



UNIVERSIDAD
PRIVADA
DEL NORTE

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“APLICACIÓN DE BIG DATA EN CIBERSEGURIDAD
UTILIZANDO INTELIGENCIA ARTIFICIAL EN LOS
AÑOS 2014 - 2023: UNA REVISIÓN DE LA
LITERATURA CIENTÍFICA”

Trabajo de investigación para optar el grado de:

Bachiller en Ingeniería de Sistemas Computacionales

Autor:

Hitler Manrique Heredia

Asesor:

Mg. Ing. Manuel Ricardo Mondragón Vilela

Lima - Perú

2019

INFORME DE SIMILITUD

APLICACIÓN DE BIG DATA EN CIBERSEGURIDAD UTILIZANDO INTELIGENCIA ARTIFICIAL EN LOS AÑOS 2014 - 2023: una revisión de la literatura científica

INFORME DE ORIGINALIDAD



FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	4%
2	repositorio.upn.edu.pe Fuente de Internet	3%
3	www.risti.xyz Fuente de Internet	2%
4	www.researchgate.net Fuente de Internet	1%
5	www.icesi.edu.co Fuente de Internet	1%
6	napier-repository.worktribe.com Fuente de Internet	1%
7	brazilianjournals.com Fuente de Internet	1%
8	Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO Trabajo del estudiante	1%

DEDICATORIA

Dedico este trabajo a aquellas personas que creyeron en mí aun cuando yo mismo no lo hice, a mi mamá, mi padre, mis hermanas y hermano que fueron el motor que echó a andar mis sueños y a mi hijo Dereck el que le dio dirección a mi vida.

AGRADECIMIENTO

Agradezco a Dios por su inmenso amor, a la Universidad Privada del Norte por mi formación, a mis maestros por sus consejos y en especial a mi maestro Ricardo Mondragón por su paciencia y apoyo.

TABLA DE CONTENIDO

INFORME DE SIMILITUD.....	2
DEDICATORIA.....	3
AGRADECIMIENTO	4
TABLA DE CONTENIDO	5
ÍNDICE DE TABLAS	6
ÍNDICE DE FIGURAS.....	7
RESUMEN.....	8
CAPÍTULO I. INTRODUCCIÓN	9
CAPÍTULO II. METODOLOGÍA.....	15
CAPÍTULO III. RESULTADOS	23
CAPÍTULO IV. CONCLUSIONES.....	35
REFERENCIAS.....	38

ÍNDICE DE TABLAS

Tabla 1 Selección de Revistas Científicas	21
Tabla 2 Relación de Artículos Seleccionados antes de su revisión final.....	24
Tabla 3 Relación de Artículos Eliminados tras su revisión final.....	28
Tabla 4 Resultados del análisis de los artículos seleccionados por Tipo de publicación y país.....	31
Tabla 5 Distribución de artículos por tipo de investigación	31
Tabla 6 Cantidad de Artículos según Bases de datos consultadas.....	32
Tabla 7 Palabras clave referenciadas en las palabras clave de los artículos seleccionados	32

ÍNDICE DE FIGURAS

Figura 1 Palabras Clave del trabajo de investigación	17
Figura 2 Artículos Seleccionados almacenados en el gestor de referencias zotero .	17
Figura 3 Flujograma de Selección de Artículos.....	20
Gráfico 1 Cantidad de Revistas por año de Publicación.....	30

RESUMEN

El desarrollo de las tecnologías ha cambiado la manera en que las personas y cosas hacen uso del internet generando oportunidades y vulnerabilidades en la seguridad de la información, el uso de estas tecnologías genera grandes volúmenes de datos que pueden ser aprovechados para el desarrollo de la inteligencia Artificial (IA) para entrenar y mejorar los algoritmos de aprendizaje automático, la ciberseguridad tiene como aliada a la IA para detectar y prevenir ataques cibernéticos.

El objetivo principal del estudio es analizar la aplicación de Big data en Ciberseguridad utilizando IA, se identificaron artículos de las bases de datos bibliográficas como Dialnet, Scielo, Google Académico, Redalyc, Proquest, Scient Direct, Scopus utilizando palabras Claves en publicaciones entre los años 2014-2023 en idioma inglés o español y tipo de publicación artículos de revistas académicas. Se obtuvo un total de 29 artículos ordenados mediante una tabla con columnas que proporcionaron una fuente de información para los análisis realizados.

Se identifico el impacto que tiene big data en la ciberseguridad mediante el empleo de IA como Machine Learning en el análisis y creación de modelos para la detección e identificación de ataques mediante el aprendizaje por análisis de inmensos volúmenes de datos proporcionados por big data.

PALABRAS CLAVES: big data, ciberseguridad, inteligencia artificial, Cybersecurity, Artificial Intelligence

CAPÍTULO I. INTRODUCCIÓN

En los últimos años los desarrollos de las tecnologías han revolucionado las formas en la que las personas hacen uso de internet tal es así que hoy en día se habla de internet de las cosas (IoT) que hace referencia a innumerables dispositivos en todo el mundo (8700 millones de dispositivos en 2020) que se pueden conectar a internet y que recopilan y comparten datos entre sí sin la intervención humana y que está diseñada para aplicarse en muchos sectores que son cruciales como la seguridad nacional ,el sector médico que son particularmente vulnerables a ataques cibernéticos porque poseen información de valor monetario y de inteligencia significativo (Javaid et al., 2023),(Paul et al., 2023), la economía con diferentes estándares y especificaciones de la industria pero lamentablemente carecen de protocolos de seguridad solidos haciéndolos vulnerables (Gerodimos et al., 2023), todo este desarrollo tecnológico ha generado un incremento acelerado en la generación de grandes volúmenes de datos (Big Data) dando lugar a desafíos para el uso de análisis de Big Data en relación a la construcción o mejoramiento de los sistemas de Ciberseguridad mediante la detección de intrusos de seguridad cibernética , para ello todo sistema debe procesar datos de tráfico de red de gran tamaño lo más rápido posible para detectar el tráfico malicioso lo antes posible, siendo la Inteligencia Artificial una Aliada para realizar esta tarea.(Valencia-Arias et al., 2022).

La inteligencia Artificial está cobrando una gran importancia en el desarrollo de las tecnologías debido a que la podemos encontrar inmersa en el ámbito administrativo o judicial, en el monitoreo de nuestra salud , sistema de asistencia vehicular, de producción

ciber física, en las finanzas, la banca y el campo militar como algoritmos, para poder alimentar la toma de decisiones algorítmicas hacen falta dos insumos importantes :gran cantidad de datos (Big data) y energía, así tenemos que los datos son los que alimentan el núcleo de la IA,sin estos su desarrollo, entrenamiento y procesamiento para la toma de decisiones no sería posible (Gil, 2021).

Según (Caiza Narvárez et al., 2022) , para el año 2017 se tenía 9 mil millones de dispositivos IoT conectados y se estima que para el 2025 sean 64 mil millones, este incremento de dispositivos conectados nos mostraría una dependencia tecnológica de la sociedad así como el incremento del riesgo que implicaría de que los sistemas sean vulnerados debido a que los dispositivos inteligentes están siendo construidos sin tener en cuenta un nivel aceptable de ciberseguridad , esto podría ser aprovechado mediante técnicas que permitan vulnerar la seguridad y con ello poner en riesgo la información personal y confidencial de los usuarios y asegura también que Big Data Analítica es capaz de recopilar, almacenar y analizar grandes cantidades de datos a través de algoritmos de correlación en la detección de anomalías para identificar ataques maliciosos y reaccionar a tiempo frente a dichas amenazas.

Según (Galeano Villar & Vargas Cisneros, 2019) los modelos de aprendizaje automático son utilizados como apoyo en la detección de transacciones sospechosas de lavado de activos en las economías de los países, valiéndose para ello de Big data para obtener información en tiempo real que permite su adecuación a un entorno cambiante siendo el algoritmo de agrupación el más utilizado en sus estudios realizados.

Según (Macias et al., s. f.) los honeypot son sistemas configurados con el único propósito de ser atacados en las intrusiones cibernéticas, se usan como señuelos para registrar las actividades maliciosas lanzada por el atacante a la red de datos, cabe mencionar que los principales ataques se producen al IoT, honeypot aporta mucha información pero también introducen un riesgo ya que al ser diseñados para ser atacado tiene una alta probabilidad de ser atacados y por ello se propone una arquitectura de seguridad para servidores web denominada Web Attacks Cognitive Patterns Classifier que brinda una solución más completa y que incorpora herramientas como Elasticsearch, Logstash y Kibana, dicho sistema se nutre de información suministrada por algoritmos de Machine Learning y Big data para determinar patrones de ataque y clasificaciones.

Según (Pabon et al., 2023) menciona que la inteligencia artificial tiene por finalidad automatizar los procesos a cualquier escala o sector, incidiendo en procesos manuales repetitivos que los humanos realizan pero con la diferencia de hacerlos a altas velocidades (análisis de datos, procesamiento de imágenes, entre otras) lo que repercute en costos y eficiencia además señala que el Grupo de Investigación de Big Data y Machine Learning aplicado a la ciberseguridad indica que debido a la gran cantidad de datos generados por nuestras actividades en la red se hace complicado la detección de ataques de seguridad por lo que se hace necesario utilizar herramientas de Big data como analítica de datos que permite apalancar los procesos tradicionales de ciberseguridad. Se han aplicado numerosos algoritmos de Machine Learning en muchas áreas de ciberseguridad que han contribuido a tener un 95% de éxito en la detección de intrusiones (Sharma et al., 2022).

Según (Quirumbay Yagual et al., 2022) Actualmente se genera y recopila una gran cantidad de datos (Big Data) como resultado de la implementación de las tecnologías en Auge lo cual

conlleva un reto para la Ciberseguridad que se caracteriza como la colección de tecnologías y procesos diseñados para proteger las computadoras, redes ,programas y datos contra actividades maliciosas, ataques , daños o accesos no autorizados, todo ello conlleva a la necesidad de implementar medidas de seguridad haciendo uso de técnicas de aprendizaje basadas en grandes cantidades de datos la que combina aspectos de aprendizaje automático o inteligencia artificial como las redes neuronales artificiales y las redes de aprendizaje profundo(Machine Learning y Deep Learning) para la detección de intrusiones .

Según (Urcuqui et al., 2016) el internet conecta alrededor de tres mil millones de usuarios en el mundo y es un número que se incrementa cada año, es gracias a esta tecnología que las personas, las compañías y los dispositivos realizan tareas diversas que generan una difusión de grandes volúmenes de información sensible y la falta de conocimiento en seguridad en el desarrollo de aplicaciones web ha generado el incremento de ataques a sitios web mediante distintas vulnerabilidades como inyecciones SQL, pérdida de autenticación, secuencias de comandos en sitios cruzados, re direcciones que en algunos casos tiene por finalidad realizar una modificación no autorizada en la página web (Defacement); existen distintas técnicas y sistemas para la detección de ataques que generan defacement en una página web, técnicas como análisis dinámico, estático, la utilización de inteligencia artificial (mediante la identificación de patrones haciendo uso de Big data) y el análisis sobre el tráfico de la red que permita identificar el ataque y su tipo antes de generarse el defacement.

Así (Wiafe et al., 2020) los delitos cibernéticos están tomando mayor complejidad lo que conlleva a que los métodos de ciberseguridad actuales deban ser robustos e inteligentes. los ciberataques se caracterizan por un alto nivel de sofisticación que hace necesaria la adopción de Inteligencia Artificial o agentes inteligentes para combatirlos (esto debido a la gran

cantidad de datos que se manejan), dentro del estudio se tomó referencia a los algoritmos de IA que se han venido implementando como: AdaBoost, CNN, SVM, KNN, ANN, K-Means, Q-Learning, Random Forest, RNN, Decisions Trees donde los estudios que abordaron el aprendizaje automático muestran que ANN y sus métodos relacionados son efectivos para la ciberseguridad.

Según (Castro Salaverry et al., s. f.) en la actualidad los dispositivos móviles facilitan la vida a millones de usuarios, en él se realizan muchas tareas y se almacenan información confidencial, estos dispositivos tienden a ser atacados por malware del tipo Ransomware y como consecuencia en muchos casos se tiene que realizar el pago para poder recuperar el acceso a sus teléfonos(para el 2022 se estima que se pagaron 17 millones de dólares como rescate de datos), es por ello que surgió la necesidad de utilizar una herramienta de Análisis como Machine Learning que mediante enfoques de aprendizaje profundo (J48 Decision Tree, Naive Bayes, R-PackDroid, Artificial Neutral Network, NFV/SDN, Support Vector Machine, Random Forest y K-Nearest Neighbors) facilitan la detección de Ransomware con altos porcentajes de efectividad siendo SVM el más utilizado para dicha detección.

Según (Castellanos Rojas et al., 2020) la ciberseguridad surgió como la necesidad de proteger la información en referencia a diferentes ataques de software malicioso que genera el robo de datos privados que generan grandes pérdidas para lo cual se tuvo que desarrollar diferentes estrategias para combatir el robo de datos siendo una de ellas la aplicación de inteligencia Artificial mediante la Red Neuronal Artificial(RNA) que es un grupo interconectado de nodos agrupadas en niveles las cuales se fortalece con cada ataque mediante la técnica de aprendizaje Autónomo (Machine Learning) que se nutre de colecciones masivas de datos(Big Data) para desarrollar algoritmos y consolidar una

capacidad lógica eficiente la cual , por tal motivo las RNA demuestran ser algoritmos eficientes para reducir los ataques de spam, Ingeniería Social o cualquier otro tipo de técnica que intente vulnerar los sistemas de seguridad.

Según (Rodrigues et al., 2022) en la actualidad se puede explotar nuevas oportunidades a través de la tecnología IA que es la capacidad de un sistema para interpretar correctamente datos externos, aprender de dichos datos y utilizar esos aprendizajes para lograr objetivos y tareas específicos a través de una adaptación flexible

Ante lo expuesto se realizó la presente investigación a fin de responder a la pregunta ¿Cuál ha sido el impacto de la aplicación de big data en Ciberseguridad utilizando inteligencia artificial en los años 2014 - 2023? y para poder dar respuesta a dicha pregunta se plantea como objetivo analizar la aplicación de Big data en Ciberseguridad utilizando Inteligencia Artificial en los años 2014 – 2023 a través de los artículos científicos.

CAPÍTULO II. METODOLOGÍA

Tipo de estudio

Se realizó una revisión sistemática tomando como referencia la adaptación del protocolo prisma (Moher et al., 2009). La pregunta de investigación fue definida como ¿Cuál ha sido el impacto de la aplicación de big data en Ciberseguridad utilizando inteligencia artificial en los años 2014 – 2023?

Criterios de elegibilidad

Se han considerado en la revisión sistemática 29 artículos científicos de los años 2014 - 2023 en idioma inglés y español.

Se considero solo artículos de investigación con temáticas que hacen referencia a:

- ✓ Big Data y su relación con Ciberseguridad.
- ✓ Big data y su importancia en el desarrollo de la Inteligencia Artificial.
- ✓ Inteligencia Artificial y su contribución a la ciberseguridad.
- ✓ Relación entre Big Data, Ciberseguridad e Inteligencia Artificial.

Fuentes de Información

Para poder realizar el trabajo de revisión se consultaron los bases de datos bibliográficas como Dialnet, Scielo, Google Académico, Redalyc, Proquest, Scient Direct,

Scopus utilizando palabras Claves como Big Data, Ciberseguridad, Inteligencia Artificial, Cybersecurity, Artificial Intelligence.

Estrategia de búsqueda

La estrategia utilizada para la recopilación de revistas fue realizar una búsqueda en las bases de datos bibliográficas como Dialnet, Scielo, Google Académico, Redalyc, Proquest, Scient Direct, Scopus, usando palabras clave junto con la combinación de operadores booleanos para hacer más eficiente la búsqueda ((CIBERSEGURIDAD) AND ("INTELIGENCIA ARTIFICIAL") , BIG DATA + "CIBERSEGURIDAD" , BIG DATA + "CIBERSEGURIDAD" + "INTELIGENCIA ARTIFICIAL" , "INTELIGENCIA ARTIFICIAL" + "CIBERSEGURIDAD" , (CIBERSEGURIDAD) AND ("INTELIGENCIA ARTIFICIAL") AND ("BIG DATA") , "ARTIFICIAL INTELLIGENCE" + "CYBERSECURITY"), teniendo presente que sus contenidos estuvieran dentro de la misma línea de investigación y que sean solo artículos de investigación o revista científicas así como sus fechas de publicación se encuentren dentro de los años 2014 – 2023.

Figura 1

Palabras Clave del Trabajo de Investigación

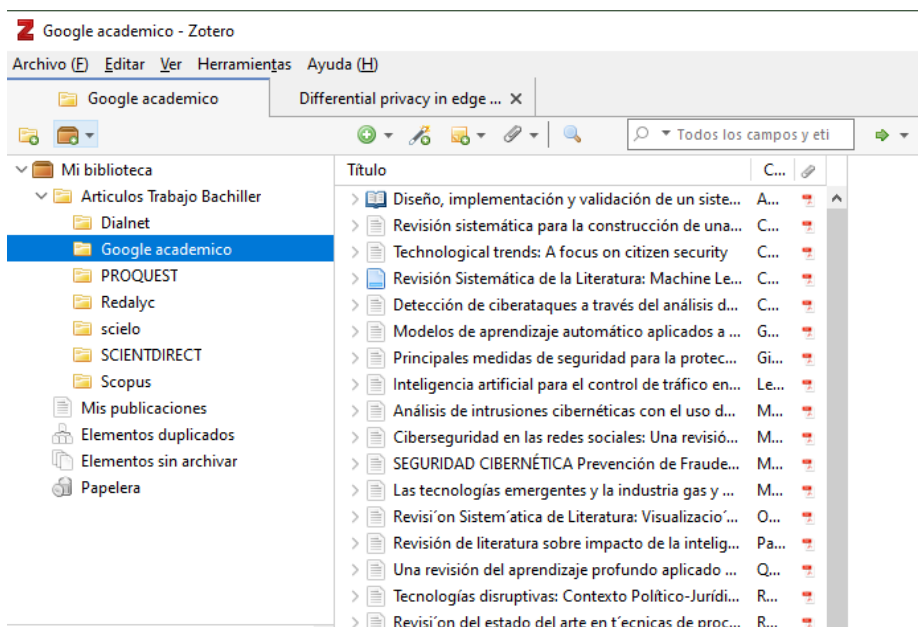


Nota: Fuente elaboración propia

Además, se usó como gestor de referencias bibliográficas a Zotero para Ordenar los artículos, así como insertar las citas y referencias en el trabajo de investigación. En Zotero se separó en carpetas los artículos por bases de datos para una mejora apreciación.

Figura 2

Artículos Seleccionados Almacenados en el Gestor de Referencias Zotero



Nota: Fuente elaboración propia

Proceso de selección de estudios

Para la selección de estudios se tuvieron en cuenta los criterios tanto de inclusión como de exclusión, así del total de estudios encontrados se fueron excluyendo aquellos que distaban en su enfoque y contexto con los objetivos de la presente revisión, excluyendo así aquellos también que a pesar de cumplir con los requisitos de inclusión presentaban el problema de no poder acceder a la información completa del artículo por ser de paga y por tal motivo hacían difícil el poder profundizar en el contenido de dicho artículo. En total el proceso de selección se realizó en tres fases, la primera fase en la que se realizó una selección rápida basado en las palabras en alguna de las palabras clave considerando los criterios de inclusión y exclusión (se obtuvo un total de 101 estudios), en la segunda fase se revisaron los estudios considerando su relevancia y coincidencias con las palabras clave (se obtuvieron 59 estudios) y en la tercera fase se realizó una revisión más profunda y analizando los objetivos y enfoques alineados a los objetivos obteniendo de esta manera los 29 estudios.

Criterios de inclusión y exclusión de las revistas científicas.

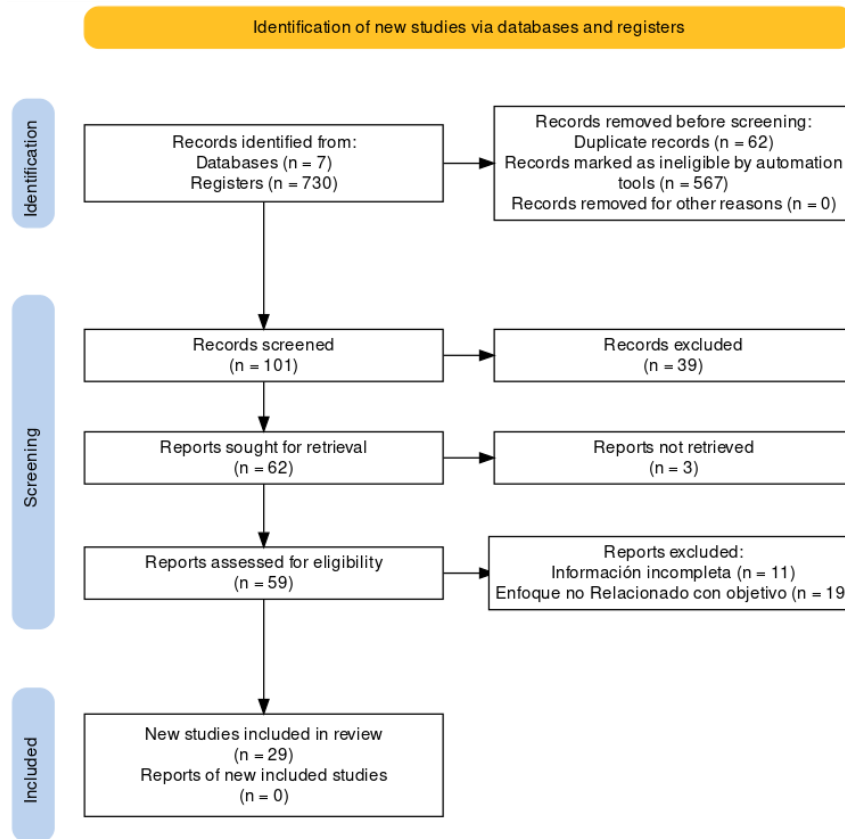
Los criterios de inclusión y exclusión empleados fueron que pertenezcan al rango de años 2014 al 2023, que sean en idioma inglés o español, que sean trabajos con rigor científico de preferencia artículos de investigación, que contengan las palabras clave al menos 1 de ellas y que guarden relación con el objetivo de nuestro estudio. Se realizó una búsqueda teniendo como criterios de inclusión y exclusión el periodo de tiempo del 2014 al 2023 obteniendo entre el 2020 al 2023 un total de 24 revistas seleccionadas (83%) además se consideraron

revistas en el idioma inglés y español, observando el predominio de las revistas en español dentro de nuestra selección con un total de 17 (59%) y en inglés 12 (41%).

Utilizando las palabras clave y los conectores lógicos se obtuvieron en un inicio un total de 730 Coincidencias de las cuales eran de Scielo (4), Google Académico (134), Redalyc (385), Dialnet (1), Proquest (96), Scient Direct(61), Scopus (49), en una revisión rápida se descartaron 629 porque no guardaban relación con la línea de investigación del presente trabajo (relación entre Big data, Inteligencia Artificial, Ciberseguridad) 62 de los cuales estaban duplicados , de las 101 revistas seleccionadas en una revisión rápida se realizó una revisión rápida buscando el contexto de las palabras claves dentro de los resúmenes y objetivos planteados llegando a descartar en esta oportunidad 42 trabajos de investigación, 3 de los cuales se descartaron porque no se podía acceder al informe por ser de paga.

De los 59 Archivos seleccionados se realizó una revisión más exhaustiva encontrando que 11 de dichos archivos no tenían la información completa y 19 al ser leída completamente se encontró que no estaban en el contexto del presente trabajo de investigación quedando finalmente 29 trabajos que han sido la base del presente trabajo.

Figura 3
Flujograma de Selección de Artículos



Nota: Fuente elaboración propia

Tabla 1

Selección de Revistas Científicas

Título	Tipo de publicación	País	Idioma	Año de Publicacion	Años antigüedad	Tipo estudio	Criterios de Calidad
Revisión Sistemática Para La Construcción De Una Arquitectura Con Tecnologías Emergentes Iot, Técnicas De Inteligencia Artificial, Monitoreo Y Almacenamiento De Tráfico Malicioso	Articulos De Investigacion	España	Español	2022	1	Investigacion Descriptiva	Alto
Tendencias Tecnológicas: Un Enfoque En La Seguridad Ciudadana	Articulos De Investigacion	Colombia	Español	2021	2	Investigacion Descriptiva	Medio
Detección De Ciberataques A Través Del Análisis De Mensajes De Redes Sociales: Revisión Del Estado Del Arte	Articulos De Investigacion	México	Español	2020	3	Investigacion Descriptiva	Alto
Modelos De Aprendizaje Automático Aplicados A La Detección De Transacciones Sospechosas De Lavado De Activos En Entidades Financieras: Una Revisión Sistemática De La Literatura	Trabajo de Investigacion	Perú	Español	2019	4	Investigacion Descriptiva	Alto
Análisis De Intrusiones Cibernéticas Con El Uso Del Honeypots. Una Revisión Sistemática	Articulos De Investigacion	Brasil	Español	2021	2	Investigacion Documental	Alto
Revisión De Literatura Sobre Impacto De La Inteligencia Artificial Y Su Aplicación En El Ecuador	Articulos De Investigacion	Ecuador	Español	2023	0	Investigacion Documental	Alto
Antidefacement - State Of Art	Articulos De Investigacion	Colombia	Español	2016	7	Investigacion Documental	Medio
Artificial Intelligence For Cybersecurity: A Systematic Mapping Of Literature	Articulos De Investigacion	No Detalla	Inglés	2020	3	Investigacion Documental	Alto
Revisión Sistemática De La Literatura: Machine Learning Para La Detección De Ransomware En Dispositivos Móviles	Articulos De Investigacion	Perú	Español	2022	1	Investigacion Documental	Alto
Redes Neuronales Artificiales Y Estado Del Arte Aplicado En La Ciberseguridad	Articulos De Investigacion	Colombia	Español	2020	3	Investigacion Documental	Alto
Ciberseguridad. Presentación Del Dossier	Revista	Ecuador	Español	2017	6	Investigacion Documental	Medio
Artificial Intelligence, Digital Transformation And Cybersecurity In The Banking Sector: A Multi-Stakeholder Cognition-Driven Framework	Articulos De Investigacion	No Detalla	Inglés	2022	1	Investigacion Documental	Medio
Tendencias Investigativas En El Uso De Tecnologías De Big Data En Sistemas De Ciberseguridad	Articulos De Investigacion	No Detalla	Español	2022	1	Investigacion Documental	Alto
Retos Para La Regulación Jurídica De La Inteligencia Artificial En El Ámbito De La Ciberseguridad	Articulos De Investigacion	México	Español	2021	2	Investigacion Documental	Alto
Security Control For Website Defacement	Articulos De Investigacion	Colombia	Inglés	2017	6	Investigacion Documental	Medio

Título	Tipo de publicación	País	Idioma	Año de Publicacion	Años antigüedad	Tipo estudio	Criterios de Calidad
Prospectiva De Ciberseguridad Nacional Para Colombia A 2030	Articulos De Investigacion	Colombia	Español	2022	1	Investigacion Documental	Medio
La Ciberseguridad En La Era De Hipercompetitividad: ¿Puede La Ue Afrontar Los Nuevos Retos?	Articulos De Investigacion	España	Español	2022	1	Investigacion Documental	Medio
Una Comparativa De Los Esquemas De Ciberseguridad De China Y Estados Unidos	Articulos De Investigacion	Colombia	Español	2021	2	Investigacion Documental	Medio
Revisión De Las Tecnologías Presentes En La Industria 4.0	Articulos De Investigacion	Colombia	Español	2020	3	Investigacion Documental	Medio
Riesgos Y Vulnerabilidades De La Denegación De Servicio Distribuidos En Internet De Las Cosas	Articulos De Investigacion	Colombia	Español	2019	4	Investigacion Documental	Alto
Iot: Communication Protocols And Security Threats	Articulos De Investigacion	No Detalla	Inglés	2023	0	Investigacion Documental	Alto
The Rise Of Machine Learning For Detection And Classification Of Malware: Research Developments, Trends And Challenges	Articulos De Investigacion	España	Inglés	2020	3	Investigacion Documental	Alto
Towards Insighting Cybersecurity For Healthcare Domains: A Comprehensive Review Of Recent Practices And Trends	Articulos De Investigacion	India	Inglés	2023	0	Investigacion Documental	Medio
Artificial Intelligence For Cybersecurity: Literature Review And Future Research Directions	Articulos De Investigacion	Slovenia	Inglés	2023	0	Investigacion Documental	Alto
Digitization Of Healthcare Sector: A Study On Privacy And Security Concerns	Articulos De Investigacion	No Detalla	Inglés	2023	0	Investigacion Documental	Alto
Explainable Artificial Intelligence For Cybersecurity	Articulos De Investigacion	No Detalla	Inglés	2022	1	Investigacion Documental	Medio
Differential Privacy In Edge Computing-Based Smart City Applications: Security Issues, Solutions And Future Directions	Articulos De Investigacion	No Detalla	Inglés	2023	0	Investigacion Documental	Alto
A Systematic Literature Review Of Blockchain Cyber Security	Articulos De Investigacion	No Detalla	Inglés	2020	3	Investigacion Documental	Medio
A Blockchain-Based Architecture And Framework For Cybersecure Smart Cities	Articulos De Investigacion	No Detalla	Inglés	2023	0	Investigacion Documental	Alto

Nota: Elaboración Propia de las revistas seleccionadas entre los años 2014 al 2023

CAPÍTULO III. RESULTADOS

Proceso de selección de estudios examinados

La búsqueda de las revistas científicas dio como resultado 59 revistas originales con fechas de publicación entre los años 2014 al 2023. La extracción de datos de los estudios se realizaron estructurando una tabla con los encabezados como bases de datos, título, tipo de publicación, país, idioma, año de publicación, Editorial, Tipo de estudio, criterios de calidad como se muestra en la tabla 1 en la que se puede observar que los estudios seleccionados fueron una del año 2016, dos del año 2017, cuatro del año 2017, tres del año 2018, cinco del 2019, doce del año 2020, ocho del año 2021, catorce del año 2022, diez del año 2023 y 1 que no detalla pertenecientes a las bases de datos bibliográficas Dialnet (1), Google Académico (21), Ieeaccess (1), Proquest (4), Redalyc(19), Scielo(1), Scientdirect(11), Scopus(1) como se detalla en la tabla 2.

Una vez seleccionados los 59 artículos se realizó una revisión minuciosa teniendo en consideración en la relevancia de dichas investigaciones con respecto a los objetivos del presente trabajo llegando a anular un total de 30 artículos los que fueron catalogados como calidad baja, los artículos son mostrados en la tabla 3.

Tabla 2

Relación de Artículos Seleccionados Antes de su Revisión Final

Base de Datos	Título	Tipo de Publicación	País	Idioma	Año de Publicación	Editorial	Tipo estudio	Criterios de Calidad
Dialnet	Redes Neuronales Artificiales Y Estado Del Arte Aplicado En La Ciberseguridad	Articulos De Investigacion	Colombia	Español	2020	Revista Matices Tecnológicos	Investigacion Documental	Alto
Google Academico	Revisión Sistemática Para La Construcción De Una Arquitectura Con Tecnologías Emergentes Iot, Técnicas De Inteligencia Artificial, Monitoreo Y Almacenamiento De Tráfico Malicioso	Articulos De Investigacion	España	Español	2022	Ieee Access	Investigacion Descriptiva	Alto
Google Academico	Tendencias Tecnológicas: Un Enfoque En La Seguridad Ciudadana	Articulos De Investigacion	Colombia	Español	2021	Ingeniería Solidaria	Investigacion Descriptiva	Medio
Google Academico	Detección De Ciberataques A Través Del Análisis De Mensajes De Redes Sociales: Revisión Del Estado Del Arte	Articulos De Investigacion	México	Español	2020	Research In Computing Science	Investigacion Descriptiva	Alto
Google Academico	Modelos De Aprendizaje Automático Aplicados A La Detección De Transacciones Sospechosas De Lavado De Activos En Entidades Financieras: Una Revisión Sistemática De La Literatura	Articulos De Investigacion	Perú	Español	2019	Universidad Peruana Unión	Investigacion Descriptiva	Alto
Google Academico	Principales Medidas De Seguridad Para La Protección De Información Y Datos En La Nube: Una Revisión Sistemática	Articulos De Investigacion	Perú	Español	2023	Ingeniería Investiga	Investigacion Descriptiva	Baja
Google Academico	Inteligencia Artificial Para El Control De Tráfico En Redes De Datos: Una Revisión	Articulos De Investigacion	Colombia	Español	2022	Entre Ciencia E Ingeniería ³	Investigacion Documental	Baja
Google Academico	Análisis De Intrusiones Cibernéticas Con El Uso Del Honeypots. Una Revisión Sistemática	Articulos De Investigacion	Brasil	Español	2021	Revista Brasileña De Ciencias Aplicadas	Investigacion Documental	Alto
Google Academico	Ciberseguridad En Las Redes Sociales: Una Revisión Teórica	Articulos De Investigacion	Colombia	Español	2021	Revista Uniandes Episteme	Investigacion Documental	Baja
Google Academico	Las Tecnologías Emergentes Y La Industria Gas Y Oil: Una Revisión Bibliográfica	Articulos De Investigacion	Argentina	Español	2022	Cuadernos De Investigación Serie Universidad	Investigacion Descriptiva	Baja
Google Academico	Revisión Sistemática De Literatura: Visualización De Seguridad	Articulos De Investigacion	Costa Rica	Español	No Detalla	Latinoamericana De Ciencia Y Risti -	Investigacion Documental	Baja
Google Academico	Revisión De Literatura Sobre Impacto De La Inteligencia Artificial Y Su Aplicación En El Ecuador	Articulos De Investigacion	Ecuador	Español	2023	Revista Iberica De Sistemas E Lex -	Investigacion Documental	Alto
Google Academico	Tecnologías Disruptivas: Contexto Políticojurídico, Desafíos Y Oportunidades En Latinoamérica	Articulos De Investigacion	Venezuela	Español	2021	Revista De La Facultadad	Investigacion Documental	Baja

Base de Datos	Título	Tipo de Publicación	País	Idioma	Año de Publicación	Editorial	Tipo estudio	Criterios de Calidad
Google Académico	Revisión Del Estado Del Arte En Técnicas De Procesamiento De Lenguaje Natural Para Análisis De Malware	Artículos De Investigación	México	Español	2020	Centro De Investigaci On En	Investigacion Documental	Baja
Google Académico	La Protección De Datos Personales En Ecuador Una Revisión Histórica-Normativa De Este Derecho Fundamental En El País Suramericano	Artículos De Investigación	Ecuador	Español	2023	Computaci Visual Review. International	Investigacion Documental	Baja
Google Académico	Framework Conceptual De Ciberseguridad Para Aplicaciones De Internet De Las Cosas	Artículos De Investigación	Colombia	Español	2018	Visual Universidad Autónoma De	Investigacion Descriptiva	Baja
Google Académico	Una Revisión De La Revolución Industrial 4.0 Y Sus Métodos De Implementación En Las Nuevas Industrias	Artículos De Investigación	Colombia	Español	2022	Bucaramanga Encuentro Internacional De	Investigacion Documental	Baja
Google Académico	Tecnologías De La Información Y Las Comunicaciones En La Era De La Cuarta Revolución Industrial: Tendencias Tecnológicas Y Desafíos En La Educación En Ingeniería	Artículos De Investigación	Colombia	Español	2020	Entre Ciencia E Ingeniería	Investigacion Documental	Baja
Google Académico	Campus Inteligente: Tendencias En Ciberseguridad Y Desarrollo Futuro	Artículos De Investigación	Colombia	Español	2018	Revista Facultad De Ingeniería	Investigacion Descriptiva	Baja
Google Académico	Modelo De Ciberseguridad Para El Sector De Salud Pública: 2018-2020	Artículos De Investigación	Perú	Español	2020	Universidad Privada Del Norte	Investigacion Documental	Baja
Google Académico	Una Revisión Del Aprendizaje Profundo Aplicado A La Ciberseguridad	Artículos De Investigación	Ecuador	Español	2022	Revista Científica Y Tecnológica Upse Grupo De	Investigacion Documental	Baja
Google Académico	Revisión Sistemática De La Literatura: Machine Learning Para La Detección De Ransomware En Dispositivos Móviles	Artículos De Investigación	Perú	Español	2022	Investigación Tendencia E Innovación	Investigacion Documental	Alto
Ieeaccess	Artificial Intelligence For Cybersecurity: A Systematic Mapping Of Literature	Artículos De Investigación	No Detalla	Inglés	2020	Ieee Access	Investigacion Documental	Alto
Proquest	Evaluación de riesgos en ciberseguridad: una revisión bibliométrica	Artículos De Investigación	Colombia	Español	2022	Revista Ibérica de Sistemas e Tecnologías Urvio,	Investigacion Documental	Baja
Proquest	Ciberseguridad. Presentación Del Dossier	Revista	Ecuador	Español	2017	Revista Latinoameric ana De	Investigacion Documental	Medio
Proquest	Artificial Intelligence, Digital Transformation And Cybersecurity In The Banking Sector: A Multi-Stakeholder Cognition-Driven Framework	Artículos De Investigación	No Detalla	Inglés	2022	Elsevier	Investigacion Documental	Medio
Proquest	Tendencias Investigativas En El Uso De Tecnologías De Big Data En Sistemas De Ciberseguridad	Artículos De Investigación	No Detalla	Español	2022	Revista Iberica De Sistemas E Tecnologías Revista	Investigacion Documental	Alto
Redalyc	Tecnología De Contenedores Y Su Aplicación En El Aprendizaje De Ciberseguridad: Una Revisión Sistemática De Literatura	Artículos De Investigación	México	Español	2020	Electrónica De Computación	Investigacion Documental	Baja
Redalyc	Antidfacepment - State Of Art	Artículos De Investigación	Colombia	Español	2016	Sistemas Y Telemática	Investigacion Documental	Medio
Redalyc	Hechos Ciberfísicos: Una Propuesta De Análisis Para Ciberamenazas En Las Estrategias Nacionales De Ciberseguridad	Artículos De Investigación	Ecuador	Español	2019	Urvio, Revista Latinoameric ana De	Investigacion Documental	Baja
Redalyc	Peligros De Las Redes Sociales: Cómo Educar A Nuestros Hijos E Hijas En Ciberseguridad	Artículos De Investigación	Costa Rica	Español	2019	Revista Electrónica Educare	Investigacion Documental	Baja

Base de Datos	Título	Tipo de Publicación	País	Idioma	Año de Publicación	Editorial	Tipo estudio	Criterios de Calidad
Redalyc	Cien Amenazas A La Seguridad Global: Panorama De La Dignidad Humana En El Siglo Xxi	Revista	Colombia	Español	2022	Revista Científica General José María	Investigacion Doctoral	Baja
Redalyc	Análisis De Métodos Y Técnicas Existentes Para Minimizar Agujeros De Seguridad Al Usar Códigos Qr	Articulos De Investigacion	Colombia	Español	2019	Revista Uis Ingenierías	Investigacion Documental	Baja
Redalyc	Conceptualización De Una Estrategia De Ciberseguridad Para La Seguridad Nacional De México	Articulos De Investigacion	Mexico	Español	2018	Revista Internacional De Ciencias Sociales Y Urvio,	Investigacion Documental	Baja
Redalyc	Internet, La Nueva Era Del Delito: Cibercrimo, Ciberterrorismo, Legislación Y Ciberseguridad	Articulos De Investigacion	Ecuador	Español	2017	Revista Latinoamericana De	Investigacion Documental	Baja
Redalyc	Retos Para La Regulación Jurídica De La Inteligencia Artificial En El Ámbito De La Ciberseguridad	Articulos De Investigacion	Mexico	Español	2021	Revista Ius	Investigacion Documental	Alto
Redalyc	La Política Brasileña De Ciberseguridad Como Estrategia De Liderazgo Regional	Articulos De Investigacion	Ecuador	Español	2017	Urvio, Revista Latinoamericana De Científica	Investigacion Documental	Baja
Redalyc	Sistema Inteligente De Monitoreo Para Condiciones Ambientales En Industria 4.0	Articulos De Investigacion	Mexico	Español	2021	Instituto Politécnico Nacional	Investigación Experimental	Baja
Redalyc	Security Control For Website Defacement	Articulos De Investigacion	Colombia	Inglés	2017	Sistemas & Telemática	Investigacion Documental	Medio
Redalyc	Prospectiva De Ciberseguridad Nacional Para Colombia A 2030	Articulos De Investigacion	Colombia	Español	2022	Revista Científica General José María	Investigacion Documental	Medio
Redalyc	La Ciberseguridad En La Era De Hipercompetitividad: ¿Puede La Ue Afrontar Los Nuevos Retos?	Articulos De Investigacion	España	Español	2022	Revista Cidob D'Afers Internacionals	Investigacion Documental	Medio
Redalyc	Una Comparativa De Los Esquemas De Ciberseguridad De China Y Estados Unidos	Articulos De Investigacion	Colombia	Español	2021	Oasis	Investigacion Documental	Medio
Redalyc	Identificación De Activos Y Ciberactivos Críticos En Sistemas De Transmisión De Energía Eléctrica	Articulos De Investigacion	Colombia	Español	2020	Tecnura	Investigacion Documental	Baja
Redalyc	¿Qué Seguridad? Riesgos Y Amenazas De Internet En La Seguridad Humana	Articulos De Investigacion	España	Español	2016	Araucaria. Revista Iberoamericana De	Investigacion Documental	Baja
Redalyc	Ciberseguridad En La Justicia Digital: Recomendaciones Para El Caso Colombiano	Articulos De Investigacion	Colombia	Español	2021	Revista Uis Ingenierías	Investigacion Documental	Baja
Redalyc	Revisión De Las Tecnologías Presentes En La Industria 4.0	Articulos De Investigacion	Colombia	Español	2020	Revista Uis Ingenierías	Investigacion Documental	Medio
Scielo	Riesgos Y Vulnerabilidades De La Denegación De Servicio Distribuidos En Internet De Las Cosas	Articulos De Investigacion	Colombia	Español	2019	Revista De Bioética Y Derecho	Investigacion Documental	Alto

Base de Datos	Título	Tipo de Publicación	País	Idioma	Año de Publicación	Editorial	Tipo estudio	Criterios de Calidad
Scientdirect	Cybersecurity Challenges In Vehicular Communications	Articulos De Investigacion	No Detalla	Inglés	2020	Vehicular Communications	Investigacion Documental	Baja
Scientdirect	Trustworthy Ai And Robotics: Implications For The Aec Industry	Articulos De Investigacion	Estados Unidos	Inglés	2022	Automation In Construction	Investigacion Documental	Baja
Scientdirect	Iot: Communication Protocols And Security Threats	Articulos De Investigacion	No Detalla	Inglés	2023	Internet Of Things And Cyber-Physical Journal Of	Investigacion Documental	Alto
Scientdirect	The Rise Of Machine Learning For Detection And Classification Of Malware: Research Developments, Trends And Challenges	Articulos De Investigacion	España	Inglés	2020	Network And Computer Journal Of	Investigacion Documental	Alto
Scientdirect	Blockchain For Healthcare Systems: Architecture, Security Challenges, Trends And Future Directions	Articulos De Investigacion	No Detalla	Inglés	2023	Network And Computer Cyber Security And Applications	Investigacion Documental	Baja
Scientdirect	Towards Insighting Cybersecurity For Healthcare Domains: A Comprehensive Review Of Recent Practices And Trends	Articulos De Investigacion	India	Inglés	2023	Information Fusion	Investigacion Documental	Medio
Scientdirect	Artificial Intelligence For Cybersecurity: Literature Review And Future Research Directions	Articulos De Investigacion	Slovenia	Inglés	2023	Information Fusion	Investigacion Documental	Alto
Scientdirect	Digitization Of Healthcare Sector: A Study On Privacy And Security Concerns	Articulos De Investigacion	No Detalla	Inglés	2023	Ict Express	Investigacion Documental	Alto
Scientdirect	Explainable Artificial Intelligence For Cybersecurity	Articulos De Investigacion	No Detalla	Inglés	2022	Computers And Electrical Engineering	Investigacion Documental	Medio
Scientdirect	Differential Privacy In Edge Computing-Based Smart City Applications: Security Issues, Solutions And Future Directions	Articulos De Investigacion	No Detalla	Inglés	2023	Array	Investigacion Documental	Alto
Scientdirect	A Systematic Literature Review Of Blockchain Cyber Security	Articulos De Investigacion	No Detalla	Inglés	2020	Digital Communications And Networks	Investigacion Documental	Medio
Scopus	A Blockchain-Based Architecture And Framework For Cybersecure Smart Cities	Articulos De Investigacion	No Detalla	Inglés	2023	Ieee Access	Investigacion Documental	Alto

Nota: Elaboración Propia de las revistas seleccionadas entre los años 2014 al 2023

Tabla 3

Relación de Artículos Eliminados tras su Revisión Final

Base de Datos	Título	Tipo de Publicación	País	Idioma	Año de Publicación	Editorial	Tipo estudio	Criterios de Calidad
Google Académico	Principales Medidas De Seguridad Para La Protección De Información Y Datos En La Nube: Una Revisión Sistemática	Articulos De Investigacion	Perú	Español	2023	Ingeniería Investiga	Investigacion Descriptiva	Baja
Google Académico	Inteligencia Artificial Para El Control De Tráfico En Redes De Datos: Una Revisión	Articulos De Investigacion	Colombia	Español	2022	Entre Ciencia E Ingeniería3	Investigacion Documental	Baja
Google Académico	Ciberseguridad En Las Redes Sociales: Una Revisión Teórica	Articulos De Investigacion	Colombia	Español	2021	Revista Uniandes Episteme	Investigacion Documental	Baja
Google Académico	Las Tecnologías Emergentes Y La Industria Gas Y Oil: Una Revisión Bibliográfica	Articulos De Investigacion	Argentina	Español	2022	Cuadernos De Investigación Serie Universidad	Investigacion Descriptiva	Baja
Google Académico	Revisión Sistemática De Literatura: Visualización De Seguridad	Articulos De Investigacion	Costa Rica	Español	No Detalla	Latinoamericana De Ciencia Y Lex -	Investigacion Documental	Baja
Google Académico	Tecnologías Disruptivas: Contexto Políticojurídico, Desafíos Y Oportunidades En Latinoamérica	Articulos De Investigacion	Venezuela	Español	2021	Revista De La Facultad Centro De Investigaci	Investigacion Documental	Baja
Google Académico	Revisión Del Estado Del Arte En Técnicas De Procesamiento De Lenguaje Natural Para Análisis De Malware	Articulos De Investigacion	Mexico	Español	2020	Computaci Visual	Investigacion Documental	Baja
Google Académico	La Protección De Datos Personales En Ecuador Una Revisión Histórica-Normativa De Este Derecho Fundamental En El País Suramericano	Articulos De Investigacion	Ecuador	Español	2023	Review. International Visual Universidad	Investigacion Documental	Baja
Google Académico	Framework Conceptual De Ciberseguridad Para Aplicaciones De Internet De Las Cosas	Articulos De Investigacion	Colombia	Español	2018	Autónoma De Bucaramanga Encuentro	Investigacion Descriptiva	Baja
Google Académico	Una Revisión De La Revolución Industrial 4.0 Y Sus Métodos De Implementación En Las Nuevas Industrias	Articulos De Investigacion	Colombia	Español	2022	Internacional De Educación	Investigacion Documental	Baja
Google Académico	Tecnologías De La Información Y Las Comunicaciones En La Era De La Cuarta Revolución Industrial: Tendencias Tecnológicas Y Desafíos En La Educación En Ingeniería	Articulos De Investigacion	Colombia	Español	2020	Entre Ciencia E Ingeniería	Investigacion Documental	Baja
Google Académico	Campus Inteligente: Tendencias En Ciberseguridad Y Desarrollo Futuro	Articulos De Investigacion	Colombia	Español	2018	Revista Facultad De Ingeniería	Investigacion Descriptiva	Baja
Google Académico	Modelo De Ciberseguridad Para El Sector De Salud Pública: 2018-2020	Articulos De Investigacion	Perú	Español	2020	Universidad Privada Del Norte	Investigacion Documental	Baja
Google Académico	Una Revisión Del Aprendizaje Profundo Aplicado A La Ciberseguridad	Articulos De Investigacion	Ecuador	Español	2022	Revista Científica Y Tecnológica Upse	Investigacion Documental	Baja

Base de Datos	Título	Tipo de Publicación	País	Idioma	Año de Publicación	Editorial	Tipo estudio	Criterios de Calidad
Proquest	Evaluación de riesgos en ciberseguridad: una revisión bibliométrica	Artículos De Investigación	Colombia	Español	2022	Revista Ibérica de Sistemas e Tecnologías de Información	Investigacion Documental	Baja
Redalyc	Tecnología De Contenedores Y Su Aplicación En El Aprendizaje De Ciberseguridad: Una Revisión Sistemática De Literatura	Artículos De Investigación	Mexico	Español	2020	Electrónica De Computación, Informática, Urvio, Revista Latinoamericana De Estudios De Seguridad	Investigacion Documental	Baja
Redalyc	Hechos Ciberfísicos: Una Propuesta De Análisis Para Ciberamenazas En Las Estrategias Nacionales De Ciberseguridad	Artículos De Investigación	Ecuador	Español	2019	Revista Electrónica Educare	Investigacion Documental	Baja
Redalyc	Peligros De Las Redes Sociales: Cómo Educar A Nuestros Hijos E Hijas En Ciberseguridad	Artículos De Investigación	Costa Rica	Español	2019	Revista Científica General José María Córdova	Investigacion Documental	Baja
Redalyc	Cien Amenazas A La Seguridad Global: Panorama De La Dignidad Humana En El Siglo Xxi	Revista	Colombia	Español	2022	Revista Uis Ingenierías	Investigacion Documental	Baja
Redalyc	Análisis De Métodos Y Técnicas Existentes Para Minimizar Agujeros De Seguridad Al Usar Códigos Qr	Artículos De Investigación	Colombia	Español	2019	Revista Internacional De Ciencias Sociales Y Urvio, Revista Latinoamericana De Estudios De Seguridad	Investigacion Documental	Baja
Redalyc	Conceptualización De Una Estrategia De Ciberseguridad Para La Seguridad Nacional De México	Artículos De Investigación	Mexico	Español	2018	Revista Latinoamericana De Estudios De Seguridad Científica	Investigacion Documental	Baja
Redalyc	Internet, La Nueva Era Del Delito: Ciberdelito, Ciberterrorismo, Legislación Y Ciberseguridad	Artículos De Investigación	Ecuador	Español	2017	Instituto Politécnico Nacional	Investigacion Documental	Baja
Redalyc	La Política Brasileña De Ciberseguridad Como Estrategia De Liderazgo Regional	Artículos De Investigación	Ecuador	Español	2017	Tecnura	Investigacion Documental	Baja
Redalyc	Sistema Inteligente De Monitoreo Para Condiciones Ambientales En Industria 4.0	Artículos De Investigación	Mexico	Español	2021	Araucaria. Revista Iberoamericana De Filosofía,	Investigacion Documental	Baja
Redalyc	Identificación De Activos Y Ciberactivos Críticos En Sistemas De Transmisión De Energía Eléctrica	Artículos De Investigación	Colombia	Español	2020	Revista Uis Ingenierías	Investigacion Documental	Baja
Redalyc	¿Qué Seguridad? Riesgos Y Amenazas De Internet En La Seguridad Humana	Artículos De Investigación	España	Español	2016	Journal Of Network And Computer Applications	Investigacion Documental	Baja
Redalyc	Ciberseguridad En La Justicia Digital: Recomendaciones Para El Caso Colombiano	Artículos De Investigación	Colombia	Español	2021		Investigacion Documental	Baja
Scientdirect	Cybersecurity Challenges In Vehicular Communications	Artículos De Investigación	No Detalla	Inglés	2020	Vehicular Communications	Investigacion Documental	Baja
Scientdirect	Trustworthy Ai And Robotics: Implications For The Aec Industry	Artículos De Investigación	Estados Unidos	Inglés	2022	Automation In Construction	Investigacion Documental	Baja
Scientdirect	Blockchain For Healthcare Systems: Architecture, Security Challenges, Trends And Future Directions	Artículos De Investigación	No Detalla	Inglés	2023		Investigacion Documental	Baja

Nota: Elaboración Propia

Características de los estudios

Uno de los criterios y por ello consideración importante para seleccionar los artículos fue considerar el rango específico de años en los que se habían publicado dichos artículos considerando nuestro estudio Aplicación de Big data en ciberseguridad utilizando inteligencia artificial en los años 2014 – 2023, el gráfico 2 detalla el estadístico detallado por año del total de las 29 revistas finales.

Gráfico 1

Cantidad de Revistas por Año de Publicación



Nota: Cantidad de revistas por año de publicación: Elaboración Propia

Como se puede apreciar en el gráfico el mayor porcentaje de artículos se han presentado entre los años 2023 (24.14%), 2022 (24.14%), 2020 (20.69%), 2021 (13.79%), 2019 (6.90%), 2017 (6.90%), 2016 (3.45%).

El análisis sobre los tipos de publicación de los artículos seleccionados por país se detalla en la Tabla 4 en donde se muestra detallado por país y tipo de publicación de los 29 artículos seleccionados.

Tabla 4

Resultados del Análisis de los Artículos Seleccionados por Tipo de Publicación y País

País	Artículos De Investigación	Revista	Trabajo de Investigación	Total, general
Brasil	1			1
Colombia	8			8
Ecuador	1	1		2
España	3			3
India	1			1
México	2			2
No Detalla	9			9
Perú	1		1	2
Slovenia	1			1
Total, general	27	1	1	29

Fuente: Elaboración propia

Se observa en la tabla 4 que el país de Colombia es el que tiene la mayor cantidad de artículos de los seleccionados ya que tiene 8 artículos seleccionados de los cuales 8 son Artículos de investigación, esto considerando de las revistas que detallan su país de origen ya que también se encontraron 9 artículos de investigación en los que no se pudo evidenciar el país de origen; en total se evidencia 3 tipos de publicaciones como son artículos de investigación, revista y Trabajo de Investigación donde el 93% del total de artículos son artículos de investigación debido a que se priorizó como criterio de inclusión este tipo de artículos como prioritarios.

Tipo de investigación

Se observa según la tabla 5 que el mayor porcentaje de los artículos seleccionados son de tipo documental (86.2%) y descriptiva (13.8%).

Tabla 5

Distribución de Artículos por Tipo de Investigación

Tipo de investigación	Cantidad Artículos	Porcentaje
Investigación Descriptiva	4	13.8%
Investigación Documental	25	86.2%
Total, general	29	100%

Fuente: Elaboración propia

Tipos de fuentes

Se observa en la tabla 6 que de las 29 Revistas finales seleccionadas el porcentaje más alto lo tiene la base de datos Scient direct (27.6%) luego Redalyc (24.1%) y Google Académico con (24.1%) siendo estos las 3 bases de datos con un mayor porcentaje (75.8%) de representación del presente trabajo.

Tabla 6

Cantidad de Artículos según Bases de Datos Consultadas

Base de Datos	Cantidad de Artículos	Porcentaje
Dialnet	1	3.4%
Google Académico	7	24.1%
leeaccess	1	3.4%
Proquest	3	10.3%
Redalyc	7	24.1%
Scielo	1	3.4%
Scientdirect	8	27.6%
Scopus	1	3.4%
Total general	29	100.0%

Fuente: Elaboración propia

Análisis comparativo

Se observo que de los 29 artículos seleccionados el 55% está relacionado a Ciberseguridad o Cybersecurity, 34% a Inteligencia Artificial o Artificioal Intelligence y solo 10% a Big data lo que según el análisis se observa que la aplicación de big data esta implícita dentro de la inteligencia artificial según lo encontrado en la lectura completa de los artículos.

Tabla 7

Palabras Clave Referenciadas en las Palabras Clave de los Artículos Seleccionados

Big Data	Ciberseguridad	Inteligencia Artificial	Cybersecurity	Artificial Intelligence	Total
3	7	5	9	5	29
10%	24%	17%	31%	17%	100%

Fuente: Elaboración Propia

Con lo expuesto en la tabla 7 se aprecia que las combinaciones de palabras que más relevancia tuvieron fueron las de Ciberseguridad o Cybersecurity y las de Inteligencia Artificial o Artificial Intelligence siendo estas un indicio de que dichas aportaciones nos brindan puntos en común para poder responder la pregunta de investigación ¿Cuál ha sido el impacto de la aplicación de big data en Ciberseguridad utilizando inteligencia artificial en los años 2014 – 2023?

Para poder responder dicha pregunta se realizó un análisis comparativo entre los artículos investigados con relación al presente tema de investigación, encontrándose que las palabras claves tuvieron un alto impacto en los resultados para poder afirmar el importante aporte de Big data que si bien es cierto en muchos de los artículos no aparece de manera explícita pero si está de manera implícita en contextos como grandes volúmenes de datos demostrando su importancia al alimentar de datos a disciplinas basadas en inteligencia artificial para poder tomar decisiones acertadas e interactuar máquina – máquina mediante un ciclo de aprendizaje donde como se ha mencionado se requiere interactuar de manera constante con datos para identificar patrones que puedan ser implementados y ser convertidos en modelos de análisis. Si bien es cierto la inteligencia Artificial data de años anteriores al auge de Big Data, pero es precisamente con este auge de Big data que se ha visto potenciada al nutrirse de los datos procesados y aprender de ellos creando y reconociendo patrones que permiten desarrollar soluciones sofisticadas de analítica para todo tipo de sectores y dentro de ellos la Ciberseguridad.

Ciberseguridad e inteligencia artificial son de las palabras que han tenido un mayor impacto explícito en los artículos investigados en donde se evidencia el incremento de los ciberataques tanto en volumen como en complejidad esto en relación con el desarrollo del internet de las cosas , siendo a su vez está sumamente vulnerable a ciberataques y es allí donde esta hace uso de la inteligencia Artificial la cual a través de sus tecnologías como Machine Learning y el procesamiento del lenguaje natural aprenden a identificar patrones dentro de los grandes volúmenes de datos ordenados que le proporciona Big data y aprender de ellos para así poder anticiparse a las amenazas y ataques.

Por lo tanto, mediante la respuesta a la pregunta de este trabajo se puede afirmar que Big data impacta positiva y directamente en la ciberseguridad ya que como se ha evidenciado

en los trabajos de investigación la IA se nutre de big data para poder desarrollarse y la IA se sitúa como una aliada de la ciberseguridad debido a que aprende continuamente gracias a los miles de millones de datos con que los expertos la nutren pudiendo así identificar, priorizar, analizar y anticipar amenazas en tiempos donde según el foro económico mundial por ejemplo menciona que en el 2021 hubo un incremento del 151% de ciberataques a nivel mundial.

CAPÍTULO IV. CONCLUSIONES

Discusión

El impacto de la aplicación de Big data en ciberseguridad utilizando inteligencia Artificial es positivo debido a que big data ha potenciado el desarrollo de la inteligencia Artificial en sus diversas aplicaciones y la ha convertido en una Aliada importante para la ciberseguridad en la detección de ataques y esto también lo ha comprendido el estado de Colombia, el peligro ahora se encuentra en las redes y el uso de las mismas y por ello está impulsando el desarrollo de sus sectores de tecnología y educación enfocados en la ciberseguridad para la implementación de arquitecturas que den soporte al desarrollo de Big data siendo empleada para la Inteligencia Artificial y esta a su vez para la Seguridad ciudadana (Cardona, 2021) ya que omitir el seguimiento de los nuevos desarrollos de la inteligencia de seguridad en materia de seguridad representa una posición temeraria para cualquier empresa o estado (Martínez, 2022).

En la actualidad toda la población está expuesta a diversas amenazas dentro de ellas los ciberataques como los que se producen haciendo uso de las redes sociales frente a las cuales se ha obtenido buenos resultados haciendo uso de algoritmos de aprendizaje automático para la detección de este tipo de amenazas (Coyac-Torres et al., s. f.).

En efecto, periódicamente la población mundial recibe información sobre nuevos ciberdelitos que pueden tener diversos orígenes, pero el mismo efecto de perjudicar a las personas (Hirare, 2017), esta situación ha generado alianzas como las de la unión Europea que busca hacer frente a la proliferación de amenazas a su ciberseguridad desarrollando un marco institucional con una agencia de ciberseguridad altamente desarrollada y que hace uso

de los recursos de la inteligencia Artificial y otras tecnologías disruptivas (Munkøe & Mölder, 2022), esta iniciativa también intenta ser replicada por China y estado unidos(Orozco, 2021) por cuenta propia mostrando que la ciberseguridad ha pasado hacer un factor competitivo donde los grandes volúmenes de datos (Big data) son protagonistas de alimentar toda la estructura en inteligencia artificial para garantizar el anticipar y detectar vulnerabilidades en los diversos sistemas.

Vivimos en la era de la digitalización la cual nos trae repercusiones que afecta el impacto negativo y positivo de estas sobre cómo nos relacionamos y la cantidad de información que producimos como producto de nuestra huella digital y ello sin incluir el internet de las cosas que representaría un problema de seguridad (Rozo-García, 2020) y todo esto muestra la tendencia a depender de la tecnología de la sociedad lo que nos expone frente a la vulnerabilidad y riesgo que presenta el IoT frente al tratamiento de la información (Márquez Díaz, 2019) lo cual nos llevaría al auge de la aplicación de las técnicas de aprendizaje automático como parte de la AI para la clasificación y detección de Malware(Gibert et al., 2020) mediante la implementación de soluciones prácticas de ciberseguridad basadas en IA las que han evolucionado en el dominio de la ciberseguridad (Kaur et al., 2023).

Así se tiene que la IA y sus derivados se utilizaron con herramientas poderosas para analizar procesar los datos capturados para poder lograr un razonamiento efectivo al abordar problemas de seguridad (Taylor et al., 2020) aunque a la fecha también se puede usar Blockchain , big data y algoritmos de inteligencia Artificial que proporciona un marco sólido y confiable para las ciudades inteligentes (Bekkali et al., 2023).

Conclusiones

En este trabajo se realizó una revisión sobre el impacto de la aplicación de Big data en ciberseguridad utilizando inteligencia artificial en los años 2014 – 2023. Lo más importante de esta revisión fue comprobar tras la revisión de los artículos el impacto de Big data en el desarrollo tanto de la inteligencia Artificial (es alimentada con datos por Big Data) como también de la ciberseguridad ya que la ciberseguridad hace uso de la inteligencia Artificial para hacer frente a los retos que trae consigo la digitalización e internet de las cosas que han abierto un universo de posibilidades al generar volúmenes inmensos de datos y con ello oportunidades que los atacantes pueden utilizar para vulnerar las fuentes de información que gracias al aprendizaje continuo y generación de modelos de inteligencia artificial estos comportamientos y ataques pueden identificarse mediante el análisis de miles de datos en tiempo real que no sería posible sino se contara con Big data y la inteligencia Artificial en la seguridad informática.

Es importante reconocer que se puede clasificar en 3 los problemas de privacidad de los datos : privacidad de los datos, privacidad de la información y privacidad del conocimiento sin embargo lo que se ha vuelto una gran preocupación es la seguridad de los datos que abarca la privacidad, disponibilidad y la integridad de los datos (Yao et al., 2023) por tal la ciberseguridad está adoptando la inteligencia artificial para hacer frente a dicha incertidumbre siendo Machine Learning una de las más aplicadas al campo de la ciberseguridad.

Para los siguientes estudios se puede abarcar el tema desde un enfoque de como la Inteligencia Artificial puede ser utilizada para ataques por ciberdelincuentes ya que como se sabe los modelos usados para prevenir e identificar ataques e intrusiones podrían ser tomados mediante ingeniería inversa.

REFERENCIAS

- Bekkali, A. E., Essaïdi, M., & Boulmalf, M. (2023). A Blockchain-Based Architecture and Framework for Cybersecure Smart Cities. *IEEE Access*, 1-1. <https://doi.org/10.1109/ACCESS.2023.3296482>
- Caiza Narváez, J. J., Márceles Villalba, K., & Amador Donado, S. (2022). *Revisión sistemática para la construcción de una arquitectura con tecnologías emergentes IoT, técnicas de inteligencia artificial, monitoreo y almacenamiento de tráfico malicioso.* <https://doi.org/10.1109/RITA.2022.3217183>
- Cardona, L. A. L. (2021). Technological trends: A focus on citizen security. *Ingeniería Solidaria*, 17(1), Article 1. <https://doi.org/10.16925/2357-6014.2021.01.02>
- Castellanos Rojas, B. S., Cortés Rodríguez, C. U., Espitia Osorio, D. J., & Garzón Bello, Y. T. (2020). Redes neuronales artificiales y estado del arte aplicado en la ciberseguridad. *Revista Matices Tecnológicos*, 12, 58-63.
- Castro Salaverry, C. R., Bravo Huivin, E. K., & Cieza Mostacero, S. E. (s. f.). *Revisión Sistemática de la Literatura: Machine Learning para la Detección de Ransomware en Dispositivos Móviles - ProQuest.* Recuperado 28 de julio de 2023, de <https://www.proquest.com/openview/cd91b567d2231af11494e7f1ab0ea8dd/1?pq-origsite=gscholar&cbl=1006393>
- Coyac-Torres, J. E., Sidorov, G., & Aguirre-Anaya, E. (s. f.). *Detección de ciberataques a través del análisis de mensajes de redes sociales: Revisión del estado del arte.*
- Galeano Villar, A. J., & Vargas Cisneros, Z. N. (2019). Modelos de aprendizaje automático aplicados a la detección de transacciones sospechosas de lavado de activos en entidades financieras: Una revisión sistemática de la literatura. *Universidad Peruana Unión.* <https://repositorio.upeu.edu.pe/handle/20.500.12840/2519>

- Gerodimos, A., Maglaras, L., Ferrag, M. A., Ayres, N., & Kantzavelou, I. (2023). IoT: Communication protocols and security threats. *Internet of Things and Cyber-Physical Systems*, 3, 1-13. <https://doi.org/10.1016/j.iotcps.2022.12.003>
- Gibert, D., Mateu, C., & Planes, J. (2020). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. *Journal of Network and Computer Applications*, 153, 102526. <https://doi.org/10.1016/j.jnca.2019.102526>
- Gil, A. A. B. (2021). Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad. *Revista IUS*, 15(48), 9-34.
- Hirare, C. S. (2017). Ciberseguridad. Presentación del dossier. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, 20, 8-15.
- Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, 1, 100016. <https://doi.org/10.1016/j.csa.2023.100016>
- Kaur, R., Gabrijelčić, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804. <https://doi.org/10.1016/j.inffus.2023.101804>
- Macias, H. J. R., Márquez, J. F. R., & Cabrera, C. S. P. (s. f.). *Análisis de intrusiones cibernéticas con el uso del Honeypots. Una revisión sistemática Análise de invasões cibernéticas usando Honeypots. Uma revisão sistemática.*
- Márquez Díaz, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. *Revista de Bioética y Derecho*, 46, 85-100.
- Martínez, J. J. C. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, 20(40), 814-832.

- Munkøe, M., & Mölder, H. (2022). La ciberseguridad en la era de hipercompetitividad: ¿puede la Union Europea afrontar los nuevos retos? *Revista CIDOB d'Afers Internacionals*, 131, 69-94.
- Orozco, G. A. P. (2021). Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos. *Oasis*, 34, 107-126.
- Pabon, J., Aizaga, M., Recalde, H., & Toasa G, R. M. (2023). Revisión de literatura sobre impacto de la inteligencia artificial y su aplicación en el Ecuador. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, E55, 100-113.
- Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, S2405959523000243. <https://doi.org/10.1016/j.icte.2023.02.007>
- Quirumbay Yagual, D. I., Castillo Yagual, C. A., & Coronel Suárez, I. A. (2022). *Una revisión del aprendizaje profundo aplicado a la ciberseguridad*. <https://repositorio.upse.edu.ec/handle/46000/8231>
- Rodrigues, A. R. D., Ferreira, F. A. F., Teixeira, F. J. C. S. N., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, 60, 101616. <https://doi.org/10.1016/j.ribaf.2022.101616>
- Rozo-García, F. (2020). Revisión de las tecnologías presentes en la industria 4.0. *Revista UIS Ingenierías*, 19(2), 177-191.
- Sharma, D. K., Mishra, J., Singh, A., Govil, R., Srivastava, G., & Lin, J. C.-W. (2022). Explainable Artificial Intelligence for Cybersecurity. *Computers and Electrical Engineering*, 103, 108356. <https://doi.org/10.1016/j.compeleceng.2022.108356>
- Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, 6(2), 147-156. <https://doi.org/10.1016/j.dcan.2019.01.005>

Urcuqui, C. C., Peña, M. G., Osorio Quintero, J. L., & Navarro Cadavid, A. (2016). Antidefacement. *Sistemas y Telemática*, 14(39), 9-27. <https://doi.org/10.18046/syt.v14i39.2341>

Valencia-Arias, A., Arias Vargas PhD, F., Garces Giraldo, L., Vélez Bernal, O., Benjumea Arias, M., & Bermeo Giraldo, M. (2022). Tendencias investigativas en el uso de tecnologías de Big Data en sistemas de ciberseguridad. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 49, 410-420.

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access*, 8, 146598-146612. <https://doi.org/10.1109/ACCESS.2020.3013145>

Yao, A., Li, G., Li, X., Jiang, F., Xu, J., & Liu, X. (2023). Differential privacy in edge computing-based smart city Applications: Security issues, solutions and future directions. *Array*, 19, 100293. <https://doi.org/10.1016/j.array.2023.100293>