

UNIVERSIDAD CATÓLICA DE CUENCA



Universidad
Católica
de Cuenca

Maestría en Ciberseguridad

**Informe de Investigación previo a la obtención del título de Magíster en
Ciberseguridad**

Tema: Revisión sistemática de la evolución de las amenazas cibernéticas: Un enfoque integral para mejorar la ciberseguridad a lo largo del tiempo

Autor: Ing. Pablo Javier Santillán Sánchez.

Asesores: Ing. Miguel Andrade López. Mg
Ing. Juan Carlos Ortega Castro. Mg

Cuenca, 2024

Certificación de Asesores

Se certifica que:

El informe de investigación “Revisión sistemática de la evolución de las amenazas cibernéticas: Un enfoque integral para mejorar la ciberseguridad a lo largo del tiempo”, de autoría del Señor Ingeniero en Computación e Informática Pablo Javier Santillán Sánchez, CC: 0917138471, ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Cuatro Ríos de Cuenca

Septiembre, 2024.

Ing. Miguel Andrade López. Mg
Asesor Científico

Ing. Juan Carlos Ortega Castro. Mg
Asesor Metodológico

Certificación de Autoría

Certifico que:

“Revisión sistemática de la evolución de las amenazas cibernéticas: Un enfoque integral para mejorar la ciberseguridad a lo largo del tiempo”, es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Septiembre, 2024.

Ing. Pablo Javier Santillán Sánchez
CC: 0917138471

Agradecimiento

En primer lugar, quiero expresar mi más profundo agradecimiento a mi madre, Lcda. Ana Sánchez B, por su amor incondicional, su apoyo constante y sus palabras de aliento a lo largo de mi vida. Sin su dedicación y sacrificio, no hubiera sido posible alcanzar este logro.

A mi novia, Dra. Zully Alfonso F, gracias por tu paciencia, comprensión y por estar a mi lado en cada paso de este camino. Tus palabras de ánimo y tu compañía han sido fundamentales para mantenerme motivado y enfocado.

A mi tutor de tesis, Ing. Juan Carlos Ortega Mg., quiero agradecerle por su guía, su paciencia y sus valiosas contribuciones. Sus consejos y su dedicación me han ayudado a superar los desafíos y a crecer como investigador.

Finalmente, quiero expresar mi gratitud a la Universidad Católica de Cuenca por proporcionarme los recursos y el ambiente académico necesario para llevar a cabo este trabajo. Gracias a todos los profesores y compañeros que me han acompañado en este recorrido académico.

Dedicatoria

Dedico esta tesis a mi madre, Lcda. Ana Sánchez B, cuya fortaleza y amor han sido mi mayor fuente de inspiración.

A mi novia, Dra. Zully Alfonso F, por su apoyo inquebrantable y por ser mi compañera en todas las circunstancias.

A mis hermanos, quienes siempre han estado allí para apoyarme y motivarme en los momentos difíciles.

A mis amigos, por su constante apoyo y por creer en mí incluso cuando yo mismo dudaba. Gracias por estar conmigo en las buenas y en las malas.

Con todo mi cariño y gratitud, les dedico este logro.

Resumen

En el mundo digital actual, la evolución de las amenazas cibernéticas es un tema crucial para instituciones públicas y privadas. El objetivo principal de este trabajo es evaluar de manera sistemática la evolución de las amenazas cibernéticas y su impacto en las instituciones. Al revisar estudios anteriores, identificamos las amenazas más significativas y las soluciones propuestas para enfrentarlas. Este análisis ofrece una base sólida para comprender la importancia de una ciberseguridad robusta y proactiva, destacando la necesidad de actualizar constantemente las defensas para proteger la información crítica, cabe señalar que en el trabajo desempeñado se explora la historia y desarrollo de estas amenazas, enfocándose en América y cómo las organizaciones han mejorado sus medidas de seguridad en respuesta.

A medida que la tecnología ha avanzado, las amenazas cibernéticas también se han vuelto más sofisticadas. Al revisar estudios anteriores, se identifican las amenazas más significativas y las soluciones propuestas, proporcionando una base sólida para comprender la importancia de una ciberseguridad robusta y proactiva.

Finalmente, este trabajo aborda la problemática de las amenazas cibernéticas desde múltiples perspectivas, incluyendo sectores específicos como la industria alimentaria y las telecomunicaciones. A través de estudios de caso y ejemplos concretos, se ilustra cómo diferentes organizaciones han respondido a estos desafíos, ofreciendo recomendaciones prácticas para fortalecer la seguridad de la información en un mundo digitalizado.

Palabras claves: Ciberseguridad, amenazas cibernéticas, vulnerabilidades, soluciones, instituciones.

Abstract

In today's digital world, the evolution of cyber threats is a crucial issue for public and private institutions. The main objective of this paper is to systematically assess the evolution of cyber threats and their impact on institutions. By reviewing previous studies, we identify the most significant threats and the solutions proposed to address them. This analysis provides a solid foundation for understanding the importance of robust and proactive cybersecurity, highlighting the need to constantly update defenses to protect critical information. It should be noted that the work explores the history and development of these threats, focusing on the Americas and how organizations have improved their security measures in response.

As technology has advanced, cyber threats have also become more sophisticated. By reviewing past studies, the most significant threats and proposed solutions are identified, providing a solid foundation for understanding the importance of robust and proactive cybersecurity.

Finally, this paper addresses the issue of cyber threats from multiple perspectives, including specific sectors such as the food industry and telecommunications. Through case studies and concrete examples, it illustrates how different organizations have responded to these challenges, offering practical recommendations to strengthen information security in a digitized world.

Keywords: Cybersecurity, cyber threats, cyber vulnerabilities, solutions, institutions.

Índice de contenidos

Certificación de Asesores	i
Certificación de Autoría.....	ii
Agradecimiento.....	iii
Dedicatoria.....	iv
Resumen.....	v
Abstract.....	vi
Índice de figuras.....	ix
Índice de tablas	ix
Capítulo I. Introducción	1
1.1 Situación problemática	1
1.2 Antecedentes	2
1.3 Fundamentación teórica	6
1.3.1 Ciberseguridad	6
1.4 Formulación del problema	11
1.5 Justificación e importancia del estudio	11
1.5.1 Alcance	12
1.6 Hipótesis	12
1.7 Objetivos	13

1.7.1	Objetivo general.....	13
1.7.2	Objetivos específicos	13
Capítulo II. Diagnóstico situacional		14
2.1	Metodología	14
2.1.1	Tipo de investigación.....	14
2.2	Método a emplear	15
2.3	Proceso de revisión	16
2.3.1	Análisis documental.....	17
Capítulo III. Propuesta		19
3.1	Esquema Prisma.....	19
3.2	Resultados	21
3.3	Discusión.....	36
Conclusiones.....		38
Recomendaciones		39
Bibliografía		40

Índice de figuras

Figura 1. <i>Diagrama de selección de artículos</i>	19
---	----

Índice de tablas

Tabla 1. Resumen de la metodología PRISMA	16
Tabla 2. <i>Cadena de búsqueda</i>	17
Tabla 3. Características de los artículos seleccionados	21
Tabla 4. Resultados	23

Capítulo I. Introducción

1.1 Situación problemática

La continua evolución de las amenazas cibernéticas representa un desafío constante para la ciberseguridad. La rápida transformación de las estrategias empleadas por individuos malintencionados ha convertido esta problemática en una lucha constante por la protección de la información, motivando a instituciones públicas y privadas a mejorar constantemente sus sistemas de seguridad para contrarrestar los cada vez más sofisticados ataques cibernéticos. Mohamed (2024) menciona que se tiene que tener una correcta protección en las aplicaciones web utilizadas en la gestión de los servicios empresariales, dado que las amenazas cibernéticas más comunes son el acceso no autorizado a la base de datos a través de inyecciones SQL.

Asimismo, Alqudhaibi et al. (2024) menciona que en la industria alimentaria la digitalización ha introducido riesgos de ciberataques, que abarcan violaciones de datos e interrupciones del sistema afectando gravemente la producción, provocando el miedo y la desconfianza entre los consumidores. Por ello la situación de las amenazas cibernéticas se ha ido agravando en las instituciones que no han implementado las medidas necesarias para mantener una sólida seguridad de la información. Por lo que, se requiere de una acción proactiva para mitigar estos riesgos, preservar la integridad de los datos generando confianza en los sistemas digitales.

Esta revisión bibliográfica se centra en la necesidad de comprender y abordar de manera eficazmente la evolución constante de las amenazas cibernéticas, las cuales impactan la vulnerabilidad de la información resguardada por instituciones públicas y privadas. Pigola et al. (2023) menciona que la ciberseguridad es esencial en la reducción de los ciberataques y para optimizar el uso de la tecnología.

De igual forma, Macas et al. (2024) propone el desarrollo de un sistema de aprendizaje profundo para la toma de decisiones en ciberseguridad adaptables frente a los crecientes ataques cibernéticos que sufren las instituciones. Además, se ha constatado que en la actualidad estas instituciones muestran un vacío en la implementación de medidas preventivas de ciberseguridad, generando considerables pérdidas económicas en América.

1.2 Antecedentes

Los ataques cibernéticos hoy en día se han vuelto una problemática en varios sectores, por lo tanto se han tomado varios artículos científicos como antecedentes para el presente estudio bibliográfico como es la investigación de Abohatem y Ba-Alwi (2024) que muestra varias normas para determinar el nivel de madurez de Yemen Telecoms y evaluar la eficacia de la protección de los sistemas de información, utilizando información relevante e informes técnicos recurrentes para reunir los datos, que fueron comparados con la normativa internacional necesaria para determinar el nivel de madurez.

A través de procesos confiables de ciberseguridad, se identificaron que las amenazas ciberseguridad están siendo más notorias y frecuentes por lo que compromete la seguridad de la información de la empresa. Yemen Telecoms ha puesto en marcha una serie de medidas de ciberseguridad, pero este análisis muestra que sus normas y procedimientos de protección del sistema de información aun cuenta con falencias latentes que deben ser analizadas. Con el fin de defender eficazmente las telecomunicaciones de Yemen contra las amenazas cibernéticas, mediante sugerencias para reforzar los sistemas de información de ciberseguridad (Abohatem y Ba-Alwi, 2024).

De igual forma, Alsmadi et al. (2024) señala que la falta de conciencia y malas prácticas en ciberseguridad han dado lugar a amenazas cibernéticas durante la pandemia de COVID-19. El propósito de esta investigación fue explorar la actitud de los usuarios hacia la adopción de un comportamiento proactivo de conciencia en ciberseguridad. Centrándonos en la teoría del comportamiento planificado, examinamos la relación entre diversos factores y su impacto en la actitud, utilizando encuestas para recopilar respuestas. Esta investigación incluyó la participación de 229 encuestados de la Universidad de Petra en Jordania.

La actitud se vio significativamente influenciada por la percepción de la influencia de los compañeros y la conciencia de las amenazas de ciberseguridad, especialmente aquellas que surgieron durante el periodo de COVID-19. Se exploraron diversas dimensiones de conocimiento entre los usuarios, abarcando aspectos relacionados con la organización, los sistemas de información y las redes sociales. Asimismo, se analizó la influencia de los pares en la conciencia de la ciberseguridad. Además, la investigación arrojó luz sobre la percepción de los usuarios respecto a los principales riesgos de ciberseguridad durante la pandemia de COVID-19.

Ahora bien, Wang et al. (2024) afirma que la atiga de alerta en la seguridad empresarial puede tener consecuencias graves, debido a que los analistas, abrumados por el gran volumen de alertas, pueden pasar por alto riesgos críticos, exponiendo a la organización a amenazas cibernéticas. Aunque la investigación se centra en reducir falsos positivos, la falta de recursos para investigar todas las alertas verdaderas persiste.

AlertPro es un software de priorización de alertas que optimiza el trabajo de los analistas al extraer características de contexto e históricas. Experimentos con datos demostraron su capacidad para descubrir ataques no revelados y fortalecer la seguridad. La inclusión de estas

características en el aprendizaje activo mejora las tasas de detección. Con un tiempo de procesamiento de 0.5 segundos, es eficiente en tiempo real. Aunque se puede mejorar con más retroalimentación, mitiga la fatiga de alerta y permite a los analistas enfocarse en amenazas prioritarias. AlertPro es una herramienta valiosa para la gestión efectiva de riesgos de seguridad (Wang et al., 2024).

De este modo, Doriguzzi-Corin y Siracusa (2024) afirma que Federated Learning (FL) atrajo la atención de la comunidad de ciberseguridad como un método para colaborativamente entrenar modelos de aprendizaje profundo sin exponer datos de capacitación. Aunque su adopción en ciberseguridad estaba en etapas iniciales, había aspectos prácticos pendientes. El algoritmo central de FL, el promedio federado, requería datos de prueba para controlar el proceso, pero compartir el tráfico de redes de prueba podía comprometer información sensible.

Así mismo, aborda la convergencia de FL en entornos dinámicos de ciberseguridad, proponiendo FLAD, un enfoque adaptativo para la detección de ataques DDoS. FLAD utilizó un mecanismo adaptativo sin compartir datos de prueba para actualizar modelos con perfiles de ataque recientes. En comparación con algoritmos FL convencionales, FLAD demostró una mayor precisión y convergencia en datos de ataques DDoS heterogéneos desequilibrados. Su robustez se confirmó en escenarios realistas de reentrenamiento con nuevos perfiles de ataques.

Por consiguiente, Raval et al. (2024) menciona que la inteligencia artificial (IA), blockchain e Internet de las Cosas (IoT) marcaron una revolución digital. Sin embargo, la falta de ciberseguridad en diversas industrias insinuó amenazas y vulnerabilidades avanzadas, especialmente a través de ataques cibernéticos. Este trabajo se enfocó en analizar las amenazas cibernéticas en sectores críticos como finanzas, agricultura, energía y salud. Se presentó una

taxonomía basada en IA para resaltar la eficacia de los mecanismos de IA en la defensa contra ciberataques a infraestructuras críticas.

Esta investigación abordó temas como privacidad de datos, sesgo algorítmico y colaboración humano-AI. Además, se propuso un marco de intercambio de datos seguro basado en IA para redes inteligentes de infraestructuras críticas, evaluado mediante medidas estadísticas. El trabajo subrayó los desafíos de investigación en sistemas críticos, haciendo hincapié en la necesidad de mecanismos basados en IA para abordarlos, especialmente en el contexto de los ataques cibernéticos.

Según Hnamte et al. (2024) señala que la creciente amenaza de ataques cibernéticos, especialmente los de denegación de servicio (DDoS), es una preocupación crucial para la seguridad de las redes. Este estudio presentó una innovadora metodología para la detección de DDoS, basada en una arquitectura de red neuronal profunda (DNN) arraigada en los principios de aprendizaje profundo (DL). El modelo destacó por su escalabilidad y adaptabilidad, permitiendo un análisis minucioso de los datos de tráfico para discernir patrones complejos indicativos de ataques DDoS.

A través de evaluaciones rigurosas con datos de tráfico auténticos respaldaron inequívocamente la eficacia del enfoque propuesto, revelando su superioridad sobre las técnicas tradicionales de detección DDoS. Este enfoque prometió fortalecer la seguridad de las redes, especialmente en entornos de red definidos por software (SDN). Además de introducir una novedosa detección DDoS en infraestructuras SDN, el estudio abordó las implicaciones prácticas y desafíos asociados al despliegue de DNNs en entornos SDN del mundo real, ofreciendo perspectivas valiosas para los profesionales de seguridad de redes.

Finalmente, Aygul et al. (2024), afirman que la necesidad de predecir la estabilidad transitoria en sistemas de energía modernos, especialmente vulnerables a ciberataques. Aunque la tecnología avanzaba, los algoritmos de aprendizaje automático no estaban preparados para contrarrestar amenazas cibernéticas sofisticadas. La investigación evaluó el impacto de los ciberataques y la integración de energías renovables en los métodos de aprendizaje automático. Esta brecha en la resiliencia de los algoritmos subraya la importancia de desarrollar enfoques más robustos para garantizar la seguridad y estabilidad de los sistemas energéticos en tiempo real.

Los métodos de predicción de estabilidad transitoria en línea fueron fundamentales para monitorear el comportamiento del sistema de energía en respuesta a perturbaciones. Sin embargo, los resultados de la investigación indicaron que, bajo ciberataques, los algoritmos de aprendizaje automático exhibieron un rendimiento insuficiente, lo que condujo a una significativa disminución en la precisión de las predicciones transitorias de estabilidad en comparación con condiciones normales de operación. Este hallazgo destacó la urgente necesidad de implementar medidas avanzadas de ciberseguridad para preservar las capacidades predictivas de los sistemas de energía en un entorno cada vez más amenazante.

1.3 Fundamentación teórica

1.3.1 Ciberseguridad

La ciberseguridad es crucial en la era digital ante la evolución de amenazas cibernéticas. Cervera García y Goussens (2024) señalan el crecimiento de la ciberdelincuencia, con consecuencias alarmantes como la filtración de datos sensibles o el secuestro de sistemas, comprometiendo la privacidad de los clientes. Sectores públicos y privados adoptan medidas sólidas de ciberseguridad mediante tecnologías de la información y comunicación (TIC). Entender

cómo estas amenazas evolucionan es fundamental para desarrollar estrategias defensivas efectivas. La protección contra ciberataques se convierte en una prioridad en la era digital para salvaguardar la integridad de datos y sistemas.

El Consejo de la Unión Europea (2024) prioriza la ciberresiliencia y defensa contra ataques cibernéticos, especialmente en sectores críticos como transporte, energía, salud y finanzas. La digitalización ofrece oportunidades, pero también expone a ciberamenazas, como demostró la reciente crisis sanitaria. Los ataques cibernéticos en Europa se vuelven más sofisticados, lo que impulsa a la UE a mejorar la protección, incluyendo el uso de encriptación cuántica para garantizar la seguridad de la comunicación y el acceso a datos por parte de autoridades judiciales y policiales. Es crucial fortalecer la ciberdiplomacia y la colaboración internacional para enfrentar estas amenazas.

La Unión Europea (UE) ha adoptado diversas medidas para hacer frente a la ciberdelincuencia, que abarcan desde la lucha contra el fraude en los pagos sin efectivo hasta la protección de menores en internet. Se destaca la creación del Centro Europeo de Ciberdelincuencia en Europol y la iniciativa EMPACT para combatir la delincuencia organizada, incluyendo la ciberdelincuencia. La UE también ha implementado normas más estrictas contra el fraude en los pagos sin efectivo.

En cuanto a la seguridad de los menores en línea, se han propuesto nuevas legislaciones y normas temporales para abordar el abuso sexual de menores en internet. Además, se ha enfocado en aspectos legales y de aplicación de la ley, como el acceso a pruebas electrónicas, cifrado y conservación de datos.

La ciberdiplomacia, las sanciones contra ciberataques y la cooperación en ciberdefensa también son parte de la estrategia de la UE. Se asigna un considerable financiamiento a través de programas como Horizonte Europa y Europa Digital, y se ha establecido el Centro Europeo de Competencia en Ciberseguridad. La UE busca abordar específicamente la ciberseguridad en infraestructuras críticas, como dispositivos conectados seguros y redes 5G. En conjunto, estas acciones reflejan un enfoque integral para proteger a la UE de las amenazas cibernéticas y promover la ciberseguridad.

La transformación digital ha redefinido nuestra vida cotidiana, eliminando fronteras geográficas y facilitando la comunicación y el trabajo a través de tecnologías como el Internet de las Cosas y la Inteligencia Artificial. Sin embargo, este cambio trae consigo desafíos, siendo la ciberseguridad crucial. En un mundo digitalizado, la protección de datos y comunicaciones es vital para salvaguardar derechos fundamentales y evitar costosas consecuencias para la sociedad, como la vulneración de la privacidad y la propiedad intelectual (Fernández Pinto y Herrera Romero, 2018). La falta de atención a este aspecto puede poner en riesgo la integridad de los ciudadanos y la estabilidad de las instituciones.

1.3.1.1 Amenazas cibernéticas

Según, Panorama de Amenazas de la ENISA (2020), la agencia de la Unión Europea dedicada a lograr un alto nivel común de ciberseguridad en toda Europa, la cual fue establecida en 2004 y se ha fortalecido mediante el Reglamento sobre la Ciberseguridad. La ENISA contribuye a la política cibernética de la UE, mejorando la confiabilidad de productos, servicios y procesos de TIC mediante programas de certificación de ciberseguridad.

Además, colabora con los Estados miembros y organismos de la UE, preparando a Europa para los desafíos cibernéticos futuros. A través del intercambio de conocimientos, capacitación y sensibilización, la Agencia trabaja con partes interesadas clave para fortalecer la confianza en la economía conectada, impulsar la resiliencia de la infraestructura de la Unión y proteger digitalmente a la sociedad y ciudadanía europea.

Entre las principales amenazas cibernéticas que han afectado a instituciones públicas y privadas se encuentran el malware, ataques basados en la web, phishing, ataques a aplicaciones web, spam, DDoS, robos de identidad, filtración de datos, amenazas internas, botnets, manipulación física, daños, robos y pérdidas, filtración de información, ransomware, ciberespionaje y criptosequestro.

1.3.1.2 Evolución de las amenazas cibernéticas

A lo largo de las últimas décadas, la evolución de las amenazas cibernéticas ha ido de la mano con el desarrollo de la tecnología. En sus inicios, las preocupaciones se centraban en virus y malware relativamente simples, como el famoso gusano Morris en la década de 1980 (Securita Operation Center, 2022). Con la conectividad a Internet, la escala y sofisticación de las amenazas aumentaron drásticamente. A medida que la sociedad se volcaba a la era digital, el panorama cibernético se vio inundado por ataques de phishing, que buscaban engañar a usuarios para obtener información sensible.

Con la propagación de los troyanos y la creación de botnets amplificaron el alcance y el impacto de los ciberataques. La transición hacia el siglo XXI trajo consigo la aparición de amenazas más sigilosas, como el ransomware, que cifra datos cruciales exigiendo pagos para su

liberación. Asimismo, M. Francisco (2023) los ataques dirigidos, conocidos como APTs, evidenciaron la presencia de actores cibernéticos altamente organizados y respaldados por estados.

En la actualidad, el panorama de amenazas cibernéticas se enfrenta a desafíos complejos y en constante evolución. La inteligencia artificial se ha convertido en una herramienta tanto para atacantes como para defensores, añadiendo una capa adicional de sofisticación a los ciberataques. Los ataques basados en la nube, el secuestro de identidad y la manipulación de la información se han vuelto preocupaciones omnipresentes (Núñez, 2024).

Ahora bien, Cen et al. (2024) menciona que los ataques de ransomware han proliferado globalmente, constituyendo una grave amenaza cibernética para la infraestructura digital. Desde individuos hasta entidades críticas, como empresas comerciales y centros médicos, son objetivos. Estos ataques emplean cifrado avanzado, dificultando la recuperación de datos sin una clave de descifrado. La detección temprana de actividades maliciosas es esencial para la protección eficaz.

A medida que la ciberseguridad se enfrenta a estos desafíos actuales, la anticipación de amenazas emergentes, como posibles ciberataques a la infraestructura de inteligencia artificial, se vuelve imperativa. La evolución continua de las amenazas cibernéticas demanda estrategias adaptativas y colaborativas entre gobiernos, empresas y profesionales de la ciberseguridad para garantizar la protección de la sociedad digital.

La tecnología IoT y las Redes de Sensores Inalámbricos (WSN) enfrentan desafíos de ciberseguridad, como malware y ataques DDoS. Para abordar estos problemas, se propone el Sistema de Soporte de Decisiones Inspirado en la Naturaleza para el Agrupamiento Seguro (NIDSC). Este enfoque utiliza un modelo de confianza híbrido y el algoritmo Differential Evolution para seleccionar Cluster Heads (CH), mejorando la seguridad con mínimo consumo de

recursos. En comparación con métodos existentes, NIDSC muestra un rendimiento superior en términos de throughput, entrega de paquetes, retraso, sobrecarga de comunicación y consumo de energía en escenarios de prueba (Qureshi y Shandilya, 2022).

La Red Definida por Software (SDN) busca proporcionar flexibilidad y control centralizado en las redes futuras, pero su arquitectura presenta vulnerabilidades que generan preocupaciones de seguridad, especialmente ante ataques DDoS aprovechando la programabilidad y control central. A pesar de la vulnerabilidad, SDN puede utilizarse para contrarrestar ataques (Wabi et al., 2023).

1.4 Formulación del problema

¿Cómo han evolucionado las amenazas cibernéticas a lo largo del tiempo?

1.5 Justificación e importancia del estudio

Este proyecto se justifica mediante una revisión bibliográfica de artículos científicos recientes que analizan ataques cibernéticos a instituciones y proponen soluciones para mitigar sus efectos. La evolución constante de las amenazas cibernéticas representa un desafío para la ciberseguridad, instando a instituciones públicas y privadas a mejorar sus sistemas de seguridad continuamente. Mohamed (2024) destaca la importancia de la protección en aplicaciones web, especialmente en la gestión de servicios empresariales, donde amenazas comunes como las inyecciones SQL requieren atención específica.

Alqudhaibi et al. (2024) resaltan los riesgos de ciberataques en la industria alimentaria, afectando la producción y generando desconfianza debido a la falta de medidas de seguridad. La problemática científica se centra en comprender y abordar eficazmente la evolución de las amenazas cibernéticas, impactando la vulnerabilidad de la información resguardada por

instituciones. Pigola et al. (2023) subrayan la esencialidad de la ciberseguridad para reducir ciberataques.

Mientras que la propuesta de Macas et al. (2024) para un sistema de aprendizaje profundo destaca la necesidad de adaptabilidad ante amenazas crecientes. La investigación busca entender cómo las instituciones fortalecen sus sistemas de seguridad frente a la evolución de los ataques cibernéticos, revisando medidas tomadas y destacando la importancia de la ciberseguridad para la protección de datos y la estabilidad económica.

1.5.1 Alcance

El presente trabajo de investigación aborda la evolución de las amenazas cibernéticas y su impacto en las instituciones públicas y privadas, particularmente en América, este estudio se centra en comprender como las amenazas cibernéticas han ido evolucionando en el tiempo, desde los primeros incidentes hasta los que se producen en la actualidad y como las instituciones han ido mejorando las seguridades en respuesta a estos ataques cibernéticos, el alcance de esta investigación se encuentra limitado a la revisión bibliográfica de estudios realizados con anterioridad.

1.6 Hipótesis

Se espera que la investigación bibliográfica revele una evolución constante de las amenazas cibernéticas, desde los primeros incidentes hasta las amenazas más recientes. Se hipotetiza que esta evolución estará impulsada por avances tecnológicos, cambios en el panorama geopolítico y la creciente sofisticación de los actores maliciosos. Además, se espera identificar patrones específicos en las tácticas y técnicas utilizadas, así como en las vulnerabilidades más explotadas a lo largo de las décadas.

1.7 Objetivos

1.7.1 Objetivo general

Evaluar las amenazas cibernéticas a través de una revisión sistemática de literatura, para comprender su evolución y como se fortalecen las instituciones.

1.7.2 Objetivos específicos

- Realizar una revisión de la bibliografía sobre la evolución de las amenazas cibernéticas de lo largo del tiempo.
- Identificar las amenazas cibernéticas que han impactado a las empresas a lo largo del tiempo.
- Examinar las soluciones propuestas para hacer frente a las amenazas cibernéticas.

Capítulo II. Diagnóstico situacional

2.1 Metodología

La metodología empleada en esta revisión bibliográfica se basó en la identificación de fuentes de información pertinentes que abordaran la investigación documental sobre los ataques cibernéticos sufridos por empresas tanto públicas como privadas a lo largo de los años recientes. A partir de estas fuentes, se recopilaron los datos esenciales necesarios para alcanzar los objetivos propuestos.

El propósito de esta revisión radica en discernir el impacto de las amenazas cibernéticas en las empresas a lo largo del tiempo y examinar las soluciones implementadas en respuesta a estas. Además, se establecieron criterios para la selección de documentos, los cuales fueron analizados y discutidos con el fin de extraer información sobre el tema investigativo.

2.1.1 Tipo de investigación

La presente revisión literaria adopta un enfoque cualitativo que permitió realizar un análisis sistemático de la información. A través de este enfoque se llevó a cabo la comparación y selección de los resultados desde el momento de la recolección de datos para llevar a cabo la revisión bibliográfica que permita identificar las amenazas cibernéticas (Hernández-Sampieri y Torres, 2018).

Los artículos seleccionados para el estudio se encuentran relacionados directamente con las variables de la investigación para comprender de una manera integral el panorama actual de la ciberseguridad. Asimismo, se sustentará con un tipo narrativo a través de relatos detallados de eventos, experiencias o situaciones que permiten a los investigadores capturar aspectos cualitativos

de un fenómeno de estudio, los artículos científicos se enfocaran en situaciones reales que permitan identificar el estado actual de la investigación (Sobrido Prieto y Rumbo Prieto, 2018).

Asimismo, se llevó a cabo una investigación descriptiva que facilitó la búsqueda y exploración de datos provenientes de investigaciones previas. El propósito fue verificar la información obtenida y controlar varios aspectos de los artículos revisados. A través de un análisis situacional, se examinó el estado actual de las amenazas cibernéticas, abordando aspectos como el tipo de amenaza predominante, los sectores afectados por estos ataques y las medidas de ciberseguridad implementadas para contrarrestarlos (Sobrido Prieto y Rumbo Prieto, 2018).

2.2 Método a emplear

Para la gestión de la información, se utilizó el método PRISMA, garantizando la transparencia y la reproducibilidad del proceso de selección de estudios, basada en criterios de inclusión estableciendo las características esenciales para que los artículos de revisión sean seleccionados para el estudio. Asimismo, los criterios de exclusión se establecerán las características que no cumplen con los requisitos de la investigación y conllevaran a su eliminación de la revisión. Este método permitió recopilar información relevante y significativa para abordar los aspectos clave de la ciberseguridad en la actualidad (Page et al., 2021).

Este método PRISMA se lleva a cabo a través de diagramas donde se describe el proceso de selección de artículos para la revisión que se muestran en los resultados, según Page et al. (2021). La selección de artículos se llevará a cabo de manera cuidadosa, priorizando la calidad y la pertinencia de los estudios para garantizar la fiabilidad de la revisión. A continuación, en la Tabla 1 se muestran los puntos a seguir del método PRISMA que permitan alcanzar los objetivos.

Tabla 1.*Resumen de la metodología PRISMA*

Sección	Ítem
Criterios de elegibilidad	Criterios de inclusión y exclusión
Fuentes de información	Scopus, ScienceDirect, Web of Science
Cadenas de búsqueda	(TITLE-ABS-KEY ("Cyber threats") AND TITLE-ABS-KEY ("Cybersecurity")) (TITLE-ABS-KEY ("Cyber threats") AND TITLE-ABS-KEY ("evolution")) (TITLE-ABS-KEY ("Cyber threats") AND TITLE-ABS-KEY ("impact")) (TITLE-ABS-KEY ("Cyber threats") AND TITLE-ABS-KEY ("risks"))
Proceso de selección	Se llevó a cabo un procedimiento de exclusión utilizando los criterios de idoneidad, eliminación de duplicados y revisión completa del texto.
Proceso de recopilación de datos	Scimago se usó como fuente de información sobre los datos de las revistas.
Métodos de síntesis	La información resultante de los estudios incluidos en la revisión se distribuye en tablas para su mejor comprensión.

Nota. En esta tabla se muestran los puntos a seguir del método PRISMA con el fin de lograr los objetivos

2.3 Proceso de revisión

Para la recolección de la información se realizaron búsquedas en las diferentes bases de datos digitales como son Scopus, Science Direct y Web of Science, con el objetivo de obtener datos de gran relevancia mediante las cadenas de búsqueda a través de palabras clave y términos booleanos (And, Or, Not). Los resultados obtenidos se sometieron a criterios de elegibilidad donde también se aplicaron filtros dentro de las bases de datos que permitieron recopilar información relevante para la revisión sistemática.

2.3.1 Análisis documental

Criterios de Inclusión

- Tiempo: Entre el año 2019 y 2024.
- Tipos de documento: Artículos originales, estudios observacionales, descriptivos, transversales.
- Idioma: inglés y español.
- Accesibilidad: Acceso libre.
- Contenido: Información referente al tema.
- Estudios relacionados con ciberseguridad.

Criterios de Exclusión

- Tiempo: Antes del 2019 y después del 2024.
- Tipo de documento, tesis, páginas web, revisiones y libros.
- Contenido: Información que no sea referente al tema.
- Accesibilidad: Acceso restringido.
- Estudios que no estén relacionados con ciberseguridad.

Al establecer los criterios de selección, se llevaron a cabo búsquedas en diversas bases de datos, entre las que se incluyeron Scopus, Science Direct y Web of Science. Estas búsquedas arrojaron un total de **17** artículos, como se detalla en la Tabla 2 que se presenta a continuación:

Tabla 2.

Cadenas de Búsqueda

Base de datos	Cadena	Fecha de Búsqueda	Resultado
Scopus	TITLE-ABS-KEY("cyberattack*" OR "cyber attack*" OR "cyber-attack*" OR "cyber threat*" OR "cybersecurity threat*") AND TITLE-ABS-KEY("evolution" OR "historical development" OR	7/5/2024	1557

	"temporal trend*" OR "time series" OR "timeline" OR "chronology" OR "history")		
	TITLE-ABS-KEY("cyberattack*" OR "cyber attack*" OR "cyber-attack*" OR "cyber threat*" OR "cybersecurity threat*") AND TITLE-ABS-KEY("impact" OR "consequence*" OR "implication*" OR "effect*" OR "business impact*" OR "economic impact*") AND TITLE-ABS-KEY("solution*" OR "mitigation" OR "countermeasure*" OR "security measure*" OR "preventive measure*") AND TITLE-ABS-KEY("evolution" OR "historical development" OR "temporal trend*" OR "time series" OR "timeline" OR "chronology" OR "history")	7/5/2024	215
	("cyberattacks" OR "cyber attacks" OR "cyber-attacks" OR "cyber threats" OR "cybersecurity threats") AND ("evolution" OR "historical development" OR "temporal trends" OR "time series")	7/5/2024	5796
ScienceDirect	("cyberattacks" OR "cyber threats") AND ("impact" OR "consequences") AND ("solutions" OR "mitigation") AND ("evolution" OR "time series")	7/5/2024	2514
	TS=(cyberattack* OR "cyber attack*" OR "cyber-attack*" OR "cyber threat*" OR "cybersecurity threat*") AND TS=(evolution OR "historical development" OR "temporal trend*" OR "time series" OR "timeline" OR chronology OR history) AND TS=(type OR technique* OR strategy OR method* OR tactic* OR pattern*)	7/5/2024	223
WoS	TS=(cyberattack* OR "cyber attack*" OR "cyber-attack*" OR "cyber threat*" OR "cybersecurity threat*") AND TS=(evolution OR "historical development" OR "temporal trend*" OR "time series" OR "timeline" OR chronology OR history) AND TS=(impact OR effect* OR consequence* OR implication* OR "business impact*" OR "economic impact*") AND TS=(solution* OR mitigation OR countermeasure* OR "security measure*" OR "preventive measure*")	7/5/2024	1354

Nota. Se establecen las cadenas de búsqueda (variables) para facilitar el encuentro de información.

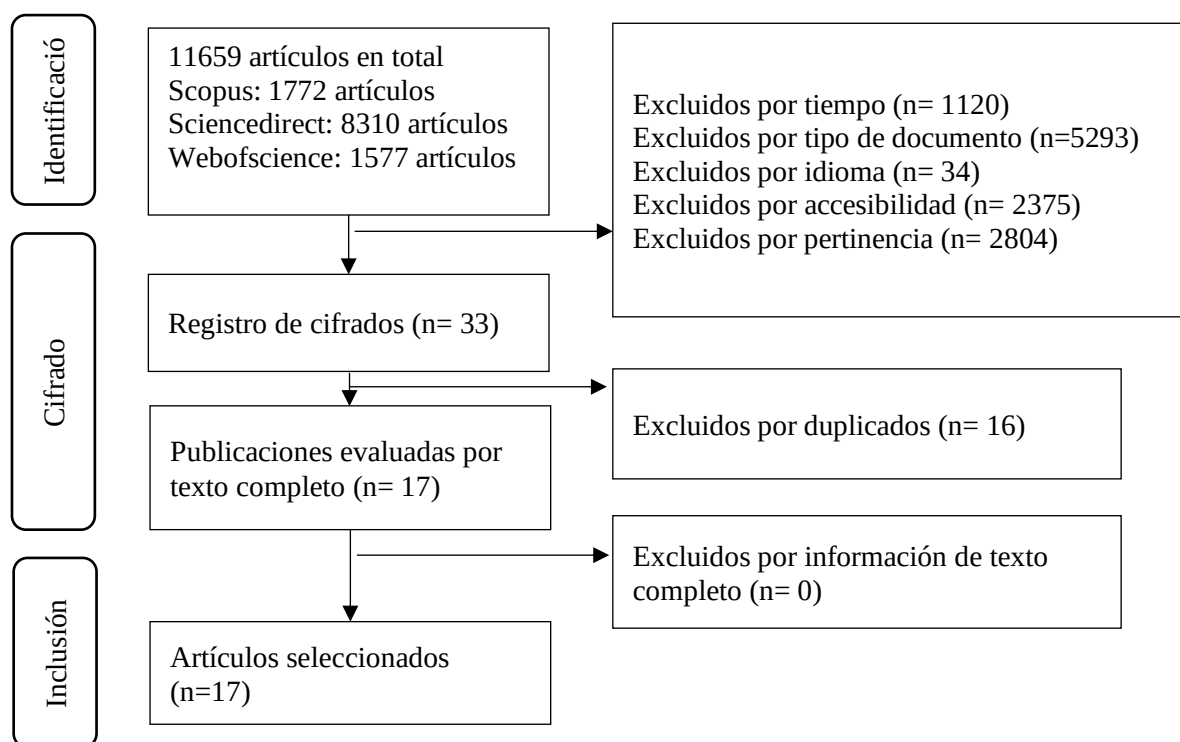
Capítulo III. Propuesta

3.1 Esquema Prisma

El cuadro PRISMA ilustra el proceso de selección de artículos, donde inicialmente se identificaron 11659 artículos (Scopus: 1772, Sciencedirect: 8310, Web of Science: 1577). Tras aplicar criterios de exclusión, se eliminaron 1120 por tiempo, 5393 por tipo de documento, 34 por idioma, 2375 por accesibilidad y 2804 por pertinencia, quedando 33 artículos. Luego, se excluyeron 16 por duplicidad resultando en 17 artículos seleccionados para el estudio. Ningún artículo fue excluido por texto completo. El proceso de selección se detalla en el diagrama a continuación.

Figura 1.

Diagrama de selección de artículos



Nota.: Se destaca la selección de artículos a través del esquema Prisma

La literatura reciente en el campo de la ciberseguridad ha examinado una variedad de aspectos de este tema, incluidas las técnicas para recopilar y analizar datos de inteligencia de amenazas cibernéticas y cómo la inteligencia artificial generativa afecta la privacidad y la

seguridad. Como se observa en el trabajo de Amaro et al. (2022), los estudios han subrayado la importancia de desarrollar marcos metodológicos sólidos que permitan la recolección, el procesamiento y la visualización de datos de inteligencia de amenazas.

La seguridad de los sistemas ciberfísicos y la detección de anomalías en redes complejas son otros temas importantes abordados en la literatura. Para mejorar la seguridad de estos sistemas, investigaciones como las de Gaba et al. (2024) y ADAK et al. (2023) se enfocan en soluciones prácticas de aprendizaje profundo y técnicas avanzadas de detección de anomalías. Los trabajos de Gutiérrez et al. (2024) y Meland et al. (2021), por ejemplo, muestran cómo el análisis detallado y las técnicas innovadoras pueden mejorar significativamente la defensa contra ciberataques en una variedad de industrias mediante el uso de algoritmos de resampling y análisis retrospectivo de incidentes de seguridad marítima.

A continuación, se presenta unas tablas resúmenes de una recopilación efectuada de estudios claves como los mencionados anteriormente, además se destacan los avances en detección de anomalías, la seguridad en sistemas ciberfísicos, y las estrategias para la clasificación de ciberataques. Los artículos seleccionados, publicados en revistas científicas de alto impacto, proporcionan una visión integral y actualizada de los desafíos y soluciones emergentes en ciberseguridad, reflejando tanto los progresos técnicos como las tendencias futuras en la protección de infraestructuras críticas y la gestión de amenazas cibernéticas.

3.2 Resultados

Tabla 3.

Características de los artículos seleccionados

N°	Autores	Título	Año	Revista	DOI
1	Amaro et al., 2022	Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data	2022	Applied Sciences (Switzerland)	10.3390/app12031205
2	Gutiérrez et al., 2024	A detailed study of resampling algorithms for cyberattack classification in engineering applications	2024	PeerJ Computer Science	10.7717/peerj-cs.1975
3	Meland et al., 2021	A retrospective analysis of maritime cyber security incidents	2021	TransNav	10.12716/1001.15.03.04
4	Gaba et al., 2024	Advancements in enhancing cyber-physical system security: Practical deep learning solutions for network traffic classification and integration with security technologies	2024	Mathematical Biosciences and Engineering	10.3934/mbe.2024066
5	ADAK et al., 2023	Anomaly Detection with Gradient Boosting Regressor on HVAC Systems	2023	Journal of Polytechnic	10.2339/politeknik.1379049

6	Zhao et al., 2024	Application-Layer Anomaly Detection Leveraging Time-Series Physical Semantics in CAN-FD Vehicle Networks	2024	Electronics (Switzerland)	10.3390/electronics13020377
7	Lounis y Zulkernine, 2020	Attacks and Defenses in Short-Range Wireless Technologies for IoT	2020	IEEE Access	10.1109/ACCESS.2020.2993553
8	Haner y Knake, 2021	Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity	2021	Journal of Cybersecurity	10.1093/cybsec/tyab003
9	Amanowicz y Kamola, 2022	Building Security Awareness of Interdependent Services, Business Processes, and Systems in Cyberspace	2022	Electronics (Switzerland)	10.3390/electronics11223835
10	Fayans et al., 2020	Cyber security threats in the microbial genomics era: Implications for public health	2020	Eurosurveillance	10.2807/1560- 7917.ES.2020.25.6.1900574
11	Malik et al., 2022	Cyber threats: Taxonomy, impact, policies, and way forward	2022	KSII Transactions on Internet and Information Systems Applied Sciences (Switzerland)	10.3837/tiis.2022.07.017
12	Feeken et al., 2022	Detecting and Processing Anomalies in a Factory of the Future	2022	Sciences (Switzerland)	10.3390/app12168181

13	Alhakami, 2024	Evaluating modern intrusion detection methods in the face of Gen V multi-vector attacks with fuzzy AHP-TOPSIS	2024	PLoS ONE	10.1371/journal.pone.0302559
14	Sultana et al., 2020	Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology	2020	BMC Medical Informatics and Decision Making	10.1186/s12911-020-01275-y
15	Gupta et al., 2023	From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy	2023	IEEE Access	10.1109/ACCESS.2023.3300381
16	Ceccarelli et al., 2018	Threat analysis in systems-of-systems: An emergence-oriented approach	2018	ACM Transactions on Cyber-Physical Systems	10.1145/3234513
17	Yaacoub et al., 2020	Cyber-physical systems security: Limitations, issues and future trends	2020	Microprocessors and Microsystems	10.1016/j.micpro.2020.103201

Nota. Se destaca las principales características de los artículos destacados por medio del Método Prisma

Tabla 4

Resultados

Nº	Autores	Título	Evolución de las Amenazas Cibernéticas	Impacto de Amenazas Cibernéticas a instituciones	Soluciones Propuestas ante las Amenazas Cibernéticas
----	---------	--------	--	--	--

1	Amaro et al., 2022	Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data	Aumentan los ciberataques dirigidos a pequeñas y grandes empresas. Los atacantes explotan las debilidades del sistema, lo que lleva a una demanda urgente de ciber protección. Surgió la inteligencia de ciber amenazas para reconocer indicadores de ciberataques.	El aumento de los ciberataques afecta a la seguridad y el funcionamiento de las instituciones. Falta de profesionales para satisfacer la demanda urgente de ciber protección. Las actualizaciones ad hoc de CTI debilitan la mitigación de ciberataques y la evitación de vulnerabilidades.	Implementa herramientas en tiempo real para comprender y neutralizar rápidamente las amenazas. Desarrollar metodologías que simplifiquen los datos sobre ciber amenazas para un análisis eficaz. Compartir la información sobre amenazas para promover el conocimiento de la situación y la adopción de soluciones rápidas.
2	Gutiérrez et al., 2024	A detailed study of resampling algorithms for cyberattack classification in engineering applications	Los ciberataques evolucionan debido a la interconexión de las industrias y a las sofisticadas soluciones de ciberseguridad. Los conjuntos de datos de ciberataques reales presentan un	Los ciber amenazas afectan negativamente a la seguridad de los datos, las operaciones y la reputación de las instituciones. Las instituciones se enfrentan a pérdidas financieras y consecuencias legales debido a los ciberataques	Los algoritmos de remuestreo mejoran la detección y clasificación de ciberataques en entornos industriales. Los mecanismos de defensa basados en IA mejoran las medidas de ciberseguridad frente a las ciber amenazas en evolución.

			desequilibrio sesgado hacia determinados tráficos. Las medidas de ciberseguridad se mejoran mediante algoritmos de remuestreo para la clasificación de ciberataques.	
3	Meland et al., 2021	A retrospective analysis of maritime cyber security incidents	Las amenazas terroristas en el sector marítimo, en el punto de mira. Ataques de ciber espionaje a Corea del Sur y Japón por "Icefog". El ciberataque a la naviera iraní IRISL provocó la pérdida de datos.	Las instituciones se enfrentan a cortes, robo de información, manipulación y espionaje debido a las actualizaciones periódicas. ciber amenazas. Los ciberataques se dirigen a puertos mal protegidos, lo que provoca costosas interrupciones. Los métodos de acceso remoto en sistemas cerrados crean aperturas de ataque.
4	Gaba et al., 2024	Advancements in enhancing cyber-	Benigno, DoS, R2L, U2R son categorías comunes de	Desarrollar modelos DL para la detección de anomalías en

	physical system security: Practical deep learning solutions for network traffic classification and integration with security technologies	ciberataques. DoS tiene operaciones, provocando datos CPS de forma eficaz. como objetivo hacer que pérdidas financieras y daños a la reputación. Ataques generalización de los modelos las redes o sitios web sean como el DoS hacen DL para la identificación de inaccesibles para los usuarios. Los ataques inaccesibles las redes, ciberataques. Integrar DL con U2R escalan privilegios afectando negativamente a tecnologías de seguridad para obtener el control la experiencia del usuario. mejorar la seguridad de los administrativo de los SPI. sistemas. .	
5	ADAK et al., 2023	Anomaly Detection with Gradient Boosting Regressor on HVAC Systems	Las ciber amenazas evolucionan con la interrupción del IoT en las operaciones, sistemas de calefacción, pérdidas financieras y dañan la reputación. Los ataques se dirigen a sistemas críticos, provocando daños el firmware para evitar se aprovecha para y gastos sustanciales. Los vulnerabilidades. Forme al comprometer sistemas métodos de detección de personal en las mejores críticos. Los ataques a anomalías mejoran la prácticas de ciberseguridad sistemas de calefacción, ciberseguridad y protegen para mitigar las amenazas. ventilación y aire acondicionado pueden autorizado.

- provocar daños considerables.
- 6 Zhao et al., 2024 Application-Layer Anomaly Detection Leveraging Time-Series Physical Semantics in CAN-FD Vehicle Networks Ataques DoS, fuzzing, replay y spoofing simulados en investigación. El método Physical Semantics-Enhanced Anomaly Detection (PSEAD) consigue una gran precisión. Función de pérdida de Huber óptima para reconocer mensajes de ataque. Las ciber amenazas afectan a la seguridad, integridad y continuidad operativa de los datos de las instituciones. Las instituciones se enfrentan a pérdidas financieras, daños a su reputación e información sensible comprometida. Las ciber amenazas pueden interrumpir los servicios, provocando tiempos de inactividad y pérdidas de productividad. Red LSTM con mecanismo de autoatención para la captura de información temporal. Tasa de clasificación errónea del 0,64% en ataques de repetición. Mejora de la precisión en más de un 4% en comparación con los métodos existentes.
- 7 Lounis y Zulkernine, 2020 Attacks and Defenses in Short-Range Wireless Technologies for IoT El historial de ciber amenazas incluye el ataque Mirai dirigido a dispositivos IoT en 2016. El ataque Stuxnet en 2011 tuvo como objetivo filtraciones de datos, Los ciberataques interrumpen las operaciones y provocan pérdidas financieras. Los ataques pueden dar lugar a filtraciones de datos, Los ataques de canal lateral pueden mitigarse mediante enmascaramiento y asignación condicional. Implementación de protocolos RFID para

		infraestructuras críticas comprometiendo	dificultar los ataques de canal
		como las redes eléctricas.	información sensible. Las lateral.
			empresas se enfrentan a
			daños en su reputación
			debido al éxito de los
			ciberataques.
8	Haner y Knake, 2021	Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity	Botnets utilizadas para Los ciberataques interrumpen las operaciones, provocando pérdidas financieras y daños a la reputación. Los ataques DDoS y extorsión de ransomware. Ataques distribuidos de denegación de servicio (DDoS) empreses se enfrentan a violaciones de datos, robos y amenazas de extorsión. Los ciberataques pueden utilizarse para el robo de identidad, el espionaje y los ataques DDoS.
9	Amanowicz y Kamola, 2022	Building Security Awareness of Interdependent Services,	Los ciberataques son cada vez más sofisticados y complejos. La adquisición de información sobre amenazas en tiempo real para la concienciación sobre

Business Processes, and Systems in Cyberspace de información sobre pérdidas financieras y daños seguridad empresarial. amenazas en tiempo real a la reputación. Las Modelización de entidades del es crucial para la seguridad interdependencias ciberespacio para predecir de las empresas. Los complican la gestión de la amenazas y mejorar la modelos de simulación seguridad, provocando resistencia. Mejora de la predicen la evolución de efectos en cascada y concienciación en materia de las amenazas y orientan las consecuencias económicas. seguridad mediante análisis mejoras operativas. Las La concienciación sobre la basados en la simulación para interdependencias ciberseguridad es crucial la protección frente a complican los procesos de para anticiparse a las amenazas. mitigación y recuperación. amenazas y proteger los objetivos empresariales.

- 10 Fayans et al., 2020 Cyber security threats in the microbial genomics era: Implications for public health Los ciberataques evolucionan con los avances tecnológicos y el aumento de las vulnerabilidades. Pérdida de confidencialidad, integridad y disponibilidad de los datos de la empresa. Los sistemas comprometidos pueden utilizarse como vectores de propagación, afectando a las redes. Los ciberataques pueden dar lugar a la Desarrollo de herramientas de vigilancia para secuenciar el ADN de los ciberataques. Evaluar el impacto y la probabilidad de los vectores de ataque con expertos mundiales. Considerar las amenazas en el desarrollo de la tecnología de secuenciación del ADN.

			filtración de datos personales sensibles.	Aplicar medidas de ciberseguridad en el desarrollo de software bioinformático. Realizar evaluaciones de riesgos frecuentes para actualizar las políticas de salud pública.
11	Malik et al., 2022	Cyber threats: Taxonomy, impact, policies, and way forward	Las ciber amenazas surgieron con la evolución de la tecnología informática. Las ciber amenazas incluyen el ciberterrorismo y la ciberguerra. El malware se utiliza habitualmente en las ciber amenazas.	Los ciberataques paralizan las operaciones y cuestan millones en daños. El ransomware cifra los datos y exige un pago para recuperarlos. El malware para detectar ataques avanzados. Mayor atención a la protección de las tecnologías VoIP frente a los ataques de malware
12	Feeken et al., 2022	Detecting and Processing Anomalies in a Factory of the Future	Las ciber amenazas han evolucionado con el aumento de la automatización y la comunicación en	Los ciberataques provocan daños financieros y costes indirectos. Las amenazas internas plantean riesgos debido al acceso a secretos

fábricas. Los ciberataques comerciales. Los clave para la prevención de a la cadena de suministro competidores se dedican al ciberataques aprovechan los servicios espionaje industrial y al de terceros para sabotaje corporativo. comprometer los objetivos. Los ciberdelincuentes atacan activos y disfrazan sus actividades para evitar consecuencias legales.

- 13 Alhakami, Evaluating modern intrusion detection methods in the face of Gen V multi-vector attacks with fuzzy AHP-TOPSIS 2024
- Generación I: Centrada en Daños a los servicios, Los ataques multivectoriales la prevención de virus para erosión de la confianza, Gen V requieren sistemas PC autónomos. exposición de la adaptativos de detección de Generación II: La información. Desafíos a la intrusos. El análisis del ciberdelincuencia existencia corporativa, comportamiento y la organizada lleva al interrupción de los integración de la inteligencia desarrollo de cortafuegos e servicios, erosión de la sobre amenazas mejoran la IDS. Generación III: confianza de la sociedad. precisión de la detección. Los Transición a la mecanismos de respuesta explotación de eficientes son cruciales para la vulnerabilidades defensa contra las ciber informáticas, que requiere amenazas

una seguridad de parches.

Generación IV: Los ciberataques se volvieron sofisticados, exigiendo soluciones de seguridad creativas.

- | | | | | | |
|----|----------------------|---|---|---|--|
| 14 | Sultana et al., 2020 | Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology | Amenazas de Internet clasificadas como interceptación, fabricación, modificación e interrupción. El aumento de las violaciones de datos dio lugar a debates sobre la seguridad en Internet. Las vulnerabilidades incluyen el fraude, el robo de identidad y los ciberataques. | Las filtraciones de datos provocan la exposición de información sensible y violaciones de la privacidad. Las ciber amenazas causan pérdidas financieras y dañan la reputación institucional. Las instituciones se enfrentan a consecuencias legales debido a las violaciones de datos y los ciberataques. | Se implementa la autenticación de dos factores para la seguridad del inicio de sesión. Utiliza blockchain para una pista de auditoría inmutable de las instancias de acceso a los datos. Emplea un control de acceso basado en funciones para garantizar la propiedad de los datos. Descentraliza los datos en blockchain e IPFS para la verificación entre pares. |
| 15 | Gupta et al., 2023 | From ChatGPT to ThreatGPT: Impact of Generative AI in | Los ciberataques evolucionan con la IA, aumentando su | Las ciber amenazas interrumpen las operaciones y provocan | Las herramientas GenAI ayudan en la automatización de la ciberdefensa y la |

Cybersecurity and Privacy

sofisticación y eficacia. Los ataques asistidos por IA transformaron los vectores de los ciberataques, empoderando a los ciberdelincuentes. Las herramientas GenAI benefician tanto a los defensores como a los atacantes en ciberseguridad. GenAI permite la respuesta automatizada a incidentes, la inteligencia sobre amenazas y la codificación segura. Los atacantes aprovechan GenAI para la ingeniería social, el phishing y la creación de malware.

pérdidas financieras. Las instituciones se enfrentan a violaciones de datos que comprometen información sensible. Los ataques pueden dañar la reputación y erosionar la confianza entre las partes interesadas.

inteligencia sobre amenazas. GPT-4 genera guías de respuesta a incidentes para una ciberdefensa rápida. ChatGPT identifica patrones y comportamientos de ataque para la ciberdefensa.

- 16 Ceccarelli et al., 2018 Threat analysis in systems-of-systems: An emergence-oriented approach
- Los ciberataques evolucionan debido a los cambios en los sistemas y a las nuevas amenazas. Las herramientas de análisis de amenazas se adaptan a la evolución de los ciberataques para las consecuencias. El malware corrompe los sistemas internos, provocando las interrupciones operativas. Las intrusiones en los subsistemas en los sistemas de comunicación interrumpen los servicios físicos. Las amenazas estructurales se dirigen a componentes específicos sin tener en cuenta las interacciones dentro del sistema.
- Los ciberataques pueden poner en peligro los aparatos inteligentes de las redes domésticas. Las debilidades de seguridad en sistemas críticos pueden acarrear graves administradores de SoS ciberfísicos. Amenazas emergentes y amenazas internas, provocando estructurales clasificadas en enfoques de análisis de amenazas. La metodología de análisis de amenazas identifica las amenazas emergentes y determina las estrategias de mitigación correspondientes.
- La metodología de análisis de amenazas identifica las amenazas emergentes en los sistemas en evolución. Se proponen estrategias de gestión de riesgos para administrar de SoS ciberfísicos. Amenazas emergentes y amenazas internas, provocando estructurales clasificadas en enfoques de análisis de amenazas. La metodología de análisis de amenazas identifica las amenazas emergentes y determina las estrategias de mitigación correspondientes.

- 17 Yaacoub et al., 2020 Cyber-physical systems security: Limitations, issues and future trends Ataques físicos que han sufrido los sistemas industriales CPS en los últimos años. Los ciberataques causan pérdidas económicas y violaciones de la gestión de la información en las empresas. La mitigación de riesgos requiere una estrategia de gestión bien construida. Implantar medidas de seguridad cibernética y física. Ciberataques clasificados por motivos políticos, religiosos y delictivos pueden provocar desde 2000. Las ciber interrupciones operativas en organismos responsables. Las amenazas se centraron en las empresas. Analizar los ciberataques y coordinarse con los responsables. la seguridad del IoT industrial debido a varios motivos.

Nota. Análisis de los principales resultados de los artículos seleccionados

3.3 Discusión

La evolución de las amenazas cibernéticas ha sido un tema de creciente preocupación en los últimos años, como lo destacan Amaro et al. (2022) al señalar que los ciberataques han aumentado significativamente, afectando tanto a pequeñas como a grandes empresas debido a las debilidades explotadas en los sistemas. Gutiérrez et al. (2024) subrayan que la interconexión de las industrias y el desarrollo de soluciones de ciberseguridad más sofisticadas han influenciado esta evolución, creando conjuntos de datos sesgados hacia ciertos tipos de tráfico. Por su parte, Meland et al. (2021) ponen de manifiesto las amenazas específicas al sector marítimo y las infraestructuras críticas, como el ciberespionaje dirigido a Corea del Sur y Japón, lo que refleja una preocupación global por la seguridad cibernética en diferentes sectores.

El impacto de estas amenazas es significativo y multifacético. Gutiérrez et al. (2024) y Gaba et al. (2024) coinciden en que los ciberataques afectan gravemente la seguridad de los datos, las operaciones y la reputación de las instituciones, llevando a pérdidas financieras y consecuencias legales. Zhao et al. (2024) añaden que estos ataques afectan la seguridad, integridad y continuidad operativa de los datos, provocando tiempos de inactividad y pérdidas de productividad. Además, Lounis y Zulkernine (2020) enfatizan que los ataques a infraestructuras críticas como las redes eléctricas pueden resultar en interrupciones significativas, pérdidas financieras y filtraciones de datos sensibles, subrayando la necesidad de una protección robusta en estos sectores.

Las soluciones propuestas para mitigar estas amenazas son diversas y abarcan desde el uso de tecnologías avanzadas hasta la implementación de políticas globales. Amaro et al. (2022) proponen el uso de herramientas en tiempo real para neutralizar rápidamente las amenazas y desarrollar metodologías que simplifiquen el análisis de datos sobre ciberamenazas, promoviendo

la adopción de soluciones rápidas a través del intercambio de información. Gutiérrez et al. (2024) sugieren mejorar la detección y clasificación de ciberataques mediante algoritmos de remuestreo y mecanismos de defensa basados en inteligencia artificial. Gaba et al. (2024) y Zhao et al. (2024) destacan la implementación de modelos de aprendizaje profundo para la detección de anomalías y la mejora de la seguridad de los sistemas ciberfísicos, evidenciando la importancia de la innovación tecnológica en la ciberseguridad.

Sin embargo, existen enfoques contrastantes en la literatura. Mientras que Amaro et al. (2022) y Gutiérrez et al. (2024) se centran en el análisis de datos y algoritmos de inteligencia artificial para la detección de amenazas, Meland et al. (2021) y Lounis y Zulkernine (2020) se enfocan en mejorar la seguridad a través de la educación y la implementación de medidas avanzadas en sectores específicos. Haner y Knake (2021) recomiendan la implementación de protocolos anti-spoofing y el fortalecimiento de las normas cibernéticas globales a través de acuerdos multilaterales, contrastando con las soluciones tecnológicas y metodológicas específicas propuestas por otros autores. Estas diversas perspectivas reflejan la complejidad de las amenazas cibernéticas y la necesidad de enfoques multidisciplinarios para abordar los desafíos de seguridad en el entorno digital actual.

Conclusiones

La evolución de las amenazas cibernéticas ha demostrado ser un proceso continuo y en expansión. La interconexión creciente de las industrias y el desarrollo de tecnologías de ciberseguridad más avanzadas han influido significativamente en la naturaleza de los ciberataques, presentando tanto nuevos desafíos como oportunidades para mejorar la seguridad. Es esencial mantenerse actualizado con las tendencias emergentes en ciberseguridad para anticipar y combatir eficazmente las amenazas futuras.

Las empresas han experimentado un impacto notable debido a las amenazas cibernéticas, afectando sus operaciones internas y su reputación. Los ataques pueden provocar pérdidas financieras importantes y complicaciones legales, además de generar costos asociados con la interrupción de operaciones y la pérdida de productividad. Los riesgos son aún mayores para las infraestructuras críticas, cuya vulnerabilidad puede tener graves implicaciones para la seguridad nacional y la estabilidad económica.

Las soluciones propuestas para enfrentar las amenazas cibernéticas son variadas y reflejan la diversidad de desafíos presentados. Se destacan herramientas avanzadas y algoritmos de inteligencia artificial para mejorar la detección y neutralización de amenazas en tiempo real, así como modelos de aprendizaje profundo para la identificación de anomalías y la protección de sistemas ciberfísicos. Además, se sugiere un enfoque más integral que incluye la implementación de normas cibernéticas globales y acuerdos multilaterales, indicando que la cooperación internacional es clave para abordar las amenazas cibernéticas a gran escala.

Recomendaciones

Para optimizar la detección y neutralización de amenazas cibernéticas, es esencial implementar herramientas que operen en tiempo real y desarrollar algoritmos avanzados. Estos métodos permiten una respuesta rápida y eficaz frente a los ciberataques, ofreciendo protección tanto a pequeñas como a grandes empresas. La aplicación de modelos de aprendizaje profundo en la detección de anomalías y en la mejora de la seguridad de los sistemas ciberfísicos resulta igualmente crucial, ya que han demostrado ser efectivos en la identificación y mitigación de ciber amenazas.

Asimismo, se recomienda fomentar la cooperación internacional mediante la creación de normas cibernéticas globales y la firma de acuerdos multilaterales para reforzar la defensa contra ataques a gran escala. La educación y formación en ciberseguridad, especialmente en sectores críticos, es fundamental para mejorar la capacidad de respuesta ante los ataques. Además, el intercambio de información sobre ciber amenazas entre organizaciones es vital, ya que facilita la adopción de soluciones rápidas y efectivas, promoviendo una defensa más sólida y coordinada contra las amenazas cibernéticas.

Bibliografía

- Abohatem, A. Y., y Ba-Alwi, F. M. (2024). Cybersecurity Maturity Assessment of Information Systems for Yemen Telecoms. *International Journal of Intelligent Systems and Applications in Engineering*, 12(8s), 539–548.
- ADAK, M. F., KİBAR, R., y OVAZ, K. (2023). Anomaly Detection with Gradient Boosting Regressor on HVAC Systems. *Journal of Polytechnic*, 0900, 0–3. <https://doi.org/10.2339/politknik.1379049>
- Alhakami, W. (2024). Evaluating modern intrusion detection methods in the face of Gen V multi-vector attacks with fuzzy AHP-TOPSIS. *PLoS ONE*, 19(5 May), 1–14. <https://doi.org/10.1371/journal.pone.0302559>
- Alqudhaibi, A., Krishna, A., Jagtap, S., Williams, N., Afy-Shararah, M., y Salonitis, K. (2024). Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. *Discover Food*, 4(1). <https://doi.org/10.1007/S44187-023-00071-7>
- Alsmadi, D., Maqousi, A., y Abuhussein, T. (2024). Engaging in cybersecurity proactive behavior: awareness in COVID-19 age. *Kybernetes*, 53(1), 451–466. <https://doi.org/10.1108/K-08-2022-1104>
- Amanowicz, M., y Kamola, M. (2022). Building Security Awareness of Interdependent Services, Business Processes, and Systems in Cyberspace. *Electronics (Switzerland)*, 11(22). <https://doi.org/10.3390/electronics11223835>
- Amaro, L. J. B., Azevedo, B. W. P., de Mendonca, F. L. L., Giozza, W. F., Albuquerque, R. de O., y Villalba, L. J. G. (2022). Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data. *Applied Sciences (Switzerland)*, 12(3). <https://doi.org/10.3390/app12031205>

- Aygul, K., Mohammadpourfard, M., Kesici, M., Kucuktezcan, F., y Genc, I. (2024). Benchmark of machine learning algorithms on transient stability prediction in renewable rich power grids under cyber-attacks. *Internet of Things (Netherlands)*, 25. <https://doi.org/10.1016/J.IOT.2023.101012>
- Ceccarelli, A., Zoppi, T., Vasenev, A., Mori, M., Ionita, D., Montoya, L., y Bondavalli, A. (2018). Threat analysis in systems-of-systems: An emergence-oriented approach. *ACM Transactions on Cyber-Physical Systems*, 3(2). <https://doi.org/10.1145/3234513>
- Cen, M., Jiang, F., Qin, X., Jiang, Q., y Doss, R. (2024). Ransomware early detection: A survey. *Computer Networks*, 239. <https://doi.org/10.1016/J.COMNET.2023.110138>
- Cervera García, A., y Goussens, A. (2024). Cybersecurity and use of ICT in the health sector. *Atencion Primaria*, 56(3). <https://doi.org/10.1016/J.APRIM.2023.102854>
- Consejo de la Unión Europea. (2024, January 25). *Ciberseguridad: cómo combate la UE las amenazas cibernéticas*. Consejo de La Unión Europea. <https://www.consilium.europa.eu/es/policies/cybersecurity/>
- Doriguzzi-Corin, R., y Siracusa, D. (2024). FLAD: Adaptive Federated Learning for DDoS attack detection. *Computers and Security*, 137. <https://doi.org/10.1016/J.COSE.2023.103597>
- Fayans, I., Motro, Y., Rokach, L., Oren, Y., y Moran-Gilad, J. (2020). Cyber security threats in the microbial genomics era: Implications for public health. *Eurosurveillance*, 25(6), 1–8. <https://doi.org/10.2807/1560-7917.ES.2020.25.6.1900574>
- Feeken, L., Kern, E., Szanto, A., Winnicki, A., Kao, C. Y., Wudka, B., Glawe, M., Mirzaei, E., Borchers, P., y Burghardt, C. (2022). Detecting and Processing Anomalies in a Factory of the Future. *Applied Sciences (Switzerland)*, 12(16), 1–24. <https://doi.org/10.3390/app12168181>

- Fernández Pinto, M., y Herrera Romero, W. R. (2018). *Revolución 4.0 y Ciberseguridad. Universidad Del Rosario.*
- Gaba, S., Budhiraja, I., Kumar, V., y Makkar, A. (2024). Advancements in enhancing cyber-physical system security: Practical deep learning solutions for network traffic classification and integration with security technologies. *Mathematical Biosciences and Engineering*, 21(1), 1527–1553. <https://doi.org/10.3934/mbe.2024066>
- Gupta, M., Akiri, C., Aryal, K., Parker, E., y Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*, 11(July), 80218–80245. <https://doi.org/10.1109/ACCESS.2023.3300381>
- Gutiérrez, Ó. M., Núñez, J. C. S., Ávila, M., y Caro, A. (2024). A detailed study of resampling algorithms for cyberattack classification in engineering applications. *PeerJ Computer Science*, 10. <https://doi.org/10.7717/peerj-cs.1975>
- Haner, J. K., y Knake, R. K. (2021). Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity. *Journal of Cybersecurity*, 7(1), 1–15. <https://doi.org/10.1093/cybsec/tyab003>
- Hernández-Sampieri, R., y Torres, C. P. M. (2018). *Metodología de la Investigación: Las Rutas Cuantitativa, Cualitativa y Mixta.* Edamsa Impresiones.
- Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J., y Sugali, M. N. (2024). DDoS attack detection and mitigation using deep neural network in SDN environment. *Computers & Security*, 138, 103661. <https://doi.org/10.1016/J.COSE.2023.103661>
- Lounis, K., y Zulkernine, M. (2020). Attacks and Defenses in Short-Range Wireless Technologies for IoT. *IEEE Access*, 8, 88892–88932. <https://doi.org/10.1109/ACCESS.2020.2993553>

- M, F. (2023, October 26). *Amenazas Persistentes Avanzadas (APT)*. LinkedIn. https://es.linkedin.com/pulse/amenazas-persistentes-avanzadas-apt-francisco-moraga-fgiff?trk=public_post
- Macas, M., Wu, C., y Fuertes, W. (2024). Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems. *Expert Systems with Applications*, 238. <https://doi.org/10.1016/J.ESWA.2023.122223>
- Malik, A. W., Abid, A., Farooq, S., Abid, I., Nawaz, N. A., y Ishaq, K. (2022). Cyber threats: Taxonomy, impact, policies, and way forward. In *KSII Transactions on Internet and Information Systems* (Vol. 16, Issue 7). <https://doi.org/10.3837/tiis.2022.07.017>
- Meland, P. H., Bernsmed, K., Wille, E., Rødseth, J., y Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav*, 15(3), 519–530. <https://doi.org/10.12716/1001.15.03.04>
- Mohamed, N. (2024). Securing transportation web applications: An AI-driven approach to detect and mitigate SQL injection attacks. *Journal of Transportation Security*, 17(1). <https://doi.org/10.1007/S12198-023-00269-X>
- Núñez Mateo, R. A. (2024, January 22). *Inteligencia Artificial y Ciberseguridad: Desafíos y Oportunidades*. LinkedIn. https://www.linkedin.com/pulse/inteligencia-artificial-y-ciberseguridad-desaf%C3%ADos-n%C3%BA%C3%B1ez-mateo--dggpe?trk=news-guest_share-article
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Alonso-Fernández, S. (2021). Declaración PRISMA 2020: una guía actualizada para la

publicación de revisiones sistemáticas. *Revista Española de Cardiología*, 74(9), 790–799.

<https://doi.org/10.1016/j.recesp.2021.06.016>

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Revista Española de Cardiología*, 74(9), 790–799. <https://doi.org/10.1016/J.RECESP.2021.06.016>

Panorama de Amenazas de la ENISA. (2020). Amenazas principales Informe Panorama de Amenazas de la ENISA . *ENISA*.

Pigola, A., Da Costa, P. R., Ferasso, M., y Cavalcanti da Silva, L. F. (2023). Enhancing cybersecurity capability investments: Evidence from an experiment. *Technology in Society*, 102449. <https://doi.org/10.1016/J.TECHSOC.2023.102449>

Qureshi, S. G., y Shandilya, S. K. (2022). Nature-inspired adaptive decision support system for secured clustering in cyber networks. *Multimedia Tools and Applications*. <https://doi.org/10.1007/S11042-022-13336-7>

Raval, K. J., Jadav, N. K., Rathod, T., Tanwar, S., Vimal, V., y Yamsani, N. (2024). A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions. *International Journal of Critical Infrastructure Protection*, 44. <https://doi.org/10.1016/J.IJCIP.2023.100647>

Securita Operation Center. (2022, November 30). *El primer gusano informático de la historia cumple 34 años*. INFORDISA. <https://www.infordisa.com/soc/el-primer-gusano-informatico-de-la-historia-cumple-34-anos/>

- Sobrido Prieto, M., y Rumbo Prieto, J. M. (2018). La revisión sistemática: pluralidad de enfoques y metodologías. *Enfermería Clínica*, ISSN 1130-8621, Vol. 28, Nº. 6, 2018, Págs. 387-393, 28(6), 387–393.
<https://dialnet.unirioja.es/servlet/articulo?codigo=6661150&info=resumen&idioma=ENG>
- Sultana, M., Hossain, A., Laila, F., Taher, K. A., y Islam, M. N. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics and Decision Making*, 20(1), 1–10.
<https://doi.org/10.1186/s12911-020-01275-y>
- Wabi, A. A., Idris, I., Olaniyi, O. M., y Ojeniyi, J. A. (2023). DDOS ATTACK DETECTION IN SDN: Method of attacks, Detection techniques, Challenges and Research Gaps. *Computers & Security*, 103652. <https://doi.org/10.1016/J.COSE.2023.103652>
- Wang, X., Yang, X., Liang, X., Zhang, X., Zhang, W., y Gong, X. (2024). Combating alert fatigue with AlertPro: Context-aware alert prioritization using reinforcement learning for multi-step attack detection. *Computers and Security*, 137. <https://doi.org/10.1016/J.COSE.2023.103583>
- Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., y Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 77, 103201. <https://doi.org/10.1016/j.micpro.2020.103201>
- Zhao, R., Luo, C., Gao, F., Gao, Z., Li, L., Zhang, D., y Yang, W. (2024). Application-Layer Anomaly Detection Leveraging Time-Series Physical Semantics in CAN-FD Vehicle Networks. *Electronics (Switzerland)*, 13(2). <https://doi.org/10.3390/electronics13020377>

Anexos