Estrategia de ciberseguridad para Michoacán, análisis y selección de alternativas

Cybersecurity strategy for Michoacán, analysis and selection of alternatives

Mario Gómez[1]
Cecilia Patricia Navarrete Soriano[2]
Jerjes Aguirre Ochoa[3]

Recibido: 10 de marzo de 2025 Aprobado: 28 de abril de 2025
DOI: https://doi.org/10.33110/cimexus200103

Resumen

La ciberseguridad se ha convertido en un factor crucial y determinante para garantizar una interacción segura y respetuosa en el ciberespacio, protegiendo la privacidad, la seguridad de la información y los derechos digitales, con el fin de crear un entorno digital confiable e inclusivo. Esta investigación tiene como objetivo identificar los principales componentes que podrían formar parte de una estrategia de ciberseguridad en el Estado de Michoacán, México. Para ello, se realizó una encuesta a un grupo de expertos en ciberseguridad conformado por los integrantes de las diferentes Unidades de Policía Cibernética a nivel nacional (2023). La metodología utilizada fue el modelado de ecuaciones estructurales de mínimos cuadrados parciales (SEM-PLS). Los resultados principales muestran que el cibercrimen y la seguridad de información son variables determinantes para la ciberseguridad. Estos hallazgos destacan que el cibercrimen no es una amenaza aislada y que la seguridad de la información es un elemento crucial para combatir las amenazas en el ciberespacio. Ambas variables tienen una relación causal y son fundamentales, requiriendo una atención integral en la formulación de estrategias efectivas en materia de ciberseguridad.

Palabras clave: ciberseguridad, cibercrimen, seguridad de la información y ciberespacio.

1 Autor de correspondencia. Profesor Investigador. Universidad Michoacana de San Nicolás de Hidalgo, Instituto de Investigaciones Económicas y Empresariales, México. ORCID: https://orcid.org/0000-0002-1178-108X. Correo electrónico: mgomez@umich.mx

2 Universidad Michoacana de San Nicolás de Hidalgo, Instituto de Investigaciones Económicas y Empresariales, (ININEE). Directora de la Policía Cibernética. Fiscalía General del Estado de Michoacán, México. ORCID: https://orcid.org/0000-0002-0722-5064. Correo electrónico: 2026806f@umich.mx

3 Profesor Investigador. Universidad Michoacana de San Nicolás de Hidalgo, Instituto de Investigaciones Económicas y Empresariales, México. ORCID: https://orcid.org/0000-0001-7858-5166. Correo electrónico: jerjes.aguirre@umich.mx

Abstract

Cybersecurity has become a crucial and determining factor in ensuring safe and respectful interaction in cyberspace, protecting privacy, information security, and digital rights, in order to create a trustworthy and inclusive digital environment. This research aims to identify the main components that could be part of a cybersecurity strategy in the State of Michoacán, Mexico. To this end, a survey was conducted among a group of cybersecurity experts made up of members of the different Cyber Police Units nationwide (2023). The methodology used was structural equation modeling with partial least squares (SEM-PLS). The main results show that cybercrime and information security are determining variables for cybersecurity. These findings highlight that cybercrime is not an isolated threat and that information security is a crucial element in combating threats in cyberspace. Both variables are causally related and fundamental, requiring comprehensive attention in the formulation of effective cybersecurity strategies.

Keywords: cybersecurity, cybercrime, information security and cyberspace.

Introducción

Las tecnologías de la información y comunicación (TIC's) desempeñan un papel fundamental en la humanidad, abarcando diversas herramientas, servicios y procesos que permiten almacenar, procesar y transmitir grandes cantidades de información. Estas tecnologías incluyen servicios de comunicación, servicios de información, desarrollo de software, infraestructura de red, tecnologías emergentes, aplicaciones web y la automatización, que permiten la conectividad global y la creación de redes interpersonales. Esta evolución tecnológica ha transformado la forma en que nos comunicamos e interrelacionamos (Turban et al., 2018). En este contexto, la ciberseguridad se convierte en un factor crucial y decisivo para garantizar la seguridad y confiabilidad de estas interacciones, protegiendo la integridad y privacidad de la información en un entorno cada vez más interconectado.

A pesar de los beneficios que las TIC´s han aportado, su interconectividad también presenta escenarios de riesgo en el ciberespacio. Los usuarios están expuestos a diversas amenazas como el robo de datos, fraude, suplantación de identidad, ransomware, phishing, ataques de denegación de servicio, inyección de código SQL, inteligencia artificial, sexting, grooming, pharming, doxing, accesos no autorizados, virus informáticos, entre otros Sain (2018). La falta de conocimiento sobre estas amenazas ha llevado a la aparición de comportamientos arriesgados que han dado lugar a un tipo de delincuencia cibernética en Internet, conocido como cibercrimen.

El creciente uso de las Tecnologías de Información y Comunicación ha generado un entorno propicio para el cibercrimen. La dependencia digital ha ampliado la superficie de ataque, ofreciendo a los ciberdelincuentes numerosas oportunidades para explotar vulnerabilidades. La falta de concientización sobre los riesgos cibernéticos agrava esta situación, permitiendo a los atacantes desarrollar técnicas cada vez más sofisticadas. Como resultado el cibercrimen ha incrementado, afectando no solo a individuos sino también a empresas e incluso Gobiernos. Los ataques cibernéticos, como el ransomware, las intrusiones y el robo de datos, representan una amenaza significativa para la seguridad y la continuidad de las operaciones.

El objetivo de esta investigación es analizar el impacto del cibercrimen y la seguridad de la información en la ciberseguridad del Estado de Michoacán, México.

El presente artículo está estructurado de la siguiente manera: Primero, se presenta la justificación destacando la necesidad de comprender y mitigar los riesgos del cibercrimen y mejorar la seguridad de la información, se muestra, mediante estadísticas, como las investigaciones realizadas por la Policía Cibernética han incrementado continuamente, subrayando la importancia de ciberseguridad

A continuación en el marco teórico, se realiza una revisión de la literatura, examinando estudios previos sobre ciberseguridad, riesgos y amenazas en el ciberespacio.

Posteriormente, se describe la metodología utilizada detallando el método para probar la hipótesis en ciberseguridad, definiendo las particularidades y relaciones causales entre las variables para demostrar su fortaleza.

En la sección de resultados, se presentan los hallazgos obtenidos mediante la técnica de segunda generación PLS-SEM (Partial Least Squares Structural Equation Modeling), utilizada para estudios exploratorios. Esta herramienta estadística permite analizar las relaciones entre variables latentes y observables en un modelo teórico.

Finalmente, en las conclusiones, se propone el diseño de una estrategia específica para Michoacán. Además, se proporciona una base sólida para futuras investigaciones, mejorando la toma de decisiones y la implementación de acciones específicas para enfrentar los desafíos en ciberseguridad.

Justificación

La ciberseguridad emerge como una necesidad imperante ante el uso generalizado del ciberespacio en la era digital. Según Caballero y Cilleros (2019), diversas comunidades intercambian información en el ciberespacio, enfrentando constantes amenazas sin la debida concientización de los riesgos. Trim y Lee (2021) indican que la ciberseguridad incluye mecanismos, sistemas, estrategias y protocolos para prevenir y proteger el ciberespacio contra el acceso no autorizado, salvaguardando los principios de seguridad de la información.

El incremento de usuarios de las tecnologías de la información y comunicaciones ha creado un escenario en el que los riesgos y amenazas se han multiplicado exponencialmente. Esta dependencia tecnológica ha generado una amplia superficie de ataque, proporcionando a los ciberdelincuentes numerosas oportunidades para explotar diversas vulnerabilidades. Entre ellas, la falta de concientización sobre los riesgos se destaca como un campo fértil para el desarrollo de ataques cada vez más sofisticados.

Bajo estas condiciones, el cibercrimen surge como consecuencia directa de la explotación de estas vulnerabilidades, sumado la dificultad de rastrear a los ciberdelincuentes debido a la sofisticación de los vectores de ataque. Esto hace que estas amenazas sean más difíciles de detectar y contrarrestar, contribuyendo al crecimiento de la impunidad en este tipo de riesgos (Franco, 2018).

Estos riesgos no solo afectan a los usuarios, sino que también representan amenazas significativas, reales y palpables para las empresas e incluso el gobierno. Las organizaciones dependen de las TIC´s para la gestión de datos y la prestación de servicios públicos y privados a la sociedad, sin los mecanismos o controles de seguridad adecuados, pueden ser víctimas de diversos ciberdelincuentes, enfrentándose a diversas amenazas o ataques como ransomware, intrusiones, robo de datos, malware, virus, ataques a infraestructuras críticas entre otros.

La ausencia de seguridad de la información y de los conocimientos necesarios para salvaguardar los datos compromete la integridad de estos, provocando riesgos y vulnerabilidades. La falta de concientización y capacitación abre la puerta a diversas amenazas como el phishing, robo de datos, fuga de información, ransomware, ataques de ingeniería social, entre otros. En este contexto, datos recopilados en el año 2021 y presentados en julio del año 2022 muestran que el Estado de Michoacán ocupó el primer lugar a nivel nacional en Ciberacoso, con un 28.8 % de usuarios que experimento algún tipo durante el año anterior (Instituto Nacional de Geografía y Estadística [INEGI], 2022). Esta preocupante estadística podría deberse a la falta de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de los datos.

En este sentido, la seguridad de la información evita, entre otras cosas, la difusión no autorizada de información personal como fotografías e información de contacto y la manipulación de imágenes, que los acosadores utilizan en el ciberespacio. Así, esta variable juega un papel crucial en la lucha contra el cibercrimen, informando sobre los riesgos y amenazas en esta interacción digital y fortaleciendo la ciberseguridad.

El Estado de Michoacán, no ha sido ajeno al cibercrimen. A medida que el uso de internet crece a nivel mundial, más usuarios, empresas y gobiernos se adentran en el ciberespacio, utilizándolo como un medio de comunicación, que ofrece una amplia gama de herramientas y conectividad en línea. Esta interconectividad brinda un campo amplio para que los ciberdelincuentes se aprovechen de estas oportunidades.

Una muestra de esto, se refleja en la Tabla 1, donde se presenta información recabada del portal de Transparencia y Acceso a la Información Pública del Estado de Michoacán. La tabla muestra cómo las investigaciones realizadas por la Policía Cibernética han incrementado continuamente cada año desde 2016 hasta 2023.

Tabla 1
Estadísticas de colaboraciones Policía Cibernética.

Año	Colaboraciones Policía Cibernética	Variación porcentual con respecto al año inmediato anterior
2016	373	—
2017	413	10.72%
2018	630	52.54%
2019	1,238	96.50%
2020	1,730	39.74%
2021	1,931	11.61%
2022	2,915	51.03%
2023	4,003	37.32%
TOTAL. .	**13,233**	

Fuente: Elaboración propia con información del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), (2024).

De la problemática descrita surge el interés por investigar el aumento de los delitos cibernéticos y la creciente vulnerabilidad de la información en el Estado de Michoacán, lo que evidencia la necesidad de una estrategia de ciberseguridad robusta. Este artículo busca comprender la compleja relación entre el cibercrimen y la seguridad de la información, con el objetivo de identificar los componentes clave que deben considerarse para desarrollar una estrategia integral que aborde de manera efectiva los desafíos de la ciberseguridad en la entidad.

La investigación tiene como objetivo estudiar el efecto del cibercrimen y la seguridad de la información en la ciberseguridad en el Estado de Michoacán, México. Partiendo de la hipótesis de que ambas variables influyen significativamente en la ciberseguridad, especialmente dado el aumento continuo de delitos y conductas de riesgo asociados a la creciente conectividad.

Marco teórico

La base teórica de esta investigación se apoya en autores que han establecido los cimientos para el desarrollo de la ciberseguridad, entre los que destacan: Bruce Schneier (2000), Whitfield y Hellman (2022), Stallings (2017), Santos (2019), Vergara y Huidobro (2016), Caballero y Cilleros (2019) y Arroyo et al. (2020).

La ciberseguridad se define como un conjunto integral de reglas, técnicas, controles y prácticas recomendadas diseñadas para proteger los activos de información de individuos, empresas y gobiernos contra los riesgos presentes en el ciberespacio. Esta disciplina abarca una amplia gama de estrategias, prácticas y tecnologías destinadas a salvaguardar la información y la infraestructura tecnológica, garantizando así la protección de la sociedad frente a las amenazas digitales. La ciberseguridad no solo involucra la implementación de medidas técnicas, sino también el desarrollo de políticas y procedimientos que aseguren la confidencialidad, integridad y disponibilidad de la información.

Según Ferrer (2021), Parada y Errecaborde (2018) y Rayón y Gómez (2014), el cibercrimen se refiere a actividades delictivas que se perpetran mediante el uso de equipos de cómputo y afectan la interacción entre usuarios, empresas y gobiernos en el ciberespacio. Este fenómeno abarca una amplia gama de delitos cibernéticos, que pueden implicar la utilización de tecnología como medio para llevar a cabo infracciones o como el propio objetivo de la actividad delictiva. El cibercrimen puede incluir acciones como el robo de datos, fraudes en línea, suplantación de identidad, ataques de denegación de servicio, entre otros. Ambos autores coinciden en que la tecnología, ya sea como herramienta para cometer delitos o como blanco de los mismos, juega un papel central en estas actividades ilícitas, destacando la complejidad y el alcance de las amenazas en el entorno digital actual.

Por otra parte Ellis y Mohan (2019) definen la seguridad de la información como la capacidad de salvaguardar la confidencialidad, integridad y disponibilidad de la información, y también consideran otros atributos esenciales como la confiabilidad, autenticidad y el no repudio. La norma ISO 27001 (2014) complementa esta definición, describiendo la seguridad de la información como un conjunto de medidas proactivas y reactivas diseñadas para mantener y proteger estos principios fundamentales. Esta norma establece un marco para gestionar la seguridad de la información mediante la implementación de controles adecuados que previenen y responden a los riesgos. La combinación de estas perspectivas subraya la importancia de asegurar no solo la protección básica de la información, sino también su validez, la capacidad de verificar su origen y autenticidad, y la garantía de que las acciones realizadas no puedan ser negadas posteriormente.

En este sentido Callanan y Tropina (2015) y Hamelink (2016) describen el ciberespacio como una infraestructura tecnológica que incluye redes de computadoras, servidores, dispositivos móviles y otros elementos físicos que posibilitan la transmisión y almacenamiento de datos. Esta infraestructura también abarca sistemas de información, como software y aplicaciones que gestionan, procesan y analizan la información. Además, el ciberespacio es un área virtual ilimitada geográficamente, conformada por diversas tecnologías digitales. No solo incluye el uso de computadoras conectadas en red, sino también la interacción de usuarios a través de plataformas digitales, servicios

en línea y redes sociales, permitiendo que la información y las interacciones en línea sucedan mediante diversos protocolos de comunicación, que son las reglas y estándares que regulan la interacción entre los diferentes elementos del ciberespacio.

Metodología

Diseño de la investigación

La presente investigación adopta un diseño no experimental, descriptivo y correlacional. Este enfoque permite examinar el objeto de estudio de manera clara y detallada, recolectando los datos en un único momento y bajo un enfoque mixto, facilitando así una comprensión más integral del fenómeno en estudio (Hernández-Sampieri y Mendoza, 2018). Se eligió este diseño porque es el más adecuado para analizar y explicar el efecto del cibercrimen y la seguridad de la información sobre la ciberseguridad, proporcionando una visión completa y precisa de las relaciones entre estas variables.

Muestra

La investigación se sustenta en un instrumento de medición aplicado a una muestra no probabilística de 76 expertos en ciberseguridad pertenecientes a las diferentes Unidades de Policía Cibernética[4] a nivel nacional, las cuales forman parte del Modelo Homologado de Unidades de Policía Cibernética que se crea en el año 2017 para responder a los desafíos que México comenzó a enfrentar en el ámbito cibernético, inicialmente relacionados con conductas de riesgo y delitos en línea.

La recopilación de datos se realizó mediante un formulario de Google Forms, enviada por correo electrónico a cada experto.

La literatura académica respalda sólidamente el uso de grupos de expertos como recurso investigativo en el campo de la ciberseguridad. Según Kaplan y Garrick (1981), los grupos de expertos son una técnica efectiva en la evaluación de riesgos, ya que permiten integrar conocimientos especializados y experiencias prácticas para abordar desafíos complejos.

A partir de las opiniones y experiencias recopiladas de estos expertos, es posible obtener información clave para sustentar la elaboración de una estrategia efectiva en ciberseguridad. Los expertos en ciberseguridad suelen tener una amplia experiencia, conocimiento especializado, poseen un profundo entendimiento de las amenazas cibernéticas actuales, las vulnerabilidades comunes y las mejores prácticas para protegerse contra posibles ataques. Al estar en contacto directo con los usuarios y conocer la problemática a nivel nacional,

4 En México muchos de los expertos en ciberseguridad forman parte de las 47 Unidades de Policía Cibernética pertenecientes a las Secretarías de Seguridad Pública, Fiscalías/Procuradurías de las 31 entidades federativas y la Ciudad de México y/o de la División General Científica de la Guardia Nacional.

los expertos pueden ofrecer una visión global y contextualizada de la situación actual de la ciberseguridad en Michoacán, lo cual es fundamental para diseñar estrategias efectivas.

Variables

Se seleccionaron como variables independientes el Cibercrimen y la Seguridad de la información; y como variable dependiente a la Ciberseguridad. La elección de estas variables se fundamenta en una revisión exhaustiva de la literatura existente. Diversos estudios han señalado la influencia crítica del cibercrimen y la seguridad de la información en la ciberseguridad, destacando su relevancia en la protección de datos y la mitigación de riesgos en el entorno digital. Por mencionar, Ferrer (2021) y Parada y Errecaborde (2018) subrayan cómo el cibercrimen afecta directamente la seguridad digital, mientras que Rayón y Gómez (2014) detallan las múltiples facetas del cibercrimen que ponen en riesgo a la ciberseguridad. En lo que respecta a la seguridad de la información Ellis y Mohan (2019) la norma ISO 27001 (2014) muestran la importancia de mantener la confidencialidad, integridad y disponibilidad de los datos como pilares de la ciberseguridad. Esta fundamentación teórica proporciona una base sólida para la investigación, permitiendo analizar cómo estos factores interactúan y afectan la ciberseguridad en el Estado de Michoacán, México.

Técnicas e instrumentos de recolección de datos

El instrumento diseñado para el acopio de los datos es un cuestionario basado en una escala de Likert (1932) método desarrollado en el campo de las ciencias sociales, esta escala asigna una puntuación matemática a cada ítem, permitiendo diferenciar la importancia de cada aspecto evaluado. El cuestionario se estructura de manera en que los participantes puedan expresar su nivel de acuerdo o desacuerdo con diversas afirmaciones relacionadas con el cibercrimen, la seguridad de la información y la ciberseguridad. En resumen, la Tabla 2 presenta la estructura del instrumento de medición y la distribución del número de preguntas por cada sección.

Tabla 2
Estructura del instrumento por variables

	Variables	Dimensiones	Número de preguntas
Variable independiente.	Cibercrimen Seguridad de la información	4 2	6 5
Variable dependiente.	Ciberseguridad	6	6
Total dimensiones y preguntas		12	17

Fuente: Elaboración propia con base en el instrumento 2023.

En relación con el cibercrimen, se indagó sobre la importancia de diversos factores que se convirtieron en indicadores para la variable, tales como 1) La falta de conocimiento de los internautas sobre el uso seguro del ciberespacio, 2) La insuficiente supervisión del tiempo que los menores pasan en línea, 3) La carencia de un marco legal robusto, 4) La escasez de personal capacitado y de equipos especializados, así como 5) La ausencia de campañas de concienciación y prevención. Estas preguntas son cruciales para lograr una comprensión más profunda de las causas y el impacto del ciberdelito en la ciberseguridad.

En cuanto a la seguridad de la información se les preguntó sobre 1) La relevancia de fomentar una cultura de seguridad que abarque a usuarios, empresas y el sector gubernamental, además de 2) La necesidad de establecer políticas adecuadas, 3) Realizar campañas de concienciación y formar equipos de respuesta. Estas medidas son fundamentales para garantizar la confidencialidad, integridad y disponibilidad de los activos de información frente a amenazas, ataques y accesos no autorizados tanto en entornos físicos como digitales.

Después de aplicar el cuestionario para el acopio de los datos, se procedió a darle un tratamiento estadístico, para examinar y obtener resultados y conclusiones a través del modelado de ecuaciones estructurales.

Modelización de ecuaciones estructurales

Las técnicas multivariantes de segunda generación superan muchas limitaciones de las técnicas de primera generación. El modelado de ecuaciones estructurales (SEM) se destaca por su capacidad para incorporar variables latentes que miden aspectos no directamente observables. Existen dos tipos principales de modelos SEM: los basados en covarianza (CB-SEM) y los de mínimos cuadrados parciales (PLS-SEM) (Hair, et al., 2017). En este estudio, se utiliza el enfoque PLS-SEM.

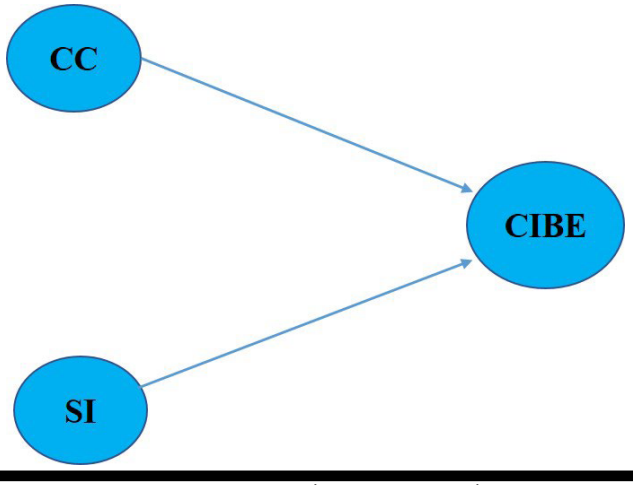
Para Hair et al. (2017), el enfoque PLS-SEM emplea el análisis de la varianza y es más flexible al no requerir supuestos paramétricos estrictos respecto a la distribución de los datos y el tamaño de la muestra, permitiendo evaluar relaciones causales complejas y por su capacidad predictiva. Para el objeto de este estudio, es esencial comprender las relaciones causales entre diferentes aspectos del cibercrimen y la seguridad de la información. El enfoque PLS-SEM permite examinar cómo estas variables están interconectadas y cómo afectan directa o indirectamente a la ciberseguridad en el Estado de Michoacán, proporcionando una base sólida para el desarrollo de estrategias efectivas.

El nomograma permite visualizar gráficamente las conexiones entre las variables (constructos) facilitando la comprensión de la lógica detrás de la relación hipotética que se busca verificar. En este estudio, el Cibercrimen (CC) y la Seguridad de la Información (SI) son las variables que se hipotetiza influyen en la Ciberseguridad (CIBE) en el Estado de Michoacán, México. La

Figura 1 presenta la especificación del modelo estructural, ilustrando cómo estas variables están interrelacionadas y destacando las rutas causales que serán evaluadas.

Y = Ciberseguridad
X1= Cibercrimen
X2= Seguridad de la información

***Figura* 1**
Nomograma de la ciberseguridad.



Fuente: Elaboración propia en Smart PLS con base en Hair et al. (2017).

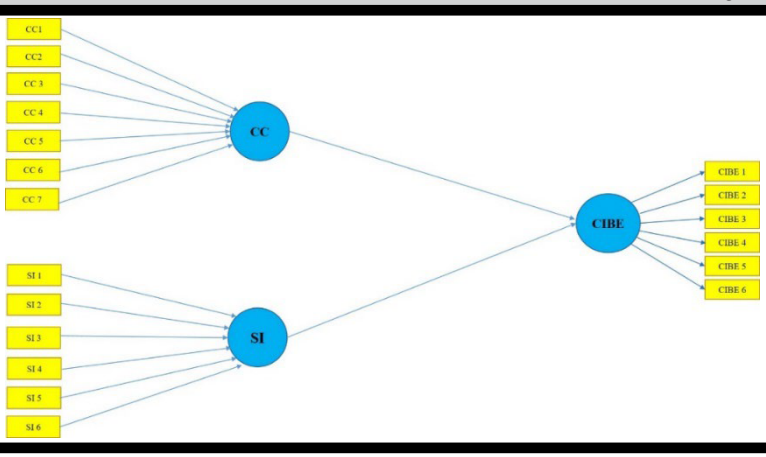
Resultados y discusión

Evaluación del modelo de medida o externo

Para la estimación del modelo, se utilizó el software estadístico SMART-PLS, versión 4, como primer paso se realizó una evaluación del modelo de medida externo y del modelo estructural, seguido de realizar un análisis de los resultados obtenidos. Se presentó el nomograma que muestra la lógica de la relación hipotética que se busca comprobar. La Figura 2 muestra la relación entre las variables latentes y los indicadores, con el propósito de presentar las relaciones causales planteadas en el modelo.

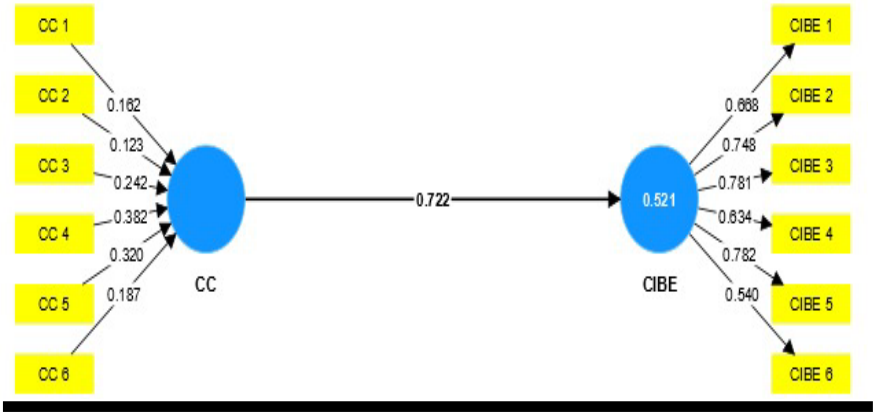
Una vez cargados los datos en el software Smart PLS, el proceso comienza con la validación convergente de las variables latentes, con lo que se espera obtener valores superiores a 0,7 (Hair et al., 2017). Posteriormente, se examinó la intensidad del coeficiente de trayectoria que conecta ambos constructos. La Figura 3 muestra la variable independiente CC y la variable dependiente CYBE. Se observa que el valor obtenido es 0.722, no presentando problemas de validez convergente por lo que la variable CC pasa a formar parte del modelo.

Figura 2
Relación estructural variables latentes e indicadores Ciberseguridad.



Fuente: Elaboración propia en Smart PLS con base en Hair et al. (2017).

Figura 3
Validez convergente variable CC y CIBE.

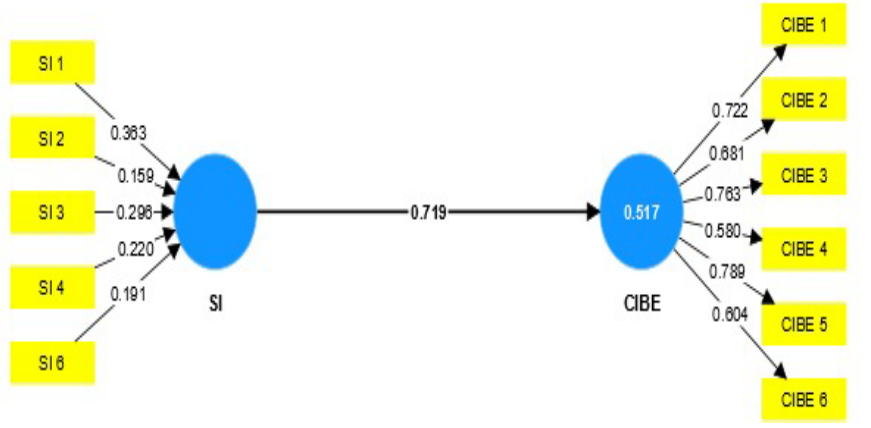


Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

En lo que respecta a la variable independiente seguridad de la información SI y la variable dependiente ciberseguridad CIBE, el valor alcanzado es de .719 no presentando problemas de validez convergente, como se aprecia en la Figura 4.

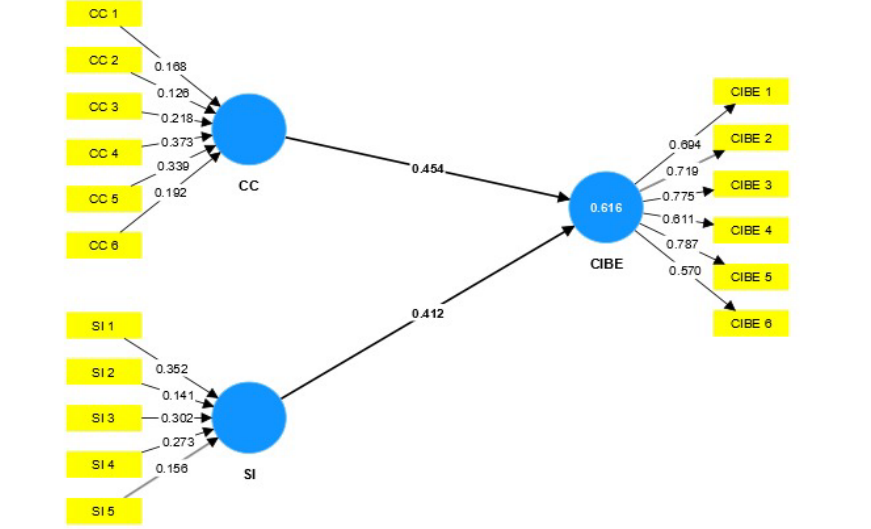
Los coeficientes de ruta se calculan para determinar las relaciones entre las variables latentes en el modelo propuesto, indicando el efecto que tiene la variable latente sobre la dependiente, donde se observa una fuerte relación entre las variables ya que los valores de los coeficientes de ruta obtenidos son 0,454 y 0,412 para CC e IS, respectivamente, como se presenta en la siguiente figura.

Figura 4
Validez convergente SI y CIBE.



Fuente: Elaboración propia en Smart PLS con base en Hair et al. (2017).

Figura 5
Coeficiente Path.



Fuente: Elaboración propia en Smart PLS con base en Hair et al. (2017).

Como segundo paso, el análisis de colinealidad se realiza utilizando valores VIF, que se calculan para cada indicador y proporcionan una estimación de cuánto está inflada la varianza de un estimador debido a la colinealidad con otros indicadores. Se busca obtener valores inferiores a 5 (Hair et al., 2017) como se muestra en la Tabla 3.

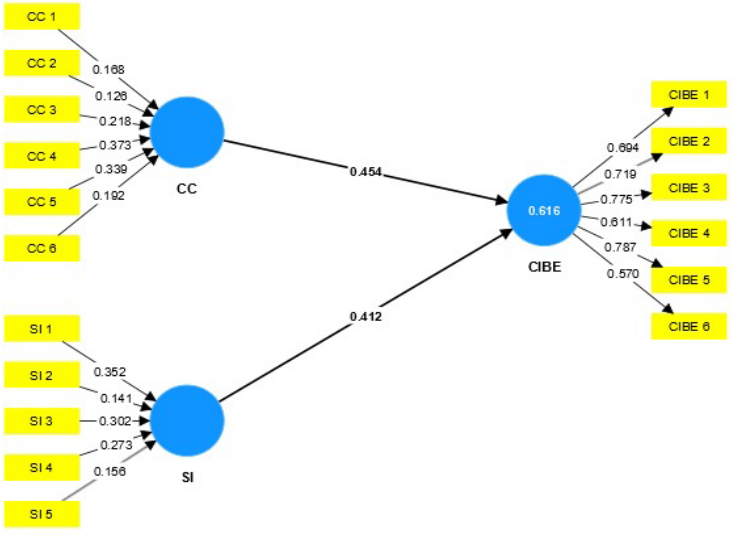
Tabla 3
Estadísticos de colinealidad (VIF).

Indicador	VIF	Indicador	VIF
CC 1	1.283	CYBE 4	1.435
CC 2	1.34	CYBE 5	1.87
CC 3	1.395	CYBE 6	1.329
CC 4	1.493	SI 1	1.748
CC 5	1.851	SI 2	1.964
CC 6	1.766	SI 3	2.175
CIBE 1	1.485	SI 4	2.146
CIBE 2	1.584	SI 5	1.97
CIBE 3	1.944		

Fuente: Elaboración propia en Smart PLS basada en Hair et al. (2017).

El modelo externo no presenta colinealidad, revelando que los indicadores brindan información única, valiosa y no redundante sobre la variable dependiente. En el siguiente paso se realiza la revisión de la significancia de los pesos estadísticos de cada uno de los indicadores, como se muestra en la Figura 6.

Figura 6
Significancia de los pesos estadísticos.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Evaluación de modelo estructural o interno

Las siguientes pruebas nos permitirán analizar la calidad del modelo y la validez de las relaciones entre las variables, por lo que se revisa la colinealidad del modelo interno, observando que las variables no presentan colinealidad, como se muestra en la Tabla 4.

Tabla 4
Estadísticos de colinealidad (VIF).

CC	CIBE	SI
CC	1.703	
CIBE		
SI	1.703	

Fuente: Elaboración propia en Smart PLS con base en Hair et al. (2017).

Posteriormente se evalúa la significancia de los caminos, lo cual es esencial para determinar si las relaciones propuestas entre las variables latentes se corresponden con la teoría subyacente propuesta en la construcción de este conocimiento, como se muestra en la Tabla 5.

Tabla 5
Significancia de los caminos.

	Muestra original (O)	Media de la muestra (M)	Desviación estándar (STDEV)	Estadísticos t (|O/STDEV|)	Valores p
CC > CYBE	0.454	0.474	0.116	3.914	0
IS > CYBE	0.412	0.413	0.112	3.662	0

Fuente: Elaboración propia en Smart PLS con base en Hair et al. (2017).

Se puede observar que los valores p obtenidos son 0.000 para ambas variables, demostrando que estos son estadísticamente significativas para el modelo. Posteriormente, se calcul***ó*** el coeficiente de determinación (R2), que muestra que las variables independientes explican la variable dependiente, obteniendo el resultado de 0.616, lo que indica que la variable dependiente ciberseguridad es explicada en un 61.6% por las variables independientes CC y SI (Tabla 6).

Tabla 6
Coeficiente de determinación R2

	R cuadrado	R cuadrado ajustada
CIBE	0.616	0.605

Fuente: Elaboración propia en Smart PLS con base en Hair et al. (2017).

Prueba de hipótesis

El cibercrimen y la seguridad de la información son factores determinantes de la ciberseguridad en el Estado de Michoacán, México. Esta hipótesis se probó utilizando la técnica bootstrap, un método de remuestreo que emplea 5000 muestras de los datos originales (Hair et al., 2017). Los resultados obtenidos muestran de manera consistentemente una relación significativa, verificando la relación hipotética con la ciberseguridad a un nivel de significancia del 1%. Esto evidencia una relación directa entre las variables de estudio.

Discusión

Los resultados de la investigación confirman la validez de la hipótesis, que plantea que el cibercrimen y la seguridad de la información, son componentes significativos para el diseño de una estrategia de ciberseguridad en el estado de Michoacán, México; por lo que con la evidencia recolectada y analizada se favorece la noción que las amenazas y riesgos en el ciberespacio y la ausencia de una seguridad de la información juegan un papel crucial en la seguridad en el internet y la integridad de la información.

El modelo presentado refleja de una manera clara que: 1) La falta de conocimiento de los internautas sobre el uso seguro del ciberespacio, 2) La insuficiente supervisión del tiempo que los menores pasan en línea, 3) La carencia de un marco legal robusto, 4) La escasez de personal capacitado y de equipos especializados, así como 5) La ausencia de campañas de concienciación y prevención, son factores clave para la ciberseguridad.

La congruencia entre los hallazgos empíricos y la hipótesis planteada resalta la premisa de que el cibercrimen no sólo es una amenaza aislada, así la seguridad de la información surge como un elemento crucial para combatir las amenazas en el ciberespacio asociadas al cibercrimen, ambos elementos son centrales y requieren una atención integral en la formulación de estrategias efectivas en materia de ciberseguridad.

Para comprobar la hipótesis planteada se utilizó el método PLS-SEM, a través del análisis estadístico se identificaron los componentes determinantes que permitirán el diseño de una estrategia de ciberseguridad en el contexto de estudio, demostrando la importancia de las variables independientes. El modelo muestra a través del coeficiente de determinación (R2) el poder predictivo de las variables independientes (Cibercrimen y Seguridad de la información) sobre la dependiente (Ciberseguridad), obteniendo el resultado de 0.616, lo que nos indica que la variable ciberseguridad se explica en un 61.6% por las variables independientes, comprobándose la fortaleza de las relaciones entre estas.

Las implicaciones de los resultados conseguidos en esta investigación son de gran relevancia para la formulación y elaboración de una estrategia que per-

mita mejorar la ciberseguridad en el Estado de Michoacán. En primer lugar, la variable Cibercrimen ha demostrado ser un factor relevante para la ciberseguridad en el estado, este hallazgo destaca la importancia de fortalecer las capacidades institucionales y legales para investigar y sancionar eficazmente los delitos cibernéticos.

Está investigación contrasta con otras investigaciones que abordan diferentes variables que influyen en la Ciberseguridad, por ejemplo Aguilar (2021), analiza las habilidades digitales en ciberseguridad de países latinoamericanos, utilizando métricas como el Índice Nacional de Ciberseguridad (NCSI) y el Índice Global de Ciberseguridad (GCI), complementados con informes del BID y la OEA. El objetivo es evaluar la preparación de los países para prevenir y gestionar ciberamenazas, considerando indicadores como; el desarrollo de políticas, educación en ciberseguridad y respuesta a ciberincidentes. Aunque México ocupa el segundo lugar (22.81%) en incidencia de cibercrimen, ha obtenido altas puntuaciones en áreas como desarrollo de políticas y estrategias de ciberseguridad, aunque estas medidas no se han traducido en una política de Estado respaldada por el gobierno y la sociedad.

La primera variable, cibercriminalidad, de acuerdo con Schneier (2016), representa una amenaza constante a la seguridad del ciberespacio y afirma que fortalecer la seguridad de los dispositivos y sistemas es fundamental para disminuir la ciberdelincuencia; por tanto se requiere de respuestas tanto tecnológicas como legales para mitigar sus impactos. Contrario a ello, la investigación demostró que para reducir el cibercrimen es necesario que se persiga y sancione a los ciberdelincuentes, ya que medidas de seguridad lógica en los dispositivos no evitan que los usuarios sigan convirtiéndose en víctimas de la cibercriminalidad.

Consecuentemente, la implementación de medidas tecnológicas tendientes a incrementar la seguridad de los activos informáticos no sería suficiente como lo afirma Schneier (2016), pues esta se realiza por medio de la instalación de medidas lógicas y físicas; las cuales en la mayoría de los casos son vulneradas por los propios hábitos de navegación de los usuarios, quienes por ignorancia o aun teniendo conocimiento de ellas, en su búsqueda de comodidad, conveniencia y confianza, a menudo optan por vulnerar las medidas de seguridad al acceder a la información o contenido deseado en la web y mantenerse conectado, lo que los lleva a tomar decisiones arriesgadas y aumenta su exposición a amenazas cibernéticas.

Aunado a lo anterior la cibercriminalidad abarca una amplia variedad de actividades, desde intrusiones informáticas con el objetivo modificar o destruir activos digitales, así como aquellas realizadas con el fin de obtener beneficios económicos o causar perjuicios en el mundo real a las personas. Para abordar efectivamente estas prácticas, es crucial actualizar el marco legal, ya que las leyes existentes a menudo no son suficientes para enfrentar los desafíos de la ciberdelincuencia en un entorno digital en constante evolución. Richardson

(2019) y Wolff (2018) argumentan que las leyes contra el cibercrimen son fundamentales para disuadir a los criminales y proteger a las víctimas. Estas leyes proporcionan un marco legal claro para identificar, procesar y sancionar a los delincuentes, lo que ayuda a crear un ambiente en el que el cibercrimen sea menos interesante y más arriesgado para los delincuentes, esto a pesar de la complejidad y globalidad de estos delitos que incrementan las dificultades para aplicar y hacer cumplir las leyes en el ámbito virtual.

La investigación resalta la importancia de perseguir a los ciberdelincuentes, ya que, sin ello, la investigación y sanción de los delitos cibernéticos resultarán infructuosas, lo que aumentaría la impunidad y fomentaría la proliferación de más ciberdelincuentes. Es fundamental adoptar medidas legales y tecnológicas actualizadas que permitan enfrentar eficazmente los constantes retos que plantea la cibercriminalidad en la sociedad moderna.

Esta necesidad de un marco normativo sólido para la ciberseguridad, se hace evidente, al menos en México, con la existencia de 14 iniciativas (ver bibliografía) que al día de hoy han llegado al Congreso de la Unión, en las que se han reunido diversas demandas sociales pero que en su diseño, parten de presiones internacionales para la adopción de convenios de cibercriminalidad que no siempre expresan ni se adecuan a la realidad mexicana o en su defecto, parten de una pobre e inadecuada interpretación de la problemática, resultando en iniciativas de ciberseguridad inoperantes, carentes de pericia técnica y malinterpretadas, lo que hace que ninguna de ellas haya logrado convertiste en ley.

Otro ejemplo de estos esfuerzos aislados y mal aplicados de la adecuación de marcos normativos de cibercriminalidad, se tiene en las adecuaciones de los códigos penales federal y locales derivadas de la mal llamada Ley Olimpia, que obligó a los congresos locales a incluir el delito dentro de su legislación, pero que en la práctica a pesar de que 31 estados han implementado está reforma, estas adecuaciones no incluyen los procedimientos y responsabilidades de los proveedores de servicios de internet (ISP) en el caso de delitos cibernéticos para que entreguen o colaboren con las autoridades investigadoras a efecto de lograr la sanción a delincuentes, la reparación a la víctima y su derecho al olvido, lo que ha contribuido en un incremento de los niveles de impunidad y el descontento por parte de las víctimas por no encontrar justicia.

En lo referente a trabajos académicos o empíricos sobre ciberseguridad para el caso de Michoacán, más allá de abordar en su conjunto la problemática de forma general, dentro de la literatura se encuentran esfuerzos aislados que analizan los ordenamientos jurídicos relacionados con el fraude informático (Valencia, 2004), delitos informáticos (Mora, 2014) o las adecuaciones al código penal del estado respecto a la violencia digital (CPEM, 2020, art 195), éstos desde una visión puramente jurídica penal de los delitos o como el caso de Navarrete y Gómez (2023) desde una visión preventiva; limitándose únicamente a examinar una faceta de ésta y no en su conjunto, visión panorámica que hace única a esta investigación.

La variable Seguridad de la información también se ha destacado como un factor decisivo del presente estudio, evidenciando la creciente necesidad manifestada por Vega (2021) de que nuestra sociedad comience a adoptar los principios y prácticas que esta rama del conocimiento ofrece.

A este respecto, algunos autores (Schneier, 2012; Areitio, 2008; Kiser, 2020) subordinan la ciberseguridad como un elemento del campo de la seguridad de la información, dispuesto para la defensa y contrataque ante la existencia de amenazas desde el campo individual o de sistemas interconectados con finalidades específicas y que dan servicio a un número limitado de usuarios (bases de datos de clientes de una empresa, transmisión de correos entre cliente-proveedor, sistemas operados por instituciones públicas o instituciones bancarias, entre otras); no obstante, en la actualidad gran parte de las interacciones sociales, ya sean económicas, académicas o de esparcimiento se realizan por medios digitales, magnificando la cantidad de sistemas individuales o interacciones que deben ser protegidas de forma individual.

Ante este panorama, el presente trabajo ofrece un cambio de paradigma en el que la ciberseguridad, se concibe como una demanda social en un entorno interconectado, en el que la interacción de innumerables sistemas de información con igual magnitud de usuarios, exige que la ciberseguridad sea extrapolada al ámbito social y con ello al Estado como responsable por su rectoría, promoción y en su caso, provisión. Es decir, la seguridad de la información se subordina a la ciberseguridad, como una variable por medio de la cual los estados pueden proteger a su población, que hoy día recibe los beneficios, pero también los padecimientos y afecciones de la interacción en ese territorio llamado ciberespacio.

En consecuencia, la Seguridad de la Información, surge no como medida tecnológica, sino vista como un enfoque integral que incluye aspectos humanos y procesos organizacionales. Los seres humanos desempeñan un papel crucial en la protección de la información, por medio de la integración de medidas de seguridad tecnológicas (ya sean física o lógicas); capacitación, concientización, la adopción de buenas prácticas y mejora de hábitos fortaleciendo con ello la seguridad durante su navegación y reduciendo la cibercriminalidad.

Es así, que la seguridad de la información se convierte en una tarea social por medio de la cual los Estados, pueden contribuir para el logro de interacciones menos riesgosas, más ordenadas y respetuosas entre cibernautas, disminuyendo por un lado, el número de víctimas de delitos ya existentes desde hace mucho tiempo como lo son el fraude, acoso o amenazas; y por el otro, la disminución de delitos que afectan directamente a los sistemas informáticos, en los que se aloja una gran cantidad de servicios indispensables para la vida diaria que incluso se podrían considerar de seguridad nacional, como lo son los financieros, de seguridad pública o de salud. Por tanto, entre más prácticas, herramientas o técnicas de seguridad informática se adopten en una sociedad, mayor será la ciberseguridad de la misma.

En complemento, así como la seguridad pública se convierte en tarea estatal en el mundo físico para proteger a los ciudadanos, sus bienes y derechos de amenazas como el crimen y la violencia; la ciberseguridad se vuelve crucial para proteger a los ciudadanos, las organizaciones y los gobiernos en el entorno digital.

Consecuentemente, la estrategia de ciberseguridad que se propone, a diferencia de las 14 iniciativas propuestas y de las inoperantes adecuaciones realizadas en algunos marcos legislativos, tiene varias ventajas en sus resultados, la primera consiste en que se concentra la experiencia acumulada de profesionales ciberseguridad, quienes durante sus años de trabajo han reunido el sentir y la frustración de víctimas de delitos que no encuentran justicia así como la impotencia de investigadores que encuentran limitaciones técnicas y legales para asistir a sus víctimas y esclarecer los delitos, por lo que nuestra propuesta parte precisamente de la recolección de esta experiencia y de su traducción en conocimiento práctico para abordar la problemática.

En segundo lugar, su diseño parte de un discernimiento específico entre los elementos más relevantes imperantes en el contexto nacional y específicamente en el de Michoacán, lo que lo hace una herramienta que se ajusta a la realidad, que propone medidas para mejorar la ciberseguridad; reducir el número de víctimas; lograr una efectiva persecución y sanción de cibercriminales; mayor justicia para las víctimas.

Por último, la ciberseguridad se erige como una tarea estatal para la protección de los datos, las conexiones entre las diferentes redes de servidores y sistemas que mantienen el ciberespacio, pero sobre todo la protección de los cibernautas y de la sociedad misma que interactúan dentro de este nuevo territorio en el que convergen derechos y obligaciones; y que, en caso de ser afectadas, exista una entidad superior que intermedie entre las partes y logre una convivencia pacífica entre las personas y así tener un espacio ciberseguro.

Conclusión

La presente investigación pone de manifiesto el problema significativo de ciberseguridad en el Estado de Michoacán, México. Los datos evidencian la falta de medidas efectivas en ciberseguridad y el incremento significativo y constante de los delitos cibernéticos, lo que subraya la necesidad urgente de desarrollar estrategias robustas de ciberseguridad para salvaguardar la seguridad y privacidad de la sociedad michoacana y las cuales representan ventajas, tales como: 1) Concientización de la sociedad; 2) Colaboración y cooperación; 3) Prevención y educación; 4) desarrollo de estrategias efectivas; y 5) Asignación adecuada de recursos, los cuales son necesarios para hacer frente al problema de ciberseguridad.

Mediante la aplicación innovadora del modelo PLS-SEM, esta investigación pionera en Michoacán ha revelado una relación causal entre el ciber-

crimen y la seguridad de la información, posicionándolos como factores determinantes de la ciberseguridad estatal. El coeficiente de determinación de 0.616 corrobora la solidez de estos hallazgos, proporcionando una comprensión cuantitativa y detallada que permite abordar las causas fundamentales del problema y diseñar estrategias de intervención más efectivas, contribuyendo así a fortalecer la ciberseguridad.

El estudio no solo amplía la literatura existente, sino que también facilita el diseño de una estrategia específica para Michoacán. Al identificar los factores clave que influyen en la ciberseguridad del Estado, se sienta un precedente para la implementación de políticas públicas y estrategias de prevención más efectivas, contribuyendo de manera tangible a la protección de los sistemas e información.

Es crucial generar mecanismos que promuevan la conciencia sobre los riesgos, desarrollando políticas, regulaciones adecuadas, procedimientos, guías de buenas prácticas y difusión, con el objetivo de reducir la brecha digital y construir una sociedad más informada y resiliente en el uso del ciberespacio.

En conclusión este artículo ha logrado una comprensión profunda de las dinámicas de la ciberseguridad en Michoacán, revelando la importancia crucial del cibercrimen y la seguridad de la información. Los hallazgos obtenidos no solo amplían el conocimiento existente, sino que también ofrecen una guía práctica para enfrentar los desafíos cibernéticos actuales y futuros. No obstante el modelo solo explica una parte del fenómeno, por lo que sería importante realizar nuevos estudios que aborden el resto del problema, más aún si consideramos la velocidad con que el ciberespacio cambia y con ello los problemas de ciberseguridad.

Referencias

Aguilar, A. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios Internacionales, 53(198), 169–197.

Fayad, O. (2015). *Iniciativa con Proyecto de Decreto por el que se Expide la Ley Federal para Prevenir y Sancionar los Delitos Informáticos.* (O. F. Unión., Ed.) México. Obtenido de http://sil.gobernacion.gob.mx/Archivos/Documentos/2015/10/asun_3291220_20151027_1445523938.pdf

Trim, P., & Lee, Y.-I. (2021). El modelo global de ciberseguridad: contrarrestar los ciberataques mediante un acuerdo de asociación resiliente. *Big Data y Computación Cognitiva*, 16.

Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* España: Paraninfo.

Arroyo, D., Gayoso, V., & Hernandez, L. (2020). *Ciberseguridad.* Madrid: CSIC.

Caballero, M. (2019). *Ciberseguridad y Transformación Digital.* España: Anaya Multimedia.

Callanan, C., & Tropina, T. (2015). *Self-and Coregulatión in Cybercrime, Cybersecurity and National Security.* Londres: Springer.

Cámara de Diputados del H. Congreso de la Unión. (8 de febrero de 2022). *Iniciativa que expide la Ley Nacional de Seguridad en el Ciberespacio.* Obtenido de http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/10/asun_4093498_20201019_1603158505.pdf

Cámara de Diputados del H. Congreso de la Unión. (8 de junio de 2023). *Iniciativa que expide la Ley Federla de Ciberseguridad.* Obtenido de https://www.diputados.gob.mx/LeyesBiblio/iniclave/65/CD-LXV-II-2P-292/02_iniciativa_292_25abr23.pdf

Cámara de Senadores del H. Congreso de la Unión. (21 de 09 de 2022). *Iniciativa con proyecto de decreto por que se reforma la Ley Gneral del.* Obtenido de https://infosen.senado.gob.mx/sgsp/gaceta/65/2/2022-11-04-1/assets/documentos/Ini_Morena_Sen_Arias_Seguridad_Cibernetica.pdf

Cámara de Senadores del H. Congreso de la Unión. (5 de marzo de 2024). *Iniciativa con proyecto de decreto por el que se expide la Ley Federal de Ciberseguridad.* Obtenido de https://infosen.senado.gob.mx/sgsp/gaceta/65/3/2024-02-14-1/assets/documentos/Inic_Morena_diversos_senadores_art_211_CPF.pdf

Cañedo, R. (2017). *Iniciativa con proyecto de decreto por el que reforma y adiciona diversas disposiciones del Código Penal Federal.* (D. A. Unión, Ed.) Mexico. Obtenido de http://sil.gobernacion.gob.mx/Archivos/Documentos/2017/10/asun_3603770_20171027_1509145588.pdf

Código Penal del Estado de Michoacán de Ocampo. (2020). *Artículo 195 [bis].* H. Congreo del Estado de Michoacán de Ocampo Septuagésima Tercera Legislatura.

Ellis, R., & Mohan, V. (2019). *Rewire Cibercecurity Governance.* USA: Wiley .

Enríquez, J. (19 de 11 de 2020). *Iniciativa con Proyecto de Decreto por el que se adiciona la fracción XIV al Artículo 5 de la Ley de Seguridad Nacional en materia de crímenes virtuales.* (S. d. Unión, Ed.) México. Obtenido de https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2020-11-04-1/assets/documentos/Inic_Morena_Sen_Enriquez_Art_5_Ciberseguridad.pdf

Ferrer, E. (2021). *Estudios de Cibercrimen.* Argentina: Olejnik.

Franco, F. (2018). *El lado oscuro de las redes Sociales: Amenazas, peligros y riesgos en el uso de las redes sociales.* España: Independently published.

García , L. (2021). *Iniciativa que reforma los Artículos 11 y 13 de la Ley de la Fiscalía General de la República, a Cargo de la Diputada Lidia García Anaya, del Grupo Parlamentario de Morena.* (d. G. Diputada Lidia García Anaya, Ed.) México. Obtenido de http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/12/asun_4291684_20211215_1638478336.pdf

González , S., & Fernández , W. (2017). *Iniciativa Con Proyecto de Decreto por el Que Reforma y Adiciona Diversas Disposiciones de los Códigos Penal Federal, y Nacional de Procedimientos Penales.* (d. P. Diputada Sofía González

Torres e Integrantes del Grupo Parlamentario del PVEM y el Diputado Waldo Fernández González, Ed.) México. Obtenido de http://sil.gobernacion.gob.mx/Archivos/Documentos/2017/11/asun_3616294_20171109_1510169467.pdf

Guerra , J. (2023). *Iniciativa con Proyecto de Decreto por el que se expide la Ley general de Ciberseguridad.* (D. F. Legislatura, Ed.) México. Recuperado el 25 de marzo de 2023, de http://sil.gobernacion.gob.mx/Archivos/Documentos/2022/12/asun_4475036_20221215_1665067316.pdf

H. Congreso de la Unión de la Ciudad de México. (3 de febrero de 2021). *Iniciativa con proyecto de decreto por el que se reforma el nombre del capítulo III "Acoso sexual".* Obtenido de https://congresocdmx.gob.mx/archivos/parlamentarios/IN_215_10_12_09_2019.pdf

H. Senado de la República LXIV Legislatura. (24 de junio de 2022). *Iniciativa con proyecto de decreto que declara el mes de octubre de cada año como el mes nacional de la Ciberseguridad.* Obtenido de https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2018-10-23-1/assets/documentos/Inic_PVEM_Mes_Ciberseguridad_231018.pdf

Hair, J., Black, W., Babin, B., & Anderson, R. (2017). *Análisis de datos multivariados.* Estados Unidos: Pearson Prentice Hall.

Hair, J., M. Hult, T., Ringle, C., Sarstedt, M., Castillo, J., Cepeda, G., & Roldán, J. (2017). *Manual de Parcial Least Squares Structural Equation Modeling.* Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE Publications, Inc.

Hamelink, C. (2016). *La ética del ciberespacio.* Siglo veintiuno editores.

Hernández-Sampieri, & Mendoza, C. (2018). *Metodología de la investigación.* México: Mc Graw Hill.

INEGI. (2022). Módulo sobre ciberacoso 2022. En *ENDUTIH* (pág. 21). MÉXICO: INEGI.

ISO. (30 de Diciembre de 2014). *Normas ISO*. Obtenido de Normas ISO: https://www.normas-iso.com/iso-27001/

Jafet, V. O. (2004). *Reglamentación del Delito de Fraude Informático en el Código Penal del Estado de Michoacán (Tesisde Licenciatura, Universidad Don Vasco A.C.).* Repositorio Institucional de la UNAM. Obtenido de http://132.248.9.195/ppt2004/0330401/0330401.pdf

Kaplan, S., & Garrick, B. (1981). On the quantitative definition of risk. Risk Analysis, 1(1), 11-27. *Risk Analysis*, 11-27.

Kiser, Q. (2020). *Ciberseguridad Una Simple Guía para Principiantes sobre Ciberseguridad, Redes Informáticas y Cómo Protegerse del Hacking en Forma de Phishing, Malware, Ransomware e Ingeniería Social.* Estados Unidos: Quinn Kiser.

Likert, R. (1932). *A technique for the measurement of attitude.* Archives of Psychology.

López, J. (13 de 10 de 2020). *Ley de Ciberseguridad del Estado de San Luis Potosi y sus Municipios.* Obtenido de https://books.google.com.mx/books?id=oXYCEAAAQBAJ&lpg=PP1&hl=es&pg=PP1#v=onepage&q&f=false

Mora, E. (2014). *Incorporación de los Delitos Informáticos al Código Penal del Estado de Michoacán (Tesis de Maestría, Universidad Michoacana de San Nicólas de Hidalgo).* Biblioteca Virtual. Obtenido de http://bibliotecavirtual.dgb.umich.mx:8083/xmlui/bitstream/handle/DGB_UMICH/573/FDCS-M-2014-0875.pdf?sequence=1&isAllowed=y

Navarrete, C., & Gómez, M. (2023). El conocimiento colectivo en ciberseguridad como respuesta al fraude cibernético en el estado de Michoacán. En C. C.-A. Editores, *Capital humano e Innovación Una realidad en el desarrollo de las organizaciones* (págs. 146-170). Altres Costa-Amic Editores.

Parada, R. A., & Errecaborde, J. D. (2018). *Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet.* Buenos Aires, Argentina: ERREIUS.

Parada, R., & Errecaborde, J. (2018). *Cibercrimen y Delitos Informácticos.* Buenos Aires, Argentina: ERREIUS.

Rayón , M., & Gómez, J. (2014). Cibercrimen: particularidades en su Investigación y Enjuiciamiento. *Anuario Jurídico y Económico Esculiarense*, 209-234.

Richardson, M. (2019). *Cyber Crime Law and Practice .* Estados Unidos: Wildy, Simmonds & Hill Publishing.

Sain, G. (2018). La estratégia gubernamental frente al crimen: la importancia de las políticas preventivas más allá de la solución penal. En R. y. Parada, *Cibercrimen y Delitos Informácticos: los nuevos tipos penales en la era de internet* (págs. 7-29). Buenos Aires, Argentina: ERREIUS.

Santos, O. (2019). *Developing Cybersecurity Programs and Policies.* Estados Unidos: Pearson Education, Inc.

Schneier, B. (2000). *Secrets & Lies.* Canada: Wiley Publishing, Inc.

Schneier, B. (2012). *Liars & Outliers Enabling the Trust That Society Needs to Thrive.* Estados Unidos: Wiley.

Schneier, B. (2016). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* Estados Unidos: W. W. Norton & Company.

Senadora de la República por el H. Congreso de la Unión del Estado de Baja California Sur. (13 de julio de 2019). *Iniciativa Ley de Seguridad Informática.* Obtenido de https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2019-03-27-1/assets/documentos/Inic_MORENA_Seguridad_Informatica.pdf

Stallings, W. (2017). *Cryptography And Network Security.* Estaso Unidos: Pearson.

Turban, E., Pollard, C., & Wood, G. (2018). *Information Technology for Management.* Estados Unidos de Norteamerica: Wiley.

Unión, S. M. (Ed.). (2020). *Iniciativa con aval del grupo Parlamentario que contiene Proyecto de decreto por el que se modifican y adicional la Ley de Seguridad Nacional y se expide la Ley General de Ciberseguridad.* México. Obtenido de http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_1599062884.pdf

Vega, E. (2021). *Seguridad de la Información.* Costa Rica: Área de Innovación y Desarrollo,S.L.

Vergara, M., & Huidobro, J. M. (2016). *Las tecnologías que cambiaron la historia.* España: Ariel, S.A.

Whitfield , D., & Hellman , M. (2022). *Democratizando la criptografía.* Nueva York, Estados Unidos: Asociación para Maquinaria de Computación.

Wolff, J. (2018). *You´ll see this message when it is too late: The Legal and Economic Aftermath of Cysersecurity Breaches (Informatio Policy).* Estados Unidos: The MIT Press.