Ciberataques en América Latina: desafíos de la era digital

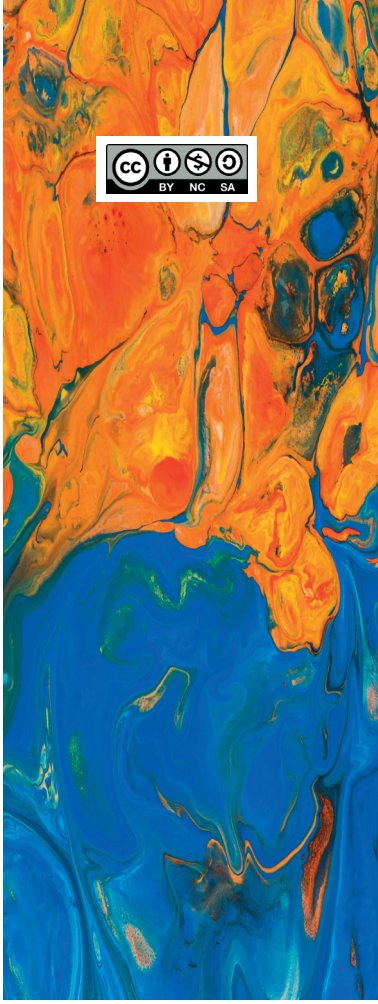
Cyberattacks in Latin America: challenges of the digital age

Aura Dolores Zambrano Rendón
Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Calceta, Manabí, Ecuador, Grupo de Investigación SISCOM, Carrera de Computación.
aura.zambrano@espam.edu.ec
https://orcid.org/0000-0002-2784-9202

Yohana Katherine Meza Talledo
Carrera de Computación, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Calceta, Manabí, Ecuador.
yohana.meza@espam.edu.ec
https://orcid.org/0009-0006-9145-6119

Cindy María Villavicencio Mendoza
Carrera de Computación, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Calceta, Manabí, Ecuador.
cindy.villavicencio@espam.edu.ec
https://orcid.org/0009-0009-9693-7204

Alex Rodolfo Rodríguez Zambrano
Carrera de Computación, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Calceta, Manabí, Ecuador.
alex.rodriguez@espam.edu.ec
https://orcid.org/0009-0009-3314-7643



© Copyright 2024. Universidad Nacional Autónoma de Nicaragua, Managua (UNAN-Managua)

Resumen

En los últimos años, América Latina ha experimentado un aumento significativo en la frecuencia y sofisticación de los ciberataques, afectando a diversos sectores como los gubernamentales, financieros, energéticos y de infraestructura crítica, así como a individuos y empresas. La región muestra vulnerabilidades debido a la falta de medidas de seguridad efectivas, escasa conciencia sobre ciberseguridad y adopción de tecnologías sin la debida protección. Esta investigación tuvo como objetivo analizar los principales aspectos de los ciberataques en América Latina. La metodología se basó en una revisión sistemática de fuentes bibliográficas. Los resultados revelan que el ransomware, phishing, DDOS, inyección de SQL, malware e ingeniería social son los ciberataques más frecuentes, con el ransomware representando el 50% de los ataques en el sector logístico. Aunque gobiernos

Palabras claves

Ciberataques, américa latina, ciberseguridad, conciencia ciudadana.

y organizaciones implementan medidas de seguridad, persiste una falta de preparación adecuada, amenazando la seguridad nacional y economía de los países latinoamericanos. Como conclusión, se requiere una acción conjunta y sostenida que incluya el fortalecimiento de las medidas de seguridad cibernética, la mejora de la educación y concientización, y el fomento de la colaboración regional para enfrentar esta amenaza en constante evolución, protegiendo eficazmente los activos digitales y la infraestructura crítica de la región.

Abstract

In recent years, Latin America has experienced a significant increase in the frequency and sophistication of cyberattacks, affecting various sectors such as government, finance, energy, and critical infrastructure, as well as individuals and businesses. The region shows vulnerabilities due to the lack of effective security measures, low cybersecurity awareness, and adoption of technologies without proper protection. This research aimed to analyze the main aspects of cyberattacks in Latin America. The methodology was based on a systematic review of bibliographic sources. The results reveal that ransomware, phishing, DDoS, SQL injection, malware, and social engineering are the most frequent cyberattacks, with ransomware accounting for 50% of attacks in the logistics sector. Although governments and organizations implement security measures, there remains a lack of adequate preparation, threatening the national security and economy of Latin American countries. In conclusion, joint and sustained action is required, including strengthening cybersecurity measures, improving education and awareness, and fostering regional collaboration to address this constantly evolving threat, effectively protecting the region's digital assets and critical infrastructure.

Keywords

Cyberattacks, *latin america*, *cybersecurity*, *citizen awareness.*

Fuente: Fotografías del IV Congreso Internacional de Vinculación con la sociedad (2024).

Introducción

Los ciberataques se han convertido en una preocupación global, con impactos significativos en economías, gobiernos y sociedades en todo el mundo. Según el Foro Económico Mundial, los ciberataques son considerados uno de los cinco principales riesgos globales en términos de probabilidad. En este contexto, América Latina enfrenta desafíos particulares debido a su rápida digitalización y las disparidades en la preparación para la ciberseguridad entre los países de la región (Aguilar, 2021).

En la última década, América Latina ha experimentado un acelerado crecimiento en el uso de tecnología de la información y comunicación (TIC), impulsando una mayor conectividad y transformando diversos aspectos de la sociedad y la economía. Sin embargo, esta creciente digitalización también ha abierto nuevas puertas para la comisión de ciberataques, convirtiéndose en una preocupación creciente para los gobiernos, empresas y ciudadanos en la región (Martínez et al., 2019).

Los ciberataques, definidos por Villar (2019) como "cualquier acción premeditada en el sistema informático que busque manipular, dañar, modificar, alterar, robar o eliminar cualquier información, software o hardware" (p. 10), pueden ser perpetrados por diversos actores, desde cibercriminales hasta agencias de espionaje e incluso estados nacionales (Aguilar, 2019). Países como Guatemala, Bolivia, Ecuador, Brasil y Perú han sido testigos de un aumento en la frecuencia y gravedad de los ciberataques en los últimos años (Aguilar, 2020).

Los ciberataques pueden tener repercusiones significativas en la economía, la privacidad, la confidencialidad y la estabilidad política de los países latinoamericanos.

La importancia de abordar esta problemática es crucial, dado que los ciberataques pueden tener repercusiones significativas en la economía, la privacidad, la confidencialidad y la estabilidad política de los países latinoamericanos (Saavedra, 2023). A pesar de los desafíos, existen oportunidades para fortalecer la ciberseguridad en la región, como la implementación de leyes de delitos informáticos o la suscripción del Convenio de Budapest (Albear, 2021).

La magnitud del problema se refleja en estadísticas alarmantes: el 78% de los líderes de seguridad en TI expresan inquietud por la insuficiente protección de sus organizaciones frente a ciberataques (Gutiérrez, 2022), mientras que el 90% de las organizaciones del sector de la salud han experimentado al menos una brecha de seguridad en los últimos tres años. Además, el 62,7% de las empresas perciben un aumento en los ciberataques desde el inicio de la pandemia de COVID-19 (Yanulis, 2023).

El presente trabajo tiene como objetivo analizar los principales aspectos de los ciberataques más frecuentes en América Latina, evaluando las respuestas de gobiernos y empresas ante su aumento en los últimos cinco años. Se examinarán las iniciativas adoptadas para combatir esta problemática, destacando la necesidad de un enfoque holístico y adaptable a la evolución tecnológica para abordar la inseguridad cibernética en la región.

Materiales y métodos

Revisión sistemática de la literatura

Este estudio empleó una revisión sistemática de la literatura como metodología principal. Se elige este método por su capacidad para sintetizar de manera rigurosa y objetiva la evidencia disponible sobre los ciberataques en América Latina, minimizando sesgos y proporcionando una base sólida para la toma de decisiones en ciberseguridad (Arias et al., 2021). El proceso se desarrolló en cuatro fases principales:

Fase 1: Definición de las preguntas de investigación

Se formularon las siguientes preguntas de investigación, alineadas con el objetivo de analizar los principales aspectos de los ciberataques más frecuentes en América Latina:

1. ¿Cuáles son los tipos de ciberataques más comunes en América Latina durante los últimos cinco años?

2. ¿Cómo han respondido los gobiernos y las empresas de América Latina ante el aumento de ciberataques?

3. ¿Qué países de América Latina han experimentado un aumento significativo de ciberataques?

4. ¿Qué iniciativas de colaboración regional o internacional en ciberseguridad se han establecido para abordar esta problemática?

5. ¿Cómo ha evolucionado la conciencia y preparación en ciberseguridad entre las organizaciones y la población general de América Latina?

Fase 2: Especificación de los criterios de inclusión y exclusión

Se establecieron los siguientes criterios para la selección de estudios:

- **Criterios de inclusión:** Se consideró el idioma, año, país, tipos de documentos y el tema que hace referencia al objeto de estudio.

- **Criterios de exclusión:** Se eliminaron aquellos documentos que no cumplan con las características necesarias para lograr el objetivo de este estudio.

A continuación, se muestra en la tabla 1 los respectivos criterios de manera más detallada.

Tabla. 1

Criterios de inclusión y exclusión

Campos	Criterios de inclusión	Criterios de exclusión
Año	Artículos que hayan sido objeto de estudio en los últimos 5 años	Artículos cuya fecha de publicación excede los últimos 5 años
Tema	Estudios cuya temática tenga relación directa con el tema de estudio	Estudios que se referían a otra temática y no guarden relación con el tema principal
Idioma	Inglés y español	Otros
Países	Latinoamérica	Fuera de la región Latinoamericana
Resúmenes	Que contengan características y conceptos sobre la temática de estudio	Artículos que no se encuentren con disponibilidad del texto completo
Tipos de documentos	Artículos	Información de tesis, blogs y repositorios

Fase 3: Estrategia de búsqueda y extracción de los datos

Se realizó una búsqueda sistemática en bases de datos de revistas científicas indexadas, utilizando combinaciones de palabras claves como:

- Ciberataques
- América Latina
- Tipos de ciberataques
- Amenazas cibernéticas
- Ciberseguridad
- Seguridad informática

Se aplicaron filtros para limitar los resultados a artículos publicados en los últimos cinco años en español o inglés.

Para la extracción de datos, se consideraron los siguientes campos: tema, año de publicación, país de estudio, tipo de documento, idioma, resúmenes y

principales hallazgos. La tabla 2 presenta las diversas bases de datos utilizadas para extraer los artículos analizados en este estudio. La búsqueda inicial arroja 150 documentos. Tras aplicar criterios de inclusión y exclusión, filtrar por título y lectura rápida de resúmenes; se seleccionaron 70 investigaciones potencialmente relevantes para responder a las preguntas de la fase 1.

Tabla. 2

Bases de datos utilizadas para la selección de artículos

Base de datos	Criterios de inclusión y exclusión	Filtro por título	Lectura rápida de resúmenes
Scielo	7	4	6
Google Académico	29	26	19
Redalyc	5	3	2
Dialnet	3	2	2
Mendeley	17	15	13
ResearchGate	9	7	4
Total	70	57	46

Fase 4: Análisis y evaluación de la calidad de los estudios

Se evaluó rigurosamente la calidad de los estudios seleccionados mediante criterios predefinidos. Este proceso garantizó la inclusión de investigaciones que cumplen altos estándares de calidad y aportan significativamente a la comprensión de la temática. La evaluación considera la relevancia, metodología y contribución de cada estudio al contexto de los ciberataques en América Latina.

Resultados y discusión

P1. ¿Cuáles son los tipos de ciberataques más comunes en América Latina durante los últimos cinco años?

Los tipos de ciberataques más comunes son: el ransomware, phishing, ataques de denegación de servicios (DDoS), inyección de SQL, malware, ingeniería social.

Según Ávila (2023) los países de Latinoamérica han enfrentado diversos tipos de ciberataques en los últimos años, los cuales, para Quintero (2020) han afectado tanto a ciudadanos como a organizaciones en la región, generando preocupaciones sobre la seguridad informática y protección de datos. Además, Quirumbay et al., (2022) señalan que los tipos de ciberataques más comunes son: el ransomware, phishing, ataques de denegación de servicios (DDoS), inyección de SQL, malware, ingeniería social, entre otros.

En la tabla 3 se muestra una descripción de cada tipo de ciberataque y los países que han sido más afectados con éstos.

Tabla. 3

Tipos de ciberataques

Tipos de Ciberataque	Descripción	Países más afectados
Ransomware	Secuestro de información a cambio de un rescate económico.	México, Brasil, Perú
Phishing	Suplantación de identidad para robar información personal y financiera a través de emails o páginas web falsas.	Chile, Colombia, Perú
Ataques de denegación de servicios (DDoS)	Sobrecarga de los servidores para negar el acceso a los usuarios legítimos.	Brasil, México, Argentina
Inyección de SQL	Inyección de código malicioso en bases de datos para extraer, dañar o eliminar datos.	Chile, Argentina, Colombia
Malware	Software malicioso diseñado para dañar o acceder a los sistemas informáticos sin consentimiento	México, Brasil, Argentina
Ingeniería social	Manipular a los usuarios para que revelen datos importantes	México, Brasil, Colombia

Por otra parte, Díaz (2021) menciona que el ransomware ha representado el 50% de los ataques denunciados en la logística de América Latina. Asimismo, Álvarez y Montoya (2020) resaltan que el 40% de las empresas en esta región sufrieron infecciones por malware en 2019. Sin embargo, Ortega y Rojas (2023) destacan que durante la pandemia del COVID–19 los ciberataques aumentaron significativamente, de modo que, en los primeros ocho meses del año 2021 hubo un incremento del 24% en los intentos de infección, con un promedio de 35 ataques cibernéticos por segundo.

P2. ¿Cómo han respondido los gobiernos y las empresas de América Latina ante el aumento de ciberataques?

Frente al aumento de ciberataques en los últimos 5 años, las empresas de América Latina han tomado una serie de medidas para hacerle frente a esta creciente ciber amenaza, razón por la que, Parra (2022) destaca la importancia de tener una buena comunicación entre todas las partes interesadas para identificar todos los riesgos y obtener resultados efectivos. En igual forma, Morales et al., (2020) sugieren tomar medidas de seguridad en línea para proteger los datos y la información de gobiernos, empresas y ciudadanos en general.

Según la postura de Pavón et al., (2022) los gobiernos de los países latinoamericanos han desarrollado estrategias nacionales y unidades especializadas en la prevención y respuesta a incidentes, con la finalidad de mejorar la ciberseguridad debido al aumento de amenazas cibernéticas, que van desde ataques a infraestructuras críticas hasta robos de datos y ciber-espionaje. Asimismo, Tapia y Centeno (2023) indican que el sector empresarial ha incrementado sus inversiones en soluciones de seguridad informática para proteger los sistemas y la información que manejan las empresas.

No obstante, Flores y Mena (2023) proponen una guía detallada de buenas prácticas, para que las entidades financieras mitiguen estos riesgos y mejoren la respuesta empresarial ante posibles ciberataques. Además, González (2019) resalta la importancia de la ciberseguridad en un mundo híper conectado, al mismo tiempo, hace hincapié en la necesidad de implementar nuevas directivas para garantizar la seguridad y minimizar los riesgos de los ataques cibernéticos.

P3. ¿Qué países de América Latina han experimentado un aumento significativo de ciberataques?

Quiroz et al., (2020) mencionan que algunos de los países de América Latina más afectados por ciberataques en los últimos años han sido México, Brasil, Venezuela, Colombia, Chile y Argentina. Asimismo, Álvarez (2022) sostiene que México es uno de los países de la región con más ciberataques, por lo que sugiere que los gobiernos y empresas deben estar preparados para responder de manera efectiva y transparente ante esta problemática creciente.

En igual forma, Ramírez et al., (2022) coincide con algunos de los países previamente mencionados, pero también señala que Perú ha experimentado un aumento significativo de ciberataques. Además, este mismo autor considera que estas naciones han estado trabajando en mejorar sus capacidades de ciberseguridad y han experimentado avances importantes en este campo.

Por otro lado, desde la óptica de Kaspersky (2022) la cual es una de las empresas líderes mundiales en ciberseguridad y protección contra amenazas informáticas, considera que el top 5 de los países más afectados está

integrado por Brasil, México, Colombia, Perú y Ecuador, a estos le siguen Argentina, Bolivia, Chile, Venezuela, Cuba y Paraguay, así como los países centro americanos de Guatemala, Costa Rica, Panamá y el país caribeño de República Dominicana, completando de esta manera el top 15 de las naciones de la región más afectada.

P4. ¿Qué iniciativas de colaboración regional o internacional en ciberseguridad se han establecido para abordar esta problemática?

Para Montenegro et al., (2022) existen diversas iniciativas de ciberseguridad regionales e internacionales en las que participan actores como la Organización de los Estados Americanos (OEA) además, destaca la importancia de establecer marcos normativos y políticas de ciberdefensa para abordar esta problemática.

Aguilar (2019) explica la importancia de la colaboración regional e internacional en el ámbito de la ciberseguridad; los desafíos cibernéticos no conocen fronteras y requieren un enfoque coordinado y cooperativo para su mitigación. No obstante, Vinogradova (2023) describe que la Comunidad de Estados Latinoamericanos y Caribeños (CELAC) analiza las iniciativas y proyectos de ciberseguridad en los países miembros, así como la creación de centros de respuesta a incidentes cibernéticos, programas de capacitación y concientización en ciberseguridad, evidenciando de esta manera la colaboración entre los países para detectar y prevenir ciberataques.

Los tipos de ciberataques más comunes son: el ransomware, phishing, ataques de denegación de servicios (DDoS), inyección de SQL, malware, ingeniería social.

P5. ¿Cómo ha evolucionado la conciencia y preparación en ciberseguridad entre las organizaciones y la población general de América Latina?

Esquivel (2023) menciona que los gobiernos han comenzado a implementar estrategias de seguridad digital y políticas de ciberseguridad para proteger a sus ciudadanos y garantizar un ciberespacio seguro. En igual forma, Díaz (2020) destaca que ha habido un aumento considerable en el interés por parte de la población de América Latina y el Caribe, pero que aún existen desafíos significativos en la región en términos de preparación y conciencia sobre ciberseguridad.

Ramírez et al., (2022) también afirman que las organizaciones y población en general, han incrementado su nivel de preparación y conciencia ante esta creciente amenaza, por lo que sugieren seguir promoviendo la cooperación regional e internacional. Sin embargo, Morcillo (2023) adopta una visión más amplia en cuanto a la concientización ciudadana, al proponer políticas y estrategias preventivas efectivas para mitigar estos ciberdelitos.

Caamaño y Gil (2019) consideran que las organizaciones modernas deben adoptar e implementar procedimientos para evitar ataques cibernéticos a los activos de información, además, enfatiza la necesidad de contar con competencias del talento humano para administrar la ciberseguridad organizacional. De igual modo, Franco et al., (2023) recomiendan que las instituciones públicas, empresas privadas y la academia estén preparadas para comprender la problemática y establecer medidas de protección contra los ciberataques, por lo que resalta la importancia de formar profesionales capacitados desde la universidad para afrontar con éxito esta amenaza.

Los ciberataques se han convertido en una amenaza creciente para los países de América Latina en los últimos años. González (2020) indica que la región registró un crecimiento del 60% en ciberataques en 2018 con un promedio de 9 ataques por segundo. Además, Arévalo y Hernández (2021) indican que Argentina sufrió cerca de cuatro millones de ciberataques por día en 2019, siendo los bancos y entidades relacionadas los más afectados. Por otra parte, Rivero (2023) menciona un caso específico en el que el Perú fue blanco de ciberataques, afectando la seguridad nacional y la Dirección General de Inteligencia del Ministerio del Interior.

Abad (2020) examina la situación de ciberataques en Ecuador, presentando estadísticas que demuestran que este país ha sufrido un aumento considerable en el número de ciberataques, especialmente contra objetivos gubernamentales y de infraestructura crítica. Asimismo, Zambrano et al., (2023) explican que Ecuador implementó en el año 2021 el proyecto de Ley de Protección de Datos Personales como respuesta a la filtración de datos del caso Novaestrat en 2019, lo que evidencia una iniciativa a nivel nacional para abordar la problemática de la protección de datos sensibles.

Las personas afectadas por estos delitos a menudo prefieren no denunciar por la dificultad de demostrarlo, lo que puede llevar a que muchos casos queden impunes.

En otro ámbito, Nieto y Sánchez (2023) describen los tipos de ciberataques más comunes que han afectado a los diversos países de la región y que han representado una amenaza creciente para la seguridad cibernética, entre estos mencionan el ransomware, phishing, malware y ataques de denegación de servicio distribuido (DDoS). Sin embargo, Izurieta (2022) afirma que las personas afectadas por estos delitos a menudo prefieren no denunciar por la dificultad de demostrarlo, lo que puede llevar a que muchos casos queden impunes, del mismo modo, plantea algunas recomendaciones para evitar ser víctima de delitos informáticos, como establecer contraseñas seguras, no compartir contraseñas, instalar sistemas antivirus, entre otras medidas preventivas.

Finalmente, Bicalho (2021) resalta la importancia de mejorar la resiliencia digital y la conciencia sobre los riesgos asociados con la ciberseguridad, ya que es muy importante estar preparados para enfrentar esta amenaza. Asimismo, Bautista et al., (2023) sostienen que, para combatir esta amenaza los gobiernos deberían establecer agencias de ciberseguridad e invertir más en soluciones técnicas de monitoreo y rastreo de incidentes, ya que, si no se toman medidas pronto, los ciberataques seguirán creciendo en la región y poniendo en riesgo infraestructura crítica, datos sensibles de ciudadanos y la estabilidad financiera de organizaciones tanto públicas como privadas.

La importancia de mejorar la resiliencia digital y la conciencia sobre los riesgos asociados con la ciberseguridad se vuelve evidente.

Conclusiones

El análisis exhaustivo de los ciberataques en América Latina resalta la necesidad de implementar estrategias efectivas de ciberseguridad que puedan hacer frente a la sofisticación y crecimiento de las amenazas cibernéticas en la región. La importancia de mejorar la resiliencia digital y la conciencia sobre los riesgos asociados con la ciberseguridad se vuelve evidente. Sin acciones inmediatas, los ataques seguirán representando una amenaza significativa para la región, poniendo en riesgo las infraestructuras críticas, los datos sensibles de ciudadanos y la estabilidad financiera de organizaciones tanto públicas como privadas.

Se recomienda que los gobiernos de la región establezcan un marco regulatorio común para la ciberseguridad, siguiendo modelos como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Además, es crucial incrementar la inversión en educación y capacitación en ciberseguridad, con el objetivo de formar una fuerza laboral especializada capaz de hacer frente a las amenazas cibernéticas emergentes.

Referencias bibliográficas

Abad, W. (2020). CIBERATAQUES: DESAFÍOS EN EL CIBERESPACIO. Revista de la Academia de Guerra del Ejército Ecuatoriano, 13, 116-128. https://doi.org/10.24133/age.n13.2020.11

Aguilar, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. Revista Latinoamericana de Estudios de Seguridad, I (25), 5-8. https://doi.org/10.17141/urvio.25.2019.4007

Aguilar, J. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de amenazas. Revista de Estudios en Seguridad Internacional, VI (2), 2-6. https://doi.org/10.18847/1.12.2

Aguilar, M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Revista CASEDE, LIII (198). https://doi.org/10.5354/0719-3769.2021.57067

Albear, H. (2021). Ciberataque - ciberguerra en america latina y su afectación en instituciones del estado ecuatoriano. http://repositorio.ug.edu.ec/handle/redug/51106?mode=simple

Álvarez, C. (2022). Estándar para activar la obligación de comunicar sobre ciber incidentes relevantes en instituciones públicas. Revista chilena de derecho y tecnología, 11(2), 183-210. https://doi.org/10.5354/0719-2584.2021.65502

Álvarez, M., y Montoya, H. (2020). Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos. Ingeniería, 18(3), 27-51. https://doi.org/https://doi.org/10.14482/inde.38.2.006.31

Arévalo, M., y Hernández, A. (2021). Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense. CUADERNO DE INVESTIGACIONES SEMILLEROS ANDIN, 14, 93-116. https://revia.areandina.edu.co/index.php/vbn/article/view/1950/1873

Arias, E., Claros, N., Manterola, C., y Astudillo, P. (2021). Revisiones sistemáticas de la literatura. Qué se debe saber acerca de ellas. Revista Elsevier, IX(3), 149-155. https://doi.org/10.1016/j.ciresp.2011.07.009

Ávila, F. (2023). Ransomware, una amenaza latente en Latinoamérica. 24, 49-58. https://doi.org/10.15517/isucr.v24i49

Bautista, F., Santiago, Y., y Serrano, G. (2023). Seguridad en Sistemas de Autenticación: Análisis de Vulnerabilidades y Estrategias de Mitigación. XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan, 11(22), 39-43. https://doi.org/10.29057/xikua.v11i22.10802

Bicalho, F. (2021). Infraestructura resiliente: un imperativo para el desarrollo sostenible en América Latina. https://repositorio.cepal.org/bitstream/handle/11362/46646/1/S2000675_es.pdf

Caamaño, E., y Gil, R. (2019). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. NOVUM, 20(3), 8-15. https://www.redalyc.org/journal/5713/571361695004/

Díaz, A. (2020). Predicción de áreas con usuarios vulnerables a ciberataques. https://repositorio.unab.cl/xmlui/bitstream/handle/ria/13990/a130367_Lisboa_M_Prediccion_de_areas_con_usuarios_vulnerables_2020_Tesis.pdf?sequence=5yisAllowed=y

Díaz, R. (2021). Estado de la ciberseguridad en la logística de América Latina y el Caribe. CEPAL, 21(228), 1-68. https://repositorio.cepal.org/server/api/core/bitstreams/4b04fcfe-c0f3-4c97-af14-2c234857f433/content

Esquivel, A. (2023). EL ESTADO Y LA DEFENSA DEL CIBERESPACIO. Revista Academia de Guerra del Ejército Ecuatoriano, 16, 99-109. https://doi.org/10.24133/RCSD.VOL16.N01.2023.07

Flores, S y Mena, L. (2023). Propuesta de Buenas Prácticas para Mitigar Ciberataques en Usuarios de Entidades Financieras. Digital Publisher, 4(8), 159-173. https://doi.org/10.33386/593dp.2023.4.1652

Franco, C., Villafuerte, H., y Alzamora, A. (2023). Ciberseguridad y su relación con la empleabilidad para egresados de Ingeniería de Sistemas en una Universidad Pública. Revista de Climatología, 23, 1510-1519. https://doi.org/10.59427/rcli/2023/v23cs.1510-1519

González, R. (2019). Costo económico de los ciberataques no tipificados en las leyes dominicanas. Revista Científica, 5, 32 - 39. https://doi.org/10.59794/rscd.2019.v5i5.pp32-39

González, J. (2020). Impacto de los ciberataques en la seguridad internacional. Revista Caribeña de Ciencias Sociales, 2(3), 22-30. https://www.eumed.net/rev/caribe/2020/01/ciberataque-seguridad-internacional.html

Gutiérrez, N. (2022). Estadísticas Importantes de Seguridad Informática. Blog All systems operational: https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Izurieta, V. (2022). Delitos informáticos en Ecuador según el COIP: unanálisis documental. International Journal of Interdisciplinary Studies, 3, 75-97. https://doi.org/10.51798/sijis.v3i1.284

Kaspersky. (2022). Lista de los países más afectados de América Latina. https://latam.kaspersky.com/about/press-releases/2023_kaspersky-descubre-nullmixer-malware-que-roba-datos-bancarios-criptomonedas-y-cuentas-de-redes-sociales

Martínez, O., Combita, H., y Hernández, H. (2019). Las Tecnologías de la Información y la Comunicación y su Influencia en la Transformación de la Educación Superior en Colombia para Impulso de la Economía Global. Scielo, XXX (1), 6-9. https://doi.org/10.4067/S0718-07642019000100255

Montenegro, H., Pantoja, M., Rojas, A., y Briceño, R. (2022). Políticas públicas de ciberdefensa en Chile y Colombia: un análisis desde el rastreo de procesos. Brújula. Semilleros de Investigación, 10(20), 7-16. https://doi.org/https://doi.org/10.21830/23460628.118

Morales, J., Zambrano, A., Lectong, J., y Bravo, M. (2020). Proceso de Ciberseguridad: Guía Metodológica para su implementación. Risti, 5(29), 41-50. https://www.proquest.com/openview/d5ff3aa902bb2d9994e9ed6af1443810/1.pdf?pq-origsite=gscholarycbl=1006393

Morcillo, L. (2023). Delitos informáticos en Ecuador: Análisis de la intervención penal en casos de estafas mediante redes sociales. Revista Científico, 1, 558-573. https://revista.gnerando.org/revista/index.php/RCMG/article/view/82/76

Nieto, C., y Sánchez, A. (2023). Riesgos cibernéticos en el sector financiero colombiano situación actual y tendencias. https://digitk.areandina.edu.co/bitstream/handle/areandina/5022/Trabajo%20de%20grado.pdf?sequence=1yisAllowed=y

Ortega, B., y Rojas, J. (2023). Cómo promueven los Estados la ciberseguridad de las pymes. Interfaces, 10(17), 21-37. https://doi.org/10.26439/interfases2023.n017.6246

Parra, C. (2022). Aumento de ataques cibernéticos asociados a la cadena de suministros y como interviene la Norma BASC para mitigarlos. https://repository.unimilitar.edu.co/bitstream/handle/10654/44022/CortesParraLeidyCarolina2022.pdf.pdf?sequence=2yisAllowed=y

Pavón, E., Guaytarilla, L., Cueva, C., y Durango, K. (2022). Perspectivas sobre la ciberseguridad y ciberdefensa en América Latina. Athenea, 3(9), 26-37. https://doi.org/10.47460/athenea.v3i9.43

Ramírez, M., Rodríguez, L., y Gómez, M. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America —Proposal for a Cybersecurity. Sustainability, 14, 1-23. https://doi.org/10.3390/su14031390

Quintero, A. (2020). Impacto de la técnica de ataque de Phishing en Colombia durante los últimos cinco años. https://repository.unad.edu.co/bitstream/handle/10596/38721/jaruedaq.pdf?sequence=1yisAllowed=y

Quiroz, T., Zapata, J., y Vargas, M. (2020). Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman. Tecnológicas. 23(48), 13-20. https://doi.org/10.22430/22565337.1586

Quirumbay, I., Castillo, A., y Coronel, I. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. Revista Científica y Tecnológica UPSE, 9(1), 57-65. https://doi.org/10.26423/rctu.v9i1.671

Rivero, E. (2023). Ciberdefensa: Los Desafíos del Mundo Virtual. Revista Seguridad y Poder Terrestre, 2(2), 99-105. https://doi.org/10.56221/spt.v2i2.29

Saavedra, B. (2023). Ciberseguridad en América Latina: Retos, Preocupaciones y Oportunidades. En E. Ellis, y P. Vera, Desafíos y Amenazas a la Seguridad en América Latina (Vol. I, pp. 2-4). ieee.es. https://ceeep.mil.pe/2023/03/09/ciberseguridad-en-america-latina-retos-preocupaciones-y-oportunidades/

Tapia, A., y Centeno, D. (2023). Evaluación de la seguridad de las redes internas del área de los sistemas SCADA CNEL EP, unidad de negocios Manabí mediante OSSTMM y OPNET. Revista de Tecnologías de la Informática y las Comunicaciones, 7, 27 - 39. https://doi.org/10.33936/isrtic.v7i1.5558

Vinogradova, E. (2023). Las tecnologías de inteligencia artificial y el auge de las amenazas cibernéticas en América Latina. Russian Academy of Science, 3, 34-48. https://doi.org/10.31857/S0044748X0024415-5

Yanulis, B. (2023). Noticias de ciberseguridad en América Latina. GlobalSign Blog GMO: https://www.globalsign.com/es/blog/es-blog-noticias-ciberseguridad-en-america-latina-abril

Zambrano, A., Cedeño, L., Loor, M., y Zambrano, A. (2023). Análisis de los derechos a la intimidad y privacidad sobre los datos personales en la legislación ecuatoriana. Revista de Tecnologías de la Informática y las Comunicaciones, 7(1), 7 - 18. https://doi.org/10.33936/isrtic.v7i1.5793