Revista Científica DISCIPLINARES (2025). Vol. 4 (2)
ISSN: 2955-8905 (En línea)
https://iisunsa.com/index.php/Inicio/issue/archive

REVISIÓN SISTEMÁTICA

Estrategias de Ciberseguridad en la Reducción de Incidentes en Entornos de Trabajo Remoto: Una Revisión Sistemática

Cybersecurity Strategies in Incident Reduction in Remote Work Environments: A Systematic Review

Oscar Gabriel Alcazar Gutierrez

Universidad Nacional de San Agustín

https://orcid.org/0009-0001-5059-4068

Harieth Maressa Bernedo Cordova

Universidad Nacional de San Agustín

https://orcid.org/0009-0004-3113-0059

Daythia Chauca Florian

Universidad Nacional de San Agustín

https://orcid.org/0009-0009-0457-0629

Isiredhy Humberto Valdivia Ponce

Universidad Nacional de San Agustín

https://orcid.org/0009-0009-2399-3176

Recibido: 26/04/2025
Revisado: 27/06/2025
Aceptado: 28/06/2025
Publicado: 30/06/2025

Correspondencia: *

Correo electrónico: oalcazarg@unsa.edu.pe

Resumen

INTRODUCCIÓN: El incremento del trabajo remoto ha expuesto a las organizaciones a mayores riesgos de ciberseguridad, generando la necesidad de estrategias efectivas para mitigar incidentes. Este estudio aborda el impacto de diversas medidas de ciberseguridad en la reducción de riesgos en este contexto. MÉTODO: Se realizó una revisión sistemática de la literatura utilizando la metodología PRISMA. Se seleccionaron y analizaron 19 estudios relevantes de bases de datos reconocidas, centrados en autenticación multifactorial, capacitación, herramientas de monitoreo basadas en inteligencia artificial y diferencias sectoriales en la implementación de medidas de seguridad. RESULTADOS: Los hallazgos destacan que la autenticación multifactorial reduce los accesos no autorizados hasta en un 95% en sectores altamente tecnificados, mientras que las herramientas basadas en inteligencia artificial logran tasas de detección temprana superiores al 90%. Asimismo, la capacitación continua en ciberseguridad disminuye los errores humanos hasta en un 50%, fomentando una cultura organizacional más segura. Sin embargo, sectores con recursos limitados, como el educativo, enfrentan barreras significativas para implementar estas soluciones. DISCUSIÓN: Este análisis resalta la importancia de combinar tecnologías avanzadas con programas de formación continua y políticas inclusivas para cerrar las brechas sectoriales. Además, se enfatiza la necesidad de desarrollar tecnologías accesibles y marcos regulatorios sólidos para garantizar una respuesta efectiva frente a amenazas futuras.

Palabras clave: Ciberseguridad, Trabajo remoto, Autenticación multifactor, Capacitación en ciberseguridad, Inteligencia artificial.

Abstract

INTRODUCTION: The rise of remote work has increased organizational exposure to cybersecurity risks, highlighting the need for effective strategies to mitigate incidents. This study examines the impact of various cybersecurity measures on risk reduction in this context. METHOD: A systematic review of the literature was conducted using the PRISMA methodology. Nineteen relevant studies were selected and analyzed from reputable databases, focusing on multi-factor authentication, training, AI-based monitoring tools, and sectoral differences in security measures implementation. RESULTS: Findings reveal that multi-factor authentication reduces unauthorized access by up to 95% in highly tech-enabled sectors, while AI-based tools achieve early threat detection rates exceeding 90%. Continuous cybersecurity training reduces human errors by up to 50%, fostering a more secure organizational culture. However, resource-

constrained sectors, such as education, face significant barriers to implementing these solutions. DISCUSSION: This analysis underscores the importance of combining advanced technologies with continuous training programs and inclusive policies to bridge sectoral gaps. Additionally, it highlights the need to develop accessible technologies and robust regulatory frameworks to ensure effective responses to future threats.

Key words: Cybersecurity, Remote work, Multi-factor authentication, Cybersecurity training, Artificial intelligence.

Introducción

El desarrollo tecnológico a lo largo del tiempo ha cambiado los modelos tradicionales de trabajo, tales como los modelos presenciales, cuya característica principal era una supervisión directa por parte de la jefatura. En este modelo, la comunicación era cara a cara y dependía mucho del espacio físico disponible, mientras que la infraestructura de red estaba más enfocada en sistemas internos que externos, dado que los riesgos externos no eran una preocupación significativa al no haber grandes conexiones hacia el exterior. Sin embargo, la irrupción de los nuevos modelos, como el trabajo remoto, ha transformado completamente esta dinámica. Dicho modelo, impulsado notablemente durante la pandemia de COVID-19, ha llevado a las organizaciones a adaptarse a entornos digitales mucho más abiertos y a repensar sus estrategias operativas. Esta nueva forma de trabajar ha incrementado significativamente los riesgos en las empresas, tanto públicas como privadas, al abrir acceso a diferentes tipos de usuarios dentro de la organización y dejando expuestas diversas brechas de seguridad, no solo para los empleados de la organización, sino también para actores externos malintencionados. Estas vulnerabilidades han provocado un notable aumento en los incidentes cibernéticos, siendo el trabajo remoto señalado como un factor crucial en su proliferación (Čergeť & Hudec, 2023; Feng et al., 2020). Por esta razón, se vuelve imperativo no solo implementar medidas de seguridad más eficientes, sino también fomentar una cultura organizacional que priorice la ciberseguridad, desde la formación continua de los trabajadores hasta el diseño de infraestructuras tecnológicas robustas y resilientes, capaces de anticiparse a las amenazas emergentes.

El trabajo desde casa ha mostrado el lado más sensible de las empresas en temas de vulnerabilidades en red. Los últimos años han sido identificados ataques masivos, los cuales han sido orientados intencionalmente hacia los empleados que trabajan bajo esta modalidad; representando un riesgo latente de seguridad al poder acceder a datos de carácter sensible. Las empresas han realizado esfuerzos desmedidos por disminuir los riesgos sin embargo la

preocupación organizacional sigue presente en la actualidad, ya que un ataque puede ser muy perjudicial para los diferentes ámbitos de la empresa.

Teniendo en cuenta lo mencionado se determina que es imprescindible el desarrollo de planes orientados a ciberseguridad para que sean implementados en el trabajo desde casa. Este artículo se basa en la necesidad de consolidar el conocimiento actual y sugerir una alternativa práctica para optimizar las políticas de seguridad cibernética.

El artículo se divide en cinco secciones principales. La introducción expone la relevancia del tema y define los objetivos del estudio. La metodología describe el uso del enfoque PRISMA para la selección y análisis de los artículos revisados. Los resultados exponen los hallazgos principales en relación con las preguntas de investigación planteadas. La discusión analiza e interpreta estos resultados, destacando su importancia. Por último, las conclusiones, resume los aportes del estudio y propone líneas de investigación futura.

Metodología

Para realizar este artículo, se aplicó la metodología PRISMA, como una de las mejores opciones para realizar una revisión sistemática y metaanálisis a partir de investigaciones de las estrategias de ciberseguridad en la reducción de incidentes en entornos de trabajo remoto. De esta manera se pudo trabajar con más facilidad las etapas de identificación, selección y síntesis. Como guía las siguientes preguntas de investigación (PICO):

RQ1: ¿Qué tan efectiva es la autenticación multifactor en la reducción de accesos no autorizados en entornos de trabajo remoto?

RQ2: ¿Cuál es el impacto de la capacitación en ciberseguridad en la prevención de ataques de phishing en trabajadores remotos?

RQ3: ¿Existe una diferencia significativa en la cantidad de incidentes de ciberseguridad entre sectores con diferentes niveles de implementación de medidas de seguridad en trabajo remoto?

RQ4: ¿Cómo impacta la formación en ciberseguridad en la reducción de errores humanos en entornos de trabajo remoto?

RQ5: ¿Cómo contribuyen las herramientas de monitoreo de red a la detección temprana de amenazas en trabajadores remotos?

Fórmula PICO:

Población (P)

("remote workers" OR "remote employees" OR "employees" OR "organizations" OR "companies" OR "IT teams")

Intervención (I)

("cybersecurity" OR "information security" OR "data protection" OR "network security" OR "cyber protection")

Contexto (C)

("remote work" OR "telework" OR "telecommuting" OR "distance work" OR "hybrid environment" OR "post-pandemic")

Resultado (O)

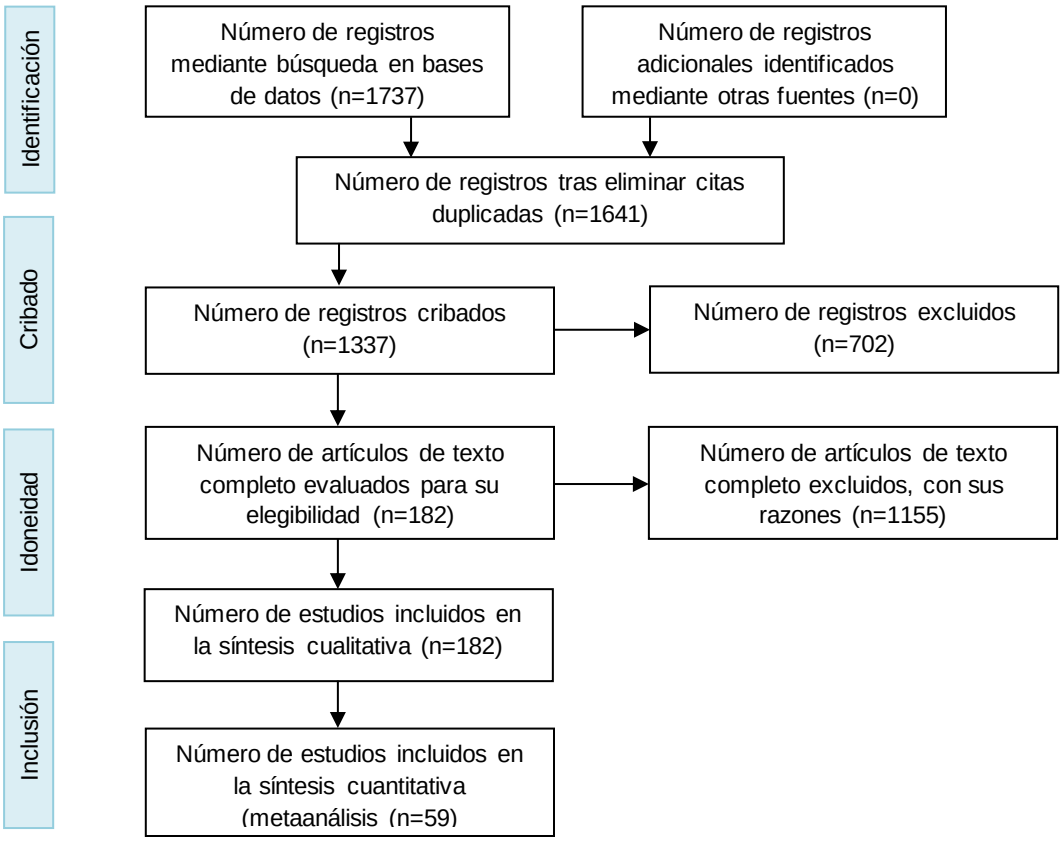
("cyberattack prevention" OR "security breach reduction" OR "security improvement" OR "sensitive information protection" OR "risk mitigation").

Definición de criterios de inclusión y exclusión:

- Utilizamos para búsqueda en bases de datos : Scopus, IEEE Xplore y ScienceDirect.
- Selección de estudios: De 50 artículos seleccionados inicialmente, se redujeron a 19, para poder llegar a este número reducido se aplicaron criterios en base a la relevancia del contenido de cada artículo, respecto a las preguntas de investigación planteadas.
- Extracción de datos: Todo fue realizado en base a las preguntas de investigación RQ1-RQ5.
- Análisis: Se efectuó a partir de la relación del artículo que correspondía con los cinco puntos principales de investigación. Los hallazgos se agruparon en torno a las preguntas de investigación, identificando y destacando los puntos de mayor interés.

Figura 1

Matriz PRISMA



Nota. Elaboración propia basada en la metodología PRISMA

Resultados y Análisis

- Sobre la eficiencia de la autenticación multifactor, esta ha resultado ser bastante efectiva según (Feng et al., 2020; Sstla et al., 2020), esta herramienta permitió que los accesos no autorizados mejoren su efectividad hasta en un 95% en los sectores más vulnerables como son el financiero y el tecnológico, sectores que han decidido implementar esta herramienta como vital barrera para su acceso. Sin embargo, en otros sectores, no se ha implementado de la misma forma, porque es una inversión que implica un costo elevado para ellos, así como han identificado que el acceso sería más complicado para su tipo de usuarios (baja usabilidad) (Pranggono & Arabo, 2021).

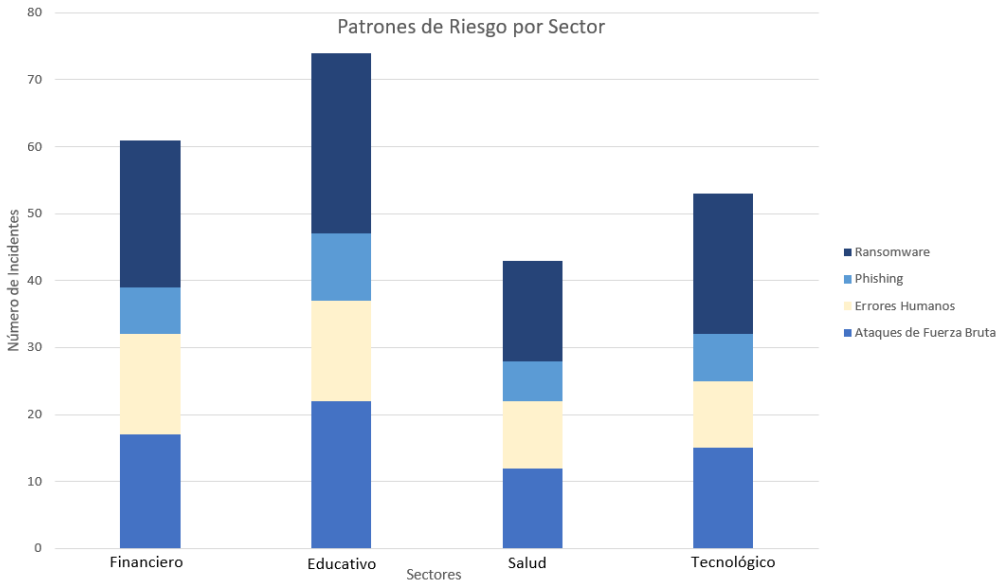
- El impacto de realizar las capacitaciones en ciberseguridad ha permitido mejorar en 60% de evitar ataques por phishing en trabajadores remotos capacitados (Pranggono & Arabo, 2021; Flores et al., 2023). A manera de reforzar estas capacitaciones, se realizaron simulaciones prácticas y entrenamientos con una frecuencia regular, de manera que los empleados identifiquen cada vez mejor los correos maliciosos, volviendo estas mejores prácticas como parte de la correcta navegación en el trabajo remoto (Nyarko & Fong, 2023).

Cabe resaltar, que este tipo de capacitaciones fortalecen la cultura organizacional de la empresa, incentivando un desempeño laboral consciente y disminuyendo los riesgos cibernéticos (Avarias et al., 2024).

- Efectivamente, se tiene una diferencia marcada en la cantidad de incidentes de ciberseguridad dependiendo del sector. Los sectores que invierten en herramientas de ciberseguridad son el financiero y el tecnológico, estas inversiones, dan fruto cuando se ven menores tasas de incidentes a diferencia de otros sectores. Por otro lado, los sectores como el educativo y el sector salud, son identificados con menor presupuesto, por lo que enfrentan mayores vulnerabilidades y políticas de seguridad menos desarrolladas (Flores et al., 2023; Whitty et al., 2024). A partir de ello, según (Jakimoski, 2023) las políticas de gobierno deben tomar especial atención a las diferencias marcadas en la figura 1, para poder mejorar la ciberseguridad en todos los sectores, y que se garantice la información sensible en todo ámbito.

Figura 2

Análisis de Patrones de Riesgo por Sector



Nota. El gráfico representa el número de Patrones de riesgo distribuidos por cada sector, es decir la cantidad de accidentes relacionados

- El impacto de recibir formación en ciberseguridad ha demostrado que puede mitigar errores humanos en entornos de trabajo remoto, identificados como una de las principales causas de incidentes cibernéticos. Programas de formación orientados en el manejo seguro

de software y configuraciones técnicas, han conseguido disminuir estos errores hasta en un 50% (Working from Home, 2020; Klein & Zwilling, 2024). Este resultado destaca la necesidad de priorizar la educación tecnológica personalizada, adaptándola a las necesidades de cada organización para maximizar su efectividad.

- Las herramientas de monitoreo de red basadas en inteligencia artificial (IA) como Tecnologías avanzadas, los firewalls inteligentes y los sistemas de detección de intrusiones, han alcanzado tasas de éxito superiores al 90% en la detección temprana de amenazas (Mandal et al., 2021; Glorin, 2021), siendo esta una importante contribución. Además, la IA mejora la trazabilidad de los ciberataques y optimiza la capacidad de respuesta mediante el análisis avanzado de datos (Sun et al., 2020). Estas soluciones, combinadas con marcos estratégicos bien diseñados, han demostrado ser esenciales para una gestión de riesgos más eficiente y proactiva en diversas organizaciones (Kanter-Ramirez et al., 2020).

Otros hallazgos relevantes:

- La integración de marcos de gestión de riesgos avanzados permite una evaluación continua de la madurez de la ciberseguridad en empresas (Jakimoski, 2023).

- Las estrategias de recuperación ante ciberataques son esenciales para minimizar pérdidas económicas y garantizar la continuidad operativa (Leroy & Zolotaryova, 2023).

- La adopción de modelos de comportamiento preventivo entre los empleados es un factor crítico para fortalecer la defensa contra incidentes cibernéticos (Wright et al., 2024).

- Autenticación multifactor: La MFA reduce accesos no autorizados hasta en un 95%, mostrando una alta efectividad en sectores financieros y tecnológicos (Feng et al., 2020; Sstla et al., 2020).

- Capacitación en ciberseguridad: Los programas formativos disminuyen incidentes de phishing hasta en un 60%, destacando el impacto de simulaciones y entrenamientos activos (Pranggono & Arabo, 2021; Flores et al., 2023).

- Diferencias sectoriales: Sectores como el educativo enfrentan mayores riesgos debido a la falta de recursos tecnológicos (Flores et al., 2023; Whitty et al., 2024).

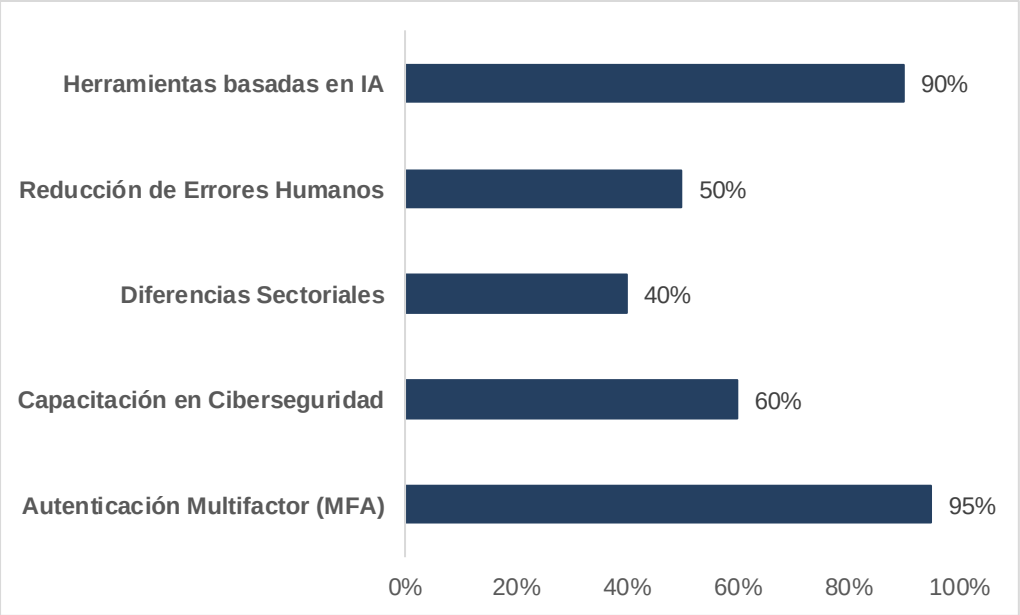
- Reducción de errores humanos: La formación continua puede reducir los errores operativos hasta en un 50%, lo que enfatiza su importancia (Working from Home, 2020).

- Herramientas basadas en IA: Tecnologías como firewalls inteligentes y sistemas de detección de intrusiones son críticas para la protección adaptativa en tiempo real (Mandal et al., 2021; Bispham et al., 2022).

Los artículos revisados muestran que la capacitación en ciberseguridad es el método más estudiado, seguida de la autenticación multifactor y las herramientas basadas en inteligencia artificial. Aunque con menor frecuencia, también se destacan los marcos de gestión de riesgos y las estrategias de recuperación, que son claves para fortalecer la seguridad y preparar a las organizaciones frente a posibles incidentes cibernéticos. Tal como se muestra en la figura a continuación:

Figura 3

Eficiencia de los métodos analizados (%)



Nota. El gráfico representa la eficiencia relativa de cada estrategia en la reducción de incidentes de ciberseguridad, basada en estudios revisados. Elaboración propia.

Discusión

La autenticación multifactor (MFA) ha demostrado ser ampliamente efectiva en la reducción de accesos no autorizados, alcanzando una disminución de hasta un 95% en sectores como el financiero y tecnológico (Feng et al., 2020; Sstla et al., 2020). Este resultado se alínea con los hallazgos de Mandal et al. (2021), quienes analizaron que la integración de MFA con herramientas de monitoreo basadas en IA aumentó aún más la precisión en la detección de

accesos no autorizados, logrando tasas de éxito superiores al 98%. Por otro lado, investigadores como Pranggono y Arabo (2021) han señalado que los sectores menos tecnificados enfrentan barreras significativas para la implementación de MFA, lo que limita su efectividad y dificulta su aplicación.

En relación a la capacitación en ciberseguridad, los programas educativos han mostrado reducir incidentes de phishing hasta en un 60%, resaltando el impacto de simulaciones y escenarios realistas (Flores et al., 2023; Nyarko & Fong, 2023). Sin embargo, Avarias et al. (2024) destacan que programas diseñados con teorías del comportamiento interpersonal pueden aumentar este porcentaje, logrando mejoras de hasta un 75% en la identificación de amenazas. Estos hallazgos demuestran la importancia de personalizar los enfoques educativos según las características del personal y los riesgos organizacionales.

Por otro lado, la utilización de herramientas basadas en inteligencia artificial (IA), como firewalls inteligentes y sistemas de detección de intrusiones, han logrado tasas de éxito superiores al 90% en la detección temprana de amenazas (Mandal et al., 2021; Glorin, 2021). Estos resultados son consistentes con los estudios de Sun et al. (2020), quienes desarrollaron modelos avanzados de trazabilidad de ataques utilizando analítica de datos, obteniendo una efectividad del 93%. La IA también ha permitido optimizar marcos de gestión de riesgos, mejorando la capacidad organizacional para enfrentar posibles incidentes (Kanter-Ramirez et al., 2020).

Si nos enfocamos en la disminución de errores humanos, la capacitación continua ha permitido disminuir los errores operativos relacionados con configuraciones incorrectas y manejo de software hasta en un 50% (Working from Home, 2020; Klein & Zwilling, 2024). Wright et al. (2024) complementan esta evidencia, resaltando que el uso de programas formativos basados en la teoría del comportamiento interpersonal puede lograr reducciones del 65% en errores humanos, reforzando la importancia de estrategias educativas adaptadas al contexto organizacional.

Finalmente, se observa que los sectores con mayores niveles de inversión, como el financiero y tecnológico, presentan menores tasas de incidentes debido a su capacidad para adoptar herramientas avanzadas (Flores et al., 2023; Whitty et al., 2024). Sin embargo, sectores como el educativo y el de salud presentan mayores desafíos significativos por la falta de recursos tecnológicos, lo que enmarca la necesidad de políticas inclusivas que nivelen estas brechas (Jakimoski, 2023).

Conclusión

La revisión sistemática de la literatura permite resaltar un notable cambio y mejora antes y después de la pandemia del COVID -19, porque el trabajo remoto fue la primera opción en el mundo para poder seguir trabajando y mantenerse a salvo.

Por ello,se dio mayor énfasis para implementar estrategias de ciberseguridad integrales que ayuden a mitigar los riesgos relacionados en el ámbito del trabajo remoto. De las principales herramientas de ciberseguridad, se tiene: La autenticación multifactor (MFA) y para complementar el uso de herramientas en ciberseguridad, se ha demostrado que la capacitación a los empleados del trabajo remoto, mejora también los resultados respecto a incidentes relacionados con el phishing, una de las principales formas de ciberataque. Además de disminuir errores humanos y promover una cultura organizacional orientada a la seguridad. Adicionalmente, las herramientas basadas en inteligencia artificial (IA), han demostrado ser altamente efectivas para prevenir accesos no autorizados y ayudan a detectar amenazas en tiempo real.

En los resultados se puede evidenciar las diferencias significativas entre sectores; mientras que el financiero y el tecnológico logran implementar soluciones avanzadas gracias a su capacidad de inversión, sectores como el educativo enfrentan mayores vulnerabilidades debido a limitaciones presupuestarias. Esto demuestra la necesidad urgente de políticas inclusivas que reduzcan las diferencias y permitan un acceso equitativo a soluciones de ciberseguridad.

Además, la combinación de tecnologías avanzadas con políticas regulatorias sólidas y formación continua, resultan ser una fusión importante a la hora de mitigar los riesgos. Este marco no solo refuerza las defensas frente a amenazas actuales, sino que también prepara a las organizaciones para futuros desafíos y retos cibernéticos, garantizando así, la continuidad operativa y minimizando el impacto económico de los posibles incidentes.

Finalmente, como trabajo a futuro, sería una excelente opción la adaptación de estrategias de ciberseguridad enfocadas en sectores vulnerables, es decir diseñar medidas de ciberseguridad específicas para sectores con menos recursos, como el educativo y el de salud. Esta investigación puede ser un punto a tratar muy importante, ya que ayudaría a diferentes organizaciones o empresas, que no tienen muchos recursos, a poder protegerse mejor de estos ciberataques, que hoy en día abundan tanto en las redes.

Referencias

Application of artificial intelligence in computer network security,. (s/f). https://doi.org/10.1088/1742-6596/1865/4/042039.

Avarias, J., Leon, F., Carrasco, R., Lobos, J., Ibsen, J., Achermann, C., Parra, J., & Soto, R. (2024). Adding cybersecurity in JAO organizational culture: do's and dont's. En L. J. Storrie-Lombardi, C. R. Benn, & A. Chrysostomou (Eds.), Observatory Operations: Strategies, Processes, and Systems X (p. 12). SPIE.

Bispham, M., Creese, S., Dutton, W. H., Esteve-González, P., & Goldsmith, M. (2022). An exploratory study of cybersecurity in working from home: Problem or enabler? Journal of Information Policy, 12, 353–386. https://doi.org/10.5325/jinfopoli.12.2022.0010

Čergeť, M., & Hudec, J. (2023). Cyber-Security Threats Origins and their Analysis. Acta polytechnica Hungarica, 20(9), 23–41. https://doi.org/10.12700/aph.20.9.2023.9.2

Feng, X., Feng, Y., & Dawam, E. S. (2020). Artificial intelligence cyber security strategy. 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech).

Flores, C., Gonzalez, J., Kajtazi, M., Bugeja, J., & Vogel, B. (2023). Human factors for cybersecurity awareness in a remote work environment. Proceedings of the 9th International Conference on Information Systems Security and Privacy, 608–616.

Glorin, S. (2021). A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan. Communications of the IBIMA, 1–7. https://doi.org/10.5171/2021.589235

Jakimoski, K. (2023). Automation Improvement in Cyber Risk Management. 2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 1–6.

Kanter-Ramirez, C. A., Lopez-Leyva, J. A., Beltran-Rocha, L., & Ferková, D. (2020). Framework for the optimal design of an information system to diagnostic the enterprise security level and management the information risk based on ISO/IEC-27001. En Lecture Notes of the Institute for Computer

Sciences, Social Informatics and Telecommunications Engineering (pp. 3–13). Springer International Publishing.

Klein, G., & Zwilling, M. (2024). The weakest link: Employee cyber-defense behaviors while working from home. Journal of Computer Information Systems, 64(3), 408–422. https://doi.org/10.1080/08874417.2023.2221200

Leroy, I., & Zolotaryova, I. (2023). Insights for economic security: Recovery strategies from cyber-attacks. 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), 1–7.

Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-based zero trust access control policy: An approach to support work-from-home driven by COVID-19 pandemic. New Generation Computing, 39(3–4), 599–622. https://doi.org/10.1007/s00354-021-00130-6

Nyarko, D. A., & Fong, R. C.-W. (2023). Cyber security compliance among remote workers. En Advanced Sciences and Technologies for Security Applications (pp. 343–369). Springer International Publishing.

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2). https://doi.org/10.1002/itl2.247

Sstla, V., Kolli, V., & Voggu, L. (2020). Predictive model for network intrusion detection system using deep learning. Revue d intelligence artificielle, 34(3), 323–330. https://doi.org/10.18280/ria.340310

Sun, N., Zhang, J., Gao, S., Zhang, L. Y., Camtepe, S., & Xiang, Y. (2020). Data analytics of crowdsourced resources for cybersecurity intelligence. En Lecture Notes in Computer Science (pp. 3–21). Springer International Publishing.

Whitty, M. T., Moustafa, N., & Grobler, M. (2024). Cybersecurity when working from home during COVID-19: considering the human factors. Journal of Cybersecurity, 10(1). https://doi.org/10.1093/cybsec/tyae001

Working from home: Cybersecurity in the age of covid-19. (2020). Issues In Information Systems. https://doi.org/10.48009/4_iis_2020_234-246

Wright, T., Ruhwanya, Z., & Ophoff, J. (2024). Using the theory of interpersonal behaviour to explain employees' cybercrime preventative behaviour during the pandemic. Information and Computer Security, 32(4), 436–458. https://doi.org/10.1108/ics-11-2023-0228