# Revisión sistemática de literatura sobre ransomware a través de un ciberataque.

# Problema de investigación

Un ciberataque es cualquier tipo de actividad hostil que utiliza numerosos medios para robar, manipular, destruir datos, o sistemas de información. Comúnmente se orientan a sistemas de información computacional, infraestructuras, redes o dispositivos informáticos personales (Perwej et al., 2021)

Ransomware una forma de ciberataque categorizado dentro de los delitos cibernéticos (Lu et al., 2020). Este tipo de ciberataque es creado con el objetivo de extorsionar y es conocido como uno de los tipos de ciberataques más frecuentes. Consiste en software que cifra los datos en la computadora de la víctima y exige un pago antes de que los datos puedan ser liberados (Perwej et al., 2021), por ejemplo, el ataque de ransomware Wannacry que se produjo en 2017 es uno de los más grandes de la historia (Lu et al., 2020) que afectaron las finanzas de empresas en todo el mundo.

En el año 2023 Fortinet realizó una encuesta a 569 líderes de ciberseguridad y personas responsables de la toma de decisiones de organizaciones en todo el mundo. Los resultados muestran que el 80 % de los encuestados expresan estar “muy” o “extremadamente” preocupados por la amenaza del ransomware. A su vez, el 78 % de las organizaciones encuestadas expresan estar “muy” o “extremadamente” preparados para impedir una violación de datos. De las organizaciones que experimentaron un incidente de ransomware, el 71 % dijo que pagó al menos una parte del rescate que se exigía, aunque el 72 % indicó que detectó el incidente en horas (por lo general, en minutos). Además, aunque casi todos los encuestados tenían ciberseguro, esto no garantizaba que se cubrieran todos los costos o que se restauraran los datos. De hecho, solo el 35 % de los afectados por ransomware recuperaron todos sus datos después del incidente. (Fortinet, 2023)

Teniendo en cuenta que el ciberataque es un tema crítico para las organizaciones, que aumenta con el desarrollo y uso de nuevas tecnologías, y que está generando problemas como pérdidas económicas, de información, daño reputacional, operatividad y competitividad es necesario adelantar investigaciones que permitan caracterizar elementos asociados con este tema. En este trabajo se propone una revisión sistemática de literatura para analizar el grado de afectación y los riesgos de las empresas víctimas de este tipo de ataques. Los resultados de este trabajo podrán servir como punto de partida para establecer mecanismos de seguridad y salvaguarda de información.

# Fase 1. Plan del estudio

Para lograr el propósito de este estudio se utiliza el protocolo de Revisión sistemática de literatura. La primera fase del protocolo establece la realización del plan de la revisión, para este caso, se definieron las preguntas de investigación. A su vez, dichas preguntas facilitan orientar el diseño de una cadena de búsqueda que será ejecutada en la base de datos que se ha seleccionado para realizar este estudio. Además, se definieron y los criterios de inclusión y exclusión para lograr una selección de los estudios claves para el objetivo de esta investigación. Se seleccionó la base de datos científica Scopus con el objetivo de encontrar la información más reciente que facilite abordar siguientes preguntas de investigación planteadas

Estas preguntas son:

**P1** ¿Cuáles son las consecuencias más comunes en un ataque cibernético?

**P2** ¿Cuáles son los riesgos más comunes a los que se ven expuestas las empresas después de sufrir un ataque cibernético?

**P3** ¿Qué medidas se están tomando para mitigar los riesgos por robo de información en un ataque cibernético?

La búsqueda de las publicaciones para dar respuesta a las preguntas de investigación se basó en la cadena de búsqueda: *ransomware AND cybersecurity AND malware,* y le aplicaremos estos criterios de inclusión y exclusión:

**CI1**. Se incluirán estudios de ataques cibernéticos en los últimos 5 años (2019-2024).

**CI2.** Se incluyen estudios clasificados por scopus en aéreas como Computer Science, Engineering, Economics, Econometrics and Finance.

**CI3.** Se incluyen estudios que estén en idioma en inglés y español.

**CE1**.Se excluyen estudios que no sean de tipo article and conference paper

**CE2**.Se excluyen estudios de ataques cibernéticos que contengan las palabras clave: Machine-learning, Machine Learning, Internet Of Things y Health Care.

# Fase 2. Ejecución del estudio

La ejecución del estudio es definida a partir de la cadena de búsqueda establecida en la fase de planeación.

La ejecución de la cadena de búsqueda en la base de datos Scopus da como resultado un total de 459 estudios capturados. Esta cantidad de estudios se obtiene sin aplicar ningún criterio de inclusión y exclusión. Sin embargo, para conseguir seleccionar los estudios que harán parte de la muestra de estudios para conducir la revisión, se aplicaron los criterios de inclusión y exclusión.

A continuación, se relaciona en la **Fig. 1 Relación del proceso de filtrado a partir de la aplicación de los CI y CE definidos**, el proceso realizado para filtrar los estudios capturados. Cada iteración de filtrado logró reducir la cantidad de documentos acotando así los estudios con el propósito de obtener aquellos relacionados con nuestro problema de investigación.

**Fig. 1.** Relación del proceso de filtrado a partir de la aplicación de los CI y CE definidos

Se entiende que después de aplicar los criterios de inclusión y exclusión, palabras claves, llegamos a un total de 255 de estudios seleccionados. Estos estudios representan la muestra total de estudios que harán parte de la revisión de literatura en curso.

# Fase 3. Análisis de resultados

# Análisis general de estudios

En esta sección se presentan los resultados obtenidos de la ejecución del estudio en la base de datos Scopus, se espera obtener respuestas a las preguntas de investigación planteadas en la etapa de planeación. Un primer análisis que se pretende mostrar relacionado con este problema de investigación es la bibliometría.

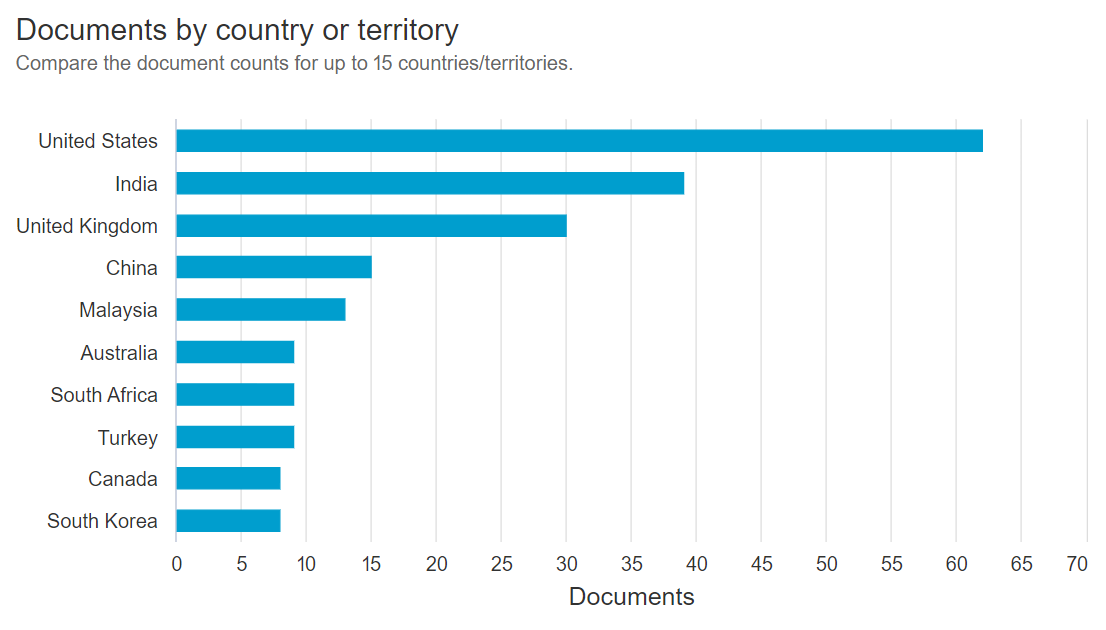
Entre los resultados generales está la tendencia de estudios por año. En la **Fig. 2. Documentos por año,** se deduce que entre los años 2019 al 2024 hay un incremento exponencial en la publicación de artículos y conference paper clasificados por el CE1. Estos estudios contienen palabras claves relacionadas con la cadena de búsqueda. El crecimiento mostrado en la Fig. 2, determina el interés por este tema de investigación, en el año 2021 se evidencia el mayor crecimiento en estudios relacionados, con un incremento del 52% en relación con el año anterior.

Gráfico, Gráfico de líneas

Descripción generada automáticamente

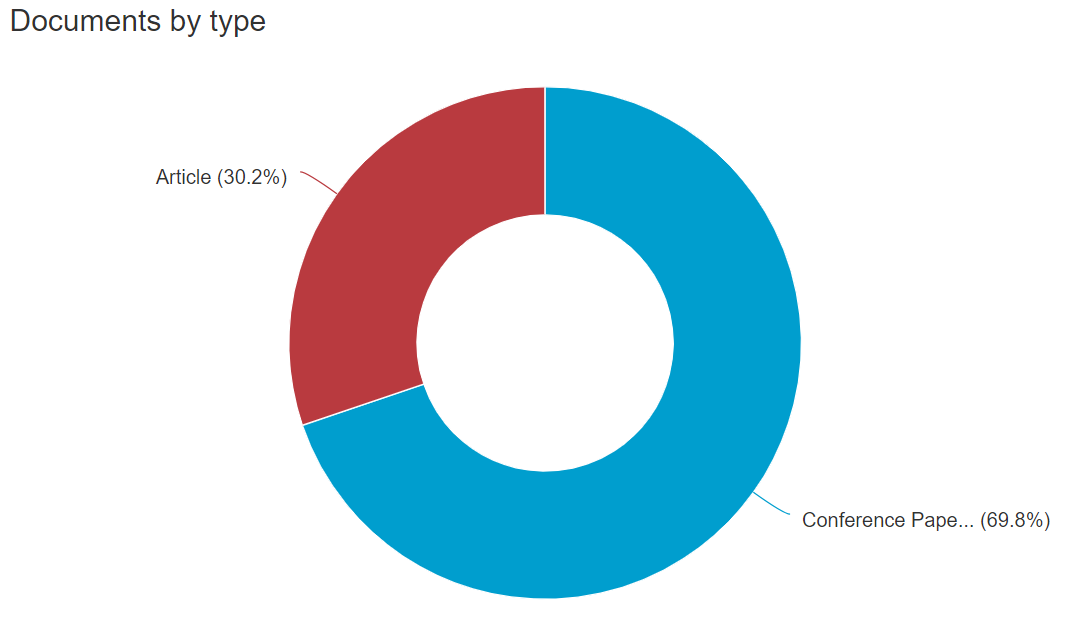
**Fig. 2.** Documentos por año

Entre los resultados generales está la tendencia por país. En la **Fig. 3. Documentos por país/territorio** se puede evidenciar que los mayores aportes en el tema provienen de Estados unidos, India y Reino Unido con un porcentaje de participación del 31%, 19% y 15% respectivamente.



**Fig. 3.** Documentos por país/territorio

Entre los resultados generales está la tendencia por tipo de documento. En la **Fig. 4 Documentos por tipo,** se evidencia que el 69.8% de la muestra de documentos corresponde a conference paper y el 30.2% a artículos científicos, lo cual permite entender que hace falta generar más artículos científicos relacionados con el área de interés ya que su porcentaje es bajo.



**Fig. 4.** Documentos por tipo

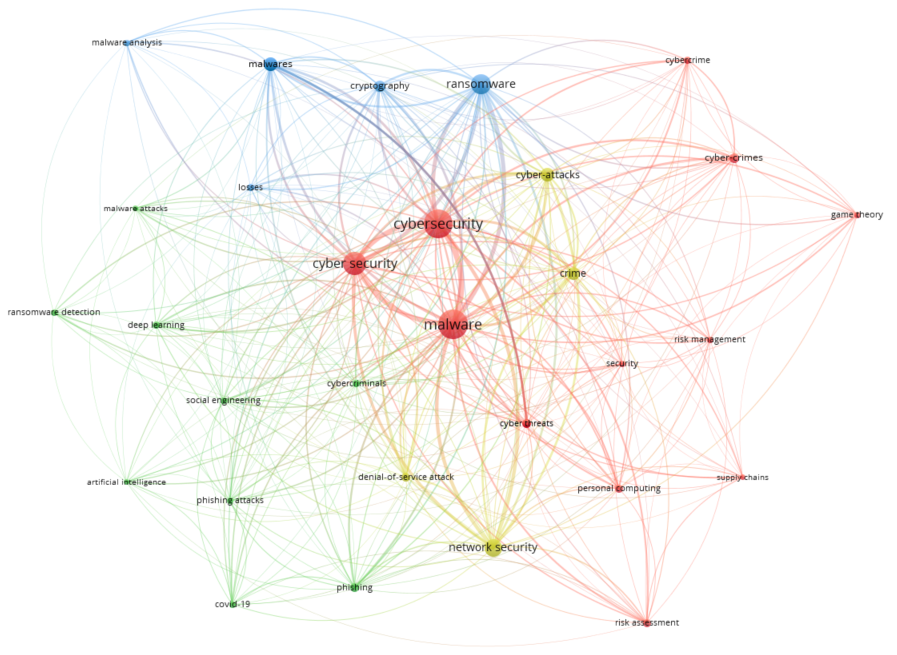
# Bibliometría

En esta sección se utilizan las imágenes generadas por la herramienta VOSviewer, la cual permite construir y visualizar redes bibliométricas para un posterior análisis de la literatura científica. Cada nodo en la red representa una entidad y cada conexión visualizada por medio de líneas, representa la relación que existe entre ellas.

Para la generación de la red en VOSviewer se procede de la siguiente manera: 1. exportar los estudios seleccionados a un archivo .csv en Scopus, únicamente después de aplicar todos los CI y CE identificados en el Plan de estudios, 2. cargar el archivo generado en la herramienta y obtener la red de conexiones.

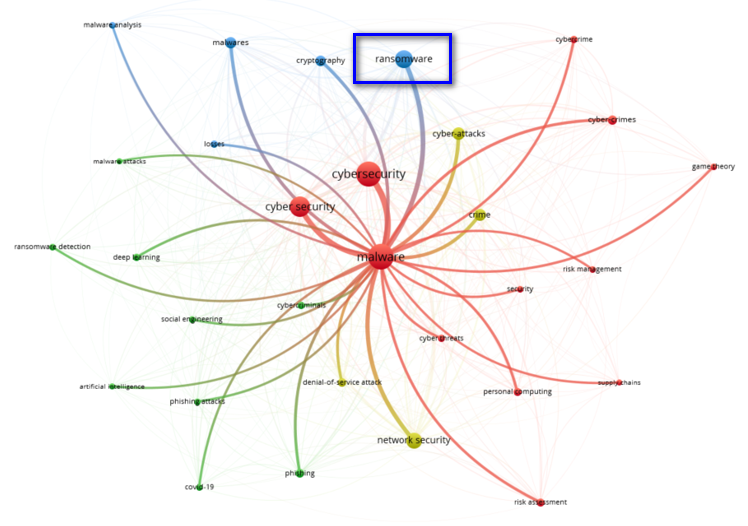
En el caso de la **Fig. 5 Grupos temáticos**, se tienen palabras claves basadas en los términos extraídos en los títulos y abstract de los 255 estudios seleccionados; este mapa se generó tomando como tipo de análisis co-ocurrencia para “todas las palabras claves”, con un mínimo número de ocurrencias de 10 por termino, lo cual permite evidenciar que se emplearan 30 palabras claves en el análisis.

El resultado, permite identificar que los cluster principales son: cybersecurity y malware, visibles en color rojo.



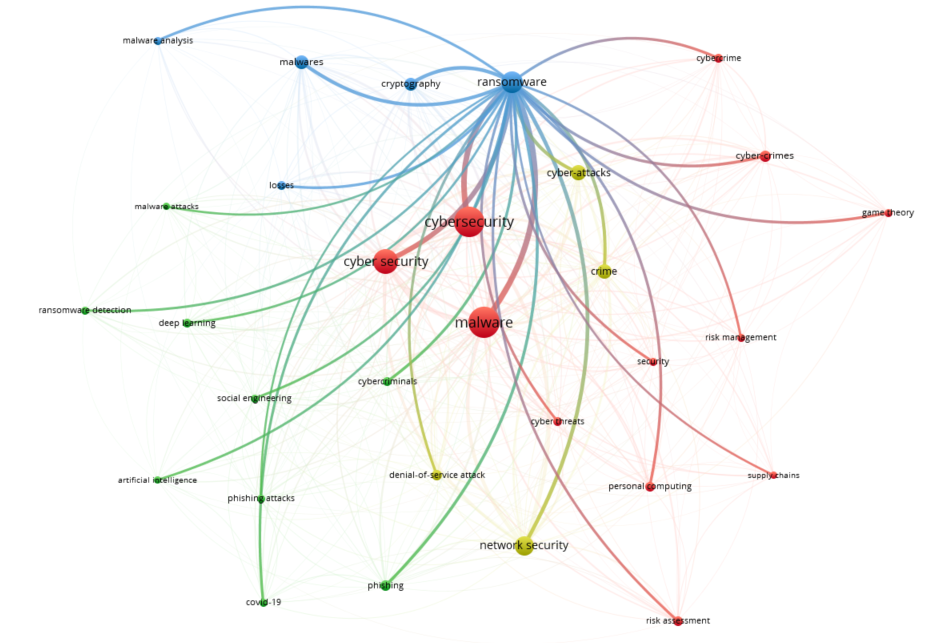
**Fig. 5**. Grupos temáticos

En la red bibliométrica se identifica que en algunos cluster predominan tanto palabras claves como colores, lo que se interpreta como una alta correlación entre los términos; en la **Fig. 6. Cluster de palabra clave: Malware,** se logra evidenciar que el nodo ransomware, que es importante en el presente estudio, si bien, tiene relación con los cluster principales, aún le falta más estudios que lo referencien para crear conexiones más fuertes.



**Fig. 6.** Cluster de palabra clave: Malware

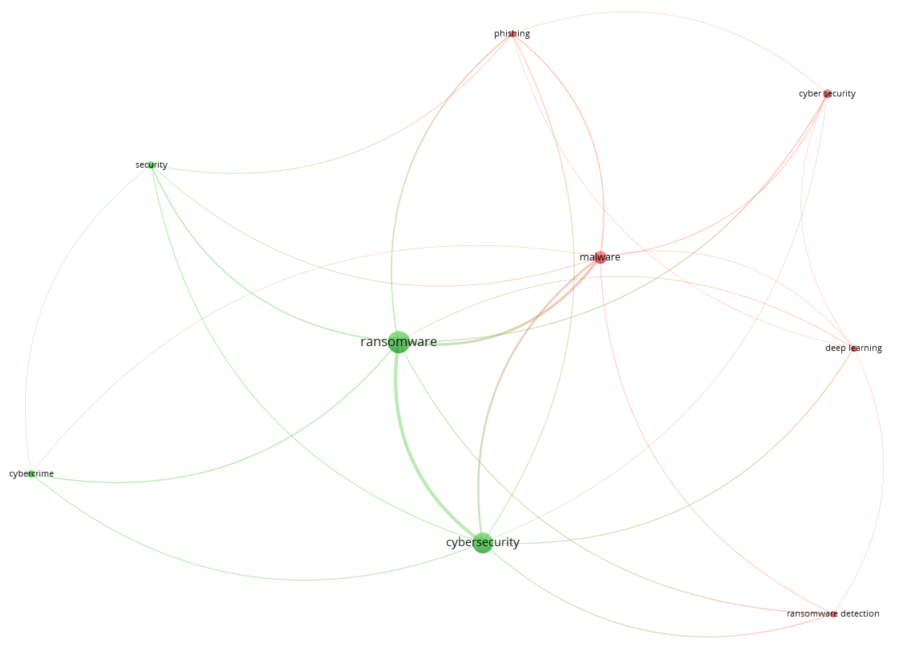
Por otra parte, en la **Fig. 7. Cluster de palabra clave: Ransomware,** se evidencia una conexión débil con los clusters principales, lo que sugiere que pueden faltar estudios en esa área que hable más sobre el ransomware como un tipo de malware que afecta la ciberseguridad .



**Fig. 7.** Cluster de palabra clave: Ransomware

En el caso de la **Fig. 8. Palabras clave por autor**, se tienen palabras claves basadas en los términos extraídos en los títulos y abstract de los 255 estudios seleccionados; este mapa se generó tomando como tipo de análisis co-ocurrencia para “todas las palabras claves por autor”, con un mínimo número de ocurrencias de 10 por termino, con 9 palabras claves seleccionadas.

El resultado, permite identificar que el cluster principal es: ransomware, visible en color verde. Lo que se puede interpretar como un término importante dentro de los estudios seleccionados, siendo predominante para los autores, aunque la ocurrencia de este término dentro del mapa general no se evidencie.



**Fig. 8.** Palabras clave por autor

# Conclusiones

En resumen, se evidencia que Estados unidos, India y Reino Unido realizaron la mayor cantidad de estudios a partir del 2021, siendo de esta forma los mayores contribuyentes a la generación de conocimiento sobre la ciberseguridad y el ransomware con un 65% de publicaciones.

Se puede verificar que en el 2021 se presentó el mayor incremento de los últimos 5 años en estudios relacionados con la ciberseguridad y el ransomware con un porcentaje del 52% de publicaciones en comparación al año anterior.

También se logra evidenciar en este estudio que falta generar más conocimiento científico sobre el tema del ransomware, ya que, aunque es un término recurrente en los estudios no es el principal.

Referencias

Fortinet. (2023). *Informe global sobre el ransomware 2023 INFORME*. https://global.fortinet.com/ai-la-lp-es-ap-global-ransomware-report2023?lsci=701Hr000001xcEfIAI&UID=ftnt-4223-68291&

Lu, G., Liu, Y., Chen, Y., Zhang, C., Gao, Y., & Zhong, G. (2020). A Comprehensive Detection Approach of Wannacry: Principles, Rules and Experiments. *Proceedings - 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2020*, 41–49. https://doi.org/10.1109/CyberC49757.2020.00017

Perwej, Dr. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12). https://doi.org/10.18535/ijsrm/v9i12.ec04