RMP
Revista dos Mestrados Profissionais
UFPE / CCSA – MGP
https://periodicos.ufpe.br/revistas/rmp
ISSN – 2317 - 0115
V. 14 - N. 2 (2025)
Recife - PE

Perfil de las investigaciones sudamericanas en ciberseguridad

Nadianne Maria dos Santos Galvão
Universidade Federal de Sergipe
nadiannegalvao@gmail.com
https://orcid.org/0009-0009-6659-5039

Nadielli Maria dos Santos Galvão
Universidade Federal de Sergipe
profa.nadielligalvao@gmail.com
https://orcid.org/0009-0000-5847-221X

Resumen – Este artículo tiene como objetivo analizar el perfil de las investigaciones sudamericanas en ciberseguridad. Para ello, se buscaron trabajos científicos en bases de datos que priorizan la producción científica de la región. La muestra estuvo conformada por 25 estudios. Como resultado, se identificó que las investigaciones sudamericanas en ciberseguridad fueron publicadas, en su mayoría, en el año 2021, en Colombia, por investigadores vinculados a la Universidad Militar de Nueva Granada, en la revista Logos Ciencia y Tecnología, siendo las pequeñas y medianas empresas el tipo organizacional más citado como objeto de estudio.

Palavras-chave: bibliometria, cibersegurança, investigación científica.

Perfil da pesquisa em cibersegurança na América do Sul

Resumo – Este artigo tem como objetivo analisar o perfil da pesquisa em cibersegurança na América do Sul. Para tanto, foram pesquisados trabalhos científicos em bases de dados que priorizam a produção científica da região. A amostra foi composta por 25 estudos. Os resultados identificaram que a maior parte da pesquisa em cibersegurança na América do Sul foi publicada em 2021 na Colômbia por pesquisadores afiliados à Universidade Militar de Nueva Granada, na revista Logos Ciencia y Tecnología. As pequenas e médias empresas (PMEs) foram o tipo organizacional mais frequentemente citado como objeto de estudo.

Palavras-chave: bibliometria, cibersegurança, pesquisa científica.

Profile of South American cybersecurity research

Abstract – This article aims to analyze the profile of South American studies on cybersecurity. To this end, scientific papers were retrieved from databases that prioritize the region's scientific production. The sample consisted of 25 studies. The results indicate that South American research on cybersecurity was mostly published in 2021, in Colombia, by researchers affiliated with the Universidad Militar de Nueva Granada, in the journal Logos Ciencia y Tecnología, with small and medium-sized enterprises being the most frequently cited organizational type as the object of study.

Keywords: bibliometrics, cybersecurity, scientific research.

Data da Submissão: 29/07/2025 - **Data de aceitação:** 08/12/2025

RMP
Revista dos Mestrados Profissionais
UFPE / CCSA – MGP
https://periodicos.ufpe.br/revistas/rmp
ISSN – 2317 - 0115
V. 14- n. 2 (2025)
Recife – PE

1. Introducción

Según David, Sankar y Azam (2023), Internet se ha convertido en una parte esencial de la vida cotidiana de las personas y, aunque este fenómeno ha traído numerosos beneficios, la preocupación de los usuarios por la privacidad, la seguridad y la protección de sus datos ha crecido de manera proporcional. No es raro encontrar datos como los presentados en el informe Cyber Security Threats, de la consultora Check Point, que muestran, por ejemplo, que en el año 2024 se registró en todo el mundo un promedio de 1.673 ciberataques por semana contra ciudadanos, empresas e incluso organismos gubernamentales (Caniato, 2025).

En este escenario, es importante destacar que, si el avance de Internet no va acompañado de políticas y prácticas de seguridad sólidas, los datos quedan expuestos a riesgos que, en consecuencia, afectan la imagen de las instituciones, tanto públicas como privadas, en las cuales la población deposita su confianza. Con el fin de mantener su reputación ante la sociedad y cumplir con leyes como la Ley General de Protección de Datos (LGPD), en Brasil, y el Reglamento General de Protección de Datos (GDPR), en el ámbito europeo, es fundamental que las empresas y las instituciones públicas implementen políticas de protección de datos y que dichas iniciativas sean de conocimiento público. Recoger datos sin el consentimiento del titular de la información infringe la LGPD en su artículo 2, que establece normas para la protección de los datos personales, como el respeto a la privacidad.

Es válido enfatizar que la Ley General de Protección de Datos (Ley n.º 13.709/2018) clasifica los tipos de datos de la siguiente manera: a) datos personales, que identifican al ciudadano de forma directa o indirecta (número de identificación, registro fiscal, correo electrónico); b) datos sensibles, vinculados a las convicciones filosóficas o religiosas, o al origen étnico del individuo; c) datos públicos, que pueden utilizarse sin requerir un nuevo consentimiento del titular, siempre que se actúe de buena fe; d) datos anonimizados, obtenidos mediante métodos que modifican la información de tal forma que se vuelve imposible identificar al titular.

Ante esta clasificación y las obligaciones legales, no se trata de una opción, sino de una obligación que las empresas adopten una postura alineada con buenas prácticas de seguridad, lo que contribuye a preservar la confianza de la sociedad en la capacidad de la organización para gestionar de manera responsable la información que le ha sido confiada. Sin embargo, algunas noticias muestran que aún hay mucho por avanzar en esta perspectiva, tanto en Brasil como en los países vecinos.

Bocconi (2025) señaló que, según un levantamiento del Banco Mundial presentado en el libro *Cybersecurity Economics for Emerging Markets* (2024), los incidentes cibernéticos en América Latina aumentaron, en promedio, un 25% al año en comparación con la última década. Los datos publicados por Check Point Research (CPR) corroboran este escenario, al mostrar que, en el segundo semestre de 2024, América Latina registró un aumento del 53% en el volumen de ataques cibernéticos en comparación con el mismo período del año anterior (Ministerio Público de Mato Grosso, 2024).

De acuerdo con los datos presentados en el informe Escenario de Riesgos Cibernéticos para el Sector Financiero de América Latina en 2025, alrededor del 79% de las empresas de América Latina fueron víctimas de ransomware, un tipo de ataque que bloquea o cifra datos y exige el pago de un rescate para restaurar el acceso. Este porcentaje es superior al promedio global, que es del 53% (Gil, 2025). Cuando se analiza más específicamente Sudamérica, esta es considerada la región más vulnerable a los ataques cibernéticos en el mundo (Zoho, 2023).

Ante esto, se vuelve urgente una articulación entre empresas, organismos públicos e investigadores, de modo que se comprendan los problemas relacionados con la ciberseguridad en diferentes regiones y, a partir de ello, se propongan soluciones para mitigar dichas vulnerabilidades. Como se señalará en la sección 2.2 de este artículo, algunos estudios ya se han dedicado al tema; sin embargo, todavía existe cierta escasez de discusiones al respecto en países emergentes, como los de América Latina y, de forma más específica, en América del Sur.

Así, ante el hecho de que América del Sur ha sido señalada como la región con mayor vulnerabilidad cibernética en el mundo, surge la motivación de comprender qué esfuerzos se están realizando para intentar revertir este panorama. Con ello, es posible identificar investigaciones científicas que aborden este tema en la región y, de este modo, conocer el perfil de lo que ha sido desarrollado por los investigadores sudamericanos.

Por ello, la cuestión que orienta esta investigación es: ¿Cuál es el perfil de las investigaciones sobre ciberseguridad desarrolladas en América del Sur? En este sentido, el objetivo de este trabajo es analizar el perfil de las investigaciones sudamericanas en ciberseguridad. Para ello, se realizó un levantamiento de artículos científicos en bases de datos que priorizan estudios de esta región, con el fin de conocer lo que ha sido producido por investigadores de este espacio territorial.

Se espera, entonces, que este estudio pueda arrojar luz sobre un tema indispensable en la contemporaneidad y, al mismo tiempo, mostrar cuánto puede aportar la región sudamericana, aun con sus dificultades. Asimismo, se busca valorar los esfuerzos de los investigadores que trabajan para enfrentar los problemas de vulnerabilidad cibernética en esta región específica, incentivando nuevos estudios que puedan dialogar entre sí y contribuir al avance de la temática.

El estudio está dividido en cinco secciones. Esta es la introducción, en la cual se presentan el contexto de la investigación y su objetivo. A continuación, se incluye una sección de conceptualización y de revisión de estudios anteriores. En la tercera sección, se expone la metodología de la investigación. Luego, en la cuarta sección, se presentan los resultados encontrados. Por último, en la quinta sección, se discuten las conclusiones del trabajo, seguidas de las referencias.

2. Ciberseguridad: Conceptos e Investigaciones Anteriores

Hay que si descorrer sobre aspectos conceptuales interesantes a relación de pesquisa.

2.1 Aspectos Conceptuales

De acuerdo con Schiliro (2023), la definición de ciberseguridad se presenta de forma simplista, vinculando el concepto a la respuesta frente a amenazas. Para él, una definición más profunda unificaría la multidisciplinariedad de las acciones de prevención, detección y respuesta. De acuerdo con Nogueira (2023) la ciberseguridad es como um

subconjunto de la seguridad digital, siendo la seguridad digital un término más amplio que abarca la protección de la información en cualquier formato digital. Así, la ciberseguridad sería el conjunto de acciones adoptadas para proteger nuestros ordenadores, teléfonos móviles, datos e internet frente a ataques.

De acuerdo con el informe *Cybersecurity threatscape for Latin America and the Caribbean: 2023–2024*, los ciberdelincuentes en América del Sur se han centrado en tres objetivos principales.El sector público y el sector financiero son los más atacados, ya que contienen grandes volúmenes de datos valiosos. En seguida, se encuentran las empresas de comercio electrónico y las industrias (Bezborodko, 2025).

En el mismo informe se señala que la ingeniería social, que explota el comportamiento humano en lugar de fallas técnicas (Agência Brasileira de Inteligência, 2021), es responsable de ser el principal tipo de ataque cibernético, estando presente en el 57 % de los ataques a organizaciones y en el 96 % de los ataques a individuos. Por su parte, el uso de malware, que consiste en la utilización de programas maliciosos desarrollados para causar daños, robar información o permitir el acceso no autorizado a sistemas (IBM, 2022), alcanza al 67 % de las organizaciones y al 79 % de los individuos.

Y entre los malwares más utilizados en las organizaciones se encuentran los ransomware, que funcionan secuestrando datos o sistemas completos mediante cifrado, volviéndolos inaccesibles hasta que se realice el pago de un rescate (Kaspersky, s. f.). A nivel individual, los spyware aparecen con mayor frecuencia. Este tipo de ataque puede registrar las teclas pulsadas, capturar contraseñas, monitorear actividades en tiempo real e incluso activar la cámara o el micrófono del dispositivo sin autorización, lo que permite el robo de datos personales y financieros de manera casi imperceptible (Fortinet, s. f.).

Pero, es válido señalar que esto no es un fenómeno reciente, ya que en 2017 se publicó una Guía de Defensa Cibernética en América del Sur, en la cual se registró que, en el año 2014, la región sudamericana tenía como principales vulnerabilidades los ataques mediante programas maliciosos (malware) y los ataques de ingeniería social, como el phishing. Lamentablemente, el escenario sigue siendo el mismo, incluso después de una diferencia de 10 años (Marques, 2021).

En un escenario tan desafiante como este, es necesario que las empresas adopten una postura preventiva frente a las vulnerabilidades. Cada institución posee demandas propias y, ciertamente, no es posible generalizar que todas las buenas prácticas adoptadas por una empresa u organismo público sean aplicables en todos los aspectos a otra organización. Sin embargo, existen determinados procesos, como el de gestión de vulnerabilidades, que ayudan a las organizaciones tanto en la prevención como en la corrección y mitigación.

El ciclo de vida de la gestión de vulnerabilidades (ilustrado en la Figura 01) comienza con la fase de descubrimiento, en la cual se realiza el inventario de todos los activos de la organización, después los mesmos serán priorizados, para, que, en la tercera etapa, se identifiquen las vulnerabilidades existentes. Una vez encontradas las vulnerabilidades, estas se clasifican de acuerdo con su criticidad, lo que permite que las más críticas reciban atención inmediata. A continuación, se desarrolla la fase de evaluación, responsable de medir el riesgo y el impacto de cada vulnerabilidad identificada.

Con base en estos resultados, se generan informes que documentan los riesgos encontrados y comunican la información relevante a los equipos responsables. Cabe

destacar la necesidad de elaborar informes a nivel técnico para el equipo encargado de corregir las vulnerabilidades identificadas, así como un informe a nivel empresarial, de modo que la gestión comprenda su importancia y fomente una cultura de gestión de vulnerabilidades dentro de la empresa. La siguiente etapa es la corrección, en la que se aplican parches, mitigaciones o ajustes de configuración para eliminar o reducir las fallas. Por último, se lleva a cabo la fase de verificación y monitoreo, que implica auditorías y un seguimiento continuo, garantizando que las medidas adoptadas funcionen correctamente y que nuevas vulnerabilidades sean detectadas con rapidez (Microsoft, s. f.).

Figura 1 – Ciclo de vida de gerenciamento de vulnerabilidades.

Dentro de este ciclo, es de suma importancia comprender que, en las fases de identificación de vulnerabilidades, generación de informes y documentación, se hace necesaria la elección de softwares para apoyar y automatizar (o no) este proceso, correspondiendo al equipo entender las demandas de la empresa. El mercado ofrece diversas plataformas gratuitas, de código abierto o de pago, como OpenVAS (Greenbone Vulnerability Management – GVM), OWASP ZAP (Zed Attack Proxy), ClamAV, entre otras, que contribuyen de manera significativa a todo este flujo (IBSEC, 2024).

Cuando se analizan problemas como los de la ingeniería social, nada resulta más eficaz que un plan de concientización dirigido a los colaboradores de la empresa y a la población en general. Dado que el actor malintencionado se aprovecha de la desinformación de los individuos para encontrar brechas y, de este modo, apropiarse de sus datos con el fin de acceder a sus cuentas personales o incluso a sectores corporativos que, en condiciones normales, deberían permanecer restringidos.

Esta concientización puede llevarse a cabo por medio de charlas, capacitaciones, cartillas digitales, folletos y materiales impresos distribuidos en los entornos corporativos, con el fin de mantener a los colaboradores siempre alerta. La Federación Brasileña de Bancos (FEBRABAN), por ejemplo, desarrolló una cartilla que aborda la ingeniería social de manera clara, accesible y comprensible para diferentes públicos, sirviendo como una importante referencia práctica para las empresas que desean fortalecer sus acciones de prevención. (link aquí).

Otro punto que fortalece la seguridad en la empresa es mantenerse siempre alineada con las normas de regulación exigidas por la federación del país en el que se encuentra establecida. De acuerdo con Solano Camargo, presidente de la Comisión de Privacidad, Protección de Datos e Inteligencia Artificial de la Orden de los Abogados de Brasil (OAB) en São Paulo, en una entrevista concedida a Pacete (2024), incluso después de seis años de la promulgación de la LGPD, una gran parte de los brasileños aún no tiene plena conciencia de que sus datos personales cuentan con protección legal. Esto ocurre principalmente debido a la ausencia de acciones realmente eficaces por parte del poder público para informar y educar a la sociedad sobre estos derechos.

Además de las leyes que contribuyen a la cuestión de la privacidad de los datos, también existen los *frameworks* internacionales, como los *CIS Controls* desarrollados por el *Center for Internet Security* (link aqui) e o *National Institute of Standards and Technology - NIST Cybersecurity Framework* (link aqui), que ofrecen directrices prácticas para la implementación de controles de seguridad, la gestión de riesgos y la protección frente a amenazas cibernéticas. Asimismo, la adopción de estándares internacionales de certificación en la gestión de la seguridad de la información, como la ISO/IEC 27001 y las demás normas de la familia ISO 27000, también demuestra el compromiso con la protección de datos, garantizando conformidad y credibilidad ante clientes, socios y organismos reguladores.

Como se mencionó anteriormente, no existe un paso a paso ni una fórmula que se aplique de manera igual a todas las empresas, ni herramientas que atiendan de forma perfecta a todas las corporaciones. Cada institución posee su propio contexto, ya sea financiero o relacionado con el número de empleados y colaboradores. Sin embargo, existen cuestiones indispensables y, frente a este escenario, se pueden adoptar medidas como: invertir en la capacitación del personal, alinearse con las leyes de protección de datos y con marcos de referencia consolidados, e implementar un plan de gestión de vulnerabilidades continuo.

Sin embargo, incluso con la existencia de procesos consolidados y buenas prácticas reconocidas internacionalmente, los países de América del Sur siguen estando altamente expuestos a escenarios de ataque cibernético. Diversos factores contribuyen a esta realidad, entre ellos la escasez de profesionales calificados en seguridad de la información, tal como lo destaca el Instituto Brasileiro de Cibersegurança (IBSEC, 2024).

Además, de acuerdo con Neuber (2025), se observan algunas barreras adicionales que dificultan la adopción de prácticas adecuadas, como la implementación de medidas de seguridad insuficientes y las limitaciones financieras que enfrentan las organizaciones. Estos aspectos evidencian hasta qué punto las empresas aún encuentran dificultades para estructurar políticas robustas de ciberseguridad, volviéndose objetivos más vulnerables a ataques e incidentes digitales.

Sin embargo, todo comienzo puede representar un avance significativo. Como se señaló anteriormente, la implementación de campañas de concientización de bajo costo, asociadas al uso de herramientas gratuitas ya consolidadas, se configura como una estrategia inicial relevante para la prevención y mitigación de riesgos. Asimismo, la participación de un equipo multidisciplinario potencia la eficacia de estas iniciativas, ya que integra diferentes perspectivas y conocimientos especializados al proceso. En adición, las investigaciones científicas también tienen mucho que aportar en este ámbito, razón por la cual se buscó identificar estudios realizados sobre esta temática.

2.2 Investigaciones Anteriores

El tema de la ciberseguridad ya viene siendo una preocupación de algunos investigadores sudamericanos, quienes buscan levantar el estado del arte sobre la temática. Algunos trabajos se enfocan en temas específicos, como **blockchain** (Alzate y Giraldo, 2023; Rueda-Castañeda et al., 2024), **contenedores** (Chingo Esquivel y Gómez Gómez, 2020), **sistemas ciberfísicos** (Amador Donado, Pardo Calvache y Mazo Peña, 2024) y la **ciberseguridad en la educación superior** (Orosco-Fabian, 2024). Otros, como León Gutiérrez et al. (2022) y Matilde-Espino y Valencia-Pérez (2023), buscan analizar el tema de la ciberseguridad sin delimitar un alcance específico.

Por su parte, incluso los trabajos de levantamiento del estado del arte realizados por investigadores sudamericanos adoptan, en su mayoría, bases de datos que privilegian investigaciones del hemisferio norte, como la base Scopus, por ejemplo (Chingo Esquivel y Gómez Gómez, 2020; Alzate y Giraldo, 2023; Orosco-Fabian, 2024; Amador Donado, Pardo Calvache y Mazo Peña, 2024). No obstante, ya existen algunos trabajos que se enfocan especialmente en investigaciones sudamericanas o latinoamericanas, como, por ejemplo, Rueda-Castañeda et al. (2024), quienes buscaron identificar los estudios latinoamericanos que aplicaron herramientas de blockchain, y León Gutiérrez et al. (2022), quienes buscaron comprender el tema de la ciberseguridad de manera general en investigaciones peruanas. A su vez, Matilde-Espino y Valencia-Pérez (2023) se enfocaron en la misma temática, pero centrándose en las investigaciones mexicanas.

3. Metodologia

Este trabajo es una investigación descriptiva, ya que buscó describir las características de las investigaciones realizadas en territorio sudamericano sobre ciberseguridad. Para organizar la muestra que sería analizada, se siguieron algunos pasos de búsqueda. En un primer momento, fue necesario seleccionar las bases de datos que serían utilizadas. Considerando que el objetivo del estudio es analizar el perfil de las investigaciones sudamericanas sobre ciberseguridad, se eligieron bases que privilegian estudios de este espacio territorial, a saber: SciELO, Redalyc y La Referencia.

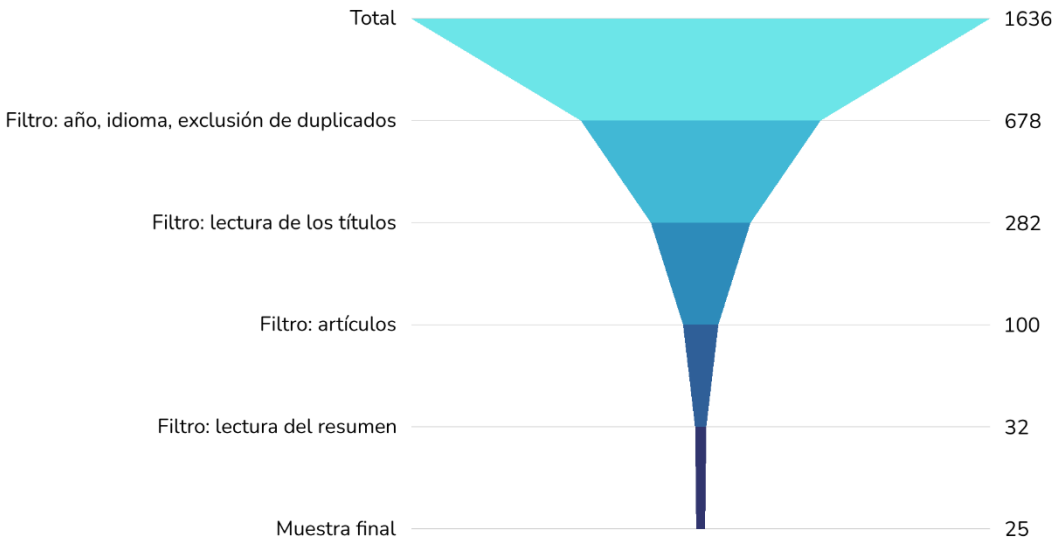
La búsqueda se realizó, en un primer momento, mediante la cadena (ciberseguridad OR cibersegurança), en el mes de junio de 2025, obteniéndose 1.636 trabajos. En seguida, se aplicó un filtro para seleccionar únicamente las investigaciones publicadas entre 2020 y 2024 (es decir, cinco años completos), en los idiomas portugués y español (idiomas oficiales de los países sudamericanos), y se excluyeron los trabajos duplicados entre las bases. Con esta primera clasificación, se seleccionaron 678 estudios.

A continuación, se realizó la lectura de los títulos de los trabajos con el fin de verificar su adherencia al tema de la investigación, que es la ciberseguridad. Esta etapa fue necesaria debido al elevado volumen de resultados obtenidos en la búsqueda inicial. De este modo, 282 trabajos continuaron siendo elegibles para formar parte de la muestra del estudio. Luego, filtramos los trabajos por tipo, seleccionando únicamente aquellos que eran artículos científicos publicados en revistas, obteniéndose un total de 100 documentos.

Los resúmenes de los 100 artículos fueron leídos y se excluyeron aquellos que eran estrictamente trabajos teóricos o de estado del arte (bibliometrías, revisiones sistemáticas y estudios afines), manteniéndose únicamente los estudios empíricos que realmente abordaban temas relacionados con la ciberseguridad, llegando así a 32 artículos

elegibles. Finalmente, con el objetivo de analizar la producción sudamericana, se excluyeron los trabajos realizados en otras regiones geográficas. De este modo, la muestra final quedó compuesta por 25 artículos. La figura 02 resume este proceso.

Figura 2 – Proceso de filtrado de los artículos de la muestra.



Para analizar los artículos, se optó por establecer algunos indicadores bibliométricos (Galvão; Schneider, 2024), seleccionados considerando lo que ya ha venido siendo adoptado en estudios anteriores, los cuales fueron discutidos en la sección 2.2 de este artículo. En el Cuadro 01 se presenta una síntesis de los indicadores seleccionados y de las investigaciones que también los han adoptado.

Cuadro 01 – Indicadores de análisis.

Indicadores	**Estudios anteriores**
Año	Chingo Esquivel e Gómez Goméz (2020); León Gutierrez *et al.* (2022); Alzate e Giraldo (2023); Matilde-Espino e Valencia-Pérez (2023); Rueda-Castañeda *et al.* (2024); Orosco-Fabian (2024).
País	Alzate e Giraldo (2023); Rueda-Castañeda *et al.* (2024); Orosco-Fabian (2024).
Autores más prolíficos	Alzate e Giraldo (2023); Matilde-Espino e Valencia-Pérez (2023); Orosco-Fabian (2024).
Instituciones de afiliación	Alzate e Giraldo (2023); Matilde-Espino e Valencia-Pérez (2023); Orosco-Fabian (2024).
Revistas	Alzate e Giraldo (2023); Matilde-Espino e Valencia-Pérez (2023); Orosco-Fabian (2024).
Palabras clave	Alzate e Giraldo (2023); Matilde-Espino e Valencia-Pérez (2023); Rueda-Castañeda *et al.* (2024); Orosco-Fabian (2024).

Fuente: Elaboración de las autoras (2025) con base en los estudios anteriores

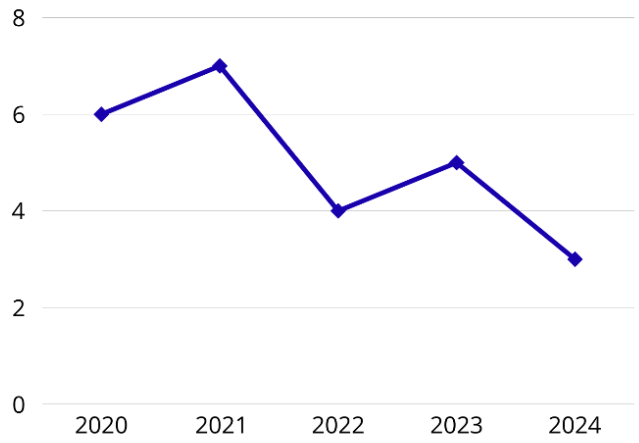
Los datos fueron organizados y analizados en hojas de cálculo de Excel, mientras que las figuras y los gráficos se elaboraron mediante herramientas gratuitas de Canva para lograr una mejor identidad visual. Todo el proceso de recopilación y análisis se llevó a cabo entre los meses de junio y agosto de 2025, y las autoras trabajaron con puntos de control semanales con el fin de revisar mutuamente las actividades, evitando sesgos en los análisis o la exclusión de estudios pertinentes. Los resultados obtenidos se presentan en la sección siguiente, la cual, además de los indicadores mencionados, incluye una breve descripción de los estudios analizados.

4. Resultados

4.1 Análisis descriptivo de la muestra

El análisis del perfil de las investigaciones se inició a partir del año de publicación. Como puede observarse en el Gráfico 01, el año 2021 fue el que presentó el mayor número de trabajos. Este resultado fue similar a los estudios de Alzate y Giraldo (2023) y Rueda-Castañeda et al. (2024), los cuales se centraron en la temática del uso de blockchain en contextos de ciberseguridad. Este incremento de artículos después del año 2020 (año de la pandemia) puede ser un reflejo de los esfuerzos de los investigadores por buscar soluciones frente al aumento de los ataques cibernéticos en ese período (Araújo, 2020).

Gráfico 01 – Cantidad de artículos por año.



Fuente: Datos de la investigación (2025).

El segundo indicador analizado fue el de los autores. Se identificaron 78 investigadores diferentes, entre autores y coautores de los estudios. Sin embargo, solo uno de ellos contó con más de un trabajo incluido en la muestra, a saber, Héctor Fernando Vargas Montoya. En cuanto al tercer indicador, relativo a los países de procedencia de los investigadores, se identificaron cinco países sudamericanos que participaron en la muestra, siendo Colombia el país con el mayor número de autores, tal como se observa en la Figura 03, resultado que también fue destacado en el estudio de Rueda-Castañeda et al. (2024).

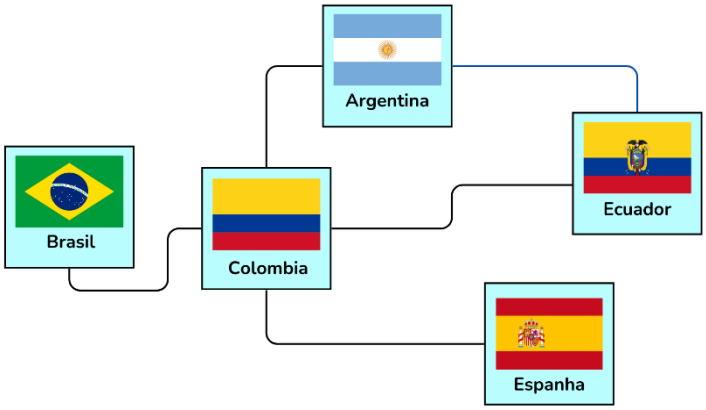
Figura 03 – Porcentaje de autores por país.

Fuente: Datos de la investigación (2025).

Es importante destacar que Colombia fue considerada el segundo país de América Latina con mayor número de ataques cibernéticos sufridos (Guzmán, 2023). En respuesta, el gobierno lanzó su plan estratégico de ciberseguridad para el período 2025–2027 (Presidencia, 2025). De este modo, puede comprenderse que los investigadores de la región también estaban comprometidos en la búsqueda de alternativas que pudieran contribuir a la discusión del tema y, así, aportar valor mediante posibles soluciones a este problema.

Además, los investigadores del país trabajaron con autores de otras regiones, incluso fuera de América del Sur (Figura 04), lo que evidencia un esfuerzo colaborativo orientado a la mitigación de los problemas relacionados con la ciberseguridad. En el ámbito de las alianzas internacionales, investigadores colombianos figuran como primeros autores en dos trabajos, mientras que brasileños y argentinos ocupan esa posición en un trabajo cada uno, ambos en coautoría con investigadores de Colombia.

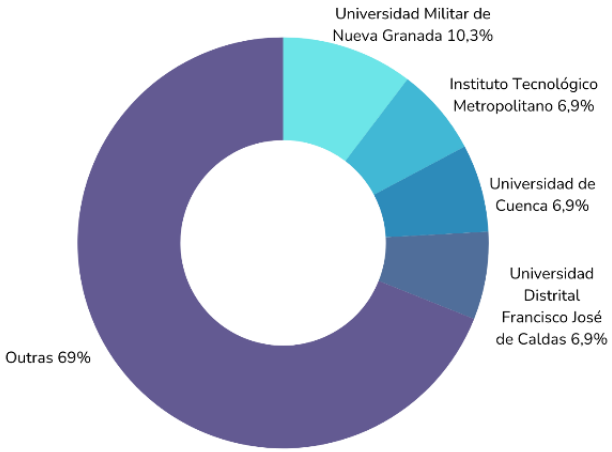
Figura 04 – Red colaborativa entre países.



Fuente: Datos de la investigación (2025)

Los autores sudamericanos estaban vinculados a 24 instituciones diferentes (cuarto indicador de análisis). La institución con mayor número de vínculos fue la Universidad Militar Nueva Granada, en Colombia, tal como se presenta en el Gráfico 02. Cabe destacar que, en dicho gráfico, la opción "otras" se refiere al conjunto de universidades que aparecieron únicamente una vez en la muestra.

Gráfico 02 – Porcentaje de participación de las instituciones en la muestra.

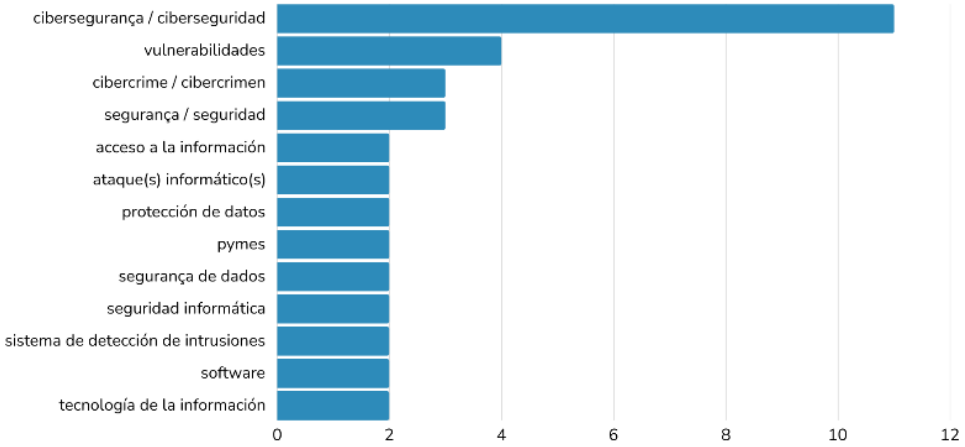


Fuente: Datos de la investigación (2025).

El quinto indicador bibliométrico analizado fue la cantidad de artículos por revista. En la muestra se identificaron 21 revistas diferentes; sin embargo, aquellas que presentaron más de un artículo fueron la Revista Logos Ciencia & Tecnología, con cuatro trabajos, y la Revista Científica General José María Córdova, con dos trabajos. De este modo, los autores interesados en publicar investigaciones sobre ciberseguridad en América del Sur pueden encontrar en estas dos revistas importantes vehículos de divulgación científica.

Por último, el indicador final analizó las principales palabras clave utilizadas por los autores para caracterizar sus artículos. Se identificaron 97 términos diferentes; no obstante, ocho de ellos fueron utilizados más de una vez, tal como se esquematiza en el Gráfico 03. El término más frecuente fue "ciberseguridad", lo cual era esperable, dado que este constituye el objeto de estudio del presente artículo. Cabe destacar que el término "protección de datos", que se encuentra entre los más citados en este trabajo, también fue destacado en el estudio de Matilde-Espino y Valencia-Pérez (2023).

Gráfico 03 – Palabras clave más utilizadas en los artículos.



Fuente: Datos de la investigación (2025).

Cabe destacar el término “pymes”, que también presentó más de una mención en la muestra y que corresponde al equivalente en español de las pequeñas y medianas empresas. En este sentido, se entiende que existe una preocupación en los estudios por garantizar la ciberseguridad de estas organizaciones. Para profundizar en el contenido de los trabajos, se pasa a la siguiente subsección.

4.2 Síntese dos trabalhos da amostra

En lo que respecta a **la gestión de riesgos**, la gobernanza y el cumplimiento, entendidos como un enfoque sistemático para hacer que la Tecnología de la Información (TI) avance de la mano con los objetivos del negocio, Caamaño Fernandez y Gil Herrera (2020) desarrollaron un trabajo centrado en el ámbito organizacional, tanto privado como público. Los autores presentaron un modelo de prevención, control y toma de decisiones a partir del análisis de métricas de vulnerabilidad (CVSS) para la priorización de riesgos. Se desarrolló un procedimiento de seis etapas que abarca la identificación, caracterización, análisis, evaluación, prevención y monitoreo de los riesgos, culminando en medidas más eficaces de control interno. El método se asemeja al ciclo recomendado por Microsoft (discutido en la sección 2.1). El procedimiento también integró valores de la ciberseguridad organizacional, la auditoría forense y la gestión del conocimiento, constituyéndose en un mecanismo preventivo y de control contra el fraude, la corrupción y los delitos cibernéticos, culminando en la prevención, el control y la toma de decisiones para empresas e instituciones dentro del contexto de la economía globalizada.

Por su parte, Bustamante García et al. (2021), con el objetivo de mejorar la gestión de la seguridad de la información en una municipalidad distrital peruana, implementaron un modelo de políticas basado en la norma ISO 27001:2013, centrado en los pilares de confidencialidad, integridad y disponibilidad. El índice de satisfacción con la gestión de la seguridad de la información aumentó del 49 % (pretest) al 96 % (postest), y más del 90 % de los participantes reconocieron mejoras significativas en la seguridad de la información En el contexto de las pequeñas y medianas empresas colombianas, Sánchez-Sánchez et al. (2021) diseñaron una herramienta para medir el nivel de seguridad de la información basada en la base de datos CVE (Common Vulnerabilities and Exposures).

La herramienta fue aplicada en una PYME del sector de tecnología e innovación, evaluando software comercial en diferentes versiones. Dicha herramienta permitió detectar vulnerabilidades de forma sistemática y preventiva, sirviendo como apoyo para la toma de decisiones estratégicas en seguridad y demostrando potencial para fortalecer la estrategia de seguridad digital de las pequeñas y medianas empresas.

Aún en el contexto de las pequeñas y medianas empresas, pero ahora ecuatorianas, Peralta Zuñiga y Aquilar Valarezo (2021) se centraron en comprender las inversiones realizadas por las empresas en su seguridad digital. Se analizaron variables como la relación costo-beneficio, el número de empleados, la filosofía empresarial, la capacitación y el mantenimiento, así como la capacidad de reacción frente a incidentes digitales. Se llegó a la conclusión de que los gestores menos tradicionales tienden a invertir más recursos en ciberseguridad, capacitar a sus empleados y mejorar la capacidad de reacción de la organización. Asimismo, se observó que el sector de servicios, especialmente las instituciones financieras, lidera las inversiones en seguridad digital. Sin embargo, la cultura empresarial en Ecuador sigue siendo predominantemente reactiva, limitándose al cumplimiento legal básico en lugar de adoptar medidas preventivas más robustas.

Con un enfoque en el sector financiero y en la creación de un modelo de madurez de la cultura de ciberseguridad, González Sánchez et al. (2023) definieron cuatro factores centrales que influyen en la madurez de la cultura de ciberseguridad: influencias externas, mecanismos organizacionales internos, comportamientos y creencias, así como valores y actitudes. El modelo de madurez propuesto (MMCCSF) contempla cuatro niveles de evolución: (0) Inexistente, (1) Limitada, (2) Proactiva y (3) Integrada. Dicho modelo mostró una alta aceptación entre especialistas, destacándose por su relevancia práctica y su aplicabilidad al sector financiero. Finalmente, en el contexto pospandémico de la COVID-19, y enfocándose en las pequeñas y medianas empresas ecuatorianas, Bueno Valero y Haz López (2022) observaron que la pandemia aceleró la transformación digital en estas organizaciones, incrementando la necesidad de ciberseguridad. Los autores identificaron debilidades en los recursos tecnológicos y riesgos asociados a la falta de conocimiento y a fallas en la gestión de la seguridad. Las empresas pasaron a percibir la ciberseguridad como un proceso de mejora continua, esencial para mitigar riesgos cibernéticos, adoptando herramientas y políticas de seguridad de la información alineadas con las normas ISO 27001 y COBIT 5.0.

Otro tema que apareció de forma recurrente fue la **prevención, detección y predicción técnica de ataques.** En este sentido, Quiroz Tascón, Zapata Jiménez y Vargas Montoya (2020) desarrollaron un modelo de predicción de ciberataques en sistemas industriales (SCADA), destinado a ser aplicado en empresas que operan procesos industriales e infraestructuras críticas (como el sector eléctrico, la manufactura y la automatización). El modelo utiliza un sistema de detección de intrusos (IDS-SNORT) en conjunto con el filtro de Kalman, con el fin de anticipar incidentes de seguridad, reducir falsos positivos y apoyar la gestión proactiva de riesgos en infraestructuras críticas. Dicho modelo demostró ser eficaz para la predicción de ataques en sistemas industriales (SCADA), permitiendo alcanzar hasta un 98 % de exactitud, con un error tendiente a cero, especialmente en ataques de escritura y lectura.

Por su parte, Janampa Patilla, Huamani Santiago y Meneses Cosnilla (2021) implementaron **Snort Open Source** como sistema de detección de intrusos (IDS) para reforzar la seguridad de la infraestructura de red en pequeñas y medianas empresas,

creando un entorno de pruebas en máquinas virtuales utilizando GNU/Linux Ubuntu y VirtualBox. Con las configuraciones adecuadas, fue posible identificar intentos de ataque como la denegación de servicio (DoS), el escaneo de puertos y los accesos a páginas no autorizadas. El recurso demostró ser capaz de capturar paquetes, analizar eventos y alertar sobre vulnerabilidades en tiempo real, cumpliendo su función como herramienta de seguridad de red.

Quirumbay Yagual, Castillo Yagual y Coronel Suárez (2022) evaluaron el uso de redes neuronales y aprendizaje profundo en áreas como la detección de intrusos, la identificación de malware, botnets, phishing, la predicción de ciberataques, los ataques de denegación de servicio y las anomalías cibernéticas. Se concluyó que el aprendizaje profundo puede contribuir a la ciberseguridad, siempre que exista una combinación adecuada entre la calidad de los datos, el rendimiento de los algoritmos seleccionados y la exploración continua de nuevas técnicas de ciencia de datos para enfrentar los desafíos emergentes de la seguridad digital.

En la búsqueda de identificar y mitigar vulnerabilidades en redes empresariales, con un enfoque en el sector financiero, Serna Ramírez et al. (2022) identificaron fallas críticas, incluyendo riesgos asociados al uso de certificados SSL con cifrados débiles. Se elaboró un plan de mitigación de riesgos que incluyó la actualización y/o sustitución de certificados y mejoras en los mecanismos de cifrado. De este modo, fue posible aplicar medidas correctivas adecuadas a múltiples riesgos, que incluso no eran conocidos por el departamento de TI ni por los empleados, debido a la falta de capacitación en seguridad digital.

Por su parte, Chanchí-Golondrino, Ospina-Alarcón y Muñoz-Sanabria (2023) buscaron caracterizar los delitos informáticos en el departamento de Cundinamarca (Colombia) a partir de técnicas de análisis exploratorio de datos y *machine learning*, con el fin de apoyar la toma de decisiones de las autoridades competentes y crear una referencia para estudios en otras regiones del país. Los investigadores utilizaron cuatro fases: adecuación de los datos, análisis exploratorio, modelado en *machine learning* y generación de información de valor agregado. Las reglas de asociación permitieron identificar relaciones entre atributos categóricos (municipio, grupo etario, tipo de víctima) y los tipos de delitos. El análisis confirmó la utilidad de la analítica de datos en el campo de la ciberseguridad, demostrando que las técnicas de *machine learning* pueden generar conocimiento estratégico para la prevención y la investigación.

También fue posible identificar trabajos enfocados en **sectores e infraestructuras críticas**, como energía, 5G, salud digital/telemedicina y servicios médicos. Esponel Ortega y Carreno Pérez (2020), con foco en el sector eléctrico, presentaron una propuesta para la identificación de activos y ciberactivos. Dicha propuesta se extiende a los agentes del sector energético responsables de la generación, transmisión, distribución y comercialización de energía, contribuyendo al fortalecimiento de la ciberseguridad en las infraestructuras críticas nacionales. Al alcanzar un consenso, los autores lograron identificar y clasificar activos y ciberactivos críticos de la infraestructura eléctrica, posibilitando que los agentes del sector reconozcan los puntos más vulnerables a ataques y preparen medidas preventivas.

Por su parte, Aranda et al. (2021) analizaron los fundamentos de la tecnología 5G, destacando su arquitectura, modelos de negocio, casos de uso e implicaciones en ciberseguridad, aplicada en el sector de las telecomunicaciones y en industrias en proceso de transformación digital. El análisis abarcó áreas como infraestructuras críticas, Internet

de las Cosas (IoT), ciudades inteligentes e industria 4.0. La investigación brindó apoyo a investigadores, gobiernos y empresas en la definición de estrategias para una implementación segura y eficiente de la tecnología 5G.

Con un enfoque en la preservación de rastros y evidencias digitales en casos de ciberincidentes en el sector de la telemedicina, Tejo-Machado et al. (2021) desarrollaron un protocolo que utiliza la informática forense como herramienta de apoyo a la toma de decisiones, inspirado en el Protocolo de Manchester, ampliamente utilizado en el ámbito médico. El protocolo define nueve niveles de acceso de usuarios (desde pacientes hasta administradores de red), priorizando la preservación de la información según el tipo de memoria (volátil o no volátil) y el nivel de urgencia. Su implementación contribuye a hospitales, clínicas, profesionales de la salud y administradores de TI, proporcionando directrices claras para la respuesta inicial a incidentes cibernéticos, con potencial de adaptación a otros sectores que manejan información crítica.

Para describir la situación de la ciberseguridad en los Servicios de Apoyo al Médico Ocupacional en Lima, Perú, Gomero-Cuadra y Sánchez-Calle (2024) observaron que más del 80 % de los establecimientos de la muestra contaban con planes de respuesta a incidentes cibernéticos y que la mayoría realizaba copias de seguridad periódicas de datos críticos, almacenadas en ubicaciones externas. Los sistemas operativos y el software eran actualizados regularmente, y el 64 % afirmó ofrecer capacitación en ciberseguridad a su personal. No obstante, los autores señalaron que estos datos positivos estaban asociados a una postura reactiva, dado que muchos de los establecimientos ya habían sufrido ataques, además de reflejar una realidad regional.

También fue posible observar la existencia de artículos con enfoque en **políticas públicas, marcos legales y cooperación**, ya sea en estrategias nacionales, relaciones civil-militares, procedimientos disciplinarios o mecanismos de cooperación. Como ejemplo, Ospina Díaz y Sanabria Rangel (2020) utilizaron el contexto pandémico de la COVID-19 en Colombia para revisar la evolución histórica de la ciberseguridad y evaluar las acciones del gobierno colombiano en el fortalecimiento de políticas y estándares de seguridad de la información. En ese año se identificó que Colombia presentaba vulnerabilidades significativas frente a las amenazas cibernéticas, agravadas por el aumento del uso de las Tecnologías de la Información y la Comunicación durante la pandemia. Asimismo, se constató un bajo número de certificaciones internacionales en seguridad de la información (como la ISO 27001) en el país.

También en el contexto colombiano, pero ahora en las relaciones cívico-militares, Cubajante Villamil et al. (2020) se centraron en definir el ciberespacio y las ciberamenazas, describir las relaciones cívico-militares en Colombia y explicar el marco institucional de las políticas de ciberseguridad y ciberdefensa del país, en especial los documentos CONPES 3701 y 3854. A partir de sus observaciones, se identificó que la política de ciberseguridad y ciberdefensa representó un cambio de tradición, ya que la iniciativa partió del sector civil y no exclusivamente de las Fuerzas Armadas. No obstante, en la fase de implementación, las Fuerzas Armadas aún concentran mayor autonomía y protagonismo, mientras que la participación civil (academia, sector privado y sociedad) es limitada. De este modo, se evidenció que el desafío de promover un mayor control democrático civil sobre las capacidades de ciberseguridad y ciberdefensa continúa vigente.

Solano Oviedo, Roldan Álvarez e Vargas Montoya (2023) propusieron una metodología de investigación forense en el entorno digital para servir como herramienta

técnica de apoyo en procesos administrativos y disciplinarios del Estado colombiano, en conformidad con la Ley 1952 de 2019 (Código General Disciplinario). La metodología de investigación forense digital fue estructurada en cinco etapas: recepción del caso, identificación de las fuentes y tipos de evidencia digital, adquisición de los elementos, examen y análisis forense y, finalmente, la elaboración del informe de hallazgos y resultados. La aplicación práctica se mostró satisfactoria para garantizar resultados confiables, asegurando la cadena de custodia y fortaleciendo el valor probatorio en los procesos disciplinarios. Sin embargo, se identificaron dificultades relacionadas con el desconocimiento de técnicas forenses específicas, lo que evidencia la necesidad de una mayor capacitación y entrenamiento.

Por último, Castillo Pulido y Jiménez Acosta (2024) identificaron un modelo de cooperación policial internacional aplicable a las diferentes manifestaciones de las amenazas cibernéticas en Colombia, en particular al Business Email Compromise (BEC). A través del estudio se observó que, a nivel nacional, el BEC está principalmente asociado a la infiltración de correos electrónicos corporativos, la suplantación de identidad y el robo de datos. En el ámbito internacional, predominan prácticas como la emisión de facturas falsas, el fraude inmobiliario y el denominado *fraude del CEO*, que consiste en manipular a empleados para realizar transferencias indebidas. Los actores más vulnerables son, en orden, los organismos multilaterales, las empresas privadas y las empresas públicas. La investigación propuso un plan de acción en tres fases: corto plazo (2024), enfocado en la sensibilización, la capacitación y el fortalecimiento de redes de cooperación; mediano plazo (2027), orientado a la adopción de tecnologías avanzadas (IA, Big Data y aprendizaje automático) y a la actualización del marco legal; y largo plazo (2030), centrado en la innovación continua en métricas como I+D y en la integración global en una red internacional de cooperación contra el cibercrimen. Los autores esperaban que el modelo contribuyera a la reducción de la incidencia de ataques BEC, así como al aumento de la capacitación en ciberseguridad y a una mayor efectividad de la cooperación policial internacional.

Un otro tema abordado por algunos trabajos fue la eficacia de los **métodos educativos y la cultura organizacional.** Esto puede observarse en el artículo de Maldonado Gudiño et al. (2024), quienes evaluaron la efectividad de diferentes métodos educativos en ciberseguridad para reducir fraudes digitales entre usuarios financieros en Ecuador. A partir de una investigación con 40 participantes, se identificaron vulnerabilidades relevantes, tales como fallas en la gestión de contraseñas, desconocimiento sobre el phishing y dificultades para reconocer sitios web falsos. Con base en estos hallazgos, se elaboró un programa educativo que combinó talleres presenciales y virtuales, cursos en línea autoguiados y campañas de sensibilización. Los resultados demostraron que los talleres presenciales y virtuales fueron los más eficaces, seguidos por los cursos en línea, mientras que las campañas de sensibilización tuvieron un impacto más limitado. De este modo, se evidenció que los métodos interactivos y personalizados son los más adecuados para fortalecer las prácticas de seguridad digital y reducir el riesgo de fraudes. Asimismo, se destacó la importancia de crear una cultura educativa, con adaptaciones del programa desarrollado por los autores para distintos perfiles demográficos y culturales.

Estrada-Esponda, Unás-Gómez y Flórez-Rincón (2021) también trabajaron el contexto pandémico de la COVID-19, al igual que Ospina Día y Sanabria Rangel (2020). Sin embargo, en esta ocasión, el enfoque estuvo en una comunidad universitaria, utilizando cuestionarios aplicados a profesores y estudiantes, evaluando variables como

el nivel de conocimiento en seguridad de la información, la incidencia de incidentes cibernéticos en el ámbito académico y la existencia de estrategias de sensibilización por parte de instituciones públicas y privadas. Como resultados, los profesores y estudiantes presentaron un nivel aceptable de conocimiento en seguridad de la información, a pesar de la ausencia de capacitación significativa por parte del gobierno o de la policía.

También apareció con frecuencia el tema de la **ingeniería de software seguro, los datos y las tecnologías emergentes**, lo que evidencia la necesidad de incorporar la seguridad desde el diseño y de abordar la criptografía, la privacidad y las nuevas superficies de ataque. Por ejemplo, López Álvarez (2020) propuso un modelo de software seguro basado en el ciclo de vida del desarrollo de software, con enfoque en la seguridad informática. Este fue aplicado en el ámbito académico, en proyectos desarrollados por estudiantes de ingeniería de software en una universidad ecuatoriana, pero su aplicación se extiende a empresas de desarrollo de software y de servicios digitales. A través de ello fue posible integrar la seguridad en el ciclo de vida del desarrollo de software, destacando que la prevención de vulnerabilidades debe comenzar ya en la fase de análisis y diseño, y no únicamente después de que el software esté terminado. El uso de las métricas OWASP y la adopción de metodologías ágiles y computación en la nube demostraron ser eficaces para adaptar rápidamente el software a las nuevas amenazas, permitiendo crear prototipos incrementales y corregir fallas de seguridad en cada iteración.

Cárdenas Sánchez y Olarte Rojas (2022) buscaron evaluar la seguridad de bases de datos y documentos encriptados utilizando los servicios de Amazon Web Services (AWS), con énfasis en el Key Management Service (KMS), Amazon Relational Database Service (RDS) y Amazon S3, verificando su eficacia frente a intentos de acceso no autorizado. Como resultado, el KMS de AWS demostró ser altamente seguro, volviendo la información ilegible en caso de ataque o robo de datos. Además, las claves maestras de encriptación, utilizadas para encriptar y desencriptar otras claves, no son accesibles para usuarios no autorizados, garantizando la seguridad interna y externa.

Becerra et al. (2023) presentaron el desarrollo de la aplicación móvil “Navega Seguro”, construida en el marco de la investigación internacional “Derecho, cambio climático y big data – Fase II”. El análisis se centró en la reutilización de datos abiertos, en las implicaciones legales del uso de aplicaciones y en los mecanismos de protección de datos y ciberseguridad aplicados a la herramienta. Como resultado, se observó que la aplicación “Navega Seguro” reutiliza datos públicos sin restricciones legales, fortaleciendo la transparencia y generando valor agregado mediante nuevos datos. También se identificó la necesidad de encriptación y de medidas de ciberseguridad para garantizar la confidencialidad, integridad y disponibilidad de la información, así como la adopción de términos y condiciones de uso con estándares internacionales.

Por su parte, la relación entre vigilancia y tecnología blockchain fue estudiada por Almada y Costa (2023). Los autores llegaron a la conclusión de que, aunque el mercado de criptoactivos, liderado por Bitcoin, demuestra el potencial de financiarización y transformación tecnológica, este presenta contradicciones vinculadas al control, ya que, si bien estas tecnologías se presentan como soluciones de seguridad y confianza, también profundizan dinámicas de monitoreo, disciplina y gestión de los flujos de información y financieros a escala global.

En suma, los trabajos recorrieron diversos sectores, empresas privadas y organismos públicos, abordando la ciberseguridad como una cuestión necesaria y urgente. Los estudios demostraron y validaron el concepto de crear una cultura empresarial

orientada a la gestión de vulnerabilidades, así como la utilización de buenas prácticas ya consolidadas por leyes y marcos de referencia, apoyadas por software existente o por la creación de nuevas soluciones. Esto evidencia que, como se mencionó anteriormente, no existe un paso a paso que abarque todos los sectores y satisfaga plenamente su seguridad en el entorno digital, pero sí existen buenas prácticas que deben seguirse independientemente del sector, ya sea público o privado. La adopción de una postura que va más allá de la mitigación demuestra que la prevención es el camino ideal.

5. Conclusión

El objetivo de este trabajo fue **analizar el perfil de las investigaciones sudamericanas sobre ciberseguridad**. Por ello, se buscó responder a la siguiente pregunta: **¿cuál es el perfil de las investigaciones sobre ciberseguridad desarrolladas en América del Sur?** Como respuesta sintética a esta pregunta, se presenta lo siguiente:

> Las investigaciones sudamericanas sobre ciberseguridad fueron publicadas, en su mayoría, en el año 2021, en Colombia, por investigadores vinculados a la Universidad Militar Nueva Granada, en la Revista Logos Ciencia & Tecnología. Los estudios abordan diversos sectores, lo que evidencia y valida el concepto de una cultura empresarial orientada a la gestión de vulnerabilidades, así como al uso de buenas prácticas relacionadas con la prevención.

De este modo, se entiende que el objetivo de este trabajo fue alcanzado. Se espera que este estudio pueda contribuir a motivar a los profesionales sudamericanos del área de la ciberseguridad a documentar y compartir sus conocimientos mediante trabajos científicos que puedan mejorar las prácticas de seguridad cibernética en la región. Asimismo, se pone de manifiesto el potencial de este espacio geográfico en la discusión del tema, dado que los estudios de revisión de la literatura presentan mayoritariamente resultados provenientes de países del hemisferio norte (América del Norte y Europa).

Como limitación de este trabajo, se señala que solo se analizaron artículos publicados en revistas científicas, mientras que otros trabajos académicos (tesis de posgrado, disertaciones, monografías de grado y artículos en congresos) también pueden contribuir a la discusión de la temática en la región. De este modo, se espera que en estudios futuros esta revisión sea ampliada, abarcando otros tipos de investigaciones académicas y científicas. Asimismo, se incentiva la ampliación de la muestra mediante la incorporación de estudios publicados en países de América Latina, incluyendo también los países de América Central.

Referencias

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Engenharia Social**: Guia para proteção de conhecimentos sensíveis. Link.

ALMADA, P.E.R.; COSTA, E.S. Open-access Controle e vigilância no capitalismo digital: uma análise da tecnologia blockchain e sua implementação empresarial. Cadernos EBAPE.BR, v.21, n.1, 1-13, 2023. https://doi.org/10.1590/1679-395120220020

ALZATE, A.; GIRALDO, D. Tendencias de investigación del blockchain en la cadena de suministro: transparencia, trazabilidad y seguridad. **Revista Universidad y Empresa**,

v.25, n.44, 1-29, 2023. https://doi.org/10.12804/revistas.urosario.edu.co/empresa/a.12451

AMADOR DONADO, S.; PARDO CALVACHE, C.J.; MAZO PEÑA, R.I. Revisión Preliminar: Ciberseguridad Para Tecnología de la Operación en la Era Cuántica Contra Ataques De Red a Infraestructuras Críticas. **Inge Cuc**, v.20, n.2, 126-143, 2024. https://doi.org/10.17981/ingecuc.20.2.2024.06

ARANDA, J. et al. 5G networks: A review from the perspectives of architecture, business models, cybersecurity, and research developments. Revista Digital Novasinergia, v.4, n.1, 1-36, 2021. https://doi.org/10.37135/ns.01.07.01

ARAÚJO, R.C. **Ataques cibernéticos aumentaram 350% em 2020**: saiba como se proteger. 2020. Link.

BECERRA, J. et al. Implicaciones jurídicas en el entorno del big data: el caso del APP Navega Seguro. **Novum Jus**, v.17, n.1, 357-388, 2023. https://novumjus.ucatolica.edu.co/article/view/5100/4612

BEZBORODKO, A. **Cybersecurity threatscape for Latin America and the Caribbean:** 2023–2024. Publicado em 10 de abril de 2025. Link

BOCCONI, M. **Incidentes cibernéticos na América Latina cresceram 25% ao ano na última década.** Publicado em 21 de janeiro de 2025. Link.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018** - Lei Geral de Proteção de Dados Pessoais (LGPD). Link.

BUENO VALERO, G.G.; HAZ LÓPEZ, L.V. Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador. **ProSciences**, v.6, n.44, 103-120, 2022. https://journalprosciences.com/index.php/ps/article/view/634/670

BUSTAMANTE GARCÍA, S. et al. Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. **Enfoque**, v.12, n.2, 69-79, 2021. https://doi.org/10.29019/enfoqueute.743

CAAMAÑO FERNANDEZ, E.E.; GIL HERRERA, R.J. Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. **Novum**, v.1, n.10, 61-80, 2020. https://revistas.unal.edu.co/index.php/novum/article/view/84210

CANIATO, B. **Vazamentos de dados no governo crescem mais de 20 vezes em 4 anos**. Publicado em 28 de janeiro de 2025. Link.

CÁRDENAS SÁNCHEZ, B.; OLARTE ROJAS, C. Análisis de seguridad entre microservicios con Amazon Web Service. **Revista Logos Ciencia & Tecnologia**, v.14, n.2, 42-52, 2022. http://www.scielo.org.co/pdf/logos/v14n2/2422-4200-logos-14-02-42.pdf

CASTILLO PULIDO, L.E.; JIMÉNEZ ACOSTA, J.F. Cooperación internacional policial ante amenazas cibernéticas en Colombia: Modalidad Business Email

Compromise. **Revista Logos Ciencia & Tecnologia**, v.16, n.1, 83-107, 2024. https://doi.org/10.22335/rlct.v16i1.1877

CHANCHÍ-GOLONDRINO, G.E.; OSPINA-ALARCÓN, M.A.; MUÑOZ-SANABRIA, L.F. Caracterización de delitos cibernéticos del departamento de Cundinamarca durante el primer semestre de 2021 mediante análisis exploratorio y aprendizaje de máquina. Ingeniería y competitividad, v.25, n.1, 1-13, 2022. https://doi.org/10.25100/iyc.v25i1.11760

CHINGO ESQUIVEL, R.A.; GÓMÉZ GÓMÉZ, O.S.G. Tecnología de contenedores y su aplicación en el aprendizaje de ciberseguridad: una revisión sistemática de literatura. **Revista electrónica De Computación, Informática, Biomédica y Electrónica**, v.9, n.2, 1-20, 2020. https://doi.org/10.32870/recibe.v9i2.186

CUJABANTE VILLAMIL, X.A. et al. Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. **Revista Colombiana de Estudios Militares y Estratégicos**, v.18, n.30, 357-377, 2020. https://doi.org/10.21830/19006586.588

DAVID, A.; SANKAR, J.G.; AZAM, M.S. Internet Users Top Concerns Ensuring Data Privacy, Security, and Protection. In: **International Conference on Multidisciplinary Research and Modern**, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4511314

ESPINEL ORTEGA, A.; CARRENO PEREZ, J.C. Identificación de activos y ciber activos críticos en sistemas de transmisión de energía eléctrica. **Tecnura**, v.24, n.65, 27-38, 2020. https://revistas.udistrital.edu.co/index.php/Tecnura/article/view/15388/16185

ESTRADA-ESPONDA, R.D.E.; UNÁS-GÓMEZ, J.L.; FLÓREZ-RINCÓN, O.E. Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. Revista **Logos Ciencia & Tecnologia**, v.13, n.3, 98-110, 2021. https://doi.org/10.22335/rlct.v13i3.1446

FEBRABAN. **Engenharia Social**: Saiba como evitar possíveis armadilhas e se proteger de golpes. Link.

FORTINET. **O que é Spyware?** Entenda o que é spyware, o que ele faz, como ataca seu PC e o que fazer. Link.

GALVÃO, N.M.; SCHNEIDER, H.N. (2024). Bibliometria. In: SCHNEIDER, H.N.; GALVÃO, N.M.; MADUREIRA, J.S. **Tutoriais**: Estado do Conhecimento e Análise Qualitativa de Dados. Iguatu, CE: Quipá Editora, 2024. Link.

GIL, P. **América latina enfrenta taxa recorde de ataques cibernéticos.** Publicado em 3 de julho de 2025. Link.

GOMERO-CUADRA, R.; SÁNCHEZ-CALLE, D. Ciberseguridad en servicios de apoyo al médico ocupacional de la ciudad de Lima. Estudio piloto. Revista Medica Herediana, v.32, n.1, 38-43, 2024. http://dx.doi.org/10.20453/rmh.v35i1.5298

GÓNZALEZ SÁNCHEZ, D.A. *et al*. Modelo de madurez de cultura organizacional de ciberseguridad para el sector financiero basado en buenas prácticas. **RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação**, v.62, 365-375, 2023. https://dialnet.unirioja.es/servlet/articulo?codigo=10050207

GUZMÁN, A. **La importancia de la Ciberseguridad en las empresas colombianas**. 2023. Link.

IBM. **O que é malware?** Publicado em 14 de abril de 2022. https://www.ibm.com/br-pt/think/topics/malware

IBSEC. **Brasil enfrenta um déficit de 750 mil profissionais de cibersegurança, aponta pesquisa.** Publicado em 18 de agosto de 2024. https://ibsec.com.br/brasil-enfrenta-um-deficit-de-750-mil-profissionais-de-ciberseguranca/?utm_source=chatgpt.com

INSTITUTO BRASILEIRO DE CIBERSEGURANÇA. **10 Ferramentas para Gestão de Vulnerabilidades**. Publicado em 08 de setembro de 2024. Link.

JANAMPA PATILLA, H.; HUAMANI SANTIAGO, H.L.; MENESES COSNILLA, Y. Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red. **Revista Cubana de Ciencias Informáticas**, v.15, n.3, 55-73, 2021. https://rcci.uci.cu/index.php/RCCI/article/view/2042

KASPERSKY. **Ransomware**: definição, prevenção e remoção. Link.

LEÓN GUTIERREZ, E.D. et al. Review of advances and changes in cybersecurity in Peru, for a digital transformation. **Innovación y Software,** v.3, n.2, 109-120, 2022. https://revistas.ulasalle.edu.pe/innosoft/article/view/62

LÓPEZ ÁLVAREZ, D.M. Método para el desarrollo de software seguro basado en la ingeniería de software y ciberseguridad. **INNOVA Research Journal**, v.5, n.31, 263-280, 2020. https://doi.org/10.33890/innova.v5.n3.1.2020.1440

MALDONADO GUDIÑO, C.W. et al. Evaluación de la efectividad de programas educativos en ciberseguridad para reducir el fraude digital entre usuarios financieros en Ecuador. **Conrado**, v.20, n.100, 186-192, 2024. http://scielo.sld.cu/pdf/rc/v20n100/1990-8644-rc-20-100-186.pdf

MARQUES, A. **Guia de Defesa Cibernética na América do Sul.** 2021. Link.

MATILDE-ESPINO, Y.; VALENCIA-PÉREZ, L.R. Análisis bibliométrico de la producción científica sobre México en temas de ciberseguridad (2015-2020). **Revista Científica Multidisciplinaria de Prospectiva**, v.29, n.3, 1-15, 2022. https://doi.org/10.30878/ces.v29n3a11

MICROSOFT. **O que é o Gerenciamento de Vulnerabilidades?** Link.

MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO. **Ataques cibernéticos crescem cerca de 70% no Brasil em um ano**. Publicado em 19 de julho de 2024. Link.

NEUBER, D. Cybersegurança: Principais desafios enfrentados por pequenas e médias empresas. **Revista Latino-Americana de Estudos Científicos**, v.6, n.27, 1-6, 2025. https://doi.org/10.55470/relaec.47085

NOGUEIRA, M. **Afinal, o que é cibersegurança?** Publicado em 28 de julho de 2023. Link.

OROSCO-FABIAN, J.R. Ciberseguridad en educación superior: una revisión bibliométrica. **Revista Digital de Investigación en Docencia Universitaria**, v.18, n.2, 1-12, 2024. http://dx.doi.org/10.19083/ridu.2024.1933

OSPINA DÍAZ, M.R.; RANGEL SAMBRIA, P.E. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. **Revista Criminalidad**, v.62, n.2, 199-217, 2020. https://doi.org/10.47741/17943108.168

PACETE, C. **Seis anos depois, o que mudou com a LGPD no Brasil?** Publicado em 14 de agosto de 2024. Link.

PERALTA ZUÑIGA, M.L.; AQUILAR VALAREZO, D.N.A. La Ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador. Contabilidad y Auditoría, v.53, 101-125, 2021. https://dspace.ucuenca.edu.ec/items/a74d94ab-01c9-4296-a965-302c1563d26c

PRESIDENCIA. **Estrategia Nacional de Seguridad Digital enfrentará amenazas cibernéticas**. 2025. Link.

QUIROZ TÁSCON, S.; ZAPATA JIMÉNEZ, J.; VARGAS MONTOYA, H.F. Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman. **TecnoLógicas**, v.23, n.48, 249-267, 2020. https://doi.org/10.22430/22565337.1586

QUIRUMBAY YAGUAL, D.I.; CASTILLO YAGUAL, C.A.; CORONEL SUÁREZ, I.A. Una revisión del aprendizaje profundo aplicado a la ciberseguridad. **Revista Científica y Tecnológica** UPSE, v.9, n.1, 57-65, 2022. https://doi.org/10.26423/rctu.v9i1.671

RUEDA-CASTAÑEDA, J.E., et al. Identificación de variables relacionadas a la seguridad informática a partir de tendencias investigativas de la tecnología Blockchain. **Revista Politécnica**, v. 20, n.40, 09-29, 2024. https://doi.org/10.33571/rpolitec.v20n40a1

SÁNCHEZ-SÁNCHEZ, P.A. et al. Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. **Información Tecnológica**, v.32, n.5, 121-128, 2021. http://dx.doi.org/10.4067/S0718-07642021000500121

SCHILIRO, F. **Towards a Contemporary Definition of Cybersecurity**. Cornell University, 2023. Link.

SERNA RAMÍREZ, S. et al. Desarrollo de un sistema de seguridad informática a partir de una auditoría sobre una red empresarial. **INGENIERÍA: Ciencia Tecnología e Innovación**, v.9, n.22, 131-151, 2022. https://doi.org/10.26495/icti.v9i2.2267

SOLANO OVIEDO, D.S.; ROLDAN ÁLVAREZ, M.A.; VARGAS MONTOYA, H.F. Investigación forense digital en entidades del Estado colombiano: acercamiento a la Ley 1952 de 2019. **Revista Logos Ciencia & Tecnología**, v.15, n.1, 122-140, 2023. https://doi.org/10.22335/rlct.v15i1.1698

TEJO-MACHADO, N. et al. Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta. Revista Colombiana de **Estudios Militares y Estratégicos**, v.19, n.33, 181-203, 2021. https://doi.org/10.21830/19006586.726

ZOHO. **The State of Email Security Awareness**. 2023. https://www.zoho.com/workplace/email-security-awareness-report-2023.html