https://repository.uaeh.edu.mx/revistas/index.php/prepa4/issue/archive

Vida Científica Boletín Científico de la Escuela Preparatoria No. 4

Publicación semestral, Vol. 13, No. 26 (2025) 47-49

Vida Científica

ISSN: 2007-4905

Ciberseguridad

Cybersecurity

Iván H. Pérez-Tavera [a]

Abstract:

Cybersecurity is essential in the digital age, influencing the economy, government, and daily life. Mexico has developed its National Cybersecurity Strategy (ENCS) based on four pillars: promoting cybersecurity culture, protecting critical infrastructures, creating agile detection capabilities, and fostering international cooperation. Additionally, the Global Cybersecurity Index (GCI) and the National Cybersecurity Index (INSC) evaluate progress in this field, highlighting strengths and weaknesses. Despite advancements, three overlooked risks emerge: vulnerabilities in critical infrastructures, disinformation generated by AI, and cyber threats impacting human rights. A proactive approach is crucial to address these challenges and ensure a secure digital environment.

Keywords:

Cybersecurity, Critical infrastructures, Disinformation, Global Cybersecurity Index, Human rights

Resumen:

La ciberseguridad es esencial en la era digital, influyendo en la economía, el gobierno y la vida diaria. México ha desarrollado su Estrategia Nacional de Ciberseguridad (ENCS) basada en cuatro pilares: promoción de cultura de ciberseguridad, protección de infraestructuras críticas, creación de capacidades de detección ágil y cooperación internacional. Además, el Índice Global de Ciberseguridad (GCI) y el Índice Nacional de Seguridad Cibernética (INSC) evalúan el progreso en esta área, destacando fortalezas y debilidades. A pesar de los avances, emergen tres riesgos desatendidos: vulnerabilidad en infraestructuras críticas, desinformación generada por IA y ciberamenazas que afectan derechos humanos. Es crucial un enfoque proactivo para abordar estos desafíos y garantizar un entorno digital seguro.

Palabras Clave*:*

Ciberseguridad, Infraestructuras críticas, Desinformación, Índice Global de Ciberseguridad, Derechos humanos

Introducción

La ciberseguridad ahora es muy importante debido a cuánto usamos la tecnología en nuestra economía, gobierno y vida cotidiana. La amenaza cibernética afecta a todos, incluidos individuos, organizaciones y gobiernos. Muchos países, como México, están haciendo planes sólidos para mantener sus importantes Los sistemas son seguros y enfrentan los riesgos porque las cosas siempre están cambiando. Entre estos esfuerzos, el Plan e Índice Nacional de Ciberseguridad de México, junto con el Índice Global de Ciberseguridad, son herramientas clave para verificar y rastrear los avances en ciberseguridad.

A medida que nos acercamos al 2024, es crucial examinar las crecientes amenazas a la ciberseguridad que a menudo pasan desapercibidas pero que pueden afectar en gran medida la economía y el orden social de un país. En este documento, hablaremos sobre el plan de México para protegerse contra los ciberataques, miraremos los rankings de ciberseguridad del mundo. y explorar tres grandes problemas de ciberseguridad de los que la gente no habla lo suficiente: puntos débiles en sistemas importantes, noticias falsas creadas por personas inteligentes

[a] Iván Horacio Pérez Tavera, Universidad Autónoma del Estado de Hidalgo | Escuela Preparatoria No. 4 | Pachuca-Hidalgo | México, https://orcid.org/0000-0001-7708-6912, Email: itavera@uaeh.edu.mx

Fecha de recepción: 08/08/2025, Fecha de aceptación: 10/04/2025, Fecha de publicación: 05/07/2025

DOI: https://doi.org/10.29057/prepa4.v13i26.14901

Estrategia Nacional de Ciberseguridad de México

El Plan Nacional de Ciberseguridad (ENCS) de México es un plan completo para detener, encontrar y manejar problemas cibernéticos que podrían dañar los sistemas informáticos y las empresas del gobierno. Este plan se centra en cuatro ideas principales: enseñar a la gente sobre la seguridad en línea, mantener seguros los sistemas importantes, encontrar y abordar los problemas rápidamente y trabajar junto con otros países

Promoción de la cultura de ciberseguridad

El primer pilar de la ENC destaca la importancia de cultivar una cultura de ciberseguridad entre individuos e instituciones. Esto abarca no sólo enseñar a las personas cómo utilizar las tecnologías de forma segura, sino también aumentar la conciencia sobre las ciberamenazas que suponen un riesgo para la población en general. Es crucial implementar programas de capacitación y campañas de concientización para mejorar la capacidad de responder eficazmente a amenazas inminentes.
El segundo pilar se centra en la identificación y protección de los activos más importantes del país, que incluyen sistemas de energía, transporte, salud y comunicaciones. La estrategia establece protocolos responsables de evaluación de riesgos y asignación de recursos especializados para fortalecer la ciberdefensa de estas infraestructuras.

El tercer pilar de la ENCS involucra la creación de capacidades para la detección ágil y eficaz de incidentes cibernéticos. Esto incluye el establecimiento de equipos de respuesta ante incidentes (CSIRT) que operen de manera coordinada a nivel nacional, proporcionando un marco donde las instituciones pueden compartir información de manera rápida y efectiva para mitigar cualquier amenaza.

Finalmente, la ENCS promueve la cooperación internacional en el ámbito de ciberseguridad. En un mundo interconectado, las amenazas cibernéticas no tienen fronteras, lo que hace fundamental la colaboración con otros países y organismos internacionales para fortalecer las defensas y compartir mejores prácticas.

Índice Global de Ciberseguridad

El Índice Global de Ciberseguridad (GCI, por sus siglas en inglés) es una herramienta desarrollada por la Unión Internacional de Telecomunicaciones (UIT) para medir el nivel de preparación y el compromiso de los países en el ámbito de la ciberseguridad. Este índice evalúa a las naciones en base a varios indicadores, incluyendo el marco jurídico, la capacidad técnica, la preparación y la cooperación internacional.

Los resultados del GCI permiten identificar las fortalezas y debilidades de cada nación en la lucha contra las amenazas cibernéticas. En el caso de México, su posición en este índice ha variado con el tiempo, reflejando tanto los avances en la implementación de políticas nacionales como las brechas que aún permanecen. Las autoridades mexicanas se han propuesto mejorar su clasificación en el GCI mediante la implementación de reformas y la asignación de mayores recursos a ciberseguridad en su plan de gobierno.

El Índice Nacional de Seguridad Cibernética (INSC) complementa el GCI a nivel nacional, proporcionando una visión más específica y contextualizada de la situación de la ciberseguridad en México. Este índice se basa en criterios que evalúan la gobernanza, la gestión de incidentes, la protección de infraestructuras críticas, la ciberdefensa, entre otros.

La importancia del INSC radica en su capacidad para ofrecer un diagnóstico claro sobre los retos que enfrenta el país en el ámbito cibernético. La recopilación y el análisis de datos permiten a las autoridades tomar decisiones informadas y diseñar políticas que fortalezcan la postura de ciberseguridad en todos los sectores.

El entorno de ciberseguridad está en constante evolución, y con el avance de la tecnología surgen nuevos riesgos que requieren la atención de expertos, gobiernos y ciudadanos. A continuación, se mencionan tres de estos riesgos globales que, a menudo, no reciben la atención que merecen.

A medida que más servicios e infraestructuras se integran en plataformas digitales, la vulnerabilidad de la infraestructura crítica aumenta exponencialmente. Desde sistemas de energía hasta redes de transporte y servicios públicos, todas estas estructuras son potencialmente susceptibles a ataques cibernéticos devastadores. Si bien se ha hablado de la protección de estas infraestructuras, la realidad es que muchas de ellas todavía operan con sistemas desactualizados y prácticas de seguridad inadecuadas. Los ataques dirigidos a estas infraestructuras no solo pueden interrumpir servicios esenciales, sino que también pueden provocar crisis humanitarias y económicas.

La proliferación de herramientas de inteligencia artificial ha llevado a un aumento sin precedentes en la capacidad

de generar desinformación de manera rápida y efectiva. Esta situación plantea un riesgo significativo, ya que las campañas de desinformación pueden desestabilizar sociedades, manipular elecciones y fomentar la polarización social. A medida que las plataformas digitales se convierten en los principales canales de comunicación, la responsabilidad de gestionar y controlar la desinformación recae tanto en los gobiernos como en las empresas tecnológicas. No obstante, la falta de regulación y consenso sobre cómo enfrentar este fenómeno presenta un desafío crítico para la ciberseguridad global.

La ciberseguridad no solo se manifiesta en la protección de datos y sistemas; también se interrelaciona profundamente con los derechos humanos. El acoso en línea, la vigilancia masiva y la restricción de la libertad de expresión son solo algunas de las formas en que las ciberamenazas pueden agravar las violaciones de los derechos humanos. La creciente utilización de tecnologías de monitoreo y vigilancia por parte de gobiernos y empresas plantea preocupaciones éticas y de privacidad que, si no se abordan adecuadamente, pueden conducir a un panorama de ciberseguridad que erosione las libertades fundamentales de los individuos.

Conclusión

La ciberseguridad se ha convertido en un aspecto crítico no solo de la política nacional, sino también de la estabilidad internacional. La Estrategia Nacional de Ciberseguridad de México, junto con los índices que miden su progreso, son vitales para entender el estado actual y los desafíos futuros en este ámbito. Sin embargo, para garantizar un entorno digital seguro, es esencial prestar atención a los riesgos emergentes que a menudo pasan desapercibidos. La vulnerabilidad de la infraestructura crítica, la desinformación impulsada por la inteligencia artificial y las ciberamenazas a los derechos humanos son solo algunas de las áreas que requieren un enfoque proactivo y una mayor conciencia por parte de la comunidad internacional. En conjunto, la investigación y la acción coordina pueden generar un cambio positivo en un panorama cibernético cada vez más desafiante.

Referencias

[1] 7 tendencias que podrían marcar el futuro de la ciberseguridad en 2030. (2024, 10 septiembre). Foro Económico Mundial. https://es.weforum.org/agenda/2023/03/7-tendencias-que-podrian-marcar-el-futuro-de-la-ciberseguridad-en-2030/

[2] Estrategia Nacional de Ciberseguridad. (2017). https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

[3] Global Cybersecurity Index. (s. f.). ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[4] NCSI :: Ranking. (s.f.). https://ncsi.ega.ee/ncsi-index/

[5] Riesgos Globales 2024: 3 riesgos de los que no se habla lo suficiente. (2024, 10 septiembre). Foro Económico Mundial. https://es.weforum.org/agenda/2024/02/riesgos-globales-2024-3-riesgos-de-los-que-no-hablamos-lo-suficiente/