Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: XII Número: Edición Especial Artículo no.:59 Período: Diciembre del 2024

TÍTULO: Seguridad digital y violencias estructurales: perspectivas y desafíos contemporáneos.

AUTORES:

1. Máster. Francisco Isaí Morales-Sáenz.
2. Dr. José Melchor Medina-Quintero.
3. Dr. Fernando Ortiz Rodríguez.

RESUMEN: El objetivo de la investigación es analizar la relación entre seguridad digital y violencias estructurales en la sociedad contemporánea. Se identifica cómo las desigualdades en el acceso tecnológico y la falta de educación aumentan la vulnerabilidad ante amenazas digitales. El estudio enfatiza la necesidad de un enfoque holístico e interdisciplinario en las estrategias de seguridad digital, integrando aspectos técnicos, sociales, éticos y legales. Se concluye que la seguridad digital robusta es esencial para construir sociedades más seguras, equitativas y resilientes. Se recomienda investigación futura para evaluar empíricamente estas interrelaciones y desarrollar marcos operativos efectivos.

PALABRAS CLAVES: seguridad digital, violencias estructurales, concientización, desarrollo sostenible.

TITLE: Digital security and structural violence: contemporary perspectives and challenges.

AUTHORS:

1. Master. Francisco Isaí Morales-Sáenz.
2. PhD. José Melchor Medina-Quintero.
3. PhD. Fernando Ortiz Rodríguez.

ABSTRACT: The aim of the research is to analyse the relationship between digital security and structural violence in contemporary society. It identifies how inequalities in technological access and lack of education increase vulnerability to digital threats. The study emphasises the need for a holistic and interdisciplinary approach in digital security strategies, integrating technical, social, ethical and legal aspects. It concludes that robust digital security is essential to building safer, more equitable and resilient societies. Future research is recommended to empirically assess these interrelations and develop effective operational frameworks.

KEY WORDS: digital security, structural violence, awareness, sustainable development.

INTRODUCCIÓN.

Las tecnologías de la información (TI) han tenido un crecimiento exponencial a lo largo de los últimos años, y han propiciado el desarrollo de los sistemas de información, que resultan relevantes para contribuir tanto en el desarrollo de actividades como en el logro de objetivos organizacionales (Holgeid et al., 2022). En el contexto empresarial contemporáneo, los recursos tecnológicos al interior de las organizaciones se han considerado como fuente de ventaja competitiva, al representarle un beneficio para mantenerse en el mercado a raíz de la trascendencia y la eliminación de fronteras comerciales para el desarrollo de sus actividades empresariales (Hérnandez y Salcedo, 2020).

La crisis sanitaria provocada por el SARS-CoV-2 propició un incremento en el uso de las tecnologías de la información derivado de las restricciones para el desarrollo de las actividades cotidianas en la sociedad, implementadas por parte de los gobiernos a nivel mundial; por lo tanto, representan una herramienta esencial para el desarrollo de las funciones dentro de la mayoría de los ámbitos de la sociedad. En lo que respecta a las organizaciones, este evento propició la implementación de las TI para el desarrollo de actividades operativas y directivas con el propósito de no mermar el desempeño de la organización por el

detenimiento de las actividades presenciales, migrando de un modelo tradicional a uno virtual con el apoyo de las TI (Morales-Sáenz et al., 2023).

En este panorama de creciente digitalización, la seguridad digital emerge como un aspecto multidimensional y complejo (Choodakowska et al., 2022), y un enfoque holístico para abordar este tema no solo permite una comprensión más profunda de los riesgos y desafíos asociados, sino que también identifica oportunidades para la innovación colaborativa y el diseño de políticas más eficientes e inclusivas (Stevens, 2018); por lo tanto, la seguridad digital se ha convertido en un pilar fundamental para la integridad operacional de organizaciones que manejen información crítica o sensible, trascendiendo su rol técnico para construirse en un elemento central de progreso y bienestar social (Kosevich, 2022; De Soto et al., 2022).

La creciente dependencia tecnológica de la sociedad ha intensificado la necesidad de implementar mecanismos de protección contra amenazas digitales (Li et al., 2019), intensificado sus preocupaciones sobre la seguridad informática para abordar los desafíos actuales (Morales-Sáenz et al., 2024).

Esta preocupación, se ve relejada en estadísticas globales, en el que el costo estimado del cibercrimen para el año 2020 ascendió a aproximadamente 945 mil millones de dólares, lo que representa un incremento alarmante del 50% en comparación con las cifras reportadas en el año 2018 (Malekos et al., 2020).

A medida que la tecnología continúa penetrando en todos los ámbitos de la sociedad, se ha incrementado la necesidad de proteger la información de los ataques informáticos (Li et al., 2019). El aumento en la sofisticación y frecuencia de los ciberataques dirigidos a sistemas e individuos vulnerables constituye una amenaza significativa para la integridad de los datos, la privacidad y la continuidad operacional de las organizaciones, especialmente aquellas con limitaciones en sus capacidades de protección y respuesta (Silaule et al., 2022).

En este contexto, la presente investigación se propone analizar la interrelación entre la seguridad digital y las violencias estructurales en la sociedad contemporánea. El objetivo principal es analizar las implicaciones de esta interacción y reflexionar sobre su importancia en el tejido social actual; asimismo, busca identificar y proponer estrategias efectivas para abordar desafíos emergentes en el ámbito de la seguridad digital.

Se aspira a contribuir significativamente al cuerpo del conocimiento existentes, ofreciendo una perspectiva integral y equitativa que fomente un desarrollo humano y social sostenible. A través de un análisis multidisciplinario, se pretende no solo aportar al debate académico, sino también proporcionar elementos valiosos para la formulación de políticas y prácticas que aborden las problemáticas de seguridad digital de manera efectiva.

DESARROLLO.

Violencias Estructurales en los Sistemas Sociales.

La revolución de las Tecnologías de la Información (TI), ha permeado en todos los estratos de la sociedad contemporánea, transformando las dinámicas políticas, económicas y sociales (Baek y Lee, 2021). Si bien la interconectividad y la digitalización de servicios han aportado innumerables beneficios, también han suscitado preocupaciones significativas en diversos ámbitos de competencia (Vasiu y Vasiu, 2018). En este contexto, resulta esencial analizar la seguridad digital desde la perspectiva de las violencias estructurales para comprender su impacto holístico en la sociedad.

El concepto de violencia estructural se refiere a los daños o perjuicios evitables que sufren los individuos debido a la distribución inequitativa del poder y los recursos en la sociedad (Kivimaa et al., 2022; Seidemann y Halling, 2019). Este fenómeno engloba las limitaciones estructurales e institucionales que impiden a los grupos marginados desarrollarse plenamente y vivir una vida que valoren. La violencia estructural se manifiesta en situaciones donde la satisfacción de las necesidades humanas básicas se ve

comprometida por procesos de estratificación social (La Parra-Casado y Tortosa, 2003), perpetuando y legitimando así las desigualdades sociales (Flynn et al., 2018; Raguz, 2019; Kleba y Reina-Rozo, 2021). En el contexto digital, la violencia estructural adquiere nuevas dimensiones, manifestándose a través de desigualdades en el acceso a tecnologías y recursos de seguridad digital (Harper, 2022). Estas disparidades afectan desproporcionadamente a grupos vulnerables por razones de clase, raza o género (Winters et al., 2019), subrayando la necesidad imperativa de considerar las dimensiones éticas y sociales en el desarrollo de capacidades de seguridad digital.

Aunque numerosos estudios han abordado la importancia de la seguridad digital para organizaciones y la sociedad (Cheng & Wang, 2022; Delgado et al., 2021), es crucial profundizar en las implicaciones éticas y morales, considerando las dimensiones humanas, sociales y organizacionales en el desarrollo de capacidades de seguridad digital (Dutton et al., 2019). Este enfoque multidimensional permite visibilizar cómo las desigualdades estructurales en el ámbito digital pueden incrementar o generar nuevas formas de violencia, tanto directa como indirecta en la sociedad contemporánea (Kleba y Reina-Rozo, 2021; Macassa, 2023).

La intersección entre seguridad digital y violencias estructurales se manifiesta en múltiples aspectos críticos. La violencia estructural digital, caracterizadas por la desigualdad digital y la exclusión social de oportunidades educativas en materia tecnológica (Harper, 2022), representa un desafío significativo que se entrelaza con los procesos de desarrollo tecnológico y la difusión del conocimiento (Greyson, 2019). Esta brecha digital no solo refleja las estructuras sociales desiguales preexistentes, sino que también las refuerza, creando un ciclo de exclusión que afecta las oportunidades educativas, laborales y de participación social de los grupos marginados.

La falta de acceso y conocimiento tecnológico incrementa la vulnerabilidad de ciertos grupos frente a amenazas y ataques digitales, limitando su capacidad para protegerse y perpetuando las violencias

estructurales (Seidemann y Halling, 2019); por lo tanto, la promoción de la alfabetización tecnológica y el acceso equitativo a recursos digitales se erigen como acciones fundamentales para empoderar a las poblaciones vulnerables y mitigar las consecuencias negativas de la ignorancia tecnológica en la sociedad.

Otro aspecto crucial es la proliferación de ataques a través de medios digitales, donde las personas pueden ser víctimas de discriminación, acoso y difamación, experimentando un impacto negativo en su bienestar mental y emocional, así como en su capacidad para participar plenamente en la sociedad digital. La falta de regulaciones y legislación adecuadas en materia de seguridad digital (Alhalafi y Veeraraghavan, 2021) crea un vacío legal que puede ser explotado para perpetuar las violencias estructurales, facilitando actividades ilegales o dañinas que repercuten en la explotación de personas vulnerables.

En este contexto, Hernández-Ramos et al. (2020) subrayan la importancia crucial de alinear los avances tecnológicos con esfuerzos regulatorios coordinados, como los que se están implementando en la Unión Europea, para abordar de manera efectiva los desafíos de la seguridad digital y mitigar sus impactos en las violencias estructurales.

La corrupción y la complicidad institucional representan elementos críticos en esta ecuación. La falta de seguridad digital, ya sea por no abordar adecuadamente las amenazas digitales o por no proteger la integridad, la privacidad y los datos de las personas, puede erosionar la confianza en las instituciones y debilitar el Estado de Derecho, propiciando las violencias estructurales (Kivimaa et al., 2022; Winters et al., 2019).

Es fundamental reconocer que la tecnología no solo refleja las estructuras sociales existentes, sino que también tiene el potencial de reproducir y amplificar la violencia estructural incrustada en ellas. La tecnología puede perpetuar normas culturales que legitiman dicha violencia, al tiempo que introduce nuevas estructuras sociales, institucionales, culturales, políticas y económicas (Hyman et al., 2016). Estas nuevas estructuras pueden generar formas emergentes de violencia estructural, afectando

desproporcionadamente a los grupos más marginados de la sociedad y las desigualdades preexistentes (Burton et al., 2021; Kivimaa et al., 2022).

Abordar la violencia estructural digital no implica rechazar las tecnologías digitales en su totalidad, sino reconocerlas como artefactos sociales y culturales complejos, susceptibles de ser reconfigurados y remodelados (Winters et al., 2019). Este enfoque permite vislumbrar oportunidades para utilizar la tecnología como herramienta de empoderamiento y transformación social, siempre y cuando se aborden de manera proactiva las desigualdades subyacentes y se implementen políticas inclusivas y equitativas.

El análisis de la seguridad digital desde la perspectiva de las violencias estructurales revela la necesidad urgente de un enfoque holístico e interdisciplinario que considere las dimensiones éticas, sociales y tecnológicas en la formulación de políticas y estrategias de seguridad digital. Solo a través de un abordaje integral que reconozca y aborde las desigualdades estructurales subyacentes, se podrá aspirar a crear un ecosistema digital más seguro, equitativo e inclusivo para todos los miembros de la sociedad.

La seguridad digital como elemento para hacer frente a las violencias estructurales.

La seguridad digital se ha convertido como un componente crítico e indispensable en la mitigación de diversas formas de violencia estructural, desempeñando un papel fundamental en la protección de información, infraestructura crítica y población (Zimmermann y Renaud, 2019). Esta relevancia se acentúa al considerar la sofisticación de la delincuencia organizada, y otros actores malintencionados utilizan frecuentemente el entorno digital para perpetrar actividades ilícitas, extorsionar y coordinar acciones violentas (Quintero, 2022). En consecuencia, la integración de la seguridad digital como parte esencial de las estrategias de seguridad para la sociedad resulta esencial.

En este contexto, la seguridad digital emerge con un elemento crucial para la protección de activos contra posibles ataques a infraestructuras críticas, incluyendo redes eléctricas, telecomunicaciones y servicios gubernamentales, elementos esenciales para el desarrollo nacional y el bienestar de los ciudadanos

(Plachkinova, 2023). Además, la implementación de estrategias integrales de seguridad digital puede contribuir significativamente a la lucha contra la delincuencia organizada transnacional, que utiliza Internet como plataforma para actividades ilícitas como el narcotráfico, la trata de personas y el lavado de dinero (Nizovtsev et al., 2022; Borelli & Greer, 2021; Nunes et al., 2016). Una gestión adecuada de la seguridad digital facilita el rastreo y monitoreo de estas actividades, proporcionando herramientas cruciales a las fuerzas del orden para identificar y desmantelar redes criminales complejas (Duxburt y Haynie, 2019).

Otro aspecto crucial es la protección de la privacidad y los datos personales de los ciudadanos, quienes se encuentran cada vez más expuestos al riesgo de robo de información personal (MacManus et al., 2013; Lamas, et al. 2023). En este sentido, la seguridad digital juega un papel fundamental en la salvaguarda de la información personal y financiera, así como en garantizar que empresas e instituciones gubernamentales adopten medidas adecuadas para proteger los datos de sus usuarios.

La seguridad digital se erige como un pilar fundamental para garantizar que las instituciones y el gobierno puedan proteger la información y los sistemas críticos del país (Hossain et al., 2024). Al abordar de manera efectiva los problemas de seguridad digital, las instituciones pueden fomentar la confianza ciudadana y demostrar su capacidad para proteger a la población de las amenazas en entornos digitales (Demertzi et al., 2023).

Un estudio reciente en Grecia (Kalogiannidis et al., 2023) explora los vínculos entre la seguridad digital y la protección civil. Los resultados demuestran que las tecnologías de seguridad digital tienen un impacto positivo en la protección civil, mientras que las prácticas de mitigación del delito cibernético tienen una influencia positiva en la seguridad social. Estos hallazgos subrayan la importancia de que tanto las agencias públicas y privadas adopten nuevas tecnologías de seguridad digital. Además, destaca que las vulnerabilidades en la seguridad digital plantean riesgos sustanciales para la infraestructura crítica,

afectando directamente el funcionamiento de los Estados, las economías y las sociedades; por consiguiente, la seguridad digital se consolida como un componente fundamental de la estrategia de seguridad integral.

Al proteger la infraestructura crítica (Mihelic y Vrhovec, 2018), combatir las actividades ilícitas en línea y garantizar la privacidad y protección de datos personales, la seguridad digital contribuye significativamente a la seguridad y el bienestar de los ciudadanos, así como al desarrollo sostenible de las naciones.

En este contexto, resulta importante reforzar los procesos, habilidades y recursos para el desarrollo de capacidades en seguridad digital que coadyuven al fortalecimiento de las capacidades colectivas y permitan atender de forma eficiente los desafíos que representan las amenazas de seguridad digital para las instituciones y la sociedad en su conjunto (Chychkan et al 2021). Este enfoque holístico e integrado de la seguridad digital no solo fortalece la resiliencia de los sistemas y las infraestructuras, sino que también contribuye a la construcción de sociedades más seguras y preparadas para enfrentar los retos del ecosistema digital.

La seguridad digital como una estrategia de protección personal y colectica en el contexto mexicano.

En México, donde la violencia representa un desafío multidimensional significativo, la seguridad digital emerge como un componente crucial de la estrategia de seguridad integral. Al proteger la infraestructura crítica (Mihelic y Vrhovec, 2018), combatir las actividades ilícitas en línea y garantizar la privacidad y protección de datos personales, la seguridad digital contribuye significativamente a la seguridad y el bienestar del ciudadano, así como al desarrollo sostenible del país (Gobierno de México, 2017).

La implementación efectiva de estrategias de seguridad digital en México va más allá de los desafíos inmediatos de protección de infraestructuras y datos, sentando las bases para un enfoque más amplio y proactivo. Este paradigma reconoce la naturaleza multifacética de la seguridad digital y su potencial para

abordar diversas formas de violencia estructural. Al expandir la comprensión del papel de la seguridad digital más allá de la mera defensa técnica, se abre un camino hacia soluciones más inclusivas y transformadoras. En este contexto, la educación y la concientización emergen como pilares fundamentales para construir una sociedad digitalmente resiliente y equitativa.

La seguridad digital desempeña un papel crucial en la atención a las violencias estructurales, al ser un elemento de apoyo en la búsqueda de soluciones para la protección de los activos digitales contra posibles ataques en cualquier ámbito dentro de la sociedad; por consiguiente, es fundamental la divulgación y concientización sobre la seguridad digital como medida para empoderar a las personas y comunidades en la prevención y respuesta a los riesgos y amenazas en línea (Ahamed et al., 2024).

La literatura académica ha propuesto diversas estrategias para abordar estos desafíos:

- Campañas de concientización sobre seguridad digital para construir cultura de seguridad digital (Cheng y Wang, 2022). Esta estrategia implica el uso de medios de comunicación y redes sociales para difundir información sobre aspectos clave de seguridad digital, proporcionando orientación sobre medidas de protección para actividades en línea. Es crucial que estas campañas sean accesibles para grupos vulnerables, como adultos mayores, que pueden enfrentar barreras adicionales en términos de acceso y comprensión de la seguridad digital (Blackwood-Brown y Levy, 2021).
- Talleres y capacitaciones (Qabajeh et al., 2018; Weir et al., 2023). Esta estrategia puede apoyar la enseñanza y capacitación de las personas en el desarrollo de habilidades y conocimientos específicos en seguridad digital. Es importante la colaboración con organizaciones locales y regionales como escuelas, empresas, ONG's y gobiernos, para coordinar esfuerzos de divulgación y compartir recursos y conocimientos en materia de seguridad digital.

- Eventos y conferencias: Participar y organizar eventos relacionados con la seguridad digital con el propósito de promover el intercambio de ideas, experiencias y buenas prácticas entre expertos, profesionales y miembros de la sociedad (Caviglione et al., 2021; Shires, 2018).

Para incidir en el proceso de construcción de sociedades más seguras, la comunidad científica propone las siguientes acciones de divulgación:

1. Vincular la seguridad digital con los derechos humanos y la justicia social: Comunicar cómo la seguridad digital está relacionada con la protección de los derechos humanos y la promoción de la justicia social, destacando la importancia de garantizar un acceso seguro y equitativo a las tecnologías de la información y la comunicación (Ruíz y de la Osa, 2021; Shackelford, 2021; Deibert, 2018).
2. Promover la colaboración y formación de alianzas entre organizaciones: Fomentar la integración de alianzas entre organizaciones del sector público y privado para incorporar la seguridad digital en sus agendas y programas, y desarrollar acciones conjuntas de divulgación y concientización en la sociedad (Gómez y Gregory, 2024).
3. Fomentar la educación y capacitación en seguridad digital: Desarrollar programas y cursos de capacitación en seguridad digital que aborden temas relacionados con la construcción de sociedades más seguras, como la resolución de conflictos en línea, la promoción del diálogo intercultural y la prevención de la radicalización y el extremismo en entornos digitales.

La implementación efectiva de estas estrategias y acciones de divulgación tiene el potencial de aumentar la conciencia pública sobre el papel crucial de la seguridad digital en la construcción de sociedades más seguras, al reducir la vulnerabilidad y fomentar la capacidad de agencia de los individuos y comunidades, contribuyendo significativamente a la creación de un ecosistema digital más resiliente.

Este enfoque integral no solo fortalece la infraestructura digital de México, sino que también sienta las bases para una sociedad más informada, empoderada y capaz de enfrentar los desafíos de seguridad en la

era digital. La promoción de una cultura de seguridad digital robusta e inclusiva es, por tanto, un elemento estratégico para el desarrollo sostenible y la cohesión social en el contexto mexicano.

CONCLUSIONES.

La seguridad digital ha emergido como un tema trascendental para organizaciones y sociedades, convirtiéndose en un pilar fundamental para el progreso y bienestar social. El incremento de la dependencia tecnológica ha acentuado la necesidad de proteger y asegurar la información frente a las crecientes amenazas digitales.

Esta investigación ha examinado la compleja interrelación entre la seguridad digital y las violencias estructurales, revelando su significativo impacto en la sociedad contemporánea. Los hallazgos subrayan la naturaleza multifacética de esta conexión y sus implicaciones para el desarrollo de políticas públicas y estrategias de seguridad integral.

Primordialmente, se ha evidenciado que la seguridad digital trasciende su papel tradicional de protección de sistemas e información, emergiendo como una herramienta fundamental en la mitigación de violencias estructurales. Al abordar las desigualdades en el acceso a la tecnología y la educación digital, la seguridad digital puede contribuir significativamente a reducir las vulnerabilidades de grupos marginados, promoviendo así una mayor equidad social en el entorno digital.

Un hallazgo clave es la necesidad imperativa de adoptar un enfoque holístico e interdisciplinario en las estrategias de seguridad digital. Este enfoque debe integrar aspectos técnicos, sociales, éticos y legales, considerando las dimensiones humanas y organizacionales, así como las implicaciones éticas de las políticas y prácticas de seguridad digital. La complejidad de los desafíos identificados demanda una perspectiva que vaya más allá de las soluciones puramente técnicas, abarcando consideraciones sociales y éticas más amplias.

La investigación enfatiza la importancia fundamental de la educación y la concientización en la construcción de una cultura de seguridad digital resiliente. Las campañas de concientización, talleres y programas educativos emergen como elementos críticos para empoderar a todos los segmentos de la sociedad, con un énfasis particular en la inclusión de grupos vulnerables. Estos esfuerzos educativos no solo mejoran la seguridad individual, sino que también contribuyen a la creación de un ecosistema digital más seguro y equitativo.

La clara conexión establecida entre la seguridad digital y la protección de los derechos humanos y la justicia social subraya la necesidad de enfocar las estrategias de seguridad digital no solo en la protección de sistemas, sino también en la promoción activa de la equidad y la justicia en el entorno digital. Este enfoque ampliado posiciona a la seguridad digital como un componente integral de los esfuerzos más amplios de justicia social y protección de derechos humanos.

También, se resalta la importancia crítica de la colaboración intersectorial. La sinergia entre organizaciones públicas, privadas y de la sociedad civil se revela como esencial para abordar eficazmente los desafíos de la seguridad digital y su impacto en las violencias estructurales. Esta colaboración no solo mejora la eficacia de las estrategias de seguridad digital, sino que también fomenta un enfoque más inclusivo y participativo.

Además, se revela el potencial significativo de la seguridad digital como factor contribuyente a los procesos de construcción de comunidades más seguras. Su papel en la prevención de conflictos y la promoción del diálogo intercultural en entornos digitales subraya su relevancia más allá de la mera protección técnica, posicionándola como un elemento clave en la construcción de sociedades más cohesivas y resilientes.

Un desafío crucial para el futuro es el desarrollo e implementación de políticas y prácticas de seguridad digital que no solo protejan contra amenazas digitales, sino que también aborden y mitiguen las violencias

estructurales subyacentes. Este enfoque integral promete no solo mejorar la seguridad digital, sino también contribuir significativamente al bienestar general de la sociedad y al logro de los Objetivos de Desarrollo Sostenible.

Dado este panorama complejo, resulta imperativo que la comunidad académica y profesional se comprometa a examinar minuciosamente los mecanismos de violencia estructural digital existentes. Este análisis crítico, representa un acercamiento hacia la comprensión de cómo las tecnologías digitales pueden, inadvertidamente, reforzar o crear nuevas formas de opresión y desigualdad.

Esta línea de investigación se perfila como esencial para avanzar en la comprensión y la optimización de la seguridad digital en el contexto de las violencias estructurales y el desarrollo social sostenible. Futuras investigaciones pueden profundizar en la evaluación empírica de las relaciones identificadas y en el desarrollo de marcos operativos robustos para la implementación efectiva de estrategias integradas de seguridad digital; además, es necesario el desarrollo de estudios que adopten enfoques metodológicos mixtos y longitudinales que permitan capturar la complejidad y dinamismo de estas interacciones, así como la colaboración interdisciplinaria para abordar las múltiples facetas de esta problemática.

REFERENCIAS BIBLIOGRÁFICAS.

1. Ahamed, B., Polas, M. R., Kabir, A. L., Sohel-Uz-Zaman, A. M., Al Fahad, A., Chowdhury, S., & Dey, M. R. (2024). Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era. SAGE OPEN, 14(1). https://doi.org/10.1177/21582440241228920
2. Alhalafi, N., & Veeraraghavan, P. (2021). Cybersecurity Policy Framework in Saudi Arabia: Literature Review. Frontiers in Computer Science, 3, 736874. https://doi.org/10.3389/fcomp.2021.736874

3. Baek, H., & Lee, H. (2021). Framework of Socio-Technology Analysis and Prescriptions for a sustainable society: Focusing on the mobile technology case. Technology in Society, 65. https://doi.org/10.1016/j.techsoc.2020.101523

4. Blackwood-Brown, C., & Levy, Y. (2021). Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. Journal of Computer Information Systems, 61(3), 195-206. https://doi.org/10.1080/08874417.2019.1579076

5. Borelli, D., & Greer, B. T. (2021). The Next Step: The California Cybersecurity Institute's Anti-Trafficking Virtual Reality Immersion Training. Anti-Trafficking Review, 17, 154-160. https://doi.org/10.14197/atr.2012211711

6. Burton, C. W., Gilpin, C. E., & Draughon, M. J. (2021). Structural violence: A concept analysis to inform nursing science and practice. Nursing Forum, 56(2), 382-388. https://doi.org/10.1111/nuf.12535

7. Caviglione, L., Wendzel, S., Mileva, A., & Vrhovec, S. (2021). Guest Editorial: Multidisciplinary Solutions to Modern Cybersecurity Challenges. Journal of Wireless Mobile Networks Ubiquitous Computing and Dependable Applications, 12(4), 1-3. https://doi.org/10.22667/JOWUA.2021.12.31.001

8. Cheng, E. C., & Wang, T. C. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Information, 13(4), 192. https://doi.org/10.3390/info13040192

9. Choodakowska, A., Kandula, S., & Przbylska, J. (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. LEX Localis Journal of Social Self-Government, 20(1), 161-192. https://doi.org/10.4335/20.1.161-192(2022)

10. Chychkan I., V., Spasiteleva, S.O.Zhdanova, Y.D. (2021). The educational environment for forming secure base behavior in cyberspace of future professionals in economics and management. Information Technologies and Learning Tools, 84354-375. https://doi.org/10.33407/itlt.v84i4.3646
11. De Soto, B. G., Georgescu, A., Mantha, B., Turk, Z., Maciel, A., & Semih, M. (2022). Construction cybersecurity and critical infraestrcutrue protection: New horizons for construction 4.0. Journal of Information Technology in Construction, 27(28), 571594. https://doi.org/10.36680/j.itcon.2022.028
12. Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. Ethics & International Affairs, 32(4), 411-424. https://doi.org/10.1017/S0892679418000618
13. Delgado, M. F., Esenarro, D., Regalado, F. F., & Reategui, M. D. (2021). Methodology based on the nist cybersecurity framework a proposal for cybersecurit management in government organizations. 3c TIC, 10(2), 123-141. https://doi.org/10.17993/3ctic.2021.102.123-141
14. Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. Applied Sciences-Basel, 13(2). https://doi.org/10.3390/app13020790
15. Dutton, W. H., Creese, S., Shillar, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? Journal of Information Policy(9), 280-306. https://doi.org/10.5325/jinfopoli.9.2019.0280
16. Duxburt, S. W., & Haynie, D. L. (2019). Criminal network security: An agent-based approach to evaluating network resilience*. Criminology, 52(2), 314-342. https://doi.org/10.1111/1745-9125.12203
17. Flynn, C., Damant, D., Lapierre, S., Lessard, G., Gagnon, C., Couturier, V., & Couturier, P. (2018). When structural violences create a context that facilitates sexual assault and intimate partner violence against street-involved young women. Women's Studies International Forum, 68, 94-103. https://doi.org/10.1016/j.wsif.2018.01.004

18. Gobierno de México. (2017). Estrategia Nacional de Ciberseguridad. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
19. Gómez, M. A., & Gregory, W. (2024). Public opinion and alliance commitments in cybersecurity an attack against all? International Interactions, 50(2), 332-348. https://doi.org/10.1080/03050629.2024.2310014
20. Greyson, D. (2019). The Social Informatics of Ignorance. Journal of the Association For Information Science and Technology, 70(4), 412-415. https://doi.org/10.1002/asi.24143
21. Harper, S. (2022). Structural Violence: Lets Face It. Analecta Política, 12(22), 1-4.
22. Hérnandez, J. G., & Salcedo, M. T. (2020). The influence and benefits of technology as a strategy in organizations. Multidisciplinary Journal for Education Social and Technological Sciences, 7(3), 32-53. https://doi.org/10.4995/muse.2020.10693
23. Hernández-Ramos, J. L., Geneiatakis, D., Kounelis, I., Steri, G., & Fovino, I. N. (2020). Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data-Protection Policies. IEEE Security & Privacy, 18(1), 28-38. https://doi.org/10.1109/MSEC.2019.2939728
24. Holgeid, K. K., Krogstie, J., Mikalef, P., Saur, E. E., & Sjøberg, D. I. (2022). Benefits management and Information Technology work distribution. IET software, 16(4), 438-454. https://doi.org/10.1049/sfw2.12062
25. Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding Local Government Cybersecurity Policy: A Concept Map and Framework. Information, 15(6), 342. https://doi.org/10.3390/info15060342

26. Hyman, I., Vahabi, M., Bailey, A., Patel, S., Guruge, S., Wilson-Mitchell, K., & Wong, J. P. (2016). Taking action on violence through research, policy, and practice. Global Health Research and Policy, 1, 1-9. https://doi.org/10.1186/s41256-016-0006-7

27. Kalogiannidis, S., Paschalidou, M., Kalfas , D., & Chatzitheodoridis, F. (2023). Relationship between Cyber Security and Civil Protection in the Greek Reality. Applied Sciences-Basel, 13(4). https://doi.org/10.3390/app13042607

28. Kivimaa, P., Brisbois, M. C., Jayaram, D., Hakala, E., & Siddi, M. (2022). A socio-technical lens on security in sustainability transitions: Future expectations for positive and negative security. Futures, 141, 102971. https://doi.org/10.1016/j.futures.2022.102971

29. Kleba, J. B., & Reina-Rozo, J. D. (2021). Fostering peace engineering and rethinking development: A Latin American view. Technological Forecasting and Social Change, 167, 120711. https://doi.org/10.1016/j.techfore.2021.120711

30. Kosevich, E. Y. (2022). Cyberspace security in Latin American Countries. Polis-Politicheskiye Issledovaniya, 3, 108-123. https://doi.org/10.17976/jpps/2022.03.09

31. La Parra-Casado, D., & Tortosa, J. M. (2003). Violencia estructural: una ilustración del concepto. Observatorio Europeo de Tendencia Sociales.

32. Lamas, S., Quintas, P., Neves, J. C., & Remondes, J. (2023). Cybersecurity, Privacy, and Data Protection: State of the Art in Iran, Nigeria, Portugal, and the USA. International Journal of Marketing, Communications and New Media(12), 1-4. https://doi.org/10.54663/2182-9306.2023.sn12.1-4

33. Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. H. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

34. Macassa, G. (2023). Does Structural Violence by Institutions Enable Revictimization and Lead to Poorer Health Outcomes? - A Public Health Viewpoint. Annals of Global Health, 89(1), 1-7. https://doi.org/10.5334/aogh.4137

35. MacManus, S. A., Caruson, K., & PcPhee, B. D. (2013). Cyersecurity at the local government: Balancing demands for trasnparency and privacy rights. Journal of Urban Affairs, 35(4), 451-470. https://doi.org/10.1111/j.1467-9906.2012.00640.x

36. Malekos, Z., Lostri, E., & Lewis, J. A. (2020). The Hidden Costs of Cybercrime. Retrieved 2 de Diciembre de 2022, from McAfee: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

37. Mihelic, A., & Vrhovec, S. (2018). Obligation to Defend the Critical Infrastructure? Offensive Cybersecurity Measures. Journal of Universal Computer Science, 24(5), 646-661.

38. Morales-Sáenz, F. I., Medina-Quintero, J. M., & Ortíz-Rodríguez, F. (2023). Bibliometrics Study of Organizational Cybersecurity. En Emerging Technologies and Digital Transformation in the Manufacturing Industry (págs. 115-139). IGI Global. https://doi.org/10.4018/978-1-6684-8088-5.ch008

39. Morales-Sáenz, F. I., Medina-Quintero, J. M., & Reyna-Castillo, M. (2024). Beyond Data Protection: Exploring the Convergence between Cybersecurity and Sustainable Development in Business. Sustainability, 16(14), 5884. https://doi.org/10.3390/su16145884

40. Nizovtsev, Y. Y., Parfylo, O. A., Barabash, O. O., Kyrenko, S. G., & Smetanina, N. V. (2022). Mechanisms of money laundering obtained from cybercrime: the legal aspect. Journal of Money Laundering Control, 25(2), 297-305. https://doi.org/10.1108/JMLC-02-2021-0015

41. Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., & Shakarian, P. (2016). Darknet and deepnet mining for proactive cybersecurity threat intelligence. IEEE Conference on Intelligence and Security Informatics (ISI), 7-12.
42. Plachkinova, M. (2023). A Taxonomy for Risk Assessment of Cyberattacks on Critical Infrastructure (TRACI). Communications of the association for information systems, 52(1).
43. Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-pishing techniques. Computer Science Review(29), 44-55. https://doi.org/10.1016/j.cosrev.2018.05.003
44. Quintero, D. M. (2022). La ciberseguridad y la ciberdefensa frente a los. Ciberespacio, Tecnología e Innovación, 1(1). https://doi.org/10.25062/2955-0270.4767
45. Raguz, M. (2019). Structural violence: Its many faces and challenges in research, policies, prevention and intervention. Journal of Prevention & Intervention in the Community. https://doi.org/10.1080/10852352.2019.1664716
46. Ruíz, S. C., & de la Osa, R. M. (2021). Big Data in health: a new paradigm to regulate, a challenge for social justice. Revista Española de Salud Pública, 95, e20202110150
47. Seidemann, R. M., & Halling, C. L. (2019). Landscape structural violence: A view from New Orleans's cemeteries. American Antiquity, 84(4), 669-683.
48. Shackelford, S. J. (2021). Shoul cybersecurity be a human right? Exploring the Shared responsibillity of cyberpeace. En Music, Business and Peacebuilding (págs. 174-197). Routledge.
49. Shires, J. (2018). Enacting expertise: Ritual and risk in cybersecurity. Politics and Governance, 6(2), 31-40. https://doi.org/10.17645/pag.v6i2.1329

50. Silaule, C. B., Makhubele, L. M., & Mamorobela, S. P. (2022). A model to reduce insider cybersecurity threats in a South African telecommunications company. South African Journal of Information Management, 24(1), 1-8. https://doi.org/10.4102/sajim.v24i1.1573

51. Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. Politics and Governance, 6(2), 1-4. https://doi.org/10.17645/pag.v6i2.1569

52. Vasiu, I., & Vasiu, L. (2018). Cybersecurity as an Essential Sustainable Economic Development Factor. European Journal of Sustainable Development, 7(4), 171-178. https://doi.org/10.14207/ejsd.2018.v7n4p171

53. Weir, C., Becker, I., & Blair, L. (2023). Incorporating software security: using developer workshops to engage product managers. Empiriral Software Engineering, 28(2). https://doi.org/10.1007/s10664-022-10252-0

54. Winters, N., Eynon, R., Geniets, A., Robson, J., & Kahn, K. (2019). Can we avoid digital structural violence in future learning systems? Learning, Media and Techonology, 17-30. https://doi.org/10.1080/17439884.2020.1708099

55. Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. International Journal of Human-Computer Studies, 131, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

DATOS DE LOS AUTORES.

1. **Francisco Isaí Morales-Sáenz**. Maestría en Dirección Empresarial. Profesor-Investigador de la Facultad de Comercio y Administración Victoria, de la Universidad Autónoma de Tamaulipas, México. Correo electrónico: fmsaenz@uat.edu.mx

2. **José Melchor Medina-Quintero.** Doctorado en Sistema de Información de la Empresa. Profesor-Investigador de la Facultad de Comercio y Administración Victoria, de la Universidad Autónoma de Tamaulipas, México. Correo electrónico: jmedinaq@uat.edu.mx

3. **Fernando Ortiz Rodríguez**. Doctorado en Gestión Estratégica de Negocios. Profesor-Investigador de la Unidad Académica Multidisciplinaria Reynosa Rodhe, de la Universidad Autónoma de Tamaulipas, México. Correo electrónico: ferortiz@uat.edu.mx

RECIBIDO: 8 de septiembre del 2024. **APROBADO:** 21 de octubre del 2024.