Instituto Superior Tecnológico VICENTE ROCAFUERTE

REVISTA INSTITUTO SUPERIOR TECNOLÓGICO VICENTE ROCAFUERTE (REVISTVR)
Vol. 1 No. 1 – 2025

Evolución de las Amenazas Cibernéticas en Redes Corporativas

Evolución de las amenazas cibernéticas en las redes corporativas

Juan Almeida Vasquez

Edison Rodríguez Sares

Evolución de las Amenazas Cibernéticas en Redes Corporativas

Evolución de las Amenazas Cibernéticas en las Redes Corporativas

Autor: Juan Almeida Vasquez[1], Edison Rodríguez Sares[2]

Cómo citar: Almeida J.,Rodriguez, E (2025). Evolución de las Amenazas Cibernéticas en Redes Corporativas .*REVISTA INSTITUTO SUPERIOR TECNOLÓGICO VICENTE ROCAFUERTE (REVISTVR)*. 1*(1)*, pp.: 1-22.

RESUMEN

El estudio tuvo como objetivo evaluar la evolución de las amenazas cibernéticas y su impacto en las redes corporativas a lo largo de la última década. Utilizando un análisis documental, se identificaron patrones y tendencias clave en el ámbito de la ciberseguridad. Los resultados revelaron un aumento significativo en la complejidad y frecuencia de los ataques, impulsado por avances tecnológicos, la globalización y la adaptación de sofisticadas técnicas delictivas. Se destacó la importancia de implementar tecnologías avanzadas, como la inteligencia artificial y el aprendizaje automático, para detectar y contrarrestar estas amenazas de manera efectiva. Además, se subrayó la necesidad de promover una cultura corporativa de seguridad cibernética entre todos los empleados, desde la alta dirección hasta el personal operativo, para mitigar los riesgos. Las conclusiones sugieren que una estrategia de seguridad adaptativa, integral y proactiva es esencial para proteger las infraestructuras críticas y asegurar la continuidad operativa de las organizaciones. Este estudio ofrece recomendaciones prácticas, como la adopción de políticas de seguridad actualizadas y la capacitación continua del personal, para fortalecer la ciberseguridad y contribuir a un entorno digital más seguro

[1] Egresado, Instituto Superior Tecnológico Vicente Rocafuerte, Guayaquil - Ecuador, js.almeida@istvr.edu.ec , https://orcid.org/0009-0003-0493-6295

[2] Docente, Instituto Superior Tecnológico Vicente Rocafuerte, Guayaquil – Ecuador, erodriguez@istvr.edu.ec, https://orcid.org/0000-0003-2182-4431

y confiable.

PALABRAS CLAVE: Amenazas cibernéticas, Redes corporativas, Malware, Ransomware, Phishing Prevención

ABSTRACT

The study aimed to evaluate the evolution of cyber threats and their impact on corporate networks over the past decade. Using a comprehensive documentary analysis, key patterns and trends in the field of cybersecurity were identified. The results revealed a significant increase in the complexity and frequency of attacks, driven by technological advances, globalization, and the adaptation of sophisticated criminal techniques. The importance of implementing advanced technologies, such as artificial intelligence and machine learning, to effectively detect and counter these threats was highlighted. Furthermore, the need to promote a corporate culture of cybersecurity among all employees, from top management to operational staff, was emphasized to mitigate risks. The conclusions suggest that an adaptive, comprehensive, and proactive security strategy is essential to protect critical infrastructures and ensure the operational continuity of organizations. This study offers practical recommendations, such as adopting updated security policies and continuous personnel training, to strengthen cybersecurity and contribute to a safer and more reliable digital environment.

KEYWORDS: Cyber threats, corporate networks, Malware, Ransomware, Phishing, Prevention

INTRODUCCIÓN

En una era en la que la transformación digital avanza a pasos agigantados, la seguridad de la información se ha convertido en un pilar fundamental para la estabilidad y confianza de las redes corporativas. La sociedad moderna está profundamente conectada con la tecnología, y cada vez se vuelve más crucial para las actividades cotidianas. La delincuencia, como era de esperar, evoluciona al ritmo de los avances tecnológicos, adaptándose a los nuevos sistemas y desarrollando innovadoras técnicas delictivas mediante la creación de tecnologías que permiten vulnerar la privacidad y los sistemas técnicos actuales. (Rozas, 2022)

Imaginemos un escenario en el que una gran empresa sufre un ataque cibernético que compromete la integridad de su infraestructura de red, resultando en la pérdida de datos sensibles y afectando su reputación. Este ejemplo no solo ilustra la gravedad de las amenazas cibernéticas actuales, sino que también resalta la importancia de estudiar y comprender su evolución.

A continuación, presento un recuadro con algunos de los ataques cibernéticos más relevantes de la historia:

Tabla 1.
Algunos de los ataques cibernéticos más relevantes de la historia

Descripción	Detalles
WikiLeaks (Noviembre 2010)	Fundada por Julian Assange en 2006, WikiLeaks ganó notoriedad en 2010 al publicar 251,287 telegramas diplomáticos. Entre ellos, se encuentran 55,000 cables relacionados con España y 40,000 más que mencionan a España.
Sony PlayStation Network (Abril 2011)	Un ataque comprometió los datos personales, incluyendo nombres y correos electrónicos, de 77 millones de cuentas de PlayStation Network. El servicio quedó inoperativo durante una semana.
Dropbox (Agosto 2012)	Aunque el ataque ocurrió en 2012, su magnitud se descubrió en 2016, afectando a más de 68 millones de usuarios. Un empleado había utilizado su contraseña de LinkedIn, lo que permitió a los hackers acceder a la red de Dropbox.
Target (Diciembre 2013)	Un ataque histórico a Target comprometió datos personales y bancarios de 70 millones de clientes durante la temporada de compras navideñas, utilizando malware en los dispositivos de punto de venta.
eBay (Mayo 2014)	eBay solicitó a 145 millones de usuarios cambiar sus contraseñas tras un ataque que comprometió datos personales. La empresa fue criticada por tardar en notificar a sus clientes.
Elecciones en EE.UU. (Diciembre 2015)	Un error de una empresa de marketing expuso la información de 191 millones de votantes estadounidenses, haciendo accesibles registros sensibles en la web.
Friend Finder	Más de 412 millones de cuentas en sitios para adultos fueron expuestas,

Descripción	Detalles
(Noviembre 2016)	resultando en extorsión y vergüenza para los usuarios afectados.
Uber (Noviembre 2017)	Uber pagó a hackers para eliminar datos robados y ocultar un ataque que expuso información personal de 57 millones de clientes y 7 millones de conductores.
Cambridge Analytica (Marzo 2018)	Cambridge Analytica utilizó información de 50 millones de perfiles de Facebook sin permiso para influir en las elecciones presidenciales de EE.UU. en 2016.
Facebook (Marzo 2019)	Números de teléfono y identificaciones de usuario de Facebook fueron expuestos en un servidor no protegido, afectando a 419 millones de usuarios.

Nota. Adaptado de "Los diez ciberataques más grandes de la década" por *Rufino Contreras, 2023.*

Tabla 2.
Algunos ciberataques del 2024

Año	Descripción	Tipo de Ataque
2024	Robo de datos personales y financieros de más de 2 millones de clientes del Banco do Brasil, utilizados para cometer delitos financieros por un total de 40 millones de reales.	Robo de Información Financiera
2024	Filtración de datos personales de más de 3 millones de usuarios de Interbank, incluyendo nombres, números de tarjetas, teléfonos, fechas de nacimiento y detalles de transacciones bancarias.	Exposición de Datos
2024	Ciberataque a Coppel, afectando a 1,800 tiendas en México, causando una pérdida de $15 millones de dólares en ingresos, atribuido al ransomware Lockbit 3.0.	Ransomware
2024	Ataque de ransomware a Air-e, afectando sistemas y servicios, y paralizando operaciones logísticas y gestión financiera.	Ransomware
2024	Ataque del grupo RansomHub a la Consejería Jurídica del Poder Ejecutivo Federal (CJEF), secuestrando más de 300GB de información, incluyendo contratos y presupuestos.	Ransomware
2024	Publicación en Telegram de más de 100 mil fotografías de ciudadanos argentinos robadas en 2021 del Registro Nacional de las Personas (RENAPER), poniendo en riesgo a las personas ante ataques de phishing y suplantación de identidad.	Filtración de Información
2024	Ataque de ransomware Medusa al Grupo Bimbo, afectando bases de datos, datos financieros, facturas, correspondencia e información de empleados y clientes.	Ransomware

Nota. Adaptado de "7 incidentes de ciberseguridad que marcaron el 2024 en América Latina" por Cristian Ali Bravo, 2024.

El presente artículo tiene como propósito analizar la evolución de las amenazas cibernéticas en redes corporativas, destacando los principales hitos y cambios en las tácticas de ataque a lo largo del tiempo. Se abordarán las generalidades y antecedentes del tema, estableciendo un marco teórico que permita contextualizar la problemática en el momento actual.

La investigación se centra en identificar las variables que intervienen en la seguridad de las redes corporativas, así como en evaluar las estrategias de prevención y mitigación de amenazas. Se revisarán estudios recientes y se destacarán los aportes de diversos autores en el campo de la ciberseguridad, proporcionando una visión integral de los desafíos y soluciones implementadas.

La justificación de este trabajo radica en la creciente necesidad de proteger las redes corporativas frente a amenazas cada vez más sofisticadas y persistentes. La importancia de fomentar una cultura de seguridad dentro de las organizaciones es crucial para minimizar los riesgos y garantizar la continuidad operativa.

En el mundo actual, es crucial generar conciencia sobre la protección de la información tanto personal como empresarial. Sin embargo, muchas pequeñas y medianas empresas en Latinoamérica todavía no disponen de personal especializado o están en el proceso de establecer un departamento de ciberseguridad. (Segovia, 2021)

Es claro que las actividades en el ciberespacio no solo ponen en peligro la información y la reputación de las personas afectadas por la sustracción de fotos personales o el hackeo de sus correos electrónicos, sino que también amenazan las infraestructuras de las entidades públicas. (Villacís, 2022)

Los objetivos de la investigación es Analizar la evolución histórica de las amenazas cibernéticas. La hipótesis planteada es que, a pesar de la evolución constante de las amenazas cibernéticas, es posible desarrollar estrategias efectivas de prevención y mitigación mediante la adopción de tecnologías avanzadas y la promoción de una cultura corporativa de seguridad.

A través de un enfoque deductivo, este artículo recorrerá de lo general a lo particular, proporcionando una secuencia lógica y cronológica que permita comprender la evolución de las amenazas cibernéticas y las respuestas de seguridad adoptadas en el entorno corporativo.

MATERIALES Y MÉTODOS

Para este estudio se empleó una metodología mixta, combinando enfoques cualitativos y cuantitativos para proporcionar una visión integral de las amenazas cibernéticas en redes corporativas. Este enfoque permitió obtener datos detallados y cuantificables, así como una comprensión profunda de las experiencias y percepciones de los profesionales en el campo de la ciberseguridad.

La información fue recopilada a través de dos métodos principales: análisis documental y análisis de incidentes reales.

1. **Análisis Documental**: Se realizó una revisión exhaustiva de artículos científicos, informes técnicos y estudios de caso publicados sobre ciberseguridad y amenazas cibernéticas en redes corporativas. Esto permitió obtener una base sólida de información y datos preexistentes que sustentan la investigación.

.

- **Muestra**: La muestra se basó en la selección de artículos científicos y estudios de caso relevantes, así como en la identificación de incidentes de seguridad significativos ocurridos en los últimos años.

Se utilizó un diseño descriptivo y exploratorio, adecuado para analizar tanto datos cuantitativos como cualitativos. El análisis documental proporcionó una visión amplia de las amenazas y estrategias de mitigación, mientras que el análisis de incidentes reales ofreció ejemplos concretos y relevantes.

Los datos recopilados a través del análisis documental y de incidentes fueron organizados y categorizados para facilitar su análisis. Se aseguró la integridad y confiabilidad de la información recopilada.

1. **Análisis Cuantitativo**: Los datos provenientes de artículos científicos y estudios de caso fueron analizados utilizando técnicas estadísticas descriptivas para identificar patrones y tendencias en las amenazas cibernéticas.
2. **Análisis Cualitativo**: Los incidentes de seguridad reales fueron analizados mediante el método de análisis de contenido, identificando temas recurrentes y categorizando la información relevante.

La información fue procesada utilizando software especializado para el análisis. Los resultados se presentaron de forma clara y concisa.

RESULTADOS Y DISCUSIÓN

La conclusión cardinal que se deriva de los resultados es que la evolución de las amenazas cibernéticas ha llevado a un aumento en la complejidad y frecuencia de los ataques, lo que requiere una constante adaptación de las estrategias de seguridad en las redes corporativas.

La tecnología ha avanzado rápidamente en los últimos 50 años, lo que ha dado lugar a una serie de ciberdelitos. Tanto la tecnología como las actividades ilegales han ido perfeccionándose conjuntamente durante todo este tiempo. Nos encontramos en medio de una revolución tecnológica sin precedentes. La Industria 4.0 ha llegado para quedarse y continuará desarrollándose, pero como cualquier revolución, también trae consigo actividades delictivas. Anteriormente, los delitos eran de naturaleza física, como el robo de bancos, asaltos violentos en las calles y diversas estafas. Sin embargo, estos delitos han evolucionado junto con la sociedad y ahora se están digitalizando de manera significativa. (Rozas, 2022)

Los delincuentes cibernéticos no solo afectan a las computadoras, sino también a teléfonos y otros dispositivos conectados. Estos ataques son efectivos gracias a la manipulación psicológica, que abarca desde llamadas telefónicas tradicionales hasta correos electrónicos y mensajes instantáneos, y a menudo resultan en ransomware. Con el avance de estas técnicas, incluido el desarrollo de malware polimórfico, se prevé un aumento significativo del riesgo de ataques de ingeniería social en Ecuador. (Garzón, Navas, Illicachi, Espinoza, & Estrella, 2024)

El análisis de varios estudios y reportes sobre ciberseguridad en Ecuador muestra una situación compleja y dinámica. Los ataques de ingeniería social han aumentado de manera alarmante, como lo refleja el considerable incremento de ciberdelitos reportados por la Policía Nacional del Ecuador. Desde el phishing hasta el smishing, estos ataques destacan una significativa vulnerabilidad en la población, a pesar de los esfuerzos del gobierno por mejorar la seguridad digital. (Garzón, Navas, Illicachi, Espinoza, & Estrella, 2024)

Los ciberconflictos, como los ciberataques, ciberguerras, ciberterrorismo y ciberdelitos, están en

constante incremento a nivel global. Esto obliga a los gobiernos a fortalecer la seguridad en el ámbito cibernético e institucionalizar la ciberseguridad y la ciberdefensa. Para desarrollar una estrategia eficaz en ciberseguridad, es necesario contar con políticas y doctrinas cibernéticas bien definidas, así como con una estructura institucional adecuada para la ciberdefensa y la seguridad. (PORTILLO, 2022)

Tras analizar los tipos más frecuentes de ataques informáticos, se puede concluir que la mejor forma de defensa radica en comprender cómo operan estos ataques y cómo logran vulnerar la seguridad de la información. Esto demuestra que los ciberdelincuentes tienen diversas alternativas para afectar los sistemas, como ataques mediante adware, denegación de servicio distribuido (DDoS), doxing, gusanos, phishing, ransomware, spyware, troyanos y virus. Estos ataques se fundamentan principalmente en explotar las vulnerabilidades humanas a través de la ingeniería social, con el fin de obtener acceso no autorizado a datos sensibles e infraestructuras críticas. (GUAÑA, y otros, 2022)

Una campaña tradicional de ransomware se hace evidente solo después de que se complete el proceso de cifrado de archivos, mediante una nota de rescate o un mensaje explicativo del evento y su propósito. Es posible que el ransomware y otros efectos secundarios se produzcan fácilmente. El ransomware gestionado por humanos se caracteriza por su prolongada ejecución y alta probabilidad de éxito. El archivo ejecutable del ransomware será detectado como una nota de rescate clara durante la operación no anunciada, aumentando la probabilidad de éxito. Es complicado identificar el tipo de amenaza y su impacto. Para responder a incidentes de este tipo, es necesario evaluar la posibilidad de que dichos incidentes puedan incluir el uso de ransomware. (Chimmanee & Jantavongso, 2024). Los ataques DDoS representan desafíos considerables para las organizaciones a nivel global, afectando de manera disruptiva la disponibilidad e integridad de sus infraestructuras de red. (Anley, Genovese, Agostinello, & Piur, 2024)

Los ataques de ransomware, que extorsionan a las víctimas bloqueando sus dispositivos o encriptando sus archivos hasta que se pague un rescate, se han convertido en una de las mayores amenazas para la seguridad de las redes. (Mingcan, Deng, Jiang, & Doss, 2024)

El ámbito de los ataques DDoS ha crecido significativamente en términos de tamaño y complejidad. Estos ataques avanzados presentan desafíos considerables, causando interrupciones en los servicios, aumentando las latencias de la red y agotando por completo los recursos informáticos. (Liu, y otros, 2024)

Tabla 3.
Algunas consecuencias de ataques de Ransomware

Descripción	Detalles
Rescates Pagados en 2023 (primeros seis meses)	$449.1 millones
Costo Total Estimado de Ataques en 2023	$898.6 millones
Ingresos por Ransomware en 2021	$939.9 millones
Empresas Afectadas por Ransomware en 2023 (hasta agosto)	>72% a nivel mundial
Empresas Afectadas por Ransomware (2018-2023)	>50% anualmente
Proporción de Ciberataques Representados por Ransomware en la Primera Mitad de 2023	24%

Descripción	Detalles
Costo Promedio de Ataque de Ransomware en 2023	$5.13 millones (13% más que en 2022)
Tiempo Promedio para Detectar y Contener un Ataque de Ransomware	Aproximadamente un año
Responsabilidad del Grupo de Ransomware LockBit en 2023	45% del total de ataques en la primera mitad del año
Porcentaje de Ataques de Ransomware que Resultaron en Pago de Rescate en el Segundo Trimestre de 2023	34% (mínimo histórico)

Nota. Adaptado de "Estadísticas relativas al Ransomware que debes conocer en 2024" por Jorge Felix, 2025.

Tabla 4.
Incremento de ataques maliciosos

Descripción	Detalles
Archivos maliciosos distribuidos al día en 2022	400,000 (incremento del 5% en comparación con 2021)
Ransomware en 2022	Incremento del 181% en comparación con 2021
Archivos maliciosos detectados en 2022	Aproximadamente 122 millones (6 millones más que en 2021)
Archivos maliciosos que atacaron dispositivos con Windows en 2022	320,000 archivos diarios (85% del total de archivos maliciosos)
Proporción de archivos maliciosos sobre Microsoft Office en 2022	Incremento del 236%
Compartición de archivos maliciosos en Android en 2022	Incremento del 10%

Nota. Adaptado de "Los ataques maliciosos crecen hasta los 400.000 diarios" por Kaspersky, 2022.

Tabla 5.
Algunas de las características del Phishing

Descripción	Detalles
Prevalencia del Phishing	El phishing es la forma más común de ciberdelincuencia y afecta a todos los sectores.
Objetivo de los Ataques de Phishing	Son comunicaciones engañosas que se presentan como fuentes confiables con la intención de obtener información sensible de las personas.
Sofisticación y Especificidad	Estos ataques se están volviendo más avanzados y dirigidos a objetivos específicos con el avance de la tecnología.
Inicio de Ciberataques	El 91% de todos los ciberataques comienzan con un correo electrónico de phishing.
Vulnerabilidad	Cualquiera puede ser víctima de un ataque de phishing bien ejecutado, independientemente de sus conocimientos tecnológicos.
Importancia de la Conciencia	Es crucial entender las tácticas de los phishers y aprender a identificar sus señales de advertencia para navegar por el mundo en línea de manera segura.
Análisis del Phishing	Se exploran datos clave sobre phishing, incluyendo tendencias globales de ataques, contramedidas, estrategias de concienciación, tipos de ataques, prevalencia, y el impacto en las víctimas, para ayudar a proteger nuestras identidades en línea.

Nota. Adaptado de "25 estadísticas de phishing que te mantendrán alerta el 2025" por Satish Shethi, 2025.

Tabla 6.
Algunas consecuencias de ataques DDos

Descripción	Detalles
Ataques DDoS Mitigados en el 1.er Trimestre de 2024	Cloudflare bloqueó automáticamente 4,5 millones de ataques DDoS, lo que representa un aumento del 50% en comparación con el año anterior.
Incremento de Ataques DDoS contra DNS	Hubo un aumento del 80% en los ataques DDoS contra DNS en comparación con el mismo período del año anterior, manteniéndose como el vector de ataque principal.
Ataques DDoS contra Suecia	Los ataques aumentaron un 466% tras su adhesión a la OTAN, replicando el patrón observado durante la adhesión de Finlandia en 2023.
Proporción de Ataques DDoS en el 1.er Trimestre de	Los ataques DDoS HTTP aumentaron un 93% interanual y un 51% respecto al trimestre anterior.

Descripción	Detalles
2024	
Ataques DDoS a la Capa de Red (Capas 3/4)	Aumentaron un 28% interanual y un 5% respecto al trimestre anterior.
Comparación de Ataques DDoS en 2023 y 2024	En el 1.er trimestre de 2024, Cloudflare mitigó el 32% del total de ataques DDoS que mitigó en todo 2023.

Nota. Adaptado de "Informe sobre las amenazas DDos en el 1.er trimestre de 2024" por Omer Yoachimik, Jorge Pacheco, 2024.

Los ciberataques representan una preocupación cada vez mayor para empresas, organizaciones y usuarios. En los últimos años, la cantidad y variedad de técnicas de ciberataque han aumentado de manera exponencial. Las aplicaciones web son uno de los vectores de ataque más frecuentemente explotados. Estas aplicaciones brindan diversas funcionalidades, como la consulta de datos, la realización de operaciones bancarias y la compra en línea. Entre los principales problemas de seguridad de las infraestructuras web se encuentran las inyecciones, en particular las inyecciones SQL. (Crespo, y otros, 2023)

Tabla 7.
Algunas consecuencias de la inyección

Descripción	Detalles
Heartland Payment Systems (2008)	Un procesador de pagos importante sufrió una de las mayores violaciones de datos debido a una inyección SQL, exponiendo aproximadamente 130 millones de números de tarjetas de crédito y débito.
Sony Pictures (2011)	La red de Sony fue gravemente comprometida por un ataque de inyección SQL que afectó a 77 millones de cuentas de PlayStation Network, costando a Sony unos 170 millones de dólares.
Yahoo! (2012)	Yahoo! Voices experimentó una violación masiva de datos que reveló cerca de medio millón de direcciones de correo electrónico y contraseñas.
TalkTalk (2015)	Este gigante de las telecomunicaciones sufrió un ataque cibernético que comprometió los datos personales de aproximadamente 157,000 clientes.

Nota. Adaptado de "¿Que es la inyección SQL? Los 4 ejemplos más terribles" por Tibor Moes, 2024.

Interpretaciones y Explicaciones

- **Principios y Regularidades**: La evolución de las amenazas cibernéticas sigue patrones de sofisticación y especialización, donde los atacantes emplean técnicas cada vez más avanzadas para vulnerar las defensas corporativas.
- **Generalizaciones del Trabajo**: Los resultados sugieren que la implementación de tecnologías avanzadas y la creación de una cultura corporativa de seguridad son esenciales para minimizar los riesgos y proteger las redes corporativas.

Novedad Científica y Perspectivas

- **Novedad Científica**: Este estudio proporciona una visión actualizada y detallada de las tendencias y amenazas cibernéticas, destacando la importancia de una respuesta adaptativa y proactiva.
- **Perspectivas teóricas**: Las conclusiones de este estudio abren nuevas vías para investigar cómo la inteligencia artificial y otras tecnologías emergentes pueden mejorar la ciberseguridad en redes corporativas.

La inteligencia artificial ha cambiado la manera en que se realizan los ciberataques, permitiendo a los ciberdelincuentes crear herramientas y técnicas más avanzadas. Esto ha llevado a un aumento tanto en la frecuencia como en la severidad de los ataques, constituyendo una amenaza considerable para la ciberseguridad. Los ciberataques basados en inteligencia artificial engloban una amplia variedad de actividades maliciosas, que incluyen la creación de noticias falsas para influir en la opinión pública, el phishing para obtener información confidencial, el robo de identidad con fines fraudulentos y la infiltración de sistemas informáticos para obtener acceso no autorizado. (Rendón, 2024)

- **Aplicaciones Prácticas**: Las empresas pueden aplicar los hallazgos de este estudio para fortalecer sus estrategias de seguridad y reducir la vulnerabilidad a ciberataques.

Pertinencia del Trabajo

- **Gestión Académica y Condición de Investigador-Docente**: Este trabajo es relevante para la gestión académica, ya que proporciona una base para futuros estudios y la formación de profesionales en ciberseguridad. Además, destaca la importancia del rol del investigador-docente en la promoción de prácticas de seguridad efectivas.

CONCLUSIÓN

Los resultados obtenidos en este estudio destacaron una evolución significativa en las amenazas cibernéticas que afectan a las redes corporativas. Este trabajo se centró en analizar la creciente sofisticación y frecuencia de estos ataques, y cómo impactan en la operatividad y economía de las empresas. La metodología utilizada, combinando análisis documental y estudios de incidentes reales, permitió identificar patrones y tendencias clave en el ámbito de la ciberseguridad.

La principal implicación de los resultados radica en la necesidad urgente de que las empresas adopten estrategias proactivas y adaptativas para proteger sus redes. Se demostró que la implementación de tecnologías avanzadas, como la inteligencia artificial para la monitorización de redes, y la promoción de una cultura corporativa de seguridad son esenciales para mitigar los riesgos y asegurar la continuidad operativa.

Mi postura frente al tema es que, aunque las amenazas cibernéticas continúan evolucionando, es posible desarrollar y aplicar medidas efectivas de prevención y mitigación. Esto requiere un enfoque integral que combine el uso de tecnologías avanzadas, la educación continua del personal y la revisión constante de políticas y procedimientos de seguridad. Los datos obtenidos y la argumentación teórica respaldan esta postura, subrayando la importancia de estar siempre un paso adelante de los ciberatacantes.

En conclusión, este estudio aporta una visión detallada y actualizada de las amenazas cibernéticas en redes corporativas y ofrece recomendaciones prácticas para fortalecer la ciberseguridad. La adopción de estas medidas no solo protegerá a las empresas de posibles ataques, sino que también garantizará la integridad y confidencialidad de la información, promoviendo un entorno digital seguro y confiable.

BIBLIOGRAFIA

Anley, M. B., Genovese, A., Agostinello, D., & Piur, V. (2024). Robust DDoS attack detection with adaptive tranfer learnig.

Bravo, C. A. (2024). 7 incidentes de ciberseguridad que marcaron el 2024 en América Latina.

Brian, K. (2024). *The Target Breach*.

Chimmanee, K., & Jantavongso, S. (2024). DIGITAL FORENSIC OF MAZE RANSOMWARE: A case of electricity distributor enterprise in ASEAN.

Contreras, R. (2023). Los diez ciberataques más grandes de la década.

Crespo, I., Campazas, A., Guerrero, Á., Riego, V., Álvarez, C., & Fernandéz, C. (2023). SQL injection attack detection in network flow data.

Felix, J. (2024). Estadísticas relativas al Ransomware que debes conocer en 2024.

Garzón, C., Navas, C., Illicachi, A., Espinoza, R., & Estrella, G. (2024). ANÁLISIS DE LOS ATAQUES DE INGENIERIÍA SOCIAL EN ECUADOR.

GUAÑA, J., SÁNCHES, A., CHÉRREZ, P., CHULDE, L., JARAMILLO, P., & PILLJO, C. (2022). *ATAQUES INFORMÁTICOS MAS COMUNES EN EL MUNDO DIGITALIZADO.*

Kaspersky. (2022). Obtenido de Kaspersky: https://www.bing.com/ck/a?!&&p=5c09b15c859951849ddd8d6a7d554d886d7eca92c5cb86e88511eece026dc2cbJmltdHM9MTczOTQ5MTIwMA&ptn=3&ver=2&hsh=4&fclid=00ecebd0-352a-65c6-2749-

fe80348564d5&psq=Nota.+Adaptado+de+%e2%80%9cLos+ataques+maliciosos+crecen+hasta+los+400.0

Liu, Y., Han, Y., Chen, H., Zhao, B., Wang, X., & Liu, X. (2024). IGED: Towards Intellegent DDos Detection Model Using Improved Generalized Entropy and DNN.

Mingcan, C., Deng, X., Jiang, F., & Doss, R. (2024). Zero-Ran Sniff: Zero-daiy ransomware early detection method based on zero-shot learning.

Moes, T. (2024). ¿Que es la inyección SQL? Los 4 ejemplos más terribles.

PORTILLO, L. A. (2022). *ANÁLISIS DE LOS TIPOS DE ATASQUES CIBRNÉTICOS OCURRIDOS EN COLOMBIA DURANTE LA PANDEMIA COVID-19 ENTRE LOS AÑOS 2020 Y 2021.*

Rendón, A. D. (2024). Impacto de la inteligencia artificial en los ciberataques.

Rozas, J. J. (2022). *CIBERDELINCUENCIA: EVOLUCIÓN Y RELACIÓN CON LA ACTUAL SITUACCÓN DE PANDEMIA. NUEVAS MODALIDADES Y NUEVAS PROBLEMÁTICAS.*

Segovia, M. R. (2021). PREVENCIÓN EN CIBERSEGURIDAD: ENFOCADA A LOS PROCESOS DE IONFRAESTRUCTURA TECNOLOGICA.

Shethi, S. (2025). 25 estadísticas de phishing que te mantendrán alerta el 2025.

Villacís, R. P. (2022). Ciberceguridad y Ciberdefensa: Perspectiva de la situación actual en Ecuador.

Yoachimik, O., & Pacheco, J. (s.f.). Nota. Adaptado de Informe sobre las amenazas DDos en el 1.er trimestre de 2024” .