control de acceso como también la inseguridad de redes debido a falta de parches con 7 menciones, mostrando también problemas en la parte de programación como el descuido en las organizaciones y usuarios en la actualización de sus aplicativos, además en cuarto puesto está el software vulnerable con 6 menciones, esto es muy conocido debido a los diferentes tipos de vulnerabilidades que posee

el software como los CVE (Common Vulnerabilities and Exposures), sobre todo por el gran impacto que puede ocasionar poseer una versión antigua donde se han detectado formas de ingresar al sistema y escalar privilegios.

Complementando al gráfico y haciendo énfasis a la vulnerabilidad más comentada entre los diversos artículos revisados, tenemos el estudio de Estrada-Esponda et al. (2021), donde realizan una encuesta para conocer las prácticas de seguridad en términos de información para el caso de una universidad. En la Figura 4, elaborado por Estrada-Esponda et al. (2021) muestran los resultados con respecto a conocimientos sobre una encuesta de seguridad en una valoración de escala tipo Likert de 1 a 5, siendo la media satisfactoria 4.

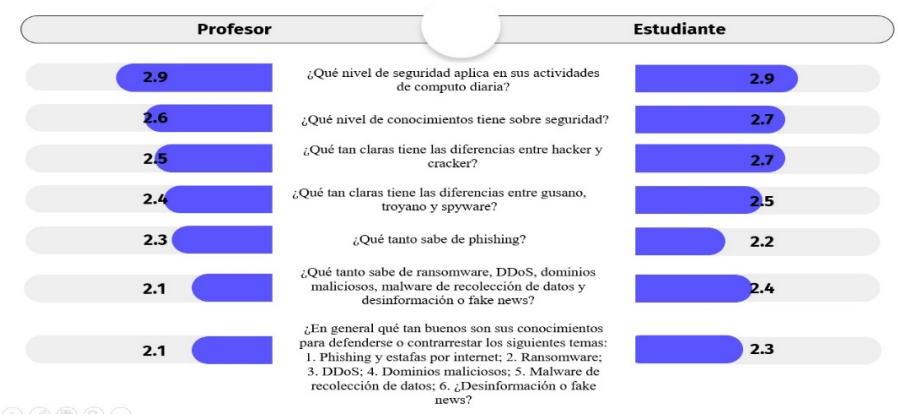

FIGURA 4.
Resultados sobre conocimientos de seguridad

Como resultado de esta encuesta se recalca el poco conocimiento sobre seguridad de parte de profesores y estudiantes, debido a que en ambos casos no logran superar la media satisfactoria, mostrando un gran problema debido a que se puede convertir en una vulnerabilidad muy común que puede ser aprovechada por un cibercriminal.

3.4. Amenazas del activo de información

Los desarrolladores están obligados a incorporar requerimientos de seguridad y requerimientos funcionales del sistema, afirma Sánchez-Bautista & Ramírez-Chávez (2022). Si tomamos en cuenta al organismo que emplea los datos nos daremos cuenta que existen amenazas de origen interno y externo, por ejemplo, las agresiones técnicas, naturales o humanas, documentadas por ISO 27001 (Erb, 2014).

Es importante distinguir las amenazas y precisar el impacto de cada una con el propósito de ejercer medidas necesarias para evitar ataques, continúa explicando Sánchez-Bautista & Ramírez-Chávez (2022) es por eso que se muestra en la Figura 5 con las principales amenazas que se da en la seguridad de información.

FIGURA 5.
Principales amenazas encontradas

Podemos inferir que tenemos como principal amenaza al malware con 14 publicaciones, hackers con 10 artículos, acceso no autorizado con 5, filtración de privacidad con 3 artículos, ataque de fuerza bruta y suplantación de Identidad (Phishing) con 2 artículos cada uno, y, por último, contando con 1 artículo tenemos a rootkit, robo de datos de transacciones y Denial of Service (DoS).

Enfocándonos en los malware, también llamados software malicioso, representan una gran amenaza para infraestructuras críticas, según Rieck et al. (2008). Este mismo autor nos menciona que estos están planeados con la única intención de causar daño a la computadora y/o redes de la víctima (servicios). Existe mucha variedad en malwares como virus, ransomware, spyware, adware, entre otros (Faruki et al., 2015).

En la Tabla 3 se definen los tipos de malware señalado por Sánchez-Bautista & Ramírez-Chávez (2022).

TABLA 3.
Tipos de malware

Tipos de malware	
Tipo	Definición
Adware	Software rastreador de datos (historial en internet) con el propósito de mostrar anuncios y ventanas emergentes.
Ransomware	Llamado "Software Extorsionador". Programa dañino que no permite el ingreso a los datos hasta que se obtenga un pago por el "rescate" de los datos. Cuando se realiza ese rescate se tendrá acceso a los datos.
Spyware	Su propósito es la recopilación de datos de usuarios, por lo que incorpora keyloggers que se encargan de registrar los datos que los usuarios teclean (información personal), tenemos a los números de tarjetas de crédito, contraseñas, teléfonos, entre otros.
Virus informáticos	Programa de computadora planteado con la única intención de extenderse de un dispositivo a otro dañando programas, borrando archivos.

Por otro lado, en la Figura 6, según Asgarkhani et al. (2017) los hackers se pueden dividir en tres tipos:

FIGURA 6.
Tipos de hackers

Los primeros deben ser considerados como una de las amenazas más peligrosas para los sistemas nacionales por el fácil acceso a sus recursos. Los segundos impulsados por el dinero atacan sus sistemas para lograr ilegalidades. Y el último, son ataques generalmente por razones políticas, mencionado por Goodin (2009).

Debido a la transparencia de la información en las transacciones existe el riesgo de que se pueda filtrar la privacidad de la identidad del usuario, describen Abunadi & Kumar (2021). La fuga de datos de clientes implica un gran riesgo en el mundo bancario ya que el cliente confía su información a este servicio, describe Triana & Pangabean (2021), además existe el robo de datos de transacciones por personas no autorizadas.

Sánchez-Bautista & Ramírez-Chávez (2022) señalan que, como robo de identidad tenemos al phishing, los delincuentes pretenden robar los datos del usuario y extraer la información personal para llevar a cabo crímenes por medio de links a páginas webs que aparentan ser fuentes verdaderas. De acuerdo con el estudio realizado por Benishti (2020), existe una pluralidad de páginas falsas donde estos delincuentes inducen a los usuarios al ingreso de datos que son de estas empresas, como se muestra en la Tabla 4.

TABLA 4.
Total de páginas falsas por empresa

Empresa	% del total de páginas falsas
PayPal	22
Microsoft	19
Facebook	15
eBay	6
Amazon	3

Fuente. Elaborado por Sánchez-Bautista & Ramírez-Chávez (2022).

Por ejemplo, siendo el caso de una biblioteca, Guerra et al. (2021) mencionan que la vulnerabilidad frecuente fue el acceso con identidad falsa, igualmente el acceso no autorizado; quien figura en la categoría de error de software, mencionado por Kitsios et al. (2022).

En cuanto a esta amenaza, Denial of Service (DoS), según Irwin (2021), es caracterizado porque el sistema está en un estado sin operar causado por la saturación de servidores generando mucho tráfico en la red y sobrecargando los recursos del sistema, de manera que el sistema fallaría y las peticiones jamás serían respondidas.

3.5. Soluciones para administrar la seguridad en los activos de información

Una vez analizado las distintas amenazas y/o vulnerabilidades de los activos de información, nos enfocaremos en soluciones que permitan gestionarlas, en la Figura 7 se tienen las principales soluciones de acuerdo a los artículos leídos.

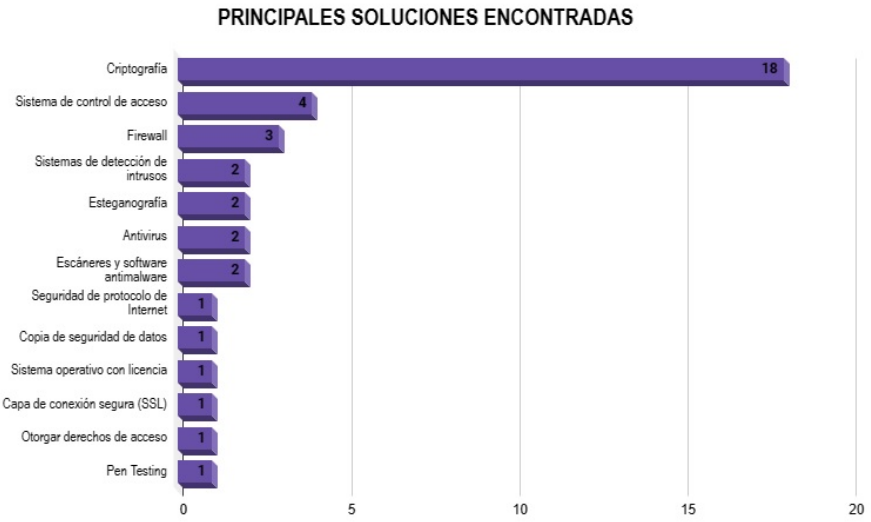

FIGURA 7.
Principales soluciones encontradas

Como solución principal tenemos a la criptografía con 18 artículos, seguida de un Sistema de control de acceso con 4 artículos, Firewall con 3 artículos, contando con 2 artículos cada uno tenemos a Sistemas de detección de intrusos (IDS), esteganografía y el antivirus; por último, otros con 1 artículo.

La palabra "criptografía", especifican Nikita & Kaur (2014) originado del griego significa «escritura oculta», es la ciencia que comprende principios y métodos para transformar un texto en otro con la finalidad de que no se interprete de manera fácil (cifrado) y ejecutar el proceso opuesto para lograr conseguir el mensaje original (descifrado).

Se divide a la criptografía en: clave simétrica o clave privada y clave asimétrica o de clave pública. La primera, dada por Roa Buendía & Sanz (2013), es definida como el compartimiento de una sola clave entre el emisor y receptor empleada para la encriptación y desencriptación del mensaje. La segunda, dada por el mismo autor, se utilizan dos claves (una pública y otra privada) a el envío de mensajes, la primera se entrega a alguna persona, en cambio, la segunda solamente a personas autorizadas. El emisor emplea la clave pública del receptor para la encriptación del mensaje y, únicamente, el receptor, con la clave privada será capaz de desencriptar ese mensaje (Maiorano, 2009).

Por ejemplo, el blockchain se basa en el algoritmo asimétrico y funciones hash (Puig Pascual, 2018). En el ámbito de finanzas según Bélen Gallego & Palomo Zurdo (2020), tenemos a: criptomonedas, criptodivisas, criptoactivos, o token.

Luego, para implementar un Sistema de control de acceso, dado por Triana & Pangabean (2021) es la instalación de fingerprint en la sala de servidores. Y si, por otro lado, el propósito es elegir un software antivirus, ten en cuenta estos pasos: En primer lugar, el antivirus debe descargarse con internet y, al mismo tiempo se necesita el monitoreo y eliminación manual tradicional de archivos para monitorear la red y el correo en tiempo real; en segundo lugar, el software debe tener un servicio de actualización en línea perfecto; tercero, los fabricantes también deben tener una red de detección de virus de respuesta rápida; en cuarto lugar, los proveedores deben poder brindar consultas antivirus completas y oportunas (Li et al., 2021).

Criptografía como solución idónea

De acuerdo a los artículos leídos, tenemos algunos algoritmos de criptografía, ver Figura 8, que serán implementados por OpenSSL, TrueCrypt y DiskCryptor; instrumentos de código abierto que estiman la velocidad del proceso de encriptar y desencriptar mediante el uso de benchmark, referido por Velasco Sánchez et al. (2017).

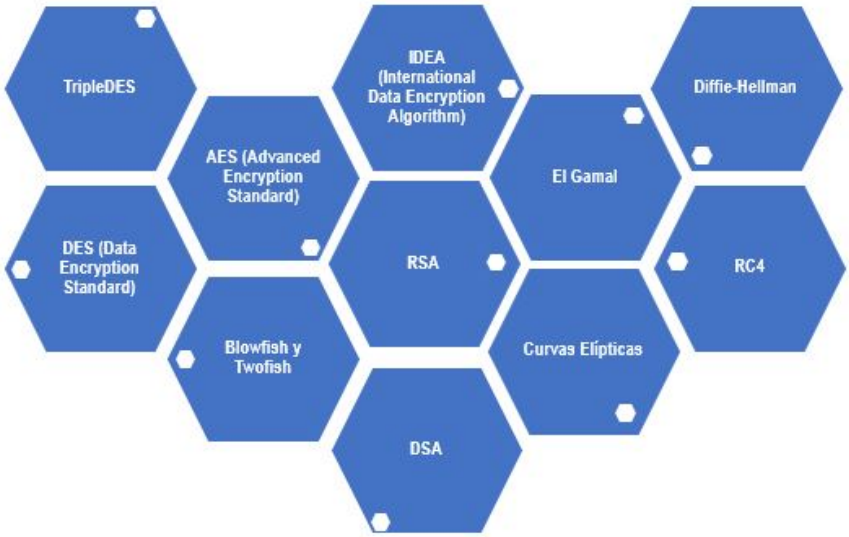

FIGURA 8.
Algoritmos de criptografía más usados

Solís et al. (2017) nos asegura que mientras más cifras tiene una clave, se estima mayor seguridad de información porque la codificación y decodificación será en un tiempo mayor, obligando a que los ataques informáticos no alcancen a descifrar esa información, asegurando la confidencialidad, autenticidad y disponibilidad de ello.

La revisión sistemática realizada nos permite profundizar tanto en las vulnerabilidades y amenazas en los activos de información. Por medio de la Figura 3 se determinó que unas de las vulnerabilidades más mencionadas en los artículos seleccionados han sido acerca del desconocimiento sobre seguridad de información, la poca frecuencia en la actualización de las aplicaciones y la falta de control de acceso; con el estudio de Estrada-Esponda et al. (2021) en la Figura 4 se refuerza el problema del desconocimiento sobre seguridad como una vulnerabilidad importante.

Por consiguiente, en la Figura 5, que habla sobre las amenazas, se resalta la priorización de mitigación y/o eliminación de los distintos tipos de malware que provocan que el dispositivo se vea afectado, para ello Sánchez-Bautista & Ramírez-Chávez (2022) brindan algunos tipos de malware en la Tabla 3 que ayudan a tener una mejor idea de cómo actúan; por otro lado, la aparición del término "hacker" y los diferentes tipos que existen nos permitirán tener un mejor concepto de quién es el que podría causar una amenaza, lo cual resulta de gran ayuda para poder detallar los posibles ataques y tener formas de contrarrestarlo.

Por último, tomando en cuenta todas las soluciones antes mencionadas en la Figura 7, la criptografía viene a ser una de las defensoras de los activos de información contra amenazas y/o vulnerabilidades porque en la comunicación entre personas, organizaciones o gobiernos se resalta la privacidad y de gran manera la confidencialidad. Si se logra extender a la criptografía, se protegerán los distintos canales de comunicación y en sí, al activo.

4. CONCLUSIONES

La tecnología ha tenido un crecimiento exponencial que ha traído consigo un aumento en ataques o robos de información ya sea del usuario común así como también de compañías, la seguridad de la información se ha vuelto imprescindible para estos casos, por lo cual existe una gran importancia en conocer las diversas formas en las que podríamos sufrir un robo, manipulación o eliminación de nuestra información de esa manera podremos construir formas para mitigar o eliminar estas amenazas, se usó la metodología PRISMA para lograr llegar a resultados concluyentes.

La identificación de las vulnerabilidades es sumamente importante debido a que nos muestra los posibles caminos que un atacante podría explotar y aquellos activos que la empresa y/o persona ofrece. El desconocimiento sobre la seguridad de información puede resultar muy perjudicial sobre todo para una empresa debido a la información que manejan y las consecuencias que pueden surgir económicamente y en su reputación en caso sufran de un ciberataque, aspectos como la falta de control de accesos o la demora en las actualizaciones de sus aplicativos contribuyen a aumentar la posibilidad de sufrir una amenaza.

A pesar de que la tecnología siempre arrastre una vulnerabilidad no impide que podamos hacer algo para mitigar las amenazas, la capacitación constante y el cumplimiento de normas como ISO 27000, así como también la criptografía o un sistema de control de acceso entre otras soluciones que se han mencionado en esta revisión tienen como finalidad mitigar estas vulnerabilidades y amenazas siendo la principal el malware, debido a las diversas formas de infección, pero además existen otras como phishing, filtraciones de datos donde las personas somos el foco principal de estos ataques, pero que con un estudio adecuado puede llegar a ser evitado y con ello una mejor seguridad de nuestra información.

La revisión demuestra las principales vulnerabilidades y riesgos de los activos de información, también se han mencionado algunas soluciones para gestionar la seguridad de estos activos, haciendo especial énfasis en la criptografía como principal método para proteger las comunicaciones y como a pesar de que existan varios algoritmos de encriptación sobre todo con el actual uso de blockchain, algunos han sido posibles de descifrar por cibercriminales, es por ello que el presente artículo aporta estos diversos algoritmos para futuros estudios de mejoras o generación de nuevos algoritmos de encriptación para salvaguardar la información.

FINANCIAMIENTO

Ninguno.

CONFLICTO DE INTERESES

No existe ningún tipo de conflicto de interés relacionado con la materia del trabajo.

CONTRIBUCIÓN DE LOS AUTORES

Conceptualización: Guevara-Vega, E. M. D
Curación de datos: Delgado-Deza, J. R.
Análisis formal: Guevara-Vega, E. M. D
Investigación: Mendoza-de-los-Santos, A. C.
Metodología: Delgado-Deza, J. R.
Supervisión: Mendoza-de-los-Santos, A. C.
Validación: Delgado-Deza, J. R.
Redacción - borrador original: Guevara-Vega, E. M. D & Delgado-Deza, J. R.

Redacción - revisión y edición: Guevara-Vega, E. M. D & Delgado-Deza, J. R.

REFERENCIAS BIBLIOGRÁFICAS

Abunadi, I., & Kumar, R. L. (2021). Blockchain and Business Process Management in Health Care, Especially for COVID-19 Cases. *Security and Communication Networks, 2021*, 1–16. https://doi.org/10.1155/2021/2245808

Alonge, C. Y., Arogundade, O. T., Adesemowo, K., Ibrahalu, F. T., Adeniran, O. J., & Mustapha, A. M. (2020). 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)*, 1–7. https://doi.org/10.1109/ICMCECS47690.2020.240911

Angraini, Megawati, & Haris, L. (2018). Risk Assessment on Information Asset an academic Application Using ISO 27001. *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, 1–4. https://doi.org/10.1109/CITSM.2018.8674294

Asgarkhani, M., Correia, E., & Sarkar, A. (2017). An overview of information security governance. *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, 1–4. https://doi.org/10.1109/ICAMMAET.2017.8186666

Bélen Gallego, A., & Palomo Zurdo, R. J. (2020). *Blockchain: un reto del siglo XXI para la Economía Social*. XVIII Congreso Internacional de Investigadores en Economía Social y Cooperativa. http://ciriec.es/wp-content/uploads/2020/09/COMUN-046-T11-GALLEGO-PALOMO-ok.pdf

Benishti, E. (2020). *50,000+ Fake Login Pages Spoofing Over 200 Brands Worldwide*. IronScale Safer Together. https://ironscales.com/blog/fake-login-pages-spoof-prominent-brands-phishing-attacks/

Erb, M. (2014). *Gestión de Riesgo*. 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). 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

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2015). Android Security: A Survey of Issues, Malware Penetration, and Defenses. *IEEE Communications Surveys & Tutorials, 17*(2), 998–1022. https://doi.org/10.1109/COMST.2014.2386139

Firdaus, N., & Suprapto, S. (2017). Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus#: PT. Petrokimia Gresik). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 2*(1), 91–100. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/702

Goodin, D. (2009). *Pro-Palestine vandals deface Army, NATO sites*. The Register. https://www.theregister.com/2009/01/10/army_nato_sites_defaced/

Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información Tecnológica, 32*(5), 145–156. https://doi.org/10.4067/S0718-07642021000500145

Irwin, L. (2021). *What is a DoS (denial-of-service) attack?* IT Governance UK. https://www.itgovernance.co.uk/blog/what-is-a-dos-denial-of-service-attack

Kativu, K. T., & Pottas, D. (2019). Leveraging intrinsic resources for the protection of health information assets. *South African Computer Journal, 31*(2). https://doi.org/10.18489/sacj.v31i2.536

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability, 14*(3), 1269. https://doi.org/10.3390/su14031269

Li, Y., Liu, R., Liu, X., Li, H., & Sun, Q. (2021). Research on Information Security Risk Analysis and Prevention Technology of Network Communication Based on Cloud Computing Algorithm. *Journal of Physics: Conference Series, 1982*(1), 012129. https://doi.org/10.1088/1742-6596/1982/1/012129

Maiorano, A. (2009). *Criptografía - Técnicas de desarrollo para profesionales* (1st ed.). Alfaomega México.

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, 21*, 100–112. https://doi.org/10.33326/26176033.2017.21.736

Nikita, & Kaur, R. (2014). A Survey on Secret Key Encryption Technique. *International Journal of Research in Engineering & Technology, 2*(5), 7–14. https://www.impactjournals.us/index.php/archives?jname=77_2&year=2014&submit=Search&page=6

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. *2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*, 1–4. https://doi.org/10.1109/ITC-CSCC.2019.8793421

Puig Pascual, A. (2018). Experiencias. Identidad digital sobre «Blockchain» a nivel nacional. *Revista Icade. Revista de Las Facultades de Derecho y Ciencias Económicas y Empresariales, 101*. https://doi.org/10.14422/icade.i101.y2017.006

Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008). Learning and Classification of Malware Behavior. In *Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 108–125). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-70542-0_6

Roa Buendía, J. F., & Sanz, F. J. (2013). *Seguridad informática* (2nd ed.). McGraw-Hill.

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 & 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

Triana, Y. S., & Pangabean, R. A. M. (2021). Risk Analysis in the Application of Financore Information Systems Using FMEA Method. *Journal of Physics: Conference Series, 1751*(1), 012032. https://doi.org/10.1088/1742-6596/1751/1/012032

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

Velasco Sánchez, P. M., Jiménez Jim´énez, M. S., & Chafla Altamirano, G. X. (2017). Análisis de los mecanismos de encriptación para la seguridad de la información en redes de comunicaciones. *SATHIRI, 12*(1), 91. 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 Ibérica de Sistemas e Tecnologias de Informação, 25*, 112–134. https://doi.org/10.17013/risti.25.112-134