ESCUELA NAVAL DE CADETES
"ALMIRANTE PADILLA"
Honor y Tradición

REVISTA DERROTERO

Seguridad y Defensa

Análisis bibliométrico años 2000-2021: modelamiento y simulación en ciberseguridad y ciberdefensa

Juan Manuel Villalobos Álvarez [1]

[1]Alumno Escuela Superior de Guerra "Brigadier General Rafael Reyes Prieto", Bogotá, Colombia. Gestión de organizaciones. Especialista en administración de seguridad. Administración de empresas.

ARMADA DE COLOMBIA

Recibido: 26/05/2021
Aprobado: 26/08/2021

Correspondencia:
juan.villalobos
@armada.mil.co

Citación:
J. Villalobos-Álvarez. Análisis bibliométrico años 2000-2021: modelamiento y simulación en ciberseguridad y ciberdefensa. Derrotero 15, número 1 (Ene-Dic) 2021.

Resumen

El presente documento tiene como propósito difundir el análisis bibliométrico sobre modelamiento y simulación en ciberseguridad y ciberdefensa entre los años 2000 y 2021, a través del empleo de un proceso metodológico aplicado a 994 artículos, el cual incluye en sus distintas fases: definición de las palabras clave, captura de los datos en el sistema Scopus y preparación de los datos, así como el procesamiento de los datos en R y su análisis correspondiente.

Este proceso arrojó como resultado la comprensión detallada del comportamiento de las publicaciones en el lapso establecido, logrando conocer que a partir del año 2015 se impulsó la mayor contribución a través de técnicas de modelamiento y simulación desde la ciencia de los datos. Se resalta la importancia del tema de estudio en los últimos cinco años y la necesidad constante de desarrollo e innovación, así como la participación de los investigadores y sus interacciones con otros, para la generación de nuevos temas asociados al modelamiento y a la simulación en ciberseguridad y ciberdefensa.

Palabras clave: bibliometría, ciberdefensa, ciberseguridad, modelamiento, simulación.

ISSN: 2027-0658 | E-ISSN: 2590-4701

Bibliometric Analysis Years 2000-2021: Modeling and Simulation in Cybersecurity and Cyberdefense[I]

Abstract

The purpose of this document is to disseminate the bibliometric analysis on modeling and simulation in cybersecurity and cyber defense between the years 2000 to 2021, using a methodological process applied to 994 articles that undergo various phases that frame the definition of keywords, data capture in the SCOPUS system, data preparation, as well as data processing in R and its corresponding analysis.

As a result, the process allowed a detailed understanding of the behavior of the publications in the established period, achieving to know that as of 2015 the greatest contribution was promoted through modeling and simulation techniques from data science. This has implied in the importance that the subject of study has recovered in the last 5 years, being part of a medium that requires constant development and innovation, which will allow to increase the participation of researchers and their interactions with others, for the generation of new topics associated with modeling and simulation in cybersecurity and cyber defense.

Keywords: bibliometrics, cyber defense, cybersecurity, modeling, simulation.

Introducción

El artículo presentado aborda un análisis bibliométrico sobre el tema asociado al modelamiento y la simulación en ciberseguridad y ciberdefensa entre los años 2000 y 2021, así como los desafíos a los cuales se enfrenta con el crecimiento imparable de los avances tecnológicos y sistemáticos que afrontarán las futuras generaciones; para ello, se acudió a la consulta de diversos artículos y documentos que gozan de indexación, para desarrollar cuatro pasos enmarcados en la definición de: las palabras clave, la captura de los datos en el sistema Scopus y su preparación, un procesamiento de los datos en R y su análisis correspondiente, lo cual coadyuvó para la obtención de resultados significativos en la investigación.

El interés de este documento en el ámbito profesional y científico viene dado por el incremento en la utilidad del modelamiento y la simulación en ciberseguridad y ciberdefensa en la actualidad, lo que se ha traducido en una mayor diversidad de usos en varias ramas de la tecnología, por consiguiente, en nuevos desafíos para la ciencia y la educación; es por ello que en el marco de la investigación surge la pregunta: ¿cuál es el comportamiento de

[I] El presente artículo de investigación es presentado como opción de grado para optar al título de Magíster en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, siendo producto del proyecto de investigación titulado "Consideraciones de ciberseguridad y ciberdefensa de cara a los retos que impone el siglo xxi", vinculado al grupo de investigación Masa Crítica, categorizado en B COL0123247, inscrito en Minciencias.

la actividad científica relacionada con el "modelamiento y simulación en ciberdefensa y ciberseguridad" entre 2000 y 2021?

La anterior pregunta se realiza porque existen pocos estudios asociados a la bibliometría en el área de ciberseguridad, sin embargo, no se encuentran estudios bibliométricos relacionados con modelamiento y simulación en ciberdefensa y ciberseguridad, por lo que se hizo necesario impulsar la iniciativa académica de estudio como mecanismo para fortalecer el conocimiento en el campo que actualmente lo requiere.

Así, este trabajo es uno de los que analizan el grado en el que se encuentra la información asociada al estudio del modelamiento y la simulación en el campo de ciberseguridad y ciberdefensa, así como mide de manera real los contenidos asociados al tema y que responden a las necesidades de un mundo que se encuentra en constante desarrollo e innovación.

Como parte de la estructura que se manejó para el desarrollo del análisis bibliométrico, se hizo necesario emplear un procedimiento metodológico que permitiese identificar palabras claves, capturar datos a través del apoyo de base de datos, prepararlos, así como su procesamiento y análisis.

De acuerdo con el desarrollo del proceso investigativo, los documentos estudiados en el análisis provienen de la base de datos Scopus, debido a que esta tiene una alta aceptación científica por su número de revistas indexadas. La búsqueda se centró en los documentos disponibles desde el año 2000 y se encontraron 994 documentos en total, entre artículos, libros, documentos de sesión, entre otros.

Posteriormente, para el análisis de la línea de tiempo entre los años 2004 y 2021 de los documentos, se evidencia que del 100 % de los documentos existentes sobre el tema, el 43,75 %, fueron escritos entre el 2019 y 2020 y el porcentaje de crecimiento anual fue del 23,26 %, lo que muestra una curva ascendente para el interés a nivel científico y un número considerable de autores que publicaron en diversos tipos de documentos.

Así, en el desarrollo del tema se mostrarán aspectos relevantes como los autores de mayor impacto, el país líder en publicaciones y otros aspectos derivados del análisis que dan a conocer la realidad actual concerniente al entorno asociado a la simulación y modelamiento en Ciberseguridad y Ciberdefensa. Para la preparación y el análisis se depuraron datos atípicos, errados o incompletos; la verificación anterior tuvo como propósito descartar la documentación que no tuviera relación con el tema de estudio.

Uno de los aspectos a resaltar de la investigación fue la identificación de la cooperación internacional existente entre los países para impulsar la producción científica, así como los principales campos de investigación que se encuentran delimitados en la ciberseguridad y la seguridad de la información, la ciencia de datos, las infraestructuras críticas y la ciberseguridad industrial.

Por último, para el procesamiento de la información, el empleo del *software* especializado Bibliometrix permitió de manera ágil la actualización de los diferentes componentes para desarrollar la bibliometría.

Metodología

Se utiliza la consulta a expertos en temas relacionados con modelamiento, simulación, ciberseguridad y ciberdefensa, así como la revisión bibliográfica de otros estudios bibliométricos realizados, tales como:

- Un análisis bibliométrico de investigaciones sobre el aprendizaje automático para la seguridad cibernética de Makawana y Jhaveri, 2018.
- Tendencias investigativas en educación en ciberseguridad: Un estudio bibliométrico de Valencia *et al.,* 2020.
- Un estudio bibliométrico del uso de la web presentado por Shukla y Gochhait, 2020.
- Un estudio bibliométrico de ciberseguridad entre 1998-2020, realizado por Elango *et al.,* 2020.

De manera general, varios estudios coadyuvaron a determinar las palabras clave a ingresar en el motor de búsqueda de la información. Se tuvieron en cuenta el análisis de la información objeto de estudio y la verificación de los modelos bibliométricos antes relacionados y se establecieron para el presente artículo las siguientes palabras clave: bibliometría, ciberdefensa, ciberseguridad, modelamiento y simulación.

Seguidamente, se procedió a la captura de datos a través de una fuente especializada, sin embargo, para desarrollar su selección fue necesario analizar los dos principales buscadores importantes para el desarrollo de una bibliometría, estas corresponden a Scopus y Web of Science, ambos tienen características únicas que reúnen la información de múltiples bases de datos internacionales, no solo de una fuente, sino que permiten concentrar mucha información.

Para el caso de Scopus, este corresponde a la mayor base de datos bibliográfica que se encuentra en actividad desde el año 2004, tiene resúmenes de literatura arbitrada y citas de artículos de revistas científicas revisadas por pares en la web; su cobertura de búsqueda cubre más de 5000 casas editoras y más de 1800 revistas indexadas, brindando así diversas herramientas inteligentes que coadyuvan al desarrollo de estudios bibliométricos valorados mediante el rendimiento de publicaciones y autores, haciendo un seguimiento exhaustivo, análisis y visualización para la investigación que se desarrolla.

Para el caso de Web of Science, este corresponde a una plataforma de información científica, cuya finalidad es proporcionar herramientas de análisis que permitan valorar la calidad científica de las publicaciones; sin embargo, sus valores de factor de impacto y del índice h tienen una correlación de 0,17, mientras que en Scopus corresponden a 0,79, es decir, su superioridad es más útil para el desarrollo de un análisis bibliométrico.

Al tener en cuenta las consideraciones socializadas anteriormente y demás ventajas que proporciona Scopus, se toma esta como base para el apoyo de la actividad investigativa del presente artículo. Posteriormente se realiza la búsqueda y la recuperación de datos y se hace la descarga y la conversión de datos a formato *.bib*, según los requerimientos de la herramienta tecnológica del estudio.

Por su parte, el registro documental se desarrolla con variables de búsqueda como: autores, género de autores, año de publicación, palabras clave, tipo de documento, nombre del documento y número de referencias presentadas en los textos que tienen como referencia directa el tema de estudio. Además, se verificó la consistencia de estos, analizando y depurando los datos de información atípica, errada o incompleta realizándole una limpieza. Esta verificación o evaluación previa tiene como fin descartar documentación científica que no tenga relación con el tema de estudio. En ese orden, durante esta etapa se hallaron 1005 registros documentales, de los cuales el 1,1 %, constituidos por 11 documentos, no cumplía las especificaciones asociadas al tema objeto de estudio, por tal motivo fueron eliminados de manera inmediata en la fase de depuración y por lo que se tomaron 994 documentos para continuar con la fase de procesamiento de los datos.

Seguidamente, para el procesamiento y el análisis de los datos se utilizó el software R (R Foundation, 2019) junto con la librería Bibliometrix (Aria, 2016), herramientas de código abierto usadas para el análisis exhaustivo del mundo científico en determinado tema, consideradas herramientas flexibles y de fácil actualización, útiles en una ciencia de constante cambio como la bibliometría (Aria y Cuccurullo, 2017, p. 959).

Esto se realiza ya que los datos procesados en R constituyen los resultados del estudio y son el objeto de análisis para la discusión y las conclusiones, es por ello que en el desarrollo del artículo se emplearon de manera específica combinaciones de datos obtenidos de 994 documentos, de los cuales se emplearon los siguientes campos del conjunto de datos recuperado para la producción de los resultados de informaciones requeridas, resaltando las siguientes: para la producción anual de documentos y porcentajes se requirieron todos los artículos escritos con su año de publicación; de igual manera, para analizar los países más productivos fue necesario tener el número de documentos y los países donde fueron publicados, no obstante, también se tomaron aquellos publicados entre múltiples países para perfeccionar el análisis; paso siguiente, para el estudio de los autores más productivos se acudió a datos que respondían al número de documentos versus autores para conocer

el comportamiento de sus publicaciones.

Fue así como se logró obtener la información de los medios de publicación y de las cantidades a través de los autores que publicaron, conociendo las principales revistas y medios empleados para difundir el tema objeto de estudio. Por su parte, la dominancia y el *ranking* de los autores se obtuvieron a través del estudio del factor de dominancia de cada uno y según los aspectos de publicación, ya sea de manera individual o donde múltiples autores fungen como primer autor.

Por su parte, para el análisis del coeficiente de ley de Lotka, se hizo necesario tener datos del número de documentos escritos y el porcentaje de autores que corresponden a 2224 autores, para desarrollar la estimación y la comparación entre las distribuciones de Lotka y las teóricas. Paso seguido, el desarrollo del acoplamiento bibliográfico requirió los datos asociados a la co-citación para obtener la red y los diferentes nodos de los autores más representativos y eruditos en el tema.

Por último, para determinar la colaboración científica existente se demandó de información de los autores y de enlaces entre las coautorías existentes entre países; sin embargo, para desarrollar un mejor análisis que obtuviera una red de co-ocurrencias de palabras clave y un análisis de correspondencias múltiples, fue necesario entrelazar los 994 documentos para detectar de manera clara los conglomerados de nodos, las áreas más sobresalientes que se encuentran y los tópicos de las tendencias asociadas al modelamiento y la simulación en ciberdefensa y ciberseguridad.

Resultados y discusión

El apartado aborda dos bloques de desarrollo, en el primero (literales de A a C) se tratan los aspectos teóricos y de estado del arte alrededor del tema de estudio, identificando tres áreas base: bibliometría, ciberseguridad y ciberdefensa, y modelamiento y simulación. El segundo bloque (literales de D a H) muestra los resultados y la discusión en cada etapa del estudio bibliométrico.

A. Bibliometría

La bibliometría emplea metodologías matemáticas y estadísticas a toda la gramática científica y sus autores, con el objetivo de estudiar y analizar la actividad científica. Por tal motivo, esta se apoya de estatutos bibliométricos, asentados en el procedimiento estadístico habitual que ha demostrado en un lapso los diferentes elementos que hacen parte de la ciencia a estudiar. Para ello, se utilizan instrumentos para calcular los indicadores bibliométricos, los cuales corresponden a medidas que suministran información relacionada

con los resultados de la actividad científica, tales como el factor de dominancia y los índices h, g y m de los autores (Aria y Cuccurullo, 2017, Elango *et al.,* 2020, Gutiérrez *et al.,* 2018, Túñez y de Pablos, 2013). La descripción de estos indicadores se trata en los resultados y la discusión en cada etapa del estudio bibliométrico.

Como acercamiento al estado del arte en bibliometría, a continuación, se presentan los estudios científicos más representativos del área:

Makawana y Jhaveri, 2018 realizaron un análisis bibliométrico de investigaciones sobre el aprendizaje automático para la seguridad cibernética, con el propósito de iluminar a los investigadores sobre las tendencias recientes de esta área de investigación, para ello analizaron 149 trabajos presentados durante la vigencia de 2015 y 2016 para presentar una vista gráfica y organizada y apoyar las futuras tendencias de investigación.

Shukla y Gochhait, 2020 presentan un estudio bibliométrico del uso de la web, relacionando que después del Covid-19 es casi seguro que la mayoría de las industrias habilitadas para las tecnologías de información aprovecharán las capacidades de la nube para promover la cultura del trabajo remoto. Por consiguiente, con las organizaciones en línea es indiscutible que la posibilidad de ataques cibernéticos aumentará de manera exponencial. Por lo tanto, es muy importante que todas las industrias habilitadas digitalmente se mantengan al tanto de las tendencias actuales, de las preocupaciones y de la investigación en curso en el campo de la ciberseguridad.

Elango *et al.,* 2020 realizaron un estudio bibliométrico de ciberseguridad entre 1998 y 2020, utilizando el directorio Web of Science para el análisis de datos, estudiando aproximadamente 2184 registros para orientar a los académicos de todo el mundo. Entre los resultados se muestra que países como EE. UU., Reino Unido, Países Bajos, Suiza, Alemania y Canadá han contribuido significativamente a la investigación relacionada con la seguridad cibernética.

Por otro lado, la *Revista Ibérica de Sistemas y Tecnologías de la Información* (Risti), en su publicación "Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico", presenta los hallazgos encontrados sobre las publicaciones académicas asociadas con la educación en ciberseguridad en el lapso comprendido entre los años 2001 y 2019. A través de la mencionada labor, se logró mostrar el crecimiento y la vigencia de la información, así como el análisis derivado de la difusión y el impacto que esta genera para las futuras investigaciones (Valencia *et al.,* 2020).

Para finalizar, es preciso concluir que existen diversos documentos que apoyan y promueven el desarrollo de la investigación que sirvieron como punto de partida para la elaboración del estudio bibliométrico sobre modelamiento y simulación en ciberseguridad y ciberdefensa, y que además permitieron enriquecer la investigación con diferentes puntos de vista.

B. Ciberseguridad y ciberdefensa

Para hablar de estos dos conceptos es preciso primero mencionar el ciberespacio, que se define como:

> El dominio global dentro del área de la información consistente en un ambiente tanto físico como virtual, compuesto por computadores (*hardware*), programas computacionales (*software*), redes, telecomunicaciones, datos, información y sistemas (computacionales, información, telecomunicaciones y otros sistemas electrónicos), que es utilizado para la interacción entre usuarios, así como para almacenar, procesar, modificar, transmitir y compartir datos e información usando las redes computacionales (Cabuya y Mahecha, 2019, p. 13).

Así, este ciberespacio se caracteriza por ser atemporal, instantáneo, ubicuo, permeable, fluido, participativo y autorregulado (Sabillon *et al.,* 2016) y se compone de tres capas que son: capa de red física, capa de red lógica y capa ciber-persona (United States Government, 2018).

El Manual de Seguridad de las Tecnologías de la Información y Comunicaciones CCN-STIC-400 define la ciberseguridad como el "conjunto de medidas para proteger la información almacenada, procesada o transmitida por los sistemas de información y comunicaciones, de manera que se aseguren o garanticen confidencialidad, integridad y disponibilidad de la información" (Comunicaciones, 2013, p. 13).

Ahora bien, el concepto de ciberseguridad bajo una visión de seguridad nacional materializa el concepto de defensa nacional digital en un conjunto de variables claves, definidas por la International Telecommunication Union (ITU como necesarias en el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación, en el contexto de una realidad digital y de información instantánea, entendiendo que la problemática de la ciberseguridad requiere un esfuerzo colectivo y coordinado entre los diferentes países (Cano, 2018).

Adicionalmente, Cano, 2018 menciona que la ciberseguridad bajo una visión de seguridad nacional involucra que cada uno de los individuos reconozcan en la información un activo fundamental que articule todas las infraestructuras críticas de la nación, donde "necesariamente debemos considerar las acciones básicas que desarrolla una nación para proteger de manera coherente, sistemática y sistémica los activos de información crítica, distribuidos en toda su infraestructura y cómo ellos impactan la operación del Estado" (Cano, 2018, p. 7).

Es en esta visión de seguridad nacional que se enmarca la ciberdefensa como "el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la

independencia, la integridad territorial, el orden constitucional o los intereses nacionales" (Departamento Nacional de Planeación, 2016, Escuela Superior de Guerra, 2019).

Lo anterior es producto de las tendencias temáticas que pueden encontrarse referente al tema y que son generadas por factores como el desarrollo de la tecnología que evoca ciertos argumentos puntuales; de la misma manera, esta evolución temática permite profundizar en la ciberseguridad y en la ciberdefensa, especialmente para encausar el desarrollo de la revisión bibliométrica que es objeto de estudio.

C. Modelamiento y simulación

A nivel internacional existe abundante *software* de modelado y simulación que puede ser empleado como una caja negra, pero esto no siempre se hace debido a los cambios frecuentes a los que se somete el análisis científico y el diseño en ingeniería, lo que conlleva a obtener variaciones determinantes en pro del conocimiento de los fundamentos del área de conocimiento.

Urquía & VillabaCarla, 2016 expresan que los métodos de simulación y modelamiento obedecen a un estudio representado bajo un modelo matemático integrado de ecuaciones y algoritmos que, a su vez, es experimentado a través de un ordenador.

El resultado de la simulación es un conjunto de datos frecuentemente voluminoso que debe ser representado gráficamente para poder ser interpretado. Adicionalmente, los autores mencionan que existen unos requisitos para el desarrollo de una simulación:

- Seleccionar la representación adecuada del sistema bajo estudio.
- Emplear los métodos numéricos adecuados para la resolución del modelo mediante el ordenador.
- Realizar los cálculos de manera eficiente en el mundo en constante evolución de la computación.
- Evaluar la precisión de los resultados producto de los experimentos.
- Realizar un análisis de los datos obtenidos al ejecutar la simulación completa del ciclo de proyecto de simulación.

Según esto y a modo de estado del arte en modelamiento y simulación en ciberseguridad y ciberdefensa, se concluye que son pocos los trabajos previos relevantes encontrados en la revisión de fuentes bibliográficas que aborden el tema concretamente, sin embargo, a continuación, se presentan los trabajos más relevantes:

Kotenko, 2005 realizó tanto el modelado como la simulación basado en agentes de la guerra cibernética entre malhechores y agentes de seguridad en internet, mediante un ejemplo de modelado y simulación de ataques de *Denegación de servicio distribuida* (DDoS) y

protección contra ellos, según aspectos como: agentes de diferentes equipos que compiten para alcanzar intenciones antagónicas, agentes del mismo equipo que cooperan para realizar intenciones conjuntas, ontologías de los ataques DDoS y los mecanismos de protección contra ellos. De esta manera, el autor determinó las variantes de estructuras de equipos de los agentes, los mecanismos de interacción y coordinación, las especificaciones de jerarquía de planes de acción y los prototipos de *software* desarrollados. Este trabajo sentó las bases para considerar modelos más flexibles ydinámicos que permitan evaluar los resultados de mejoras, en las capacidades de los equipos de ciberdefensa y el impacto de los mecanismos de cooperación.

Posteriormente, Kotenko, 2005 estudió el modelado y la simulación de múltiples agentes de ciberataques y ciberdefensa para la seguridad nacional, enfocado en la investigación de los mecanismos de ciberdefensa cooperativos distribuidos contra los ataques a la red, utilizando una simulación basada en agentes de ciberataques y mecanismos de protección cibernética que combina la simulación de eventos discretos, el enfoque de múltiples agentes y la simulación a nivel de paquete de protocolos de red. Como resultado, se generó un marco común de implementación del entorno de simulación, así como los experimentos dirigidos a la investigación de ataques a redes distribuidas y mecanismos de defensa. El autor concluyó que la cooperación en equipo conduce a la mejora esencial de la efectividad de la defensa y vislumbró la necesidad de identificar los múltiples escenarios de ataque y defensa cibernética, así como el cálculo de la probabilidad de éxito asociada a estos.

Bradshaw *et al.,* 2012 desarrollaron un marco basado en agentes para el conocimiento de la situación cibernética, el cual permite aumentar la percepción y la cognición humanas en torno a la ciberseguridad, así como la mejora cualitativa en la conciencia de la situación cibernética, relevante para las aplicaciones de sentido distribuido y otros tipos de tareas complejas de alto ritmo. El aporte de interés es el punto de vista humano y de conciencia cibernética asociado al modelo presentado para tratar la variable humana dentro del esquema de la ciberseguridad y que es aplicable a la ciberdefensa.

Pastrana *et al.,* 2015 elaboraron un marco para la asignación y ubicación óptima de redes de detección de intrusos, los cuales son sistemas distribuidos de ciberdefensa, centrados en un modelo de asignación de contramedidas y basados en un algoritmo de optimización multiobjetivo para obtener estrategias de asignación óptimas que minimicen tanto el riesgo como el costo, y que permitan diseñar y reconfigurar sistemas de ciberdefensa de manera óptima. Esta investigación presenta una metodología aplicable a la ciberdefensa del ámbito marítimo, sin embargo, este modelo se centra en un sistema específico de medidas de defensa, dando espacio para la formulación de modelos con enfoques holísticos de ciberdefensa multinivel.

Finalmente, la investigación de Lu, Li y Yang, 2018 presenta una propuesta de modelado de ciberataques y defensas en sistemas de medición local, desarrollado mediante el análisis de árboles de ataque para analizar las rutas que un ciberatacante podría seguir, incluyendo los incrementos de complejidad; posteriormente usaron la teoría de juegos para modelar las interacciones entre un atacante y un defensor, facilitando de esta manera la asignación óptima de interacciones defensivas limitadas entre estos; también probaron la asignación de recursos defensivos limitados y la generación de estrategias de protección efectivas contra diferentes combinaciones de ataques. Los resultados de esta investigación muestran un panorama de posibles salidas de modelos de interacciones relacionadas con la ciberseguridad, que aplican a la ciberdefensa y a las salidas del modelo planteado para la presente investigación, principalmente en la asignación y la locación de recursos defensivos para la reducción de las probabilidades de éxito en escenarios de ciberataques complejos.

D. Procesamiento inicial de la información

Al tener en cuenta la metodología descrita, los documentos estudiados en este análisis provienen de la base de datos Scopus, debido a que esta es de alta aceptación científica por su número de revistas indexadas, siendo la fecha de corte de la búsqueda el día 11 de marzo del 2021.

Los criterios de búsqueda para el análisis se centraron en varias palabras compuestas, centradas en el tema de estudio: "MODELAMIENTO Y SIMULACIÓN EN CIBERSEGURIDAD Y CIBERDEFENSA", y el motor de búsqueda fue el siguiente:

(TITLE (cybersecurity OR {cyber security} OR "cyber-security" OR cyberdefense OR {cyber defense} OR "cyber-defense" OR cyberdefence OR {cyber defence} OR "cyber-defence") AND TITLE (simulation OR simulate OR modeling OR modelling OR model OR "model-based.ºR modelation OR pattern OR patterning OR standard OR framework OR {game theory} OR {artificial intelligence} OR {machine learning})).

Este criterio de búsqueda tomó en cuenta la combinación de las diferentes disciplinas dentro del tema de estudio. La búsqueda se centró en los documentos disponibles desde el año 2000 y encontró 994 documentos en total, entre artículos, libros, documentos de sesión, entre otros; en un periodo entre 2004 y 2021.

Posteriormente, se procedió a realizar el análisis estadístico por medio del programa R Project for Statistical Computing, implementando el paquete "Bibliometrix" y encontrando los resultados que se muestran en los literales siguientes.

E. Análisis de línea de tiempo, producción anual y autores más productivos

El análisis de la línea de tiempo entre los años 2004 y 2021 de los documentos evidencia que, de los 994 documentos existentes sobre el tema, 433 de estos (figura 1), correspondientes al 43,75 %, fueron escritos entre el 2019 y el 2020 (figura 2), y el porcentaje de crecimiento anual fue del 23,26 %, lo que permite observar el creciente interés que el tema tiene en la actualidad a nivel científico, observando así un registro de 2577 autores que publicaron en revistas, documentos de conferencia, libros, etc., con un promedio de 5985 citas por documento y 4365 palabras clave mostradas.

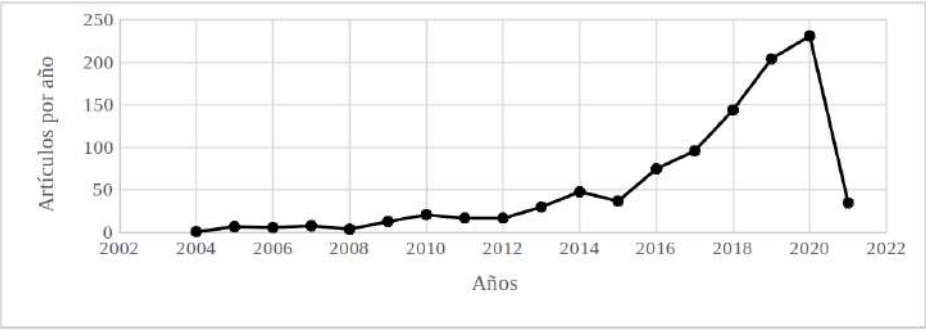

Figura 1. Producción de documentos por año

Fuente: elaboración propia.

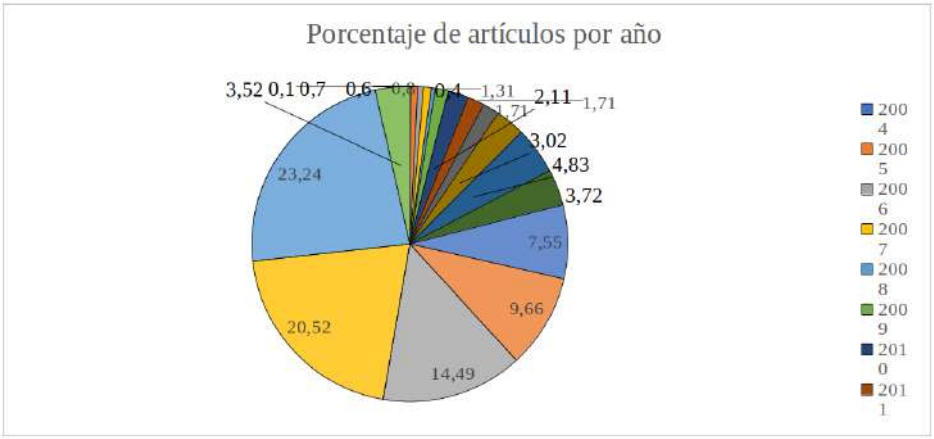

Figura 2. Porcentaje de producción de documentos de la muestra por año

Fuente: elaboración propia.

El país más productivo en cuanto al tema es Estados Unidos con 155 artículos, seguido por China con 36 y de otros países como India, Reino Unido y Australia (figura 3).

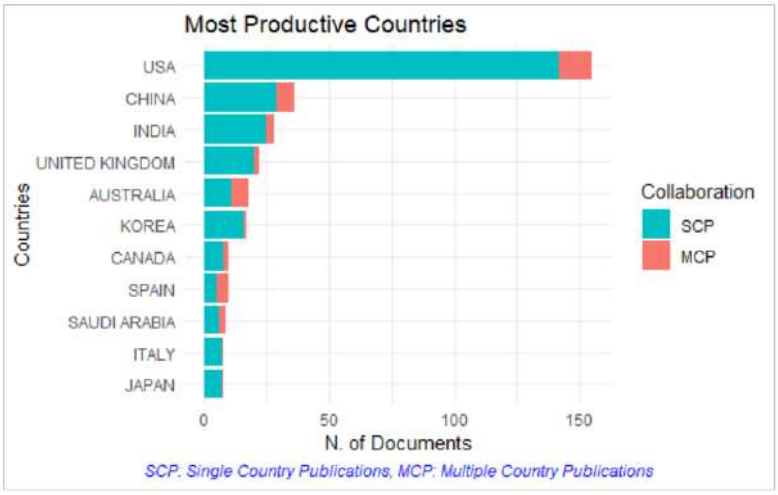

Figura 3. Países más productivos

Fuente: elaboración propia.

Los 10 autores más productivos son Lakhno (8 publicaciones), Mylrea (8), Gourisetti (7), Li (7), Pietre (7), Quinn (7), Wang (7), Chen (6), Ekstedt (6) y Leenen (6) (figura 4).

Figura 4. Autores más productivos

Fuente: elaboración propia.

Por su parte, las principales publicaciones académicas de la muestra son: *Lecture Notes in Computer Science* (44), *Advances in Intelligent Systems and Computing* (26), *ACM In-*

ternational Conference Proceeding Series (22), *Communications in Computer and Information Science* (18), *Computers and Security* (13), *European Conference on Information Warfare and Security ECCWS* (12), *Ceur Workshop Proceedings* (10), *IEEE Access* (10), *Journal of Defense Modeling and Simulation* (10), *Proceedings - IEEE Military Communications Conference Milcom* (8) y *Applied Sciences (Suiza)* (7).

Esto muestra que las revistas de ciencias de la computación, sistemas inteligentes y ciencias de la informática son las mayormente citadas en relación con el campo de estudio y contribuyen a la base investigativa en el tema de modelamiento y simulación en ciberseguridad y ciberdefensa, tal como se muestra en la tabla **I**.

Tabla I. *Ranking* de revistas sobre modelamiento y simulación en ciberseguridad y ciberdefensa

Modalidad: revista/conferencia o talleres	*Ranking*	Número de publicaciones
Lecture Notes in Computer Science	Q3	44
Advances in Intelligent Systems and Computing (serie de libros)	Q3	26
ACM international conference proceeding series	No aplica	22
Communications in Computer and Information Science	Q4	18
Computers and Security	Q1	13
European Conference on Information Warfare and Security Eccws	No aplica	12
Ceur Workshop Proceedings	No aplica	10
IEEE Acces	Q1	10
Journal of Defense Modeling and Simulation	Q3	10
Proceedings - IEEE Military Communications Conference Milcom	No aplica	8
Applied Sciences (Suiza)	Q2	7
IET Conference Publications	No aplica	7
IFIP Advances in Information and Communication Technology	Q3	7
INTECH	No aplica	7
IEEE Security and Privacy	Q1	6

Fuente: elaboración propia.

F. Índices h, g y m de los autores

El índice h es propuesto como un indicador de impacto que mide el número de investigaciones publicadas por un autor y las citas que se han obtenido de este, demostrando una correlación entre el índice y el éxito del investigador. Entonces, un número h de publica-

ciones han recibido un número mínimo h de citas (Túñez y de Pablos, 2013).

Por su parte, el índice g calcula la productividad científica determinada por el historial de publicaciones de los autores. Para obtener este cálculo son listadas las publicaciones de un autor en orden descendente de acuerdo con el número de citas recibidas por cada uno de ellos, luego este dígito se eleva al cuadrado (Túñez y de Pablos, 2013).

Finalmente, el índice m se calcula a través de la relación h/n, donde n es el número de años de carrera como investigador, lo cual representa la mediana de las citas recibidas por el índice h (Gutiérrez *et al.,* 2018).

Para el caso particular, los autores con mayor índice h son Mylrea y Ekstedt (con 4); de la misma forma, se evidencia que los autores con mejor índice g son Chen y Ekstedt (6); por otra parte, los autores con mejor índice m son Lakhno y Gourisetti (80 y 75), lo que muestra que estos últimos publican artículos más frecuentemente que los demás autores (tabla **II**).

Tabla II. Índice h, g y m de los primeros 10 autores

Autor	Índice H	Índice G	Índice M
Lakhno V	3	5	0,75
Mylrea M	4	5	1
Gourisetti SNG	3	5	0,75
Li S	3	4	0,33
Pietre-Cambacedes L	2	2	0,28
Quinn EL	2	2	0,28
Wang Y	2	2	0,4
Chen Y	3	6	0,37
Ekstedt M	4	6	0,31
Leenen L	2	3	0,22

Fuente: elaboración propia.

G. Ranking de dominancia de los autores

El factor de dominancia es la proporción que indica el número de artículos de varios autores en los que aparece un investigador considerado erudito en el tema como primer autor en las publicaciones (Elango y Rajendran, 2012). Según lo encontrado en el análisis, Gourisetti y Quinn son los dos autores de más alto nivel de dominancia, ya que de siete artículos publicados aparecen como primeros autores en cinco de ellos; luego vendría Lakhno, debido a que, de ocho artículos publicados, aparece en cinco como primer autor; los demás autores pueden verse en la tabla **III**.

Tabla III. *Ranking* de dominancia de los autores

Autor	Factor de dominancia	Total de artículos	Un solo autor	Múltiples autores	Primer autor
Gourisetti, SNG.	0,7142857	7	0	7	5
Quinn, EL.	0,7142857	7	0	7	5
Lakhno, V.	0,6250000	8	0	8	5
Wang, Y.	0,4285714	7	0	7	3
Chen, Y.	0,3333333	6	0	6	2
Pietre, L.	0,2857143	7	0	7	2
Mylrea, M.	0,2500000	8	0	8	2
Ekstedt, M.	0,1666667	6	0	6	1
Leenen, L.	0,1666667	6	0	6	1
Li, S.	0,1428571	7	0	7	1

Fuente: elaboración propia.

H. Estimación del coeficiente de la ley de Lotka

La ley de Lotka describe la frecuencia de publicación de los autores en cualquier campo de estudio y en un determinado tiempo, donde se distingue que la producción científica del tema se centra en un número determinado de autores que publican un mayor número de artículos en contraste con la cantidad de autores que tienen menos producción (Elango y Rajendran, 2012, Urbizagastegui, 1999).

Al aplicar la ley de Lotka (figura 5) se observa que existen 2224 autores que han escrito un solo artículo sobre el tema de modelamiento y simulación en ciberseguridad y ciberdefensa, el total de autores que han escrito dos artículos son 255; tres artículos son 52; cuatro artículos son 27; cinco artículos son 8; seis artículos son 3; siete artículos son 5; ocho artículos son 2 y 18 artículos es solo 1.

Al comparar la estimación teórica de la ley de Lotka y el comportamiento de la muestra estudiada se espera que no haya diferencias significativas entre las dos muestras.

Por su parte, el coeficiente Beta estimado es de 2,89, constante de 0,53 con una bondad de ajuste igual a 0,93. La prueba de dos muestras de Kolmogorov-Smirnoff proporciona un valor de p = 0,33, lo que quiere decir que no existe una diferencia significativa entre las distribuciones Lotka observadas y las teóricas (figura 6).

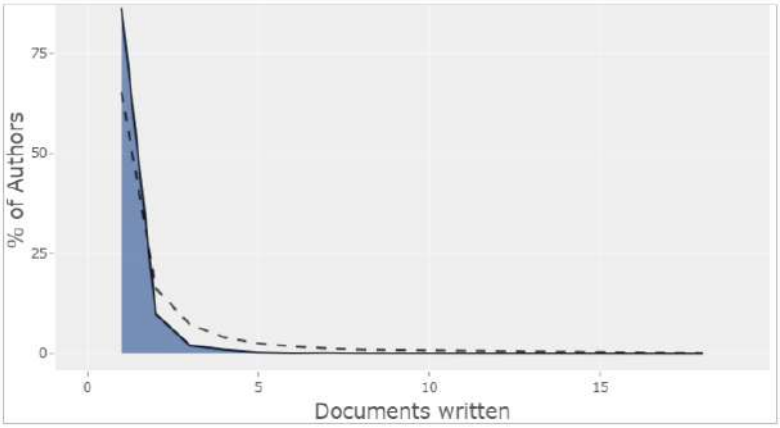

Figura 5. Estimación del coeficiente con ley de Lotka - distribución de frecuencia

Fuente: elaboración propia.

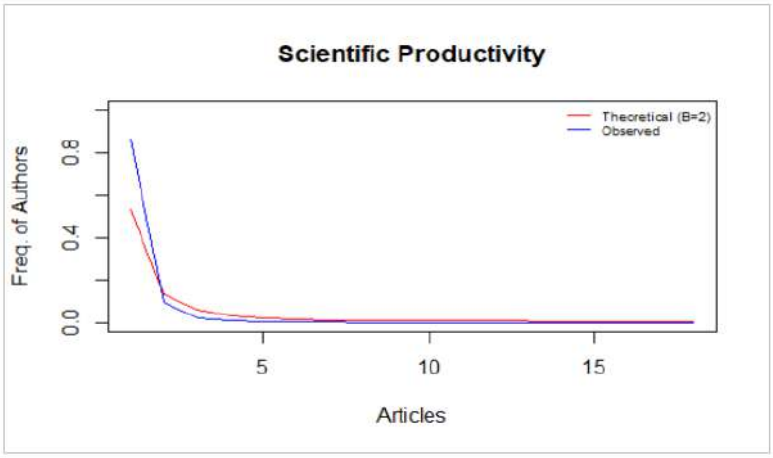

Figura 6. Comparación de la beta teórica con la observada de las distribuciones de *Lotka*

Fuente: elaboración propia.

I. Acoplamiento bibliográfico

Se afirma que, si al menos una fuente citada se encuentra en la lista de referencias de dos artículos, los dos están acoplados bibliográficamente. La fuerza del acoplamiento de ambos se calcula a partir del número de referencias compartidas en común por estos mismos, además de introducir el acoplamiento entre la co-cita, la co-ocurrencia de palabras clave y la cooperación entre países (Aria, 2016). Estos términos se explican a continuación:

Co-citación

La red de co-citación se puede observar cuando ambos artículos son citados en un tercer artículo (Aria, 2016). En la figura 7 se muestra el nodo de artículos de autores eruditos, siendo para este caso los artículos de Buczak y Guven, 2016 y Roy *et al.*, 2010 los que evidencian un nodo más grande y están espacialmente más cerca entre sí, en comparación con otros artículos menos populares como los de Johnson, 2007 y Kissel *et al.*, 2008.

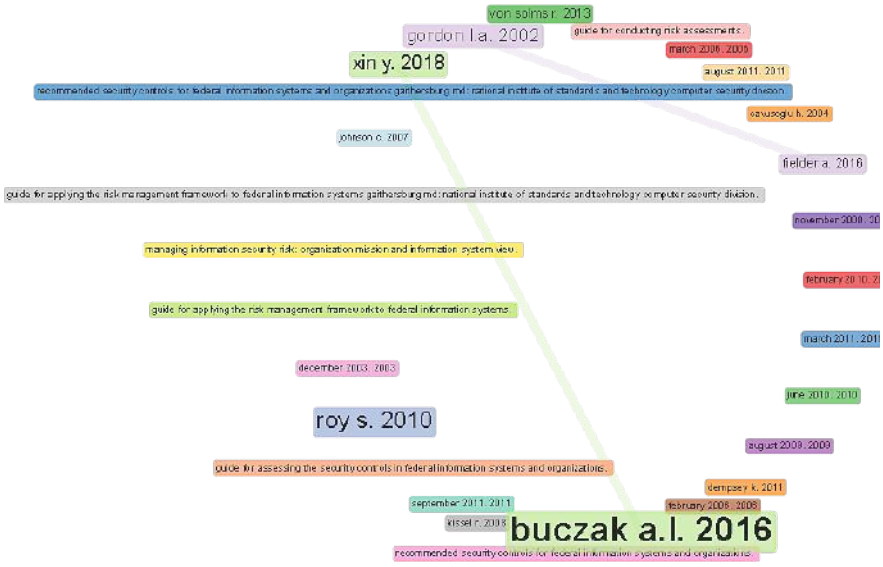

Figura 7. Red de co-citación

Fuente: elaboración propia.

Colaboración científica e internacional

Una red de colaboración científica es aquella que se estimula por medio de políticas de promoción de la investigación, mediante la financiación y tiene como objetivo la cooperación internacional para generar producción científica (Carvalho *et al.*, 2014); es aquí donde se observa que los nodos son autores y los enlaces son coautorías entre estos, si el nodo es de mayor tamaño quiere decir que hay más cantidad de autores de ese país en coautoría con otros.

En el caso del presente análisis, se evidencia que el país que más cooperación de coautorías tiene en relación con el modelamiento y la simulación en ciberseguridad y ciberdefensa

es Estados Unidos, el cual está unido con siete países, destacando sus conexiones con Reino Unido, Corea, China y Arabia Saudita; así mismo, India está unido con seis países, destacando conexiones con Canadá, España, Australia y China; y por su parte, Italia se relaciona con seis países, destacando las conexiones con Estados Unidos, Australia, Suecia y Polonia (figura 8).

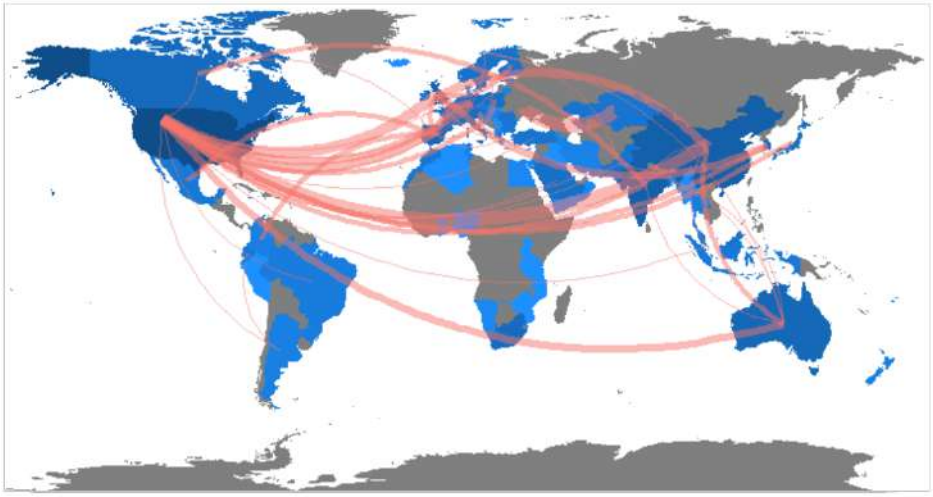

Figura 8. Colaboración científica e internacional

Fuente: elaboración propia.

Red de co-ocurrencia de palabras clave

La figura 9 muestra tres conglomerados de nodos claramente divididos: uno en color verde que es encabezado por las palabras seguridad cibernética y seguridad de los datos, acompañado de otras palabras menos concurrentes como: sistemas de control industrial, ciberamenazas, evaluación de riesgos, sistemas de seguridad, infraestructuras críticas, toma de decisiones, teoría de juegos, seguridad nacional, sistemas de información y seguridad; el otro, mostrado en color rojo, está encabezado por las palabras seguridad de la red, acompañado de otras como delito informático, inteligencia artificial, delito, ciberataque, ciberdefensa, sistemas de aprendizaje, aprendizaje automático, grandes datos, detección de intrusiones, *malware* y algoritmos de aprendizaje; por último, se puede observar un nodo de color azul, en el cual se encuentran palabras compuestas como internet de las cosas, redes eléctricas inteligentes, sistemas integrados y red de transmisión de energía eléctrica.

Se puede afirmar que uno de los nodos muestra cuál es el contexto de investigación del modelamiento y la simulación en ciberseguridad y ciberdefensa (nodo verde), mientras

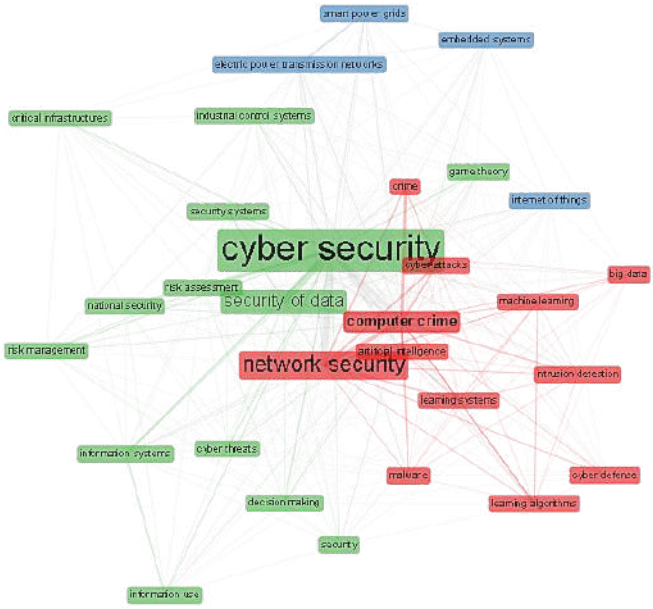

Figura 9. Co-ocurrencias de palabras clave

Fuente: elaboración propia.

que el otro nodo muestra el modo de estudio y la aplicación del concepto (rojo) y el nodo de color azul muestra temas emergentes en este tipo de investigaciones.

J. Áreas de investigación

Finalmente, se muestran las áreas de investigación que están relacionadas en torno al tema de modelamiento y simulación en ciberseguridad y ciberdefensa a través de un análisis de correspondencias múltiples (ACM), el cual analiza la homogeneidad de la matriz de indicadores para obtener una representación euclidiana de baja dimensión de los datos originales (Abdi y Velentin, 2018).

En el presente caso, la figura **10** muestra cuatro grandes campos de investigación principales claramente delimitados por colores, lográndose esto al mapear las co-ocurrencias de palabras en la colección bibliográfica; en el campo rojo se observan investigaciones relacionadas con ciberseguridad, seguridad de la red, evaluación de riesgos, ciberataques, privacidad de datos, *big data*, sistemas de información, entre otros; en el campo azul se muestran estudios de aprendizaje profundo, detección de intrusiones, sistemas de aprendizaje, mi-

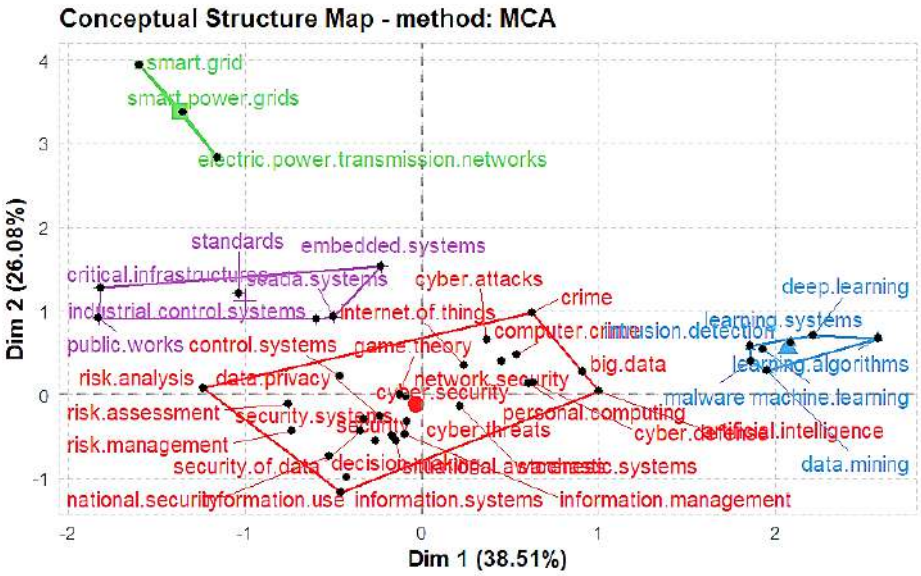

Figura 10. Estructura conceptual del campo de estudio - método MCA

Fuente: elaboración propia.

nería de datos, algoritmos de aprendizaje y aprendizaje automático de *malware*; en el nodo morado se observan investigaciones relacionadas con infraestructuras críticas, estándares, sistemas embebidos, sistemas de control industrial y palabras públicas; por último, en el nodo verde se encuentran investigaciones orientadas a red inteligente, red eléctrica inteligente y redes de transmisión de energía eléctrica.

Además, en la figura 11 se observa la tendencia temática a lo largo de los últimos años, la cual se centra en ciberseguridad, seguridad de la red, seguridad de los datos, crimen informático, evaluación de riesgos, ciberataques, control de sistemas, seguridad nacional, etc.

Conclusiones

La presente investigación tuvo como objetivo estudiar la actividad científica relacionada con "el modelamiento y la simulación en ciberseguridad y ciberdefensa" durante el transcurrir de los años 2000-2021, encontrándose que a partir del año 2004 al 2021 el interés por investigar en este estudio aumentó notablemente, principalmente a partir del 2015, dando cuenta de una preocupación académica de estudiar la ciberseguridad y la ciberdefensa desde la ciencia de datos, a través de técnicas de modelamiento y simulación, como consecuencia del incremento exponencial de la actividad en el ciberespacio.

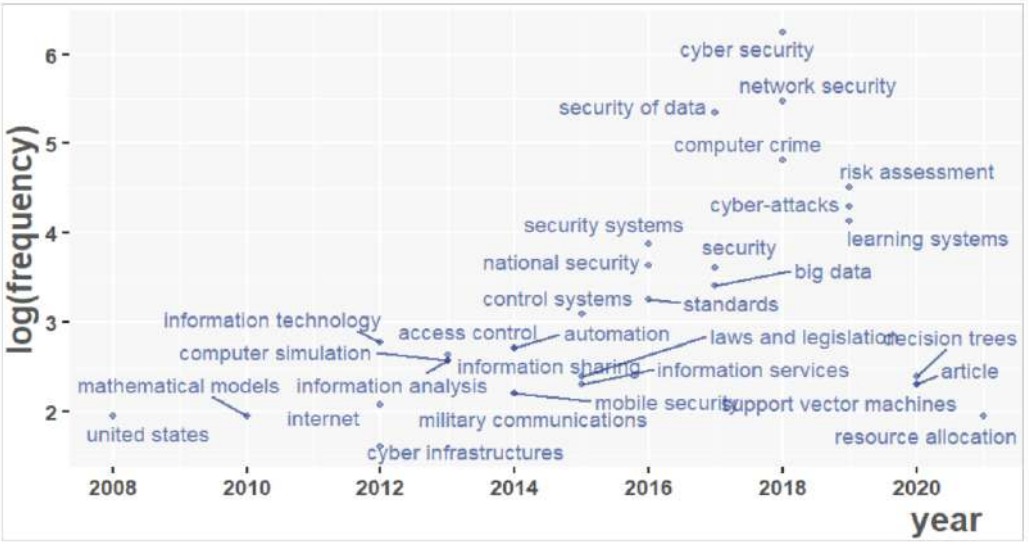

Figura 11. Dendrograma temático - Tópicos tendencia

Fuente: elaboración propia.

Los 10 autores más productivos son poco representativos en comparación con otras áreas de investigación científica, teniendo en cuenta que el más productivo del área abordada tan solo tiene ocho publicaciones del tema. En cuanto a la difusión y el impacto que tienen estas investigaciones a través de sus revistas, *Lecture Notes in Computer Science* cuenta con el mayor número de citas y en general las revistas de ciencias de la computación, sistemas inteligentes y ciencias de la informática son las mayormente citadas con relación al campo de estudio y contribuyen a la base investigativa en el tema de modelamiento y simulación en ciberseguridad y ciberdefensa.

El indicador de países muestra a Estados Unidos como el que tiene mayor impacto y el más prolífero, ratificando la importancia que tiene para esta potencia mundial la ciberseguridad y la ciberdefensa para estar preparado frente al panorama de riesgos globales en el marco de la era tecnológica.

El país que más cooperación de coautorías tiene en relación con el modelamiento y simulación en ciberseguridad y ciberdefensa es también Estados Unidos, quien se encuentra unido con siete países, seguido de India que está unido con seis países e Italia que se relaciona con seis también, mostrando una cooperación sectorial de producción científica en tres regiones diferentes.

Se destacan cuatro grandes campos de investigación, lográndose esto al mapear las coocurrencias de palabras en la colección bibliográfica, el primer campo está relacionado con

ciberseguridad y seguridad de la información, el segundo con ciencia de datos, el tercero con infraestructuras críticas y el cuarto con ciberseguridad industrial.

El análisis de los artículos más destacados refleja que la ciberseguridad y la ciberdefensa han tenido un crecimiento exponencial que demanda del desarrollo de modelos de predicción que permitan pronosticar la probabilidad de riesgo de un ciberataque en infraestructuras críticas. Igualmente, se vuelve de gran interés en el campo de la ciberdefensa, pues existen algunos modelos que abordan esta área, pero sus predicciones no son completamente acertadas y aceptadas.

Frente a la existencia de pocos estudios relacionados con la ciberdefensa y las infraestructuras críticas que permitan implementar técnicas de modelamiento y simulación para optimizar la gestión propia de cada área, es necesario que aumente la participación de los investigadores y sus interacciones con otros para la generación de nuevos temas sobre modelamiento y simulación en ciberseguridad y ciberdefensa.

Referencias

[Abdi y Velentin, 2018] Abdi, H. y Velentin, D. (2018). *Multiple correspondence analysis. Multiple Correspondence Analysis For The Social Sciences, January*, 31-55. doi: https://doi.org/10.4324/9781315516257-3 ↑Ver página 96

[Aria, 2016] Aria, M. (2016). *Bibliometrix R Package*. Recuperado de https://www.bibliometrix.org/ ↑Ver página 81, 93, 94

[Aria y Cuccurullo, 2017] Aria, M. y Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive sciencemapping analysis. *Journal of Informetrics, 11*(4), 959-975. doi: https://doi.org/10.1016/j.joi.2017.08.007 ↑Ver página 81, 83

[Bradshaw *et al.,* 2012] Bradshaw, J., Carvalho, M., Bunch, L., Eskridge, T., Feltovich, P., Johnson, M., Kidwell, D. (2012). Sol: An Agent-Based Framework for Cyber Situation Awareness. *KI - Künstliche Intelligenz, 26*, 127-140. doi: https://doi.org/10.1007/s13218-012-0179-2 ↑Ver página 86

[Buczak y Guven, 2016] Buczak, A. y Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys and Tutorials, 18*(2), 1153-1176. doi: https://doi.org/10.1109/COMST.2015.2494502 ↑Ver página 94

[Cabuya y Mahecha, 2019] Cabuya, D. y Mahecha, E. (2019). *Lineamientos Estratégicos de Ciberdefensa para el Comando General de las Fuerzas Militares de Colombia - Reservado*. Colombia: Comando Conjunto Cibernético. ↑Ver página 84

[Cano, 2018] Cano, J. (2018). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Sistemas, 119*, 1-7. Recuperado de https://acis.org.co/archivos/Revista/119/Editorial.pdf ↑Ver página 84

[Carvalho *et al.,* 2014] Carvalho, M., Travassos, C. y Coeli, C. (2014). *Redes de cooperación científica. Cad. Saúde Pública, Rio de Janeiro, 30*(2), 225-227. Recuperado https://www.scielo.br/pdf/csp/v30n2/es_0102-311X-csp-30-2-0225.pdf de doi: 10.1590/0102-311XED010214 ↑Ver página 94

[Centro Criptológico Nacional, 2013] Centro Criptológico Nacional. (2013). *Guía/Norma de seguridad de las TIC (CCN-STIC-400).* Madrid, España: Centro Criptológico Nacional. Recuperado de https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/4-ccn-stic-400-manual-stic/file.html ↑Ver página

[Departamento Nacional de Planeación, 2016] Departamento Nacional de Planeación. (2016). *CONPES 3854 - Política Nacional de Seguridad Digital*. Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf ↑Ver página 85

[Elango *et al.,* 2020] Elango, B., Matilda, S. y Jeyasankari, J. (2020). Redefining search terms for cybersecurity: A bibliometric perspective. *SSRN Electronic Journal, December*. doi: https://doi.org/10.2139/ssrn.3688394 ↑Ver página 80, 83

[Elango y Rajendran, 2012] Elango, B. y Rajendran, P. (2012). Authorship trends and collaboration pattern in the marine sciences literature: a scientometric study. *International Journal of InformationDissemination and Technology*, May 2014, 166-169. ↑Ver página 91, 92

[Escuela Superior de Guerra, 2019] Escuela Superior de Guerra. (2019). *Ciberseguridad y Ciberdefensa documentación técnica*. Innova. ↑Ver página 85

[Gutiérrez *et al.,* 2018] Gutiérrez, M., Martínez, M., Moral, J., Herrera, E. y Cobo, M. (2018). Some bibliometric procedures for analyzing and evaluating research fields. *Applied Intelligence, 48*(5), 1275-1287. doi: https://doi.org/10.1007/s10489-017-1105-y ↑Ver página 83, 91

[Johnson, 2007] Johnson, C. (2007). Safeguarding against and responding to the breach of personally identifiable information. *OMB Memorandum M-07-16*, 7. ↑Ver página 94

[Kissel *et al.,* 2008] Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J. y Gulick, J. (2008). NIST SP 800-64 Rev. 2. Security Considerations

in the System Development Life Cycle. *Information Security*. Recuperado de http://dl.acm.org/citation.cfm?id=2206279%5Cnpapers2://publication/uuid/D524BF13-D081-4554-AB83-6A82E77E6EC8 ↑Ver página 94

[Kotenko, 2005] Kotenko, I. (2005). Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in Internet. *Simulation in Wider Europe - 19th European Conference on Modelling and Simulation, ECMS 2005*, 533-543. ↑Ver página 85, 86

[Kotenko, 2007] Kotenko, I. (2007). Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security. *2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS*, 614-619. doi: https://doi.org/10.1109/IDAACS.2007.4488494 ↑Ver página

[Lu, Li y Yang, 2018] Liu, S., Li, Y. y Yang, Z. (2018). Modelling of cyber-attacks and defenses in local metering system. *Energy Procedia*, 145, 421-426. doi: https://doi.org/10.1016/j.egypro.2018.04.069 ↑Ver página 87

[Makawana y Jhaveri, 2018] Makawana, P. y Jhaveri, R. (2018). A bibliometric analysis of recent research on machine learning for cyber security. *Lecture Notes in Networks and Systems, 19*, 213-226. doi: https://doi.org/10.1007/978-981-10-5523-2_20 ↑Ver página 80, 83

[Pastrana *et al.*, 2015] Pastrana, S., Tapiador, J., Orfila, A. y Peris, P. (2015). Defidnet: A framework for optimal allocation of cyberdefenses in Intrusion Detection Networks. *Computer Networks, 80*, 66-88. doi: https://doi.org/10.1016/j.comnet.2015.01.012 ↑Ver página 86

[R Foundation, 2019] R Foundation. (2019). *The R Project for Statistical Computing (3.4.4)[software*]. Recuperado de https://www.r-project.org/ ↑Ver página 81

[Roy *et al.*, 2010] Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V. y Wu, Q. (2010). A survey ofgame theory as applied to network security. *Proceedings of the Annual Hawaii International Conference on System Sciences*. doi: https://doi.org/10.1109/HICSS.2010.35 ↑Ver página 94

[Sabillon *et al.*, 2016] Sabillon, R., Cavaller, V. y Cano, J. (2016). National cyber security strategies: Global trends in cyberspace. *International Journal of Computer Science and Software Engineering (IJCSSE), 5*(5). Recuperado de www.IJCSSE.org ↑Ver página 84

[Shukla y Gochhait, 2020] Shukla, G. y Gochhait, S. (2020). Cyber security trend analysis using web of science: A bibliometric analysis. *European Journal of Molecular and Clinical Medicine, 7*(6), 2567-2576. ↑Ver página 80, 83

[Túñez y de Pablos, 2013] Túñez, J. y de Pablos, J. (2013). El 'índice h' en las estrategias de visibilidad, posicionamiento y medición de impacto de artículos y revistas de investigación. Investigar La comunicación hoy. *Revisión de políticas científicas y aportaciones metodológicas: simposio internacional sobre política científica en comunicación*, 133-150. Recuperado de http://dialnet.unirioja.es/servlet/articulo?codigo=4227310&info=resumen&idioma=ENG ↑Ver página 83, 91

[United States Government, 2018] United States Government. (2018). *Joint Publication Cyberspace Operations*. Estados Unidos: Createspace Independent Publishing Platform. ↑Ver página 84

[Urbizagastegui, 1999] Urbizagastegui, R. (1999). La ley de Lotka y la literatura de bibliometría. *Investigación Bibliotecológica: Archivonomía, Bibliotecología e Información, 13*(27), 125-141. doi: https://doi.org/10.22201/iibi.0187358xp.1999.27.3913 ↑Ver página 92

[Urquía & VillabaCarla, 2016] Urquía, A., & VillabaCarla, M. (2016). *Métodos de simulación y modelado*. Madrid: UNED. ↑Ver página 85

[Valencia *et al.,* 2020] Valencia, A., Giraldo, M., Acevedo, Y., Garcés, L., Quiroz, J., Benjumea, M. y Patiño, J. (2020). Tendencias investigativas en educación en ciberseguridad: Un estudio bibliométrico. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, E29*(05), 225-239. ↑Ver página 80, 83