SEMILLAS DEL SABER
REVISTA CIENTÍFICA ESTUDIANTIL

Ciberseguridad y protección de datos: estrategias para proteger la información en redes y sistemas

CYBERSECURITY AND DATA PROTECTION: STRATEGIES TO PROTECT INFORMATION ON NETWORKS AND SYSTEMS

UNICATÓLICA - Fundación Universitaria Católica Lumen Gentium

Joan Sebastian Umaña Jimenez
joan.umana01@unicatolica.edu.co

Cesar Camilo Calderón Arenas
cesar.calderon02@unicatolica.edu.co

Miguel Ángel Duque Álvarez
miguel.duque01@unicatolica.edu.co

José Antonio Vélez López
jose.velez01@unicatolica.edu.co

Charlotte Burbano
cmburbano@unicatolica.edu.co

Resumen

Este artículo analiza las estrategias clave para proteger la información en un contexto de creciente ciberamenazas, destacando la relevancia de marcos normativos como la ISO/IEC 27001 y modelos como el ciclo PHVA. Utilizando una revisión teórica y un análisis bibliométrico de publicaciones entre 2004 y 2024, se observa un notable aumento en investigaciones sobre ciberseguridad, especialmente desde 2016, impulsado por normativas internacionales como el GDPR y la transformación digital. Los hallazgos subrayan la necesidad de fortalecer la investigación en Latinoamérica para abordar desafíos locales y globales. Se concluye que la implementación de sistemas de gestión, políticas alineadas con la estrategia corporativa y un enfoque continuo en la mejora de la seguridad son esenciales para mitigar riesgos, garantizar la protección de los datos y fomentar un entorno digital seguro. Este trabajo destaca vacíos en la literatura y propone líneas futuras de investigación, esenciales para la evolución del campo.

Palabras clave: Ciberseguridad, ISO 27001, Sistema de Gestión de Seguridad de la Información (SGSI), Políticas de seguridad.

Abstract

This article examines key strategies for protecting information amidst increasing cyber threats, emphasizing the importance of frameworks such as ISO/IEC 27001 and models like the PDCA cycle. Through a theoretical review and bibliometric analysis of publications from 2004 to 2024, a significant rise in cybersecurity research is observed, particularly since 2016, driven by international regulations like GDPR and digital transformation. Findings highlight the need to strengthen research in Latin America to address local and global challenges. The study concludes that implementing management systems, policies aligned with corporate strategy, and a continuous improvement approach are essential to mitigate risks, ensure data protection, and foster a secure digital environment. This work identifies gaps in the literature and proposes future research directions critical for advancing the field.

Keywords: Cybersecurity, ISO 27001, Information Security Management System (ISMS), Security policies.

Introducción

En el contexto actual, la protección de la información se ha convertido en un desafío primordial para las organizaciones y los individuos debido al incremento constante de amenazas cibernéticas. A medida que la dependencia de los sistemas y redes digitales crece, también lo hacen las vulnerabilidades, lo que genera graves riesgos para la integridad, confidencialidad y disponibilidad de los datos. Las causas de estos riesgos se deben a factores como el aumento de la sofisticación de los ciberataques, la falta de actualización en medidas de seguridad, y la exposición a accesos no autorizados. Las consecuencias para los usuarios y empresas van desde pérdidas financieras hasta daños reputacionales y compromisos legales. Por tanto, abordar estos riesgos es esencial para garantizar la continuidad y la seguridad de las operaciones en el ámbito digital.

Este artículo tiene como objetivo explorar y analizar las principales estrategias de ciberseguridad que las organizaciones pueden implementar para proteger la información almacenada y transferida a través de redes y sistemas. Se revisarán estudios previos que han sido fundamentales en el desarrollo del campo de la ciberseguridad, destacando la evolución de las técnicas y tecnologías más efectivas. Asimismo, se identificarán las problemáticas críticas actuales y las áreas que requieren investigaciones futuras, ofreciendo una visión general sobre el estado actual del conocimiento en el área.

Dado el incremento en la sofisticación de los ciberataques, resulta crucial la implementación de políticas y procedimientos robustos que permitan una respuesta rápida y efectiva ante incidentes de seguridad. En este sentido, la revisión busca combinar el conocimiento existente sobre las mejores prácticas de protección de la información, señalando aquellas áreas en las que la literatura presenta vacíos y sugiriendo nuevas líneas de investigación emergentes como esenciales para el progreso del campo.

El presente trabajo se estructura de la siguiente manera: primero, se analizará en detalle el concepto y la evolución histórica de la ciberseguridad y la protección de datos; segundo, se abordarán las políticas y estrategias más relevantes para asegurar la información; y finalmente, se discutirá el futuro de la seguridad de la información en el contexto del avance tecnológico.

Marco Teórico

La ciberseguridad, entendida como un conjunto de estrategias y procesos destinados a la protección de la información, se fundamenta en diversas teorías y estándares que permiten comprender y abordar la gestión de los riesgos asociados a los sistemas de información. Entre las teorías relevantes para este estudio se encuentran la teoría del riesgo, la gestión de seguridad de la información (SGSI), el modelo Planificar-Hacer-Verificar-Actuar (PHVA), y los marcos normativos como la norma ISO/IEC 27001.(Asana, s/f)

Teoría del riesgo y ciberseguridad: La teoría del riesgo es fundamental para comprender cómo las organizaciones deben identificar, evaluar y gestionar las amenazas a las que se enfrentan sus activos digitales. En el contexto de la ciberseguridad, los riesgos están relacionados con la posibilidad de accesos no autorizados, la pérdida de confidencialidad, la alteración de la integridad de los datos y la interrupción de la disponibilidad de los sistemas .(Modeling Cyber-Insurance: Towards a Unifying Framework - researchr publication, s/f) Esta teoría permite estructurar los procesos de identificación de amenazas y vulnerabilidades, y aplicar las medidas adecuadas para mitigar los riesgos.

Sistema de Gestión de Seguridad de la Información (SGSI): El Sistema de Gestión de Seguridad de la Información (SGSI) es un marco integral que permite a las organizaciones gestionar de manera efectiva la seguridad de sus activos informáticos. La norma ISO/IEC 27001 proporciona los requisitos necesarios para establecer, implementar, mantener y mejorar un SGSI, asegurando la protección de la información (ISO/IEC 27001, s/f). Este estándar establece la base para el desarrollo de políticas y procedimientos que fortalezcan la seguridad y aseguren la continuidad de las operaciones empresariales, minimizando los daños asociados a incidentes de seguridad. (Salvador Carrasco, 2014)

Modelo Planificar-Hacer-Verificar-Actuar (PHVA): El ciclo PHVA, también conocido como el ciclo de Deming, es un enfoque estructurado utilizado para la gestión de la seguridad y la mejora continua en los sistemas organizacionales. En el ámbito de la ciberseguridad, este modelo permite gestionar los riesgos mediante un enfoque cíclico de planificación, implementación, supervisión y ajuste de las políticas de seguridad. La fase de planificación incluye la identificación de riesgos y la definición de políticas, mientras que las fases de ejecución, verificación y ajuste garantizan la implementación efectiva y la mejora continua de las estrategias de seguridad. (Cremer et al., 2022).

Políticas de seguridad y planificación estratégica: Las políticas de seguridad son uno de los pilares fundamentales para la protección de la información dentro de cualquier organización. Estas deben estar alineadas con la estrategia corporativa, y tienen como objetivo crear un entorno seguro mediante la implementación de controles y procedimientos claros (Whitman & Mattord, 2004). Una correcta planificación de la seguridad de la red es crucial para promover una cultura de seguridad entre los usuarios y garantizar que los sistemas se mantengan protegidos frente a posibles amenazas.

Ciberseguridad y el rol de las normas ISO: La norma ISO/IEC 27001 no solo establece los requisitos para un SGSI, sino que también permite a las organizaciones implementar un enfoque sistemático para proteger sus activos de información. Esta norma, ampliamente reconocida a nivel global, facilita la evaluación de riesgos, la implementación de controles de seguridad y el seguimiento de las medidas adoptadas para garantizar la mejora continua (ISO/IEC 27001, s/f). La adopción de estas normativas asegura un control más riguroso sobre los riesgos y la protección de los activos digitales críticos.

Análisis Bibliométrico

A través de una búsqueda utilizando las palabras clave "ciberseguridad" y "seguridad de la información" en Google Scholar y OpenAlex, y considerando un rango temporal de 20 años (2004-2024), se identificaron aproximadamente 200,000 publicaciones relacionadas con estos temas.

Figura 1. Gráfico de búsqueda en rango 2000 - 2024

Fuente. Elaboración propia basado en la información en openalex.org. Generado en Microsoft Excel.

La Figura 1 en la gráfica evidencia un crecimiento sostenido en la producción científica sobre ciberseguridad y seguridad de la información entre 2003 y 2023, alcanzando un máximo en 2023 con alrededor de 800 publicaciones. Este aumento refleja la creciente relevancia de estos temas, impulsada por la transformación digital y el incremento de amenazas cibernéticas.

El periodo 2016-2023 destaca por un crecimiento acelerado, probablemente vinculado a normativas internacionales como el GDPR (2018) y mayores inversiones en tecnología. La disminución en publicaciones hacia años previos puede explicarse por la menor visibilidad de investigaciones antiguas y el desarrollo reciente del campo.

Este patrón subraya la oportunidad de fortalecer la investigación regional en Latinoamérica, abordando brechas históricas y respondiendo a desafíos locales. El análisis bibliométrico enfatiza la importancia de aumentar la investigación local y regional en ciberseguridad, sentando un precedente para fomentar la participación de más investigadores en Colombia y otros países de la región en este campo estratégico y de creciente relevancia.

Figura 2. Gráfico de búsqueda en rango 2000 - 2024

Fuente. Elaboración propia basado en la información en openalex.org. Generado en Microsoft Excel.

El mapa de la figura 2 refuerza esta idea al mostrar que la investigación en ciberseguridad está mayormente concentrada en países desarrollados, mientras que Latinoamérica, incluida Colombia, tiene una participación limitada. Esta desigualdad destaca la necesidad de impulsar la producción científica local y regional, ya que factores como la falta de inversión, infraestructura tecnológica y políticas públicas específicas han frenado su desarrollo.

Por lo tanto, este análisis bibliométrico subraya una oportunidad estratégica para que investigaciones como esta no solo contribuyan al crecimiento de la ciberseguridad en la región, sino que también establezcan un precedente para fomentar la colaboración, la formación de talento y la creación de políticas adaptadas a las necesidades locales. Incrementar la participación de investigadores en Latinoamérica es clave para fortalecer este campo crítico y posicionar a la región como un actor relevante en la agenda global de ciberseguridad.

Limitaciones de la Revisión

Una de las principales limitaciones de esta revisión radica en el acceso restringido a documentos esenciales para alcanzar plenamente los objetivos planteados. Muchos estudios, informes y datos clave en el ámbito de la ciberseguridad son de carácter privado o confidencial, particularmente aquellos relacionados con empresas y organizaciones que gestionan infraestructuras críticas. Esta restricción limita la posibilidad de obtener una visión integral y actualizada sobre las prácticas y estrategias más efectivas en el campo. Además, la ausencia de estos documentos dificulta la realización de un análisis exhaustivo de las tendencias y avances recientes en la gestión de riesgos y la protección de datos.

Para abordar esta limitación, será valioso considerar alternativas como la consulta de informes emitidos por instituciones gubernamentales, el uso de repositorios de acceso abierto y el análisis de investigaciones académicas públicas. Estas estrategias podrían enriquecer y proporcionar perspectivas complementarias que permitan un acercamiento más amplio y robusto al tema.

Selección de Fuentes

La selección de fuentes se realizó siguiendo criterios específicos que garantizaron la relevancia, calidad y diversidad de los artículos incluidos en la revisión. Los principales criterios fueron los siguientes:

1. **Tiempo:** Se definió un intervalo temporal comprendido entre los años 2000 y 2024. Este rango permitió incluir publicaciones con un enfoque histórico y actual, asegurando que la información utilizada fuese pertinente para los objetivos de la investigación.

2. **Confiabilidad:** Se emplearon bases de datos académicas reconocidas, como Google Scholar y OpenAlex, que aseguraron un alto estándar de calidad en las fuentes seleccionadas. Estas plataformas son ampliamente aceptadas en el ámbito académico por su rigor y cobertura en temas especializados.

3. **Ubicación geográfica:** Se incluyeron estudios realizados en países como España, México, Colombia y Estados Unidos. Estos países destacan por su liderazgo en avances tecnológicos y su impacto en la formulación de políticas y normativas relacionadas con la ciberseguridad. Esta diversidad geográfica contribuyó a enriquecer el análisis con perspectivas globales y regionales.

La aplicación de estos criterios permitió abordar la investigación desde una perspectiva amplia y diversa, optimizando la calidad y relevancia del análisis. Asimismo, la selección cuidadosa de las fuentes garantizó la exclusión de trabajos que no cumplían con los estándares establecidos, fortaleciendo así la coherencia y solidez de la revisión.

Resultados

Con los artículos investigados se descubre que en el pasado la concientización de las personas sobre la seguridad cibernética era casi nula y los sistemas de protección de información solo abarcan la protección local dejando así un agujero que tardaron en cubrir con la llegada y globalización del internet. Pero, los sistemas operativos en busca de seguridad empezaron pronto a establecer parámetros de seguridad mucho más complejos dando cabida a la seguridad cibernética la cual se enfoca hasta nuestro presente a la protección de la información digital.

Según lo hallado en el pasado se describe a la seguridad informática como la predecesora de la seguridad cibernética, siendo aquella la que se caracterizaba en la detección de infiltrados en redes y de fugas de información por usuarios con acceso, en los años del nacimiento de Internet 1980. el esquema de la seguridad informática estaba principalmente enfocado en el flujo de datos y la protección sobre los sistemas de información, empleando estrategias de seguridad como lo eran, encriptaciones simples y firewall el cual filtraba los paquetes con una serie de reglas básicas de protección (ID, puertos, Protocolos), aunque según el registro histórico estos mismos eran en su mayoría ignorados por las empresas debido a la falta de concientización sobre seguridad informática. Con la evolución creciente de internet y los nuevos sistemas operativos más modernos los ataques informáticos se volvieron cibernéticos y crecieron en gran medida paralelos a los sistemas de seguridad informática que evolucionaron adaptándose al nuevo entorno y ampliando sus capacidades para brindar mejor seguridad a los usuarios y empresas algunos de estos como lo son el blockchain, una evolución de estilo de encriptado por paquete o los firewalls de segunda generación, que mejoran sus reglas de seguridad al examinar directamente los paquetes para permitir el paso de aquellos que cumplan con la tabla establecida.

Todo esto nos lleva al presente donde podemos evidenciar casos de ataques cibernéticos que han logrado ser evitados, con mayor concientización de las personas, así como con el uso de firewalls especializados junto a protocolos de continuidad de servicio durante ataques DDOS, demostrando cómo los sistemas de seguridad se adaptan y evolucionan fácilmente en un entorno donde los ataques de hackers son cada vez más constantes e ingeniosos.

Por desgracia debido a la misma globalización del internet se encuentra un gran desventaja de seguridad en países por fuera del primer mundo así como una limitante en obtener y/o manejar los distintos sistemas operativos, por lo cual la documentación relacionada se encontraba altamente focalizada, resultando muy restrictiva y poco diversa, no permitiendo que se logre abarcar en diferentes entornos donde se hallará una limitante por red, equipos, estructura e incluso región. Adjunto a esto está el popular uso de las IA de las cuales aún no se ha explorado su completo potencial pero, según se pronostica, pueden marcar un antes y un después en la era tecnológica y en especial en la seguridad al usar un sistema "inteligente" para reconocer situaciones o usuarios y actuar inmediatamente al respecto, ampliando y abarcando más elementos que antes se percibían como inviables por eficiencia. Es por ello que con estos resultados se invita a la comunidad a investigar sobre el pasado de la ciberseguridad, actualizar documentación y analizar una aplicación a futuro para ayudar a más profesionales a conocer bases para aportar a futuras investigaciones.

Conclusión

La ciberseguridad es un pilar fundamental para la protección de los datos personales y/o empresariales, aún más en un entorno tan creciente como lo es el tecnológico y la red global, donde su creciente evolución le exige adaptarse constantemente a los profesionales y sistemas de seguridad para enfrentarse a la ciberdelincuencia. Sin embargo, la falta de documentación actualizada en las bases de datos o incluso restrictiva al estar muy centralizada, dichos entusiastas se encuentran con limitantes que les impiden lograr emplear una investigación innovadora que aporte a la comunidad científica para futuros desarrollos dejando así una oportunidad más a los ciberdelincuentes para sacar provecho a las nuevas tecnologías.

Recomendaciones

Para proteger los datos de posibles amenazas del internet, es importante contar con políticas de seguridad sólidas que cumplan con los estándares internacionales como ISO/IEC 27001 y actualizar de forma regular los sistemas operativos y los antivirus. Es clave seguir un enfoque sistemático utilizando la teoría del riesgo y el modelo PHVA para identificar, evaluar y reducir amenazas, con el objetivo de promover la mejora constante. Es importante invertir en infraestructura técnica y nuevas tecnologías como inteligencia artificial para detectar y responder a ataques de manera inmediata. Es crucial fomentar la investigación local en América Latina y ofrecer estímulo para el adelanto científico, la formación de nuevos talentosos y la creación de políticas públicas acordes a las necesidades de la región. Es importante mejorar la cultura de la seguridad de los usuarios, enseñarles buenas prácticas y establecer procedimientos efectivos para manejar incidentes. La investigación se enfoca en áreas como IoT y el manejo de datos para reducir futuros riesgos.

Referencias

Asana. (s/f). ¿Qué es el Ciclo Planificar-Hacer-Verificar-Actuar (PHVA)? [2024] • Asana. Asana. Recuperado el 14 de septiembre de 2024, de https://asana.com/es/resources/pdca-cycle

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698–736 https://doi.org/10.1057/s41288-022-00266-6

ISO/IEC 27001:2018. (s/f). ISO. Recuperado el 19 de octubre de 2024, de https://www.iso.org/standard/63787.html

Modeling Cyber-Insurance: Towards a Unifying Framework—Researchr publication. (s/f). Recuperado el 19 de octubre de 2024, de https://researchr.org/publication/BohmeS10-0

Salvador Carrasco, L. A. de. (2014). Los problemas estructurales en el planteamiento de la ciberseguridad. Pre-bie3, 4, 11.

Whitman, M., & Mattord, H. (2004). Principles of Information Security, 2nd Edition. Faculty Articles. https://digitalcommons.kennesaw.edu/facpubs/1430

PODCAST

CIBERSEGURIDAD Y PROTECCIÓN DE DATOS: ESTRATEGIAS PARA PROTEGER LA INFORMACIÓN EN REDES Y SISTEMAS

Joan Sebastian Umaña Jimenez
joan.umana01@unicatolica.edu.co

Cesar Camilo Calderón Arenas
cesar.calderon02@unicatolica.edu.co

Miguel Ángel Duque Álvarez
miguel.duque01@unicatolica.edu.co

José Antonio Vélez López
jose.velez01@unicatolica.edu.co