UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Ciberseguridad y robo de información: Una revisión sistemática de la literatura

TRABAJO DE INVESTIGACIÓN PARA OPTAR EL GRADO ACADÉMICO DE BACHILLER EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

AUTOR

Jose Carlos Vilchez Villegas

ASESOR

Karla Cecilia Reyes Burgos

https://orcid.org/0000-0003-3520-5076

Chiclayo, 2022

Índice

Resumen

La presente revisión sistemática de la literatura tiene como objetivo encontrar autores, países y revistas o repositorios que se puedan tomar como referentes o puntos de partida para realizar investigaciones sobre el tema de ciberseguridad orientada al robo de información. La metodología que se siguió fue la propuesta por Kitchenham, con la cual se definieron tres preguntas de investigación, una para cada tipo de referente que se busca, luego se procedió a la recopilación de artículos de investigación en las bases de datos ProQuest, ScienceDirect y CORE y después de haber aplicado criterios de inclusión y exclusión y evaluar la calidad de cada artículo mediante una escala cuantitativa se realizó la clasificación de los artículos seleccionados según su autor, revista o repositorio y país de publicación, concluyendo que, si se desea indagar en este campo, Brij Gupta se puede tomar como autor de referencia debido a que ha realizado varias investigaciones en esta área, además uno de los repositorios donde más se publica sobre el tema de ciberseguridad orientada al robo de información es arXiv.org, de donde se obtuvo el 17% de artículos que han sido analizados, finalmente se observó que de los países donde se publican investigaciones sobre este tema destacan Estados Unidos con el 26% de publicaciones e India con el 21%.

Palabras clave: Ciberseguridad, robo de información, phishing, xploits, troyanos.

Abstract

This systematic literature review aims to find authors, countries, and journals or repositories that can be used as references or starting points for conducting research on the topic of cybersecurity aimed at information theft. The methodology followed was the proposal by Kitchenham, with which three research questions were defined, one for each type of reference sought, and then the research articles were compiled in the ProQuest, ScienceDirect and CORE and after applying inclusion and exclusion criteria and evaluating the quality of each article by means of a quantitative scale, the selected articles were classified according to their author, journal or repository and country of publication, concluding that, if one wishes to inquire into In this field, Brij Gupta can be taken as a reference author because he has carried out various investigations in this area, in addition to one of the repositories where the most published information is cybersecurity-oriented theft of information is arXiv.org, from where 17% of the articles that have been analyzed were obtained; finally, the countries where research on this topic was published were searched for. the United States with 26% of publications and India with 21%.

Keywords: Cyber security, information theft, phishing, xploits, Trojans.

Introducción

Es de suma importancia reestructurar la educación sobre la ciberseguridad, actualmente pasamos gran parte de nuestro tiempo navegando por internet, a veces por temas de estudio, trabajo o simplemente entretenimiento, y en esos momentos podemos ser víctimas del robo de nuestra información. Las técnicas utilizadas para cometer delitos contra nuestra privacidad son diversas, por ejemplo, podemos ser víctimas phishing, podemos caer en xploits, ser infectados con troyanos u otro software malicioso. Dado que con el tiempo van apareciendo muchas más técnicas y perfeccionándose las que ya existen, es importante que la información que se le brinda a los usuarios para su protección se centre en corregir las ideas erróneas que guían su comportamiento actual, es decir, anteriormente se buscaba que los usuarios puedan identificar los componentes de las urls u otras señales de alerta dentro de los sitios web que visitan, pero el desarrollo de tecnologías e ingeniería social permiten que aplicaciones maliciosas pasen desapercibidas ante estos criterios de discernimiento que tienen los usuarios [1].

Existe evidencia de que el 60% de los ataques a aplicaciones web es facilitado por vulnerabilidades en el código fuente [2], sin embargo, es mucho más fácil y efectivo que los ciberdelincuentes dirijan el ataque hacia el usuario, que por distracción o desconocimiento brinda información personal sensible a los atacantes, como por ejemplo, su número de DNI o la clave de su tarjeta de crédito, incluso, a veces no es necesario que el usuario brinde directamente la información, sino que ahora los criminales de la red aprovechan que una de las modalidades preferidas por los usuarios para registrarse nuevas aplicaciones, es usar las cuentas sus redes sociales, las mismas que comparten un token de autentificación mediante el cual se puede acceder a la información que el usuario define, o en la mayoría de casos, acepta sin leer; de esta forma, si se trata de una aplicación maliciosa, se usará dicho token para ingresar a la cuenta y buscar la información que les sea útil para extorsionar o suplantar una identidad de la víctima [3]. Lo descrito anteriormente es lo que se conoce como phishing, una de las técnicas más usadas para robar información, y es de lo más común convertirse en víctima si no tomamos las precauciones necesarias.

Otra de las formas en las que pueden robarnos nuestra información es infectar nuestros dispositivos con troyanos o xploits, que le brindarán al ciberdelincuente la capacidad para seguir minuciosamente nuestra actividad, acceder a los archivos que tengamos alojados en el dispositivo y muchísimas otras cosas que sucederán silenciosamente mientras nosotros usamos de forma normal nuestro equipo.

En esta situación, y considerando que Kitchenham declara que es necesario transmitir el conocimiento para garantizar el avance de las diferentes ciencias [4], la realización de este artículo de revisión se propone como objetivo analizar la literatura existente con respecto a la ciberseguridad, orientada sobre todo al robo de información y buscar referentes en cuanto autores, países y revistas de donde se pueda obtener información de partida para realizar investigaciones. Además, se justifica en la creciente necesidad de educar a los usuarios para evitar ser víctimas de suplantación de identidad, extorsión o robo.

Metodología

Se ha utilizado la metodología propuesta por Kitchenham et al [1] , por lo que se ha estructurado en seis ítems, en el primero se definen las preguntas que guían la investigación, en el segundo ítem se describe la forma en que se realizará la búsqueda, en el tercero se plantean criterios para incluir o excluir del análisis las investigaciones de acuerdo al interés que nos genere, de igual forma en el cuarto ítem se plantean criterios de calidad que garanticen la objetividad de la información obtenida, en el quinto ítem se desarrolla el proceso de búsqueda aplicando los criterios de inclusión, exclusión y calidad para finalmente, en el sexto ítem analizar las investigaciones seleccionadas.

Preguntas de investigación

Las preguntas de investigación buscan generar respuestas de acuerdo con los objetivos planteados, por ello se definen tres preguntas, una por cada tipo de referente que se espera encontrar. Además, hay que indicar que todas las preguntas serán respondidas con información desde el año 2017 hasta el 2 de julio del 2020 y en idioma inglés.

Q1: ¿Qué autores han escrito más sobre la ciberseguridad orientada al robo de la información?

Q2: ¿Cuáles son los países donde se han publicado más investigaciones sobre el tema de ciberseguridad orientada al robo de la información?

Q3: ¿En qué revistas o repositorios se ha publicado más sobre la ciberseguridad orientada al robo de la información?

Proceso de búsqueda

Con el fin mantener el estándar de calidad de la presente revisión sistemática de la literatura, la búsqueda se ha realizado en fuentes de datos que tienen aprobación científica y sean multidisciplinarias o de algún campo relacionado con la informática, específicamente se consideraron: ProQuest, ScienceDirect y CORE.

Se definieron 5 términos de búsqueda en idioma inglés dado que son bases de datos internacionales y este idioma generará un mejor performance en la búsqueda.

T1: cyber security.

T2: data theft.

T3: phishing.

T4: xploits.

T5: trojan.

El primer y segundo término corresponden al área y tema específico que se está investigando, el tercer término se planteó por ser una de las técnicas más conocidas y usadas actualmente para el robo de información, de igual forma el tercer y cuarto término hacen referencia a software malicioso que se usa también para sustraer información de los usuarios.

A partir de los términos propuestos y los operadores AND y OR se conformó una única cadena de búsqueda que se aplicará a las tres bases de datos:

CB: cyber security AND data theft AND phishing AND (xploits OR trojan).

Criterios de Inclusión y Exclusión

Los criterios de inclusión y exclusión tienen como finalidad delimitar las características que deben poseer los artículos para ser elegibles para el análisis y posterior respuesta a las preguntas de investigación.

Tabla 1: Criterios de inclusión y exclusión

INCLUSIÓN	EXCLUSIÓN
- Investigaciones publicadas desde el año 2017 hasta el 10 de julio del 2020.	- Investigaciones fuera del rango de fechas desde 2017 hasta el 10 de julio del 2020.
- Investigaciones en idioma inglés.	- Investigaciones que no estén en idioma inglés.
- Sean de acceso libre.	- No permitan el acceso al documento completo.
- Publicaciones originales.	- Publicaciones duplicadas.
- Aborda el tema de ciberseguridad orientada al robo de información.	- Aborda temáticas distintas al robo de información.
- Artículos de investigación.	- Documentos que sean recopilaciones de otros autores.

Evaluación de la calidad

La evaluación de la calidad es necesaria para reducir el sesgo del análisis de la literatura y se basa en la aplicabilidad que se le pueda dar a los hallazgos, su validez y algunas características de diseño que influyen en la interpretación [2].

Los artículos preseleccionados deberán ser juzgados mediante una escala cuantitativa definida en base a criterios que garanticen que la presente revisión de la literatura concluya con resultados objetivos y verídicos.

- Presenta información que aporta a los objetivos de la revisión (2 puntos).
- El artículo describe el contexto en el cual desarrolla su investigación (1 punto)
- Presenta objetivos y conclusiones consistentes y con relación entre ellos (1 punto).
- El documento tiene al menos 10 páginas (1 punto).

Los puntos que se han especificado para cada criterio se han definido según la importancia e indispensabilidad que representa dentro de la investigación, por ello es que el criterio de aporte al cumplimiento con los objetivos tiene el doble de puntos que los demás. Se considerarán como investigaciones de calidad aceptable aquellas que tengan al menos 3 puntos, y serán estas las que se analicen y usen para responder las preguntas de investigación planteadas inicialmente.

Recopilación de datos

El proceso de recopilación de datos se realizó el día 10 de julio del año 2020. En primer lugar, se introdujeron los términos y la cadena de búsqueda en cada una de las bases de datos para observar la cantidad de resultados que podíamos obtener sin aplicar filtros, los resultados se muestran en la *tabla 2*. En ProQuest y Core sólo se introdujeron los términos, sin embargo, en ScienceDirect se usó la búsqueda avanzada y los términos se introdujeron en el campo "Find articles with these terms".

Tabla 2: Resultados de búsquedas sin filtros

	ProQuest	Science Direct	CORE	TOTAL
T1	944,720	17,106	2,773,887	3,735,713
T2	484,762	30,084	21,333,744	21,848,590
T3	138,630	3,987	16,336	158,953
T4	45	91	175	311
T5	858,288	14,133	206,515	1,078,936
CB	1,687	347	1,182	3,216

Según las opciones que ofrecen los buscadores avanzados de las bases de datos que se están utilizando, se aplicaron los filtros que ayuden a determinar que artículos cumplían o no con los criterios de inclusión y exclusión planteados anteriormente. En la *tabla 3* se listan los filtros y se indica en que base de datos se aplicaron.

Tabla 3: Filtros a aplicar en cada base de datos

Filtro	ProQuest	Science Direct	CORE
Fecha (2017-2020)	X	X	X
Acceso libre	X		
Evaluado por Expertos	X		
Excluir duplicados	X		
Idioma inglés	X		X
Tipo de fuente: Revista científica	X		
Tipo: Artículo de Investigación		X	

Como se observó en la *tabla 3*, no se pudieron aplicar los mismos filtros en todas las bases de datos e incluso en algunas no hubo posibilidad de aplicar criterios que son necesarios, por ejemplo, el de acceso libre, por lo que se procedió a una revisión manual para comprobar qué

artículos permitían el acceso a la totalidad de su contenido. La cantidad de documentos válidos para el análisis se redujo tal como se muestra en la *tabla 4*.

Tabla 4: Resultados de la búsqueda con filtros

Base de datos	Cantidad Inicial	Acceso Completo
ProQuest	84	84
Science Direct	52	12
CORE	161	161
TOTAL	297	257

Como siguiente paso, se procedió a filtrar según el contenido y estructura del artículo, para ser aceptado debe ser una fuente primaria de información (No ser recopilación o resumen de otros) y abordar el tema de ciberseguridad orientado al robo de información. Además, se filtrarán investigaciones duplicadas, y con esto se obtendrán los artículos que cumplan con los criterios de inclusión y exclusión, cabe resaltar que el filtro de idioma no fue necesario de aplicar en ScienceDirect ya que todas sus publicaciones son en idioma inglés. En la *tabla 5* se muestra el resultado de este proceso.

Tabla 5: Resultados de aplicar filtros manuales

Base de datos	Acceso completo	Fuentes Primarias
ProQuest	84	20
Science Direct	12	3
CORE	161	7
TOTAL	257	30

La mayoría de las publicaciones que fueron descartadas abordaban una temática de ciberseguridad, pero con una orientación distinta al robo de información. Con respecto a las publicaciones duplicadas, sólo se encontró una, y se decidió continuar trabajando con la encontrada en CORE.

Finalmente se ha evaluado la calidad de los 30 artículos preseleccionados para obtener los que serán analizados en la siguiente etapa. En la *tabla 6* se muestra la cantidad de artículos seleccionados por base de datos.

Tabla 6: Resultados al aplicar criterios de calidad

Base de datos	Fuentes Primarias	Seleccionados
ProQuest	20	14
Science Direct	3	2
CORE	7	7
TOTAL	30	23

Análisis de datos

El primer paso para el análisis será enumerar los artículos seleccionados en la etapa anterior. A continuación, pensando en responder las preguntas de investigación se incluirán

los datos de interés como el país, revista donde se publicó y su(s) autor(es). Para efectos prácticos, en el caso del país se considerará donde finalmente fue publicado el artículo y no el país del autor ni donde se desarrolló la investigación. Los resultados de esta clasificación de encuentran organizados en la *tabla 7.*

Tabla 7: Listado de artículos seleccionados para el análisis

Título	País de Publicación	Revista	Autores
ProQuest			
A Comparative Analysis of Anti-Phishing Mechanisms: Email Phishing [3]	India	International Journal of Advanced Research in Computer Science; Udaipur	Sankhwar, Shweta Pandey, Dhirendra
A Review of Trends and Issues of Cybersecurity in Academic Libraries [4]	Estados Unidos	Library Philosophy and Practice; Lincoln	Ajie, Ifeoma
A Review on Cyber Crime: Major Threats and Solutions [5]	India	International Journal of Advanced Research in Computer Science; Udaipur	Wadhwa, Amit Arora, Neerja
A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem [6]	Hong Kong	International Journal of Computer Network and Information Security; Hong Kong	Ahmet Ali Süzen
A survey on android security: development and deployment hindrance and best practices [7]	Indonesia	TELKOMNIKA; Yogyakarta	Sikder, Ratul Khan, Shohel Hossain, Shohrab Khan, Wazir Zada
Cyber espionage through Botnets [8]	Reino Unido	Security Journal; London	Bederna Zsolt Szadeczky Tamas
Cyber Security Threat Modeling for Supply Chain Organizational Environments [9]	Suiza	Future Internet; Basel	Yeboah-Ofori, Abel Islam, Shareeful
Evolution of Phishing and Business Email Compromise Campaigns in the Czech Republic [10]	Hungría	Academic and Applied Research in Military and Public Management Science; Budapest	Kolouch, Jan
Got Phished? internet Security and Human Vulnerability [11]	Estados Unidos	Journal of the Association for Information Systems; Atlanta	Goel, Sanjay Williams, Kevin Dincelli, Ersin
Internet Banking: Identity Theft And Solutions - The Nigerian Perspective [12]	Canadá	Journal of Internet Banking and Commerce; Ottawa	Ebem, Deborah Uzoamaka Onyeagba, Joseph Chinonye Ugwuonah, Geraldine Egondu
Social Engineering Attacks: A Survey [13]	Suiza	Future Internet; Basel	Salahdine, Fatima Kaabouch, Naima
Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model [14]	Suiza	Information; Basel	Airehrour, David Nisha Vasudevan Nair
Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations [15]	Hong Kong	International Journal of Computer Network and Information Security; Hong Kong	Samaneh Madanian Fan, Wenjun Lwakatare, Kevin Rong, Rong
The Evolving Landscape Of Cyber Threats [16]	India	Vidwat; Hyderabad	Ramakrishnan, Ullas P Tandon, J K
ScienceDirect			
Remote Attacks Taxonomy and their Verbal Indicators [17]	Rusia	Procedia Computer Science	Natalia Miloslavskaya
A Framework for Cyber Crime Investigation [18]	Turquía	Procedia Computer Science	Ayşe Okutan Yalçın Çebi

CORE			
Breaking the Target: An Analysis of Target Data Breach and Lessons Learned [19]	Estados Unidos	arXiv.org; Ithaca	Shu, Xiaokui Tian, Ke Ciambrone, Andrew Yao, Danfeng
Cert Strategy To Deal With Phishing Attacks [20]	Estados Unidos	arXiv.org; Ithaca	Sedaghat, Shahrzad
Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit [21]	Estados Unidos	arXiv.org; Ithaca	Nurse, Jason R C
Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions [22]	Estados Unidos	arXiv.org; Ithaca	Gupta, B B Nalin Asanka Gamagedara Arachchilage Psannis, Konstantinos E
Phishing Detection: Analysis of Visual SimilarityBased Approaches [23]	India	Security and Communication Networks	Ankit Kumar Jain Gupta, B B
Ransomware: A New Era of Digital Terrorism [24]	India	PURKH	Richa Indu Anuj Sharma
URL-based Phishing Detection using Entropy of Non-Alphanumeric Characters [25]	Japón	Waseda University Repository	Aung, Eint Yamana, Hayato

Resultados y Discusión

Los documentos seleccionados fueron revisados exhaustivamente, a continuación, se presentan los resultados obtenidos mientras se responde a las preguntas de investigación.

¿Qué autores han escrito más sobre la ciberseguridad orientada al robo de la información?

Para responder a esta pregunta, los artículos de investigación fueron clasificados y agrupados en la *tabla 8* según su autor.

Tabla 8: Clasificación de las investigaciones por autor

Autor	Publicaciones	Cantidad
Gupta, B B	[23] [22]	2
Ahmet Ali Süzen	[6]	1
Airehrour, David	[14]	1
Ajie, Ifeoma	[4]	1
Ankit Kumar Jain	[23]	1
Anuj Sharma	[24]	1
Arora, Neerja	[5]	1
Aung, Eint	[25]	1
Ayşe Okutan	[18]	1
Bederna Zsolt	[8]	1
Ciambrone, Andrew	[19]	1
Dincelli, Ersin	[11]	1
Ebem, Deborah Uzoamaka	[12]	1
Fan, Wenjun	[15]	1
Goel, Sanjay	[11]	1
Hossain, Shohrab	[7]	1
Islam, Shareeful	[9]	1
Kaabouch, Naima	[13]	1

Khan, Shohel	[7]		1
Khan, Wazir Zada	[7]		1
Kolouch, Jan	[10]		1
Lwakatare, Kevin	[15]		1
Nalin Asanka Gamagedara Arachchilage	[22]		1
Natalia Miloslavskaya	[17]		1
Nisha Vasudevan Nair	[14]		1
Nurse, Jason R C	[21]		1
Onyeagba, Joseph Chinonye	[12]		1
Pandey, Dhirendra	[3]		1
Psannis, Konstantinos E	[22]		1
Richa Indu	[24]		1
Rong, Rong	[15]		1
Salahdine, Fatima	[13]		1
Samaneh Madanian	[14]		1
Sankhwar, Shweta	[3]		1
Sedaghat, Shahrzad	[20]		1
Shu, Xiaokui	[19]		1
Sikder, Ratul	[7]		1
Szadeczky Tamas	[8]		1
Tandon, J K	[16]		1
Tian, Ke	[19]		1
Ugwuonah, Geraldine Egondu	[12]		1
Wadhwa, Amit	[5]		1
Williams, Kevin	[11]		1
Yalçın Çebi	[18]		1
Yamana, Hayato	[25]		1
Yao, Danfeng	[19]		1
Yeboah-Ofori, Abel	[9]		1
Ramakrishnan, Ullas P	[16]		1
		TOTAL	23

De los documentos seleccionados sólo Brij Gupta aparece como autor en más de una investigación, para ser exactos, aparece en dos, y ambas fueron producidas en cooperación con otros autores, pero no son las únicas obras de este autor que está afiliado al Instituto Nacional de Tecnología en Kurukshetra, India. Gupta es autor del libro “An Introduction to DDoS Attacks and Defense Mechanisms: An Analyst's Handbook” y otras obras.

Con respecto a los demás autores, si bien es cierto que en este análisis sólo aparecen en uno de los artículos, han escrito muchos más y podrían también convertirse en referentes para investigaciones posteriores, por ejemplo: Natalia G. Miloslavskaya que cuenta con 181 publicaciones, Jason R. C. Nurse con 145, Dhirendra Pandey con 103, Nalin Asanka Gamagedara Arachchilage con 81, Islam Shareeful con 49, Tamás Szádeczky con 24 y Abel Yeboah-Ofori con 11 publicaciones. Estos datos han sido recolectados del portal ResearchGate y son referenciales ya que los autores en ocasiones aparecen en publicaciones con seudónimos diferentes a los que usan regularmente.

¿Cuáles son los países donde se han publicado más investigaciones sobre el tema de ciberseguridad orientada al robo de la información?

Se han clasificado los artículos según el país donde se registró su publicación y los resultados se organizaron en la *tabla 9*.

Tabla 9: Clasificación de las investigaciones por país

País de Publicación	Publicaciones	Cantidad
Estados Unidos	[4] [11] [19] [20] [21] [22]	6
India	[3] [5] [16] [23] [24]	5
Suiza	[9] [13] [14]	3
Hong Kong	[6] [15]	2
Canadá	[12]	1
Hungría	[10]	1
Indonesia	[7]	1
Japón	[25]	1
Reino Unido	[8]	1
Rusia	[17]	1
Turquía	[18]	1
	TOTAL	23

Los resultados muestran que en Estado Unidos se ha publicado 26% de publicaciones que fueron seleccionadas, en India se encuentra 21% y le siguen Suiza con 13% y Hong Kong con 8%, en la *Figura 1* se resume de forma gráfica los datos obtenidos.

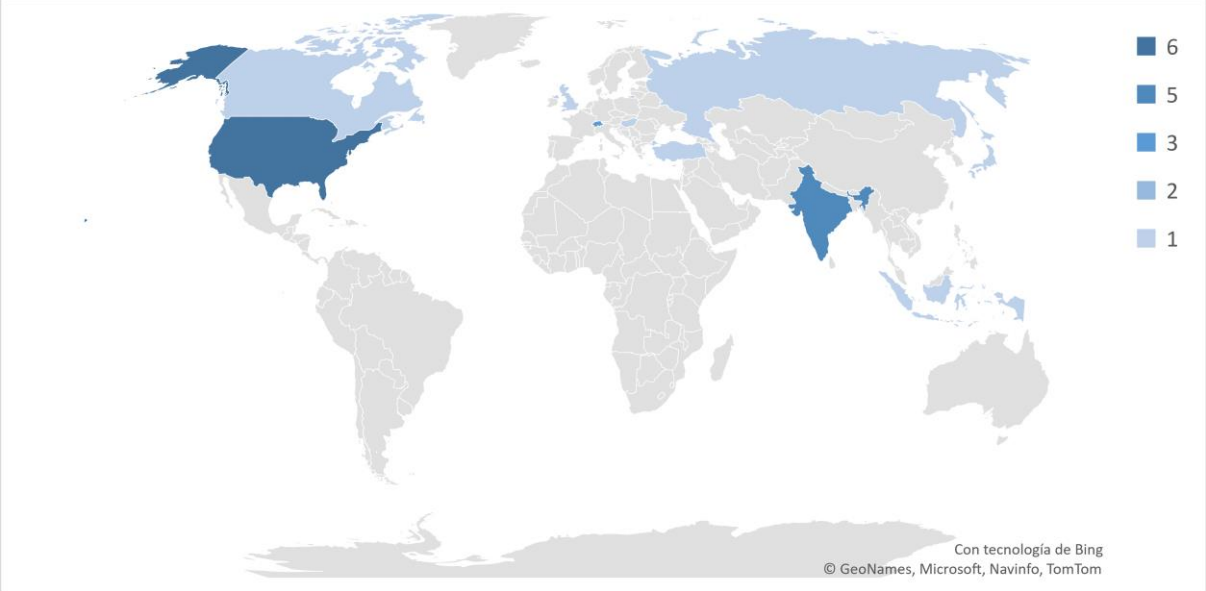

Figura 1: Cantidad de publicaciones por país

No se hace extraño que Estados Unidos destaque en investigaciones, sin embargo, algunos de los autores que publican allí son originarios de otro país e incluso han publicado también en sus países natales, por ejemplo, Brij Gupta (Gupta, B B) quien ha publicado Estados Unidos e India, este último país ubica el segundo lugar en cantidad de investigaciones seleccionadas para esta revisión. Esto se debe a que en el año 2011 ambos países firmaron un

memorando de entendimiento (MOU) para promover el intercambio de información con respecto a temas de ciberseguridad, en dicho acuerdo se involucró al CERT-In (Equipo de Respuesta a Emergencias Informáticas de la India) y el US-CERT (Equipo de preparación para emergencias informáticas de EE. UU.) [26].

En los resultados se puede observar que aparecen países cuyo idioma natal no es el inglés, sin embargo, no se encuentra entre ellos ningún país hispanohablante, no se puede considerar que el idioma sea un condicionante ya que existen investigaciones de países hispanohablantes escritos en inglés sobre otros temas, la verdadera razón se podría encontrar en estudios que ponen al descubierto una baja conciencia sobre la seguridad informática en estos países, por ejemplo, en Panamá [27], Argentina [28] o México [29].

¿En qué revistas o repositorios se ha publicado más sobre la ciberseguridad orientada al robo de la información?

La categorización de las publicaciones según la revista en la que fueron publicadas se detalla en la *tabla 10*.

Tabla 10: Clasificación de las investigaciones por revista

Revista	Publicaciones	Cantidad
arXiv.org; Ithaca	[19] [20] [21] [22]	4
Future Internet; Basel	[9] [13]	2
International Journal of Advanced Research in Computer Science; Udaipur	[3] [5]	2
International Journal of Computer Network and Information Security; Hong Kong	[6] [15]	2
Procedia Computer Science	[17] [18]	2
Academic and Applied Research in Military and Public Management Science; Budapest	[10]	1
Information; Basel	[14]	1
Journal of Internet Banking and Commerce; Ottawa	[12]	1
Journal of the Association for Information Systems; Atlanta	[11]	1
Library Philosophy and Practice; Lincoln	[3]	1
PURKH	[24]	1
Security and Communication Networks	[23]	1
Security Journal; London	[8]	1
TELKOMNIKA; Yogyakarta	[7]	1
Vidwat; Hyderabad	[16]	1
Waseda University Repository	[25]	1
	TOTAL	23

El repositorio digital arXiv.org fue de donde más investigaciones se seleccionaron para la presente revisión, allí se encuentra el 17% de artículos, le siguen las revistas “Future

Internet", "International Journal of Advanced Research in Computer Science", "International Journal of Computer Network and Information Security" y "Procedia Computer Science" con el 8% cada una, del resto de revisas sólo se seleccionó un artículo, en la *Figura 2* se resume la información.

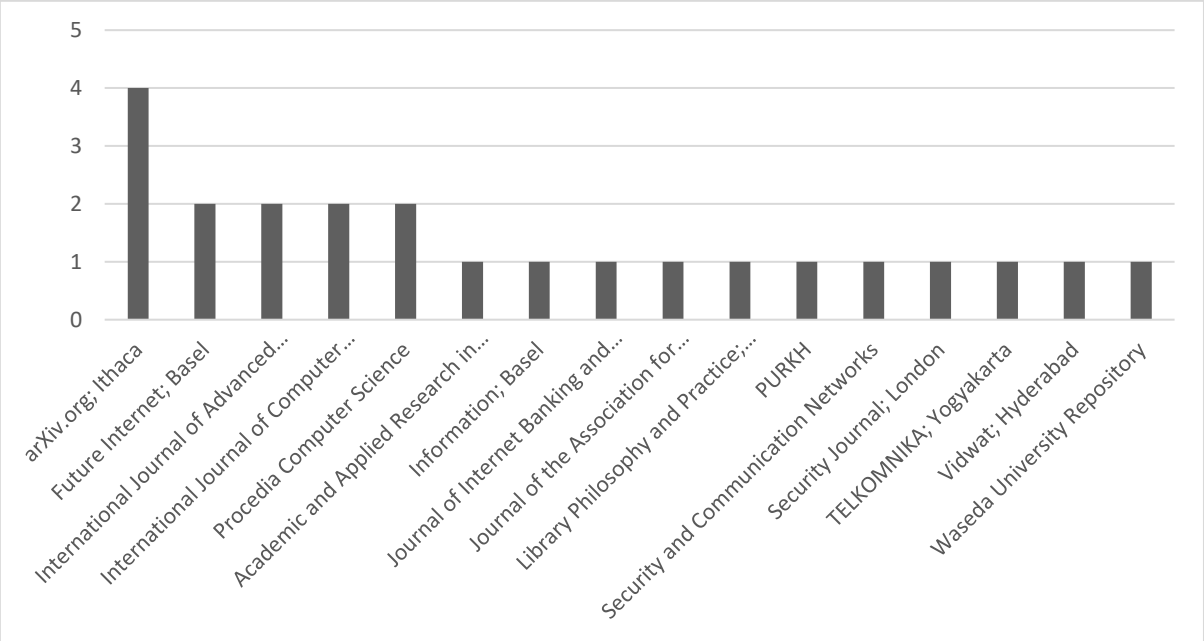

Figura 2: Cantidad de publicaciones por revista

El repositorio arXiv.org contiene artículos en campos como matemática, física, biología cuantitativa, ciencias de la computación y otros. Podría ser una buena fuente de donde obtener antecedentes para investigaciones referidas al tema de ciberseguridad orientada al robo de información, también vale la pena destacar la revista "Procedia Computer Science" que funciona desde el año 2009 y garantiza la calidad de la información que publica por trabajar directamente con la base de datos ScienceDirect.

Conclusiones

Para cumplir con los objetivos planteados en la presente revisión sistemática de la literatura se han tomado como fuentes de datos a ProQuest, ScienceDirect y CORE por su buena reputación y garantía de calidad, en cada base de datos se realizó la búsqueda de artículos con la cadena de búsqueda "cyber security AND data theft AND phishing AND (xploits OR trojan)" y los filtros planteados en los criterios de inclusión y exclusión, debido a que nos todas las bases de datos nos permitieron aplicar el total de los filtros, hubo una fase de filtrado manual donde se preseleccionaron 30 artículos a los cuales se les aplicó la

evaluación de calidad según una escala cuantitativa detallada en la sección correspondiente, y se obtuvieron finalmente 23 artículos que nos llevan a las siguientes conclusiones:

El autor que más escribe sobre la ciberseguridad orientada al robo de información es Brij Gupta, quien publica en Estados Unidos e India. Natalia G. Miloslavskaya es otra autora que se puede tomar como un claro referente por la cantidad de investigaciones que ha realizado en el campo de la seguridad informática.

Los países donde se ha publicado más sobre el tema de ciberseguridad orientado al robo de información son Estados Unidos e India, los mencionados países mantienen un acuerdo cooperativo para investigar en el campo de seguridad informática. Adicionalmente, también destacan en cantidad de publicaciones Suiza y Hong Kong.

La revista donde se publican más investigaciones sobre la ciberseguridad orientada al robo de información es arXiv.org, las investigaciones disponibles aquí se encuentran en idioma inglés, otras de las revistas reconocidas son: “Procedia Computer Science”, “Future Internet”, “International Journal of Advanced Research in Computer Science” y “International Journal of Computer Network and Information Security”.

La revisión sistemática de la literatura cumplió con encontrar referentes en cuanto a autores, países y revistas o repositorios que aportan contenidos relevantes al tema de ciberseguridad específicamente orientado al robo de información. Además, se proponen las siguientes líneas de investigación:

Medidas que toman los países para prevenir ataques informáticos y robo de información a entidades públicas.

- Algoritmos de ciberseguridad que se pueden aplicar en el desarrollo de aplicaciones.
- Medidas de protección para evitar ataques de ingeniería social.
- Estrategias para prevenir delitos informáticos en el Perú.

Agradecimientos

En primer lugar, quiero agradecer a Dios por guiar mi camino y haberme permitido realizar la presente revisión sistemática de la literatura. Gracias a la Mgtr. Karla Reyes Burgos, quien con sus conocimientos me asesoró a través de cada una de las etapas de elaboración de presente proyecto, y gracias a mi familia por ser mi soporte emocional en todo momento.

Referencias

[1] B. Kitchenham, S. Charters , D. Budgen, P. Brereton, M. Turner, S. Linkman, M. Jørgensen, E. Mendes y G. Visaggio, «Guidelines for performing Systematic Literature Reviews in Software Engineering,» Enero 2007.

[2] P. Alderson, S. Green y J. Higgins, Cochrane Reviewers' Handbook 4.2.2, Chichester: John Wiley & Sons, Ltd, 2004.

[3] Sankhwar, Shweta y Pandey, Dhirendra, «A Comparative Analysis of Anti-Phishing Mechanisms: Email Phishing,» *International Journal of Advanced Research in Computer Science*, 2017.

[4] Ajie, Ifeoma, «A Review of Trends and Issues of Cybersecurity in Academic Libraries,» *Library Philosophy and Practice*, 2019.

[5] Wadhwa, Amit y Arora, Neerja, «A Review on Cyber Crime: Major Threats and Solutions,» *International Journal of Advanced Research in Computer Science*, 2017.

[6] Ahmet Ali Süzen, «A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem,» *International Journal of Computer Network and Information Security*, 2020.

[7] Sikder, Ratul, Khan, Shohel, Hossain, Shohrab y Khan, Wazir Zada, «A survey on android security: development and deployment hindrance and best practices,» *TELKOMNIKA*, 2020.

[8] Bederna Zsolt y Szadeczky Tamas, «Cyber espionage through Botnets,» *Security Journal*, 2020.

[9] Yeboah-Ofori, Abel y Islam, Shareeful, «Cyber Security Threat Modeling for Supply Chain Organizational Environments,» *Future Internet*, 2019.

[10] Kolouch, Jan, «Evolution of Phishing and Business Email Compromise Campaigns in the Czech Republic,» *Academic and Applied Research in Military and Public Management Science*, 2018.

[11] Goel, Sanjay, Williams, Kevin y Dincelli, Ersin, «Got Phished? internet Security and Human Vulnerability,» *Journal of the Association for Information Systems*, 2017.

[12] Ebem, Deborah Uzoamaka, Onyeagba, Joseph Chinonye y Ugwuonah, Geraldine Egondu, «Internet Banking: Identity Theft And Solutions - The Nigerian Perspective,» *Journal of Internet Banking and Commerce*, 2017.

[13] Salahdine, Fatima y Kaabouch, Naima, «Social Engineering Attacks: A Survey,» *Future Internet,* 2019.

[14] Airehrour, David, Nisha Vasudevan Nair y Samaneh Madanian, «Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model,» *Information,* 2018.

[15] Fan, Wenjun, Lwakatare, Kevin y Rong, Rong, «Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations,» *International Journal of Computer Network and Information Security,* 2017.

[16] Ramakrishnan, Ullas P y Tandon, J K, «The Evolving Landscape Of Cyber Threats,» *Vidwat,* 2018.

[17] Natalia Miloslavskaya, «Remote Attacks Taxonomy and their Verbal Indicators,» *Procedia Computer Science,* 2018.

[18] Ayşe Okutan y Yalçın Çebi, «A Framework for Cyber Crime Investigation,» *Procedia Computer Science,* 2019.

[19] Shu, Xiaokui, Tian, Ke, Ciambrone, Andrew y Yao, Danfeng, «Breaking the Target: An Analysis of Target Data Breach and Lessons Learned,» *arXiv.org,* 2017.

[20] Sedaghat, Shahrzad, «Cert Strategy To Deal With Phishing Attacks,» *arXiv.org,* 2017.

[21] Nurse, Jason R C, «Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit,» *arXiv.org,* 2018.

[22] Gupta, B B, Nalin Asanka Gamagedara Arachchilage y Psannis, Konstantinos E, «Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions,» *arXiv.org,* 2017.

[23] Ankit Kumar Jain y Gupta, B B, «Phishing Detection: Analysis of Visual SimilarityBased Approaches,» *Security and Communication Networks,* 2017.

[24] Richa Indu y Anuj Sharma, «Ransomware: A New Era of Digital Terrorism,» *PURKH,* 2018.

[25] Aung, Eint y Yamana, Hayato, «URL-based Phishing Detection using Entropy of Non-Alphanumeric Characters,» *Waseda University Repository,* 2019.

[26] Leithauser, Tom, «U.S., India agree to share cyber threat information,» *Cybersecurity Policy Report,* 2011.

[27] EFE News Services, Inc., «Estudio advierte que en Panamá es poco valorada la seguridad

informática: PANAMÁ INFORMÁTICA,» *EFE News Service,* 2011.

[28] LA NACION - Argentina, «Cuestionan la seguridad informática,» *La Nación,* 2008.

[29] Vizcaino, Adriana, «Falla seguridad informatica,» *Reforma,* 2002.

[30] A. Sasse y I. Kirlappos, «Security Education against Phishing: A Modest Proposal for a Major Rethink,» IEEE Security & Privacy, 2012.

[31] E. Lebanidze, «Securing Enterprise web Aplications at the Source: An Application Security Perspective».

[32] J. M. Alonso Cebrián, *Seminario Empresarial: Ciberseguridad,* Valencia: AITEX, 2020.