ie revista de investigación educativa de la Rediech

• Volumen 16 • 2025 • e2271 • ISSN: 2448-8550 •

Ciberseguridad en instituciones de educación superior: un análisis desde la perspectiva de la teoría de la motivación de protección

Cybersecurity in higher education institutions: An analysis from the perspective of Protection Motivation Theory

Francisco Isaí Morales Sáenz • José Melchor Medina Quintero • Demian Abrego Almazan

Resumen

La importancia de la ciberseguridad en el sector educativo radica en la protección de datos e información sensible, así como en mantener un ambiente seguro y confiable para estudiantes, docentes y personal administrativo. El objetivo de la investigación es analizar los factores que influyen en el comportamiento de seguridad cibernética de los empleados en instituciones de educación superior en el noreste de México. Se utiliza la teoría de la motivación de protección, buscando comprender las motivaciones y decisiones relacionadas con las prácticas de seguridad digital. Para el método, se aplicaron 159 encuestas que fueron analizadas mediante modelado de ecuaciones estructurales con mínimos cuadrados parciales (PLS-SEM). Los resultados revelan que la conciencia de ciberseguridad influye positivamente en la autoeficacia y la eficacia de respuesta. La severidad percibida y la autoeficacia de respuesta son predictores significativos del comportamiento de ciberseguridad. Curiosamente, el hábito de protección se relaciona positivamente con la autoeficacia, pero no con la eficacia de respuesta. Además, no se encontró relación significativa entre la eficacia de respuesta y el comportamiento de ciberseguridad. Los hallazgos enfatizan la necesidad de un enfoque holístico que considere factores individuales y organizacionales para promover prácticas de seguridad efectivas en el contexto educativo mexicano.

Palabras clave: ciberseguridad, comportamiento, educación superior, protección de datos, teoría de la motivación a la protección.

Abstract

The importance of cybersecurity in the education sector lies in protecting sensitive data and information and maintaining a safe and reliable environment for students, faculty, and administrative staff. This research aims to analyze the factors influencing cybersecurity behavior of employees in higher education institutions in Northeastern Mexico. Protection Motivation Theory is used to understand the motivations and decisions related to digital security practices. For the method, 159 surveys were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). Results reveal that cybersecurity awareness positively influences both self-efficacy and response efficacy. Perceived severity and response self-efficacy are significant predictors of cybersecurity behavior. Interestingly, protection habit positively relates to self-efficacy but not to response efficacy. Moreover, no significant relationship was found between response efficacy and cybersecurity behavior. The findings emphasize the need for a holistic approach that considers individual and organizational factors to promote effective security practices within the Mexican educational context.

Keywords: cybersecurity, behavior, higher education, data protection, Protection Motivation Theory.

Recibido: 8 de agosto de 2024 | *Aprobado:* 8 de febrero de 2024 | *Publicado:* 3 de marzo de 2025
https://doi.org/10.33010/ie_rie_rediech.v16i0.2271

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

Introducción

En la era actual, el crecimiento acelerado de la tecnología ha llevado a un aumento significativo de la dependencia de las empresas y organizaciones en los recursos digitales y sistemas de información en el logro de objetivos organizacionales (Holgeid et al., 2022). Este rápido avance tecnológico ha facilitado la eficiencia y efectividad en las operaciones cotidianas, pero al mismo tiempo ha expuesto a estas instituciones a una creciente cantidad de ataques cibernéticos enfocados hacia personas y sistemas vulnerables (Morales-Sáenz et al., 2024a; Pranggono y Arabo, 2020); Asimismo, la conectividad y el intercambio de información en línea han abierto una puerta a un mundo de oportunidades, pero también han brindado a los ciberdelincuentes diversas formas de llevar a cabo operaciones ilícitas que amenazan la seguridad de los datos, la privacidad y la integridad de la información, atentando contra intereses nacionales, industriales y financieros (Dzyana et al., 2022; Hasan et al., 2021).

La evolución de las amenazas cibernéticas ha demostrado su capacidad para afectar de manera significativa a organizaciones de todos los tamaños y sectores, incluido el educativo (Ulven y Wangen, 2021). Desde ataques de *ransomware* hasta *phishing* y robo de datos, las tácticas maliciosas utilizadas por los ciberdelincuentes han demostrado su capacidad para comprometer incluso a las organizaciones más sólidas en términos de seguridad (Federal Bureau of Investigation [FBI], 2022).

La ciberseguridad, como disciplina, busca proteger los sistemas de información y redes de organizaciones de posibles ataques y daños (Furnell et al., 2021), y se ha convertido en un asunto grave, ya que las consecuencias de no garantizar un nivel

Francisco Isaí Morales Sáenz. Profesor-Investigador de la Facultad de Comercio y Administración Victoria de la Universidad Autónoma de Tamaulipas, México. Es Maestro en Dirección Empresarial por la Universidad Autónoma de Tamaulipas y actualmente cursa el Doctorado en Ciencias Administrativas en la misma institución. Su línea de investigación se enfoca en las tecnologías de información en las organizaciones. En el ámbito de la divulgación científica, ha publicado artículos en revistas de alto impacto a nivel nacional e internacional. Correo electrónico: fmsaenz@uat.edu.mx. ID: https://orcid.org/0000-0001-9740-149X.

José Melchor Medina Quintero. Profesor-Investigador de la Facultad de Comercio y Administración Victoria de la Universidad Autónoma de Tamaulipas, México. Es Doctor en Sistemas de Información de la Empresa por la Universidad Politécnica de Madrid, España. Experto en tecnologías y sistemas de información. Líder del Cuerpo Académico Consolidado "Tecnologías de Información y Estrategia". Ha escrito 47 artículos indexados en Latindex y SciELO, 29 artículos académicos publicados en revistas de alto impacto tanto nacionales como internacionales y tres libros. Correo electrónico: jmedinaq@uat.edu.mx. ID: https://orcid.org/0000-0003-3466-7113.

Demian Abrego Almazan (autor de correspondencia). Profesor-Investigador de la Facultad de Comercio y Administración Victoria de la Universidad Autónoma de Tamaulipas, México. Es Doctor en Ciencias Administrativas y profesor de tiempo completo en la UAT, donde imparte clases en licenciatura, maestría y doctorado. En el ámbito de la divulgación científica, ha publicado artículos en revistas de alto impacto a nivel nacional e internacional. Además es coautor de ponencias, libros y capítulos de libros enfocados en tecnologías, sistemas de información, administración estratégica y estadística multivariante. Desde el año 2017 forma parte del Sistema Nacional de Investigadoras e Investigadores, Nivel 2. Correo electrónico: dabrego@docentes.uat.edu.mx. ID: https://orcid.org/0000-0003-0147-8834.

adecuado de ciberseguridad pueden ser críticas, amenazando la confidencialidad, eficiencia e integridad de los sistemas de información (Morales-Sáenz et al., 2024b). Esto puede provocar riesgos de privacidad, pérdidas económicas, daños a la reputación, y exponer limitaciones administrativas (Caldarulo et al., 2022).

El sector educativo, en particular, se ha convertido en un blanco cada vez más frecuente de incidentes cibernéticos maliciosos, resultando en pérdidas financieras significativas, interrupciones académicas y violaciones masivas de datos de estudiantes y personal (Fouad, 2022). Ante esta realidad, es imperativo que las instituciones educativas establezcan procedimientos y políticas sólidas de seguridad informática para hacer frente a estas amenazas (Saeed, 2023; Taborda et al., 2021). Estas acciones son fundamentales para garantizar la integridad y confidencialidad de la información dentro de las organizaciones del sector educativo, fortaleciendo así su resiliencia ante los desafíos cibernéticos actuales.

Para abordar esta problemática, el presente estudio se enfoca en los dominios clave de la *teoría de la motivación de protección* –PMT por sus siglas en inglés–, de forma específica en la evaluación de amenazas y la evaluación de afrontamiento (Rogers, 1983). Se explora cómo la conciencia del usuario sobre los ataques cibernéticos y su evaluación de las amenazas influyen en su comportamiento de seguridad. Además se examina el impacto de los hábitos en la capacidad de los empleados para enfrentar eficazmente los riesgos cibernéticos.

El objetivo principal de esta investigación es determinar los factores que influyen en el comportamiento de seguridad cibernética de los empleados en instituciones de educación superior en el noreste de México. A través de la recopilación y análisis de datos de empleados y directivos, se busca ofrecer una visión detallada sobre los elementos que moldean las prácticas de ciberseguridad en el sector educativo, con el fin de promover un entorno digital más seguro y protegido en dichas instituciones.

En este sentido, la investigación plantea la siguiente pregunta de investigación: ¿Cómo influyen la conciencia de ciberseguridad, el hábito de protección, la severidad percibida, la autoeficacia de respuesta y la eficacia de respuesta en el comportamiento de seguridad cibernética de los empleados en instituciones de educación superior del noreste de México?

Ciberseguridad en el contexto educativo

En el contexto educativo, la ciberseguridad adquiere un papel crítico debido a la creciente integración de la tecnología en los procesos de enseñanza-aprendizaje (Bezbaruah, 2022; Valiente-Lopez y Tejera-Reyte, 2022); la adopción de plataformas educativas en línea, el uso de dispositivos móviles y la gestión de información estudiantil digitalizada son ejemplos de cómo las instituciones educativas se han vuelto más dependientes de la tecnología para su funcionamiento (Arriaza et al., 2021; Dawadi et al., 2020).

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

Tanto estudiantes y docentes como personal administrativo y directivos de instituciones educativas forman parte de la extensa transformación digital dentro del ámbito educativo (Ivari et al., 2020), y pueden ser susceptibles a prácticas poco seguras en línea, como el uso de contraseñas débiles, la divulgación inapropiada de información personal o la apertura de enlaces sospechosos (Kennison y Chan-Tin, 2020; Priestman et al., 2019). Se ha señalado que el principal problema relacionado con la seguridad cibernética es el factor humano, el cual, debido a la falta de conciencia sobre las amenazas cibernéticas y la negligencia en la aplicación de medidas de seguridad (Alsharif et al., 2022), puede abrir la puerta a posibles ciberataques que afecten no solo a la institución educativa sino también a la privacidad y seguridad de todos sus integrantes, ya que los ciberdelincuentes han demostrado capacidad para explotar las debilidades y los errores humanos derivados de una falta de comportamientos defensivos, así como la falta de conciencia sobre las amenazas cibernéticas y la negligencia en la aplicación de medidas de seguridad, que son factores que contribuyen a la fragilidad del elemento humano en el entorno digital dentro del sector educativo (Alsharida et al., 2023).

La relevancia de la ciberseguridad en el contexto educativo también se refleja en las estadísticas y cifras relacionadas con ataques cibernéticos dirigidos a instituciones educativas. Según informes recientes de Microsoft (2023), a nivel mundial el sector más vulnerable a amenazas cibernéticas como el *malware* es el sector educativo, con el 79.99%. Por lo tanto, la necesidad de estudiar y promover la ciberseguridad en este ámbito se vuelve esencial para proteger los activos digitales de las instituciones, salvaguardar la información estudiantil y garantizar un ambiente de trabajo seguro; capacitar a todos los miembros de la comunidad educativa en buenas prácticas de ciberseguridad y fomentar una cultura de seguridad en línea se convierten en elementos fundamentales para reducir la vulnerabilidad del elemento humano ante posibles amenazas cibernéticas (Sulaiman et al., 2022). Lo anterior, derivado de los registros de ataques cibernéticos hacia dichas instituciones en los años recientes, por la cantidad y el tipo de información confidencial almacenada (Kondruss, 2023). Por ejemplo, en el Reino Unido, alrededor del 62% de las instituciones de educación superior informaron haber sufrido ataques cibernéticos en el último año (GOV.UK, 2022), lo que pone de relieve la necesidad de abordar esta problemática de manera proactiva y efectiva.

Al igual que en el sector empresarial, los directivos de las instituciones educativas juegan un papel clave en la promoción de la ciberseguridad, ya que deben liderar y respaldar la implementación de medidas preventivas y protocolos de respuesta ante posibles incidentes de seguridad cibernética (Li et al., 2022). Su compromiso y apoyo en la creación de políticas de seguridad, la asignación de recursos adecuados y la capacitación del personal son fundamentales para crear una cultura de ciberseguridad sólida en toda institución educativa (European Union Agency for Cybersecurity [ENISA], 2018).

Por lo tanto, la implementación de medidas de ciberseguridad efectivas y la concientización sobre los riesgos en línea son esenciales para proteger la integridad y confidencialidad de los datos educativos, garantizando un ambiente seguro y confiable para todos los involucrados, incluyendo a estudiantes, docentes, personal administrativo y directivos, quienes se destacan como un factor relevante a considerar. Al fortalecer la protección cibernética y fomentar una cultura de seguridad en línea, las instituciones educativas podrán enfrentar de manera más sólida los desafíos que presenta el panorama actual de amenazas cibernéticas en el entorno actual.

Por otra parte, la *teoría de la motivación de protección* –PMT– es un enfoque teórico que busca comprender las motivaciones y decisiones que los individuos adoptan para protegerse y mitigar riesgos (Rogers, 1983), por lo que, en el contexto de la investigación, es enfocado hacia la seguridad cibernética. Esta teoría se ha convertido en un marco sólido para analizar el comportamiento de seguridad cibernética de los usuarios, especialmente en el ámbito laboral, donde la gestión adecuada de la seguridad de la información se vuelve esencial (Li et al., 2019; Sulaiman et al., 2022; Vrhovec y Mihelic, 2021).

Los elementos que componen la PMT incluyen la evaluación de amenazas y de afrontamiento (Atta et al., 2021). Estos dos componentes están interrelacionados y tienen un papel crucial en la toma de decisiones del individuo ante posibles riesgos y cómo reaccionar a ellos (Cummings et al., 2021). La evaluación de amenazas se refiere a la percepción del usuario sobre la gravedad y la probabilidad de que ocurran amenazas. Por otro lado, la evaluación de afrontamiento implica la percepción del usuario sobre su capacidad para manejar y responder efectivamente a las amenazas identificadas (Lahiri et al., 2021).

Desarrollo de hipótesis

La PMT proporciona un marco sólido para examinar los factores que influyen en el comportamiento de ciberseguridad en las instituciones de educación superior. A continuación se presenta el planteamiento de las hipótesis propuestas para el desarrollo del modelo de investigación.

En primer término se aborda la conciencia de ciberseguridad, la cual puede ser definida como el nivel de entendimiento de los usuarios sobre la relevancia de la seguridad de la información y las responsabilidades que conlleva (Koohang et al., 2020), desempeña un papel fundamental en la formación de comportamientos de seguridad efectivos. Khando et al. (2021) destacaron la influencia sustancial de esta conciencia en las conductas de seguridad de la información, enfatizando su rol crítico en el desarrollo de prácticas de protección robustas. Esta perspectiva se ve respaldada por los hallazgos de Torten et al. (2018), quienes establecieron una relación significativa entre la conciencia de seguridad y dos factores clave: la autoeficacia y la eficacia de respuesta. Por lo tanto, se plantean las siguientes hipótesis de investigación:

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

H1: La conciencia de ciberseguridad influye positivamente en la autoeficacia de respuesta.

H2: La conciencia de ciberseguridad influye positivamente en la eficacia de respuesta.

Ahora bien, en cuanto al hábito de protección, este se puede definir como la tendencia a realizar comportamientos de seguridad de forma automática debido al aprendizaje repetitivo (Shahbaznezhad et al., 2021). Esta conceptualización se ve reforzada por diversos estudios que subrayan su importancia en el contexto de la ciberseguridad. Tsai et al. (2016) argumentan que cuanto más arraigado está el hábito de un individuo de realizar acciones de protección, mayores son sus intenciones de implementar medidas de seguridad en línea. Este vínculo entre hábito e intención se complementa con hallazgos sobre su impacto en factores relacionados con la eficacia. Vance et al. (2012) reportaron que el hábito influye positivamente en la eficacia de respuesta, mientras que Sulaiman et al. (2022) confirmaron su impacto positivo en la autoeficacia de respuesta. Estos estudios colectivamente subrayan el papel crucial del hábito de protección en la formación de comportamientos de ciberseguridad efectivos. Por lo tanto, se proponen las siguientes hipótesis:

H3: El hábito de protección influye positivamente en la autoeficacia de respuesta.

H4: El hábito de protección influye positivamente en la eficacia de respuesta.

En cuanto a la severidad percibida, esta se define como la evaluación individual de la gravedad de las consecuencias de una amenaza de seguridad (Rogers, 1983); ha sido objeto de numerosos estudios en el ámbito de la ciberseguridad. La literatura existente proporciona evidencia sustancial de su influencia significativa en el comportamiento de los usuarios (Geil et al., 2018; Jansen y Van Schaik, 2018). Complementando estos hallazgos, Hina et al. (2019) señalan específicamente que la severidad percibida influye en la intención de comportamiento, estableciendo así un vínculo directo entre la percepción de la gravedad de las amenazas y la disposición de los individuos a adoptar medidas preventivas. Esta convergencia de evidencias subraya la importancia crucial de la severidad percibida como un factor determinante en la formación de actitudes y comportamientos de seguridad en el entorno digital. De acuerdo con lo anterior, se declara la siguiente hipótesis:

H5: La severidad percibida influye positivamente en el comportamiento de ciberseguridad.

Por otra parte, la autoeficacia de respuesta se refiere a la creencia de un individuo en su capacidad para ejecutar con éxito las acciones de respuesta recomendadas para mitigar una amenaza (Kim et al., 2024; Rhee et al., 2009). En el contexto de la ciberseguridad, se traduce en la confianza de una persona en su habilidad para implementar medidas de protección efectivas (Rajab y Eydgahi, 2019). Esta asociación se ve reforzada por estudios más recientes que amplían la comprensión del papel de la autoeficacia en el comportamiento de ciberseguridad. Por ejemplo, Jansen y Van Schaik (2018) demostraron que la autoeficacia influye positivamente en el comportamiento

preventivo en línea, mientras que Sulaiman et al. (2022) reportaron una influencia positiva de la autoeficacia de respuesta en el comportamiento de ciberseguridad del usuario. Geil et al. (2018) corroboraron estos hallazgos, evidenciando el impacto directo de la autoeficacia en el comportamiento de ciberseguridad.

Además, Vance et al. (2012) expandieron el alcance de estos hallazgos al demostrar que la autoeficacia no solo influye en el comportamiento actual sino también en la intención de adoptar prácticas de ciberseguridad. Esta distinción entre comportamiento e intención proporciona una comprensión más matizada de cómo la autoeficacia opera en diferentes etapas del proceso de toma de decisiones en seguridad, por lo tanto, se propone la hipótesis:

H6: La autoeficacia de respuesta influye positivamente en el comportamiento de ciberseguridad.

La eficacia de respuesta, definida como la creencia en la efectividad de las medidas de seguridad implementadas por la organización para mitigar las amenazas cibernéticas (Rogers, 1983), ha sido objeto de estudios con resultados divergentes en el contexto de la ciberseguridad. Por un lado, Jansen y Van Schaik (2018) demostraron que la eficacia de respuesta impacta significativamente en el comportamiento de ciberseguridad, sugiriendo una relación positiva entre la percepción de la efectividad de las medidas de seguridad y la adopción de comportamientos protectores.

Sin embargo, es importante notar que la literatura no es unánime en este aspecto. En contraste con los hallazgos anteriores, Hina et al. (2019) reportaron que la eficacia de respuesta no se relaciona significativamente con el comportamiento de ciberseguridad. Esta discrepancia en los resultados subraya la complejidad de los factores que influyen en el comportamiento de seguridad y sugiere la necesidad de considerar variables contextuales adicionales, por todo ello se propone que:

H7: La eficacia de respuesta influye positivamente en el comportamiento de ciberseguridad.

En resumen, las hipótesis planteadas buscan examinar las relaciones entre los factores clave que influyen en el comportamiento de ciberseguridad en el contexto de las instituciones de educación superior, proporcionando así una comprensión más profunda de los mecanismos que impulsan las prácticas de seguridad efectivas en estos entornos.

Método

Respecto a este fenómeno de la ciberseguridad, de acuerdo con información de Domínguez (2021), el estado de Tamaulipas se posicionó como una de las entidades a nivel nacional en denuncias realizadas a la policía cibernética, principalmente por ciberdelitos como el robo de contraseñas en redes sociales, la intrusión a sistemas de información, seguidos del *pishing*. Para el año 2020 la Policía Cibernética Estatal atendió un total de 2 mil 327 denuncias por delitos cibernéticos (Hernández, 2021),

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

lo cual muestra la tendencia creciente en la vulnerabilidad de la ciberseguridad de los ciudadanos, con diversos métodos de ataque como lo son el *malware* y el *ransonware* (por mencionar algunos), situación que se ha agravado por la pandemia también a nivel mundial.

En este sentido, se han realizado esfuerzos por organizaciones como la Red Nacional de Investigación y Educación Mexicana, que resalta la importancia de los nuevos desafíos que se presentan en el entorno y a los cuales han tenido que adaptarse las instituciones educativas de educación superior en materia de ciberseguridad para la comunidad académica, con el propósito de identificar patrones y áreas de oportunidad para mejorar sus procesos asociados a la ciberseguridad (Corporación Universitaria para el Desarrollo de Internet [CUDI], 2021). De ahí la relevancia e importancia del desarrollo del estudio en la región.

Con el propósito de dar alcance al objetivo planteado y con el apoyo de la literatura, las variables a utilizar son operacionalizadas según se muestra en la Tabla 1. En cuanto al diseño del instrumento, se desarrolló basado en las contribuciones de estudios previos en contextos diferentes, adaptando la redacción de los ítems para su aplicación en la región de estudio. Se utilizó una escala Likert de cinco puntos (1 = muy en desacuerdo, 5 = muy de acuerdo). El proceso de desarrollo del instrumento incluyó las siguientes etapas: I) revisión por expertos: la versión preliminar del instrumento fue evaluada por cuatro expertos en el tema, cuya retroalimentación permitió realizar ajustes iniciales; II) estudio piloto: se aplicó el instrumento a 31 empleados activos de instituciones educativas expertos en el tema de ciberseguridad para su validación final; este proceso resultó en la eliminación de algunos ítems, cambios en la redacción

Tabla 1
Operacionalización de las variables de estudio

Variable	Sustento teórico
Conciencia sobre ciberseguridad: conocimiento de los usuarios finales sobre las amenazas de seguridad cibernética que enfrentan y los riesgos que presentan	Li et al., 2022; Koohang et al., 2020; Alhelaly et al., 2024
Hábito de protección: actividades rutinarias y repetitivas de forma inconsciente que se convierte en rutina	Tsai et al., 2016; Vance et al., 2012; Shahbaznezhad et al., 2021
Severidad de la amenaza: condiciones adversas esperadas por los individuos que puedan ser ciertas o no	Li et al., 2022; Tsai et al., 2016
Autoeficacia: evaluación personal de las habilidades y competencias propias para implementar medidas de seguridad	Rajab y Eydgahi, 2019
Eficacia de la respuesta: creencia en que las medidas de seguridad en sí mismas son efectivas para contrarrestar amenazas de seguridad	Sulaiman et al., 2022
Comportamiento de ciberseguridad: acciones concretas que los individuos llevan a cabo para proteger la información y los sistemas de información contra amenazas cibernéticas	Alsharida et al., 2023; Hong y Furnell, 2021

Fuente: Elaboración propia.

y adecuaciones generales, y III) instrumento final: el cuestionario definitivo consta de una sección de datos demográficos (sexo, rango de edad, puesto que desempeña) y 23 ítems que miden las variables del modelo teórico propuesto.

El trabajo empírico se llevó a cabo en las instituciones de educación superior de Tamaulipas, México. Se empleó un muestreo por conveniencia, considerando que todos los empleados de las instituciones, distribuidos en las principales ciudades del estado, podían participar en el estudio. Con el objetivo de alcanzar una validez aceptable mediante el uso del *software* SmartPLS, se estableció una meta de obtener una muestra superior a 100 participantes.

La aplicación del instrumento se realizó con la colaboración de las administraciones centrales, facilitando el acceso a los participantes. La recolección de datos se efectuó tanto de manera presencial como a través de la plataforma Google Forms, durante el periodo comprendido entre febrero y mayo del 2024. Los cuestionarios se distribuyeron en las principales ciudades de Tamaulipas, con la siguiente proporción: Ciudad Victoria (30%), Tampico (25%), Nuevo Laredo (18%), Reynosa (15%) y Matamoros (12%), por lo que se obtuvieron inicialmente 184 cuestionarios, de los cuales, tras un riguroso proceso de normalización y validación de datos, se retuvieron 159 para los análisis subsecuentes.

En cuanto al análisis inferencial, se realizó mediante modelado de ecuaciones estructurales utilizando el *software* SmartPLS v4 (SmartPLS, 2022). Se empleó un procedimiento con 5,000 submuestras para garantizar la robustez de los resultados. Los análisis incluyeron cruces de variables, matriz de correlación, cargas factoriales, varianza extraída media (AVE), estadístico t, varianza explicada (R^2), coeficientes *path* estandarizados (β). Estos análisis permitieron verificar la consistencia, homogeneidad y heterogeneidad de los datos, proporcionando una base sólida para la comprobación de las hipótesis propuestas.

Resultados y análisis

El análisis demográfico de los participantes reveló una composición diversa y representativa. Se observó una ligera predominancia masculina, con un 54.1% de hombres frente a un 45.9% de mujeres. En cuanto a la edad, la distribución mostró una concentración en los grupos de edad media y avanzada: el segmento de 36 a 45 años constituyó la mayor proporción (32.7%), seguido de cerca por el grupo de 46 a 55 años (30.2%). Los mayores de 55 años representaron un 22% de la muestra, mientras que el grupo más joven, de 26 a 35 años, conformó el 15.1% restante.

En cuanto a la función dentro de la institución, se evidenció un equilibrio entre roles académicos y administrativos. Los profesores-investigadores representaron una ligera mayoría con un 54.7%, mientras que el personal administrativo constituyó el

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

45.3% de los encuestados. Esta distribución proporciona una perspectiva integral que abarca tanto el ámbito académico como el operativo de la institución. Estas características demográficas ofrecen un contexto valioso para la interpretación de los resultados, permitiendo una comprensión matizada de las percepciones y comportamientos relacionados con la ciberseguridad en el ámbito de estudio.

Subsecuentemente se procedió al análisis inferencial utilizando SmartPLS v4. Este proceso se estructuró en dos fases secuenciales, siguiendo las recomendaciones de Hair et al. (2019): a) evaluación del modelo de medida y b) análisis del modelo estructural. Esta aproximación bifásica garantiza una evaluación tanto de la fiabilidad y validez de las mediciones como de las relaciones hipotéticas entre los constructos del modelo propuesto.

Para la validación del modelo de medida primero se debe examinar la fiabilidad del ítem, esta prueba examina las cargas factoriales –λ– o bien las correlaciones simples. Para que un ítem sea aceptado es necesario que posea un valor superior a 0.707 –λ^2, 50% de la varianza es explicada– (Chin, 1998). Las cargas factoriales de los ítems superan el umbral del 0.707. Posteriormente se debe analizar la consistencia interna –fiabilidad compuesta–, la cual se estima por medio del alfa de Cronbach y requiere de un valor mínimo aceptable de 0.7 (Nunnally, 1978); los valores obtenidos exceden el valor mínimo de 0.7 para todos los constructos.

Una vez analizado el constructo de forma interna se debe analizar ahora en conjunto con los demás que conforman el modelo, para ello primero se debe verificar la validación convergente, la cual es mediante la varianza extraída media y se requiere que cumpla con un valor que se sitúe por encima de 0.50 en la que más del 50% de la varianza de la variable/constructo es proporcionado por sus ítems (Fornell y Larcker, 1981). Los valores obtenidos superan el 0.50, indicando una adecuada validez convergente. Asimismo se debe determinar la validación discriminante, para ello se utiliza el indicador Dijkstra-Henseler (rho_A), que es preciso que sea mayor a 0.7. Los valores obtenidos superan el umbral del valor mínimo aceptado, respaldando la validez discriminante de los resultados.

Es importante señalar que durante el proceso de validación del modelo de medida se tomó la decisión de eliminar algunos ítems que no cumplían con los criterios mínimos recomendados para las cargas factoriales. Específicamente, se eliminaron los siguientes ítems: HP3 –hábito de protección–, PS3 –severidad percibida–, C3 –conciencia de ciberseguridad– y ERS2 –eficacia de respuesta–. Esta depuración del modelo asegura que todos los ítems retenidos contribuyen significativamente a la medición de sus respectivos constructos, fortaleciendo así la validez y fiabilidad general del modelo de medida.

Adicionalmente, se reporta la varianza explicada –R^2– para los constructos endógenos, proporcionando una medida de la capacidad predictiva del modelo. Chin

(1998) sugiere que un valor igual o superior a 0.67 indica un efecto sustancial, 0.33 un efecto moderado, y 0.19 una determinación débil. Valores de R^2 iguales o mayores a 0.1 se consideran informativos. Los resultados respaldan la fiabilidad y validez del modelo de medida, permitiendo proceder con confianza al análisis del modelo estructural (ver Tabla 2).

Tabla 2
Fiabilidad y validez de los ítems y constructos

Constructo / Ítem		Cargas	Fiabilidad compuesta	Alpha de Cronbach	AVE	Varianza explícita R^2	rho_A
Hábito			0.912	0.855	0.775	No aplica	0.869
	HP1	0.858***					
	HP2	0.925***					
	HP4	0.856***					
Severidad percibida			0.918	0.866	0.788	No aplica	0.881
	PS1	0.884***					
	PS2	0.885***					
	PS4	0.894***					
Conciencia			0.845	0.735	0.645	No aplica	0.789
	C1	0.824***					
	C2	0.725***					
	C4	0.855***					
Autoeficacia de respuesta			0.928	0.897	0.746	0.293	0.902
	AR1	0.898***					
	AR2	0.883***					
	AR3	0.870***					
	AR4	0.845***					
Comportamiento			0.877	0.871	0.721	0.467	0.877
	CSC1	0.793***					
	CSC2	0.885***					
	CSC3	0.873***					
	CSC4	0.844***					
Eficacia de respuesta			0.906	0.902	0.836	0.234	0.906
	ERS1	0.896***					
	ERS3	0.925***					
	ERS4	0.856***					

Fuente: Elaboración propia con base en los resultados obtenidos en SmartPLS 4.

Junto con la validez convergente, la validez discriminante de los constructos es un elemento importante en la validación del modelo de medida, que se analiza a través del método de la ratio Hetero-Trait Mono-Trait –HTMT– (Tabla 3). Los valores obtenidos del análisis se encuentran dentro de los parámetros establecidos como válidos para este indicador (< 0.85) (Dijkstra y Henseler, 2015).

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

Tabla 3
Validez discriminante con HTMT

	AR	CSC	CC	ER	HP	SP
Autoeficacia_Respuesta						
Comportamiento_Ciberseguridad	0.717					
Conciencia ciberseguridad	0.564	0.433				
Eficacia_en_respuesta	0.628	0.475	0.550			
Habito de protección	0.516	0.558	0.705	0.407		
Severidad_Percibida	0.259	0.485	0.183	0.119	0.257	

Fuente: Elaboración propia con base en los resultados obtenidos en SmartPLS 4.

Una vez determinado que los ítems cumplen con lo establecido, se debe realizar la validación del modelo estructural, mediante el análisis de los coeficientes *path* estandarizados (β), los cuales se identifican a través de las relaciones entre las variables propuestas como hipótesis. Siguiendo a Chin (1998), se considera que β debe ser al menos 0.2, con una recomendación de superar 0.3 para ser considerado significativo. Adicionalmente, se consideraron los siguientes criterios para el análisis inferencial: la significancia (*p-value*), la cual debe ser menor a 0.05 ($p < 0.05$), y el *T-statistic*, con un remuestreo de 5000, donde el valor obtenido debe ser superior a 1.65 (Hair et al., 2019).

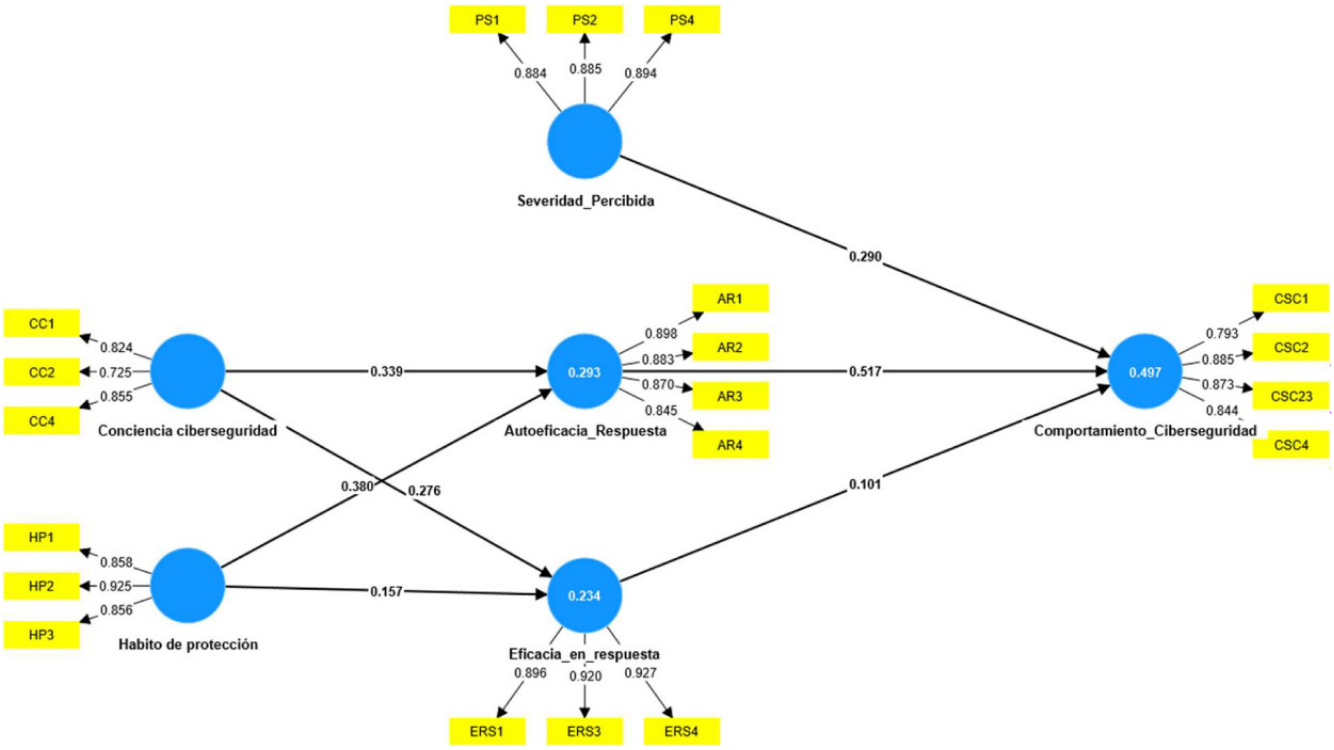
Los resultados muestran que cinco de las siete hipótesis propuestas fueron aceptadas (ver Tabla 4), superando los umbrales establecidos para los coeficientes *path*, *t-statistic* y significancia. Las hipótesis rechazadas fueron *eficacia en respuesta* versus *comportamiento de ciberseguridad* y *hábito de protección* versus *eficacia en respuesta*, que no alcanzaron los niveles de significancia requeridos. Estos hallazgos proporcionan una base sólida para la interpretación de las relaciones entre los constructos del modelo y permiten una evaluación robusta de las hipótesis planteadas en el estudio sobre ciberseguridad en instituciones de educación superior. La Figura 1 muestra en forma

Tabla 4
Evaluación de las seis hipótesis propuestas

N°	Hipótesis	Coeficiente Path (b)	T-statistic	Sig.	Comentario
H1	CSC → AR	0.339***	3.448	0.001	Aceptada
H2	CSC → ER	0.380***	3.583	0.000	Aceptada
H3	HP → AR	0.276**	2.742	0.006	Aceptada
H4	HP → ER	0.157	1.435	0.151	Rechazada
H5	SP → CC	0.290***	3.768	0.000	Aceptada
H6	AR → CC	0.517***	6.399	0.000	Aceptada
H7	ER → CC	0.101	1.52	0.129	Rechazada

Fuente: Elaboración propia con base en los resultados obtenidos en SmartPLS 4.

Figura 1
Resultados del modelo: coeficientes path y significancia estadística



Fuente: Elaboración propia con base en los resultados obtenidos en SmartPLS 4.

gráfica el modelo de investigación teórico propuesto, incluyendo las variables, los ítems con su carga factorial, los coeficientes *path* estandarizados y la varianza explicada.

Discusión

La hipótesis 1, en la que se declara que la conciencia de ciberseguridad influye en la autoeficacia de respuesta, es aceptada, ya que tiene una relación positiva y significativa ($\beta = 0.339$, $t = 3.448$, $p < 0.001$). Este hallazgo está en línea con los de Torten et al. (2018), quienes establecieron una relación significativa entre la conciencia de seguridad y la autoeficacia; además respalda la afirmación de Khando et al. (2021) sobre la influencia sustancial de la conciencia en las conductas de seguridad de la información. La conciencia de ciberseguridad, medida a través de la comprensión de las amenazas potenciales, el conocimiento de las causas de las violaciones de seguridad y la actualización constante sobre noticias e información de ciberseguridad parece fortalecer la confianza de los empleados en su capacidad para responder eficazmente a las amenazas. Esta relación sugiere que cuando los empleados están más informados y alertas sobre los riesgos cibernéticos que enfrenta su institución se sienten más capaces de tomar medidas preventivas y reactivas adecuadas, esto subraya la importancia

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

de mantener a los empleados bien informados y actualizados, como estrategia para mejorar su confianza en el manejo de situaciones de seguridad cibernética.

Respecto a la hipótesis 2, los resultados observados muestran una influencia positiva y significativa de la conciencia de ciberseguridad en la eficacia de respuesta ($\beta = 0.380$, $t = 3.583$, $p < 0.001$). Este hallazgo corrobora nuevamente los resultados de Torten et al. (2018) y extiende la comprensión sobre cómo la conciencia de ciberseguridad no solo afecta la percepción individual de las capacidades sino también la creencia en la efectividad general de las medidas de seguridad. Esta relación sugiere que cuanto más conscientes son los empleados de las amenazas y prácticas de ciberseguridad, más confianza tienen en la capacidad de su institución para proteger la información sensible. Es decir, una mayor comprensión de los riesgos y medidas de seguridad conduce a una mayor apreciación y confianza en las estrategias de protección implementadas por la institución.

En lo relacionado a la hipótesis 3, los resultados revelan una influencia positiva y significativa del hábito de protección en la autoeficacia de respuesta ($\beta = 0.276$, $t = 2.742$, $p < 0.01$). Este hallazgo concuerda con los resultados de Sulaiman et al. (2022), quienes reportaron un impacto positivo del hábito en la autoeficacia de respuesta. La relación observada sugiere que las prácticas habituales de seguridad, como el uso de contraseñas seguras, la actualización regular de configuraciones de privacidad en redes sociales, y la realización de copias de seguridad de actividades laborales importantes, contribuyen significativamente a fortalecer la confianza de los empleados en sus habilidades de ciberseguridad. Estos hallazgos sugieren que la práctica regular de comportamientos seguros no solo refuerza las habilidades técnicas sino que también aumenta la confianza general de los empleados en su capacidad para manejar amenazas de ciberseguridad en el entorno laboral.

Los resultados la hipótesis 4 del estudio no encontraron una relación significativa entre el hábito de protección y la eficacia de respuesta ($\beta = 0.157$, $t = 1.435$, $p = 0.151$). Este hallazgo contradice los estudios de Vance et al. (2012) y Geil et al. (2018), quienes reportaron una asociación positiva entre la práctica habitual de medidas de seguridad y la percepción de la eficacia general de las estrategias de ciberseguridad.

Una posible explicación de esta discrepancia es que, en el contexto específico del estudio, los hábitos individuales de protección parecen fortalecer la confianza personal en la capacidad para responder a amenazas (autoeficacia), pero no necesariamente influyen en la percepción de la efectividad de las medidas de seguridad a nivel organizacional. En otras palabras, aunque los empleados desarrollen rutinas de seguridad como el uso de contraseñas robustas, la actualización de *software* y la protección de datos, estas prácticas pueden percibirse como esfuerzos individuales sin un impacto directo en la seguridad institucional.

Otra interpretación es que los empleados podrían no estar plenamente informados sobre cómo sus hábitos personales de ciberseguridad se alinean con las políticas

organizacionales. Si las instituciones de educación superior no establecen mecanismos claros que relacionen las acciones individuales con los protocolos de seguridad organizacionales, es posible que los empleados no perciban una conexión evidente entre su comportamiento y la eficacia de las estrategias de protección institucional.

Los hallazgos de la hipótesis 5 respaldan la influencia positiva y significativa de la severidad percibida en el comportamiento de ciberseguridad ($\beta = 0.290$, $t = 3.768$, $p < 0.001$). Estos resultados están en línea con los estudios de Jansen y Van Schaik (2018) y Geil et al. (2018), quienes encontraron una influencia significativa de la severidad percibida en el comportamiento de ciberseguridad. Además confirman la afirmación de Hina et al. (2019) sobre la influencia de la severidad percibida en la intención de comportamiento. Estos resultados sugieren que cuando los empleados de las instituciones de educación superior reconocen la gravedad de las amenazas cibernéticas, son más propensos a adoptar medidas preventivas concretas. Esto resalta la importancia de educar a los empleados no solo sobre la existencia de amenazas cibernéticas sino también sobre las potenciales consecuencias severas de las brechas de seguridad. Enfatizar la gravedad de estas amenazas parece ser una estrategia efectiva para motivar la adopción de prácticas de ciberseguridad más robustas y consistentes en el entorno laboral educativo.

En cuanto a la hipótesis 6, los resultados muestran una fuerte influencia positiva de la autoeficacia de respuesta en el comportamiento de ciberseguridad ($\beta = 0.517$, $t = 6.399$, $p < 0.001$). Estos hallazgos están en línea con los de Jansen y Van Schaik (2018) y Sulaiman et al. (2022), quienes demostraron una influencia positiva de la autoeficacia en el comportamiento preventivo en línea y el comportamiento de ciberseguridad, respectivamente. La magnitud de este efecto subraya la importancia crítica de la autoeficacia en el contexto de las instituciones de educación superior. Sugiere que fomentar la confianza de los empleados en sus habilidades para implementar medidas de seguridad puede ser una de las estrategias más efectivas para mejorar el comportamiento de ciberseguridad en estas instituciones.

Por último, en la hipótesis 7 propuesta no se encontró una relación significativa entre la eficacia de respuesta y el comportamiento de ciberseguridad ($\beta = 0.101$, $t = 1.520$, $p = 0.129$). Este hallazgo es contrario a lo reportado por Jansen y Van Schaik (2018), quienes encontraron que una mayor confianza en la efectividad de las estrategias de seguridad institucionales estaba asociada con un comportamiento más proactivo en ciberseguridad. Sin embargo, estos resultados coinciden con los de Hina et al. (2019), quienes tampoco identificaron una relación significativa entre ambos factores.

Una posible explicación de esta discrepancia es que, en el contexto de las instituciones de educación superior en Tamaulipas, la percepción de que las medidas institucionales de seguridad son efectivas no necesariamente motiva a los empleados a modificar su comportamiento. Es posible que confíen en que la institución cuenta

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

con protocolos adecuados para manejar amenazas y, como consecuencia, deleguen la responsabilidad de la seguridad a la organización en lugar de asumirla a nivel individual.

Otra interpretación es que la eficacia de respuesta está más vinculada a una percepción organizacional que individual. Mientras que la autoeficacia de respuesta refleja la confianza en las propias habilidades para enfrentar amenazas, la eficacia de respuesta evalúa la confianza en que la institución tiene mecanismos efectivos para manejar incidentes de ciberseguridad. Si los empleados no perciben una relación directa entre ambas dimensiones, es comprensible que su comportamiento de ciberseguridad no se vea influenciado por la percepción de las medidas organizacionales.

Conclusiones

Este estudio ha examinado los factores que influyen en el comportamiento de ciberseguridad de los empleados en instituciones de educación superior en Tamaulipas, México, utilizando la PMT como marco de referencia. Los resultados proporcionan valiosos *insights* sobre los mecanismos que impulsan las prácticas de seguridad en este contexto específico.

En primer lugar, los hallazgos subrayan la importancia crítica de la conciencia de ciberseguridad. La influencia positiva de la conciencia tanto en la autoeficacia como en la eficacia de respuesta sugiere que los programas de educación y concientización sobre ciberseguridad son fundamentales para mejorar la confianza de los empleados en sus habilidades y en la efectividad de las medidas de seguridad institucionales. En segundo lugar, el estudio revela el papel complejo del hábito de protección. Mientras que los hábitos de seguridad influyen positivamente en la autoeficacia, sorprendentemente no mostraron una relación significativa con la eficacia de respuesta. Esto sugiere que las prácticas de seguridad individuales no necesariamente se traducen en una mayor confianza en las medidas de seguridad institucionales, lo que indica la necesidad de un enfoque más integrado en la formación de hábitos de seguridad.

La severidad percibida y la autoeficacia de respuesta emergieron como predictores significativos del comportamiento de ciberseguridad. Estos hallazgos resaltan la importancia de educar a los empleados sobre las consecuencias potenciales de las brechas de seguridad y de fortalecer su confianza en sus habilidades para implementar medidas de protección. Contrariamente a algunas investigaciones previas, no se encontró una relación significativa entre la eficacia de respuesta y el comportamiento de ciberseguridad. Este hallazgo sugiere que, en el contexto de las instituciones de educación superior en Tamaulipas, la percepción de la efectividad de las medidas de seguridad institucionales no es un factor determinante directo del comportamiento individual de seguridad.

De manera general, los resultados muestran que la conciencia de ciberseguridad, la severidad percibida y, especialmente, la autoeficacia de respuesta influyen positiva-

mente en el comportamiento de seguridad cibernética de los empleados. El hábito de protección fortalece la autoeficacia, pero no impacta directamente en la eficacia de respuesta. Por otro lado, la percepción de eficacia de las medidas organizacionales no mostró una relación significativa con el comportamiento individual, lo que sugiere que los empleados pueden delegar la seguridad en la institución en lugar de asumir un rol activo. Estos hallazgos enfatizan la necesidad de estrategias de capacitación que refuercen la confianza individual y la corresponsabilidad en ciberseguridad.

Desde una perspectiva teórica, este estudio contribuye a la literatura sobre ciberseguridad al aplicar la PMT en el contexto específico de las instituciones de educación superior en México. Los resultados subrayan la necesidad de considerar factores contextuales al aplicar teorías generales de comportamiento de seguridad. En términos prácticos, se sugieren varias estrategias para mejorar la ciberseguridad en las instituciones educativas, como: implementar programas de concientización que no solo informen sobre amenazas sino que también fortalezcan la confianza de los empleados en sus habilidades de seguridad; desarrollar estrategias que vinculen más estrechamente las prácticas de seguridad individuales con las medidas institucionales; enfatizar las consecuencias potenciales de las brechas de seguridad para aumentar la percepción de severidad, y fomentar la autoeficacia a través de capacitación práctica y retroalimentación positiva.

En cuanto a las limitaciones del estudio, este únicamente se enfocó a las instituciones de educación superior en Tamaulipas, México. Futuras investigaciones podrían expandir el alcance geográfico y comparar los resultados con otros contextos educativos y culturales. Además, sería interesante explorar más a fondo la discrepancia encontrada entre el hábito de protección y la eficacia de respuesta, así como la falta de relación entre la eficacia de respuesta y el comportamiento de ciberseguridad.

En conclusión, este estudio proporciona una comprensión más profunda de los factores que influyen en el comportamiento de ciberseguridad en las instituciones de educación superior. Los hallazgos subrayan la importancia de un enfoque holístico que considere tanto los factores individuales como organizacionales en la promoción de prácticas de seguridad efectivas dentro del contexto educativo mexicano.

Referencias

Alhelaly, Y., Dhillon, G., y Oliviera, T. (2024). Mobile identity protection: The moderation role of self-efficacy. *Australasian Journal of Information Systems*, *28*. https://doi.org/10.3127/ajis.v28.4397

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., y Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Alsharif, M., Mishra, S., y AlSheri, M. (2022). Impact of human vulnerabilities on cybersecurity. *Computer Systems Science and Engineering*, *40*(3), 1153-1116. https://doi.org/10.32604/csse.2022.019938

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

Arriaza, R. E., Mutch, C., y Mutch, N. T. (2021). When Covid-19 is only part of the picture: Caring pedagogy in higher education in Guatemala. *Pastoral Care in Education*, *39*(3), 236-249. https://doi.org/10.1080/02643944.2021.1938648

Atta, A., Zaman, N. U., y Khan, H. H. (2021). Battling the threat of workplace harassment: An appraisal based on Protection Motivation Theory. *Journal of Asian Finance Economics and Business*, *8*(6), 491-504. https://doi.org/10.13106/jafeb.2021.vol8.no6.0491

Bezbaruah, K. (2022). Information, communication and technology and its application in teaching learning process of philosophy. *International Journal of Early Childhood Special Education*, *14*(3), 3143-3146. https://doi.org/10.1207/s15566935eed1703_1

Caldarulo, M., Welch, E. W., y Freeney, M. K. (2022). Determinants of cyber-incidents amog small and medium US cities. *Government Information Quarterly*, *39*(3), 101703. https://doi.org/10.1016/j.giq.2022.101703

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, *295*(2), 295-336.

CUDI [Corporación Universitaria para el Desarrollo de Internet] (2021, jul. 1). *Resultados de la Encuesta de Ciberseguridad en IES Miembros CUDI*. http://repositorio.cudi.edu.mx/handle/11305/2186

Cummings, C. L., Rosenthal, S., y Kong, W. Y. (2021). Secondary Risk Theory: Validation of a novel model of protection motivation. *Risk Analysis*, *41*(1), 204-220. https://doi.org/10.1111/risa.13573

Dawadi, S., Giri, R. A., y Simkhada, P. (2020). Impact of COVID-19 on the education sector in Nepal: Challenges and coping strategies [Prepint]. *Sage Submissions*. https://doi.org/10.31124/advance.12344336.v1

Dijkstra, T. K., y Henseler, J. (2015). Consistent and asymptotically normal PLS estimators forlinear structural equations. *Computational Statistics & Data Analysis*, *81*(1), 10-23.

Domínguez, R. A. (2021). Ciberdelitos, alarma mundial y políticas de información en ciberseguridad: un acercamiento al contexto de Tamaulipas. En R. A. Domínguez, *Problemas sociales de información, comunicación e interacción en espacios digitales: panorama expuesto en una sociedad pandémica* (pp. 12-37). El Colegio de Tamaulipas.

Dzyana, H., Pasichnyk, V., Garmash, Y., Naumko, M., y Didych, O. (2022). The system for ensuring the information security of the organization in the context of Covid-19 based on Public. Private partnership. *IJCSNS International Journal of Computer Science and Network Security*, *22*(6), 19-24. https://doi.org/10.22937/IJCSNS.2022.22.6.4

ENISA [European Union Agency for Cybersecurity] (2018, feb. 6). *Cyber security culture in organisations*. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

FBI [Federal Bureau of Investigation] (2022). *Internet Crime Report 2022*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Fornell, C., y Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50. https://doi.org/10.2307/3151312

Fouad, N. S. (2022). The security economics of EdTech: Vendors' responsibility and the cybersecurity challenge in the education sector. *Digital Policy Regulation and Governance*, *24*(3), 259-273. https://doi.org/10.1108/DPRG-07-2021-0090

Furnell, S., Haney, J., y Theofanos, M. (2021). Pandemic parallels: What can cybersecurity learn from COVID-19? *Computer*, *54*(3). https://doi.org/10.1109/MC.2020.3046888

Geil, A., Sagers, G., Spaulding, A. D., y Wolf, J. R. (2018). Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review*, *21*(3), 317-334. https://doi.org/10.22434/IFAMR2017.0045

GOV.UK (2022, jul. 11). *Official Statistics: Educational institutions findings annex - Cyber Security Breaches Survey 2022*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022#appendix-a-further-information

Hair, J., Hult, T., Ringle, C., Sarstedt, M., Castillo, J., Cepeda, G., y Roldán, J. (2019). *Manual de Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage.

Hasan, S., Ali, M., Kurnia, S., y Thurasamy, R. (2021). Evaluating the cyber security readiness of organi-

zations and it influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Hernández, A. (2021, mar. 31). Policía de Tamaulipas recibe 2 mil 300 denuncias por delitos cibernéticos. *Milenio*. https://www.milenio.com/policia/tamaulipas-policia-recibe-2-mil-300-denuncias-delitos-internet

Hina, S., Selvam, D. D., y Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*, 101594. https://doi.org/10.1016/j.cose.2019.101594

Holgeid, K. K., Krogstie, J., Mikalef, P., Saur, E. E., y Sjoberg, D. (2022). Benefits management and information technology work distribution. *IET Software*, *16*(4), 438-454. https://doi.org/10.1049/sfw2.12062

Hong, Y., y Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*, 102710. https://doi.org/10.1016/j.jisa.2020.102710

Ivari, N., Sharma, S., y Ventä-Olkkonen, L. (2020). Digital transformation of everyday life – How COVID-19 pandemic transformed the basic education of the young generation and why information management research should care? *International Journal of Informacion Management*, *55*, 102183. https://doi.org/10.1016/j.ijinfomgt.2020.102183

Jansen, J., y Van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*, *87*, 371-383. https://doi.org/10.1016/j.chb.2018.05.010

Kennison, S. M., y Chan-Tin, E. (2020). Taking risk with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology*, *11*, 546546. https://doi.org/10.3389/fpsyg.2020.546546

Khando, K., Gao, S., Islam, S. M., y Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Society*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kim, B. J., Kim, M. J., y Lee, J. (2024). Examining the impact of work overload on cybersecurity behavior: highlighting self-efficacy in the realm of artificial intelligence. *Current Psychology*, *43*, 17146-17162. https://doi.org/10.1007/s12144-024-05692-4

Kondruss, B. (2023). Cyber attacks on universities. University ransomware attacks & data breaches worldwide. *KonBriefing*. https://konbriefing.com/en-topics/cyber-attacks-universities.html

Koohang, A., Anderson, J., Nord, J. H., y Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231-247. https://doi.org/10.1108/IMDS-07-2019-0412

Lahiri, A., Jha, S. S., Chakraborty, A., Dobe, M., y Dey, A. (2021). Role of threat and coping appraisal in protection motivation for adoption of preventive behavior during COVID-19 pandemic. *Frontiers in Public Healt*, *9*, 678566. https://doi.org/10.3389/fpubh.2021.678566

Li, L., He, W., Xu, L., Ash, I., Anwar, M., y Yuan, X. (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

Li, L., Xu, L., y He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165. https://doi.org/10.1016/j.chbr.2021.100165

Microsoft (2023). *Microsoft Security Intelligence*. https://www.microsoft.com/en-us/wdsi/threats

Morales-Sáenz, F. I., Medina-Quintero, J. M., y Rodríguez, F. O. (2024a). Seguridad digital y violencias estructurales: perspectivas y desafíos contemporáneos. *Dilemas Contemporáneos: Educación, Política y Valores*, *12*(esp.). https://doi.org/10.46377/dilemas.v12i.4486

Morales-Sáenz, F. I., Medina-Quintero, J. M., y Reyna-Castillo, M. (2024b). Beyond data protection: Exploring the convergence between cybersecurity and sustainable development in business. *Sustainability*, *16*(14), 5884. https://doi.org/10.3390/su16145884

Pranggono, B., y Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., y Sebire, N. J. (2019). Phishing in healthcare organi-

ie revista de investigación educativa de la Rediech
vol. 16 • 2025 • e2271 • ISSN: 2448-8550

sations: Threats, mitigation and approaches. *BMJ Health & Care Informatics*, *26*(1), e100031. https://doi.org/10.1136/bmjhci-2019-100031

Rajab, M., y Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211-223. https://doi.org/10.1016/j.cose.2018.09.016

Rhee, H., Cheongtag, K., y Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826. https://doi.org/10.1016/j.cose.2009.05.008

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised Theory of Protection Motivation. En J. Cacioppo y R. Petty, *Social psychophysiology* (pp. 153-177). Guildford Press.

Saeed, S. (2023). Education, online presence and cybersecurity implications: A study of information security practices of computing students in Saudi Arabia. *Sustainability*, *15*(12), 9426. https://doi.org/10.3390/su15129426

Shahbaznezhad, H., Kolini, F., y Radhidirad, M. (2021). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6), 539-550. https://doi.org/10.1080/08874417.2020.1812134

Siponen, M., Mahmood, M. A., y Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006

SmartPLS (2022). *SmartPLS 4*. https://www.smartpls.com

Sulaiman, N. S., Fauzi, M. A., Hussain, S., y Wider, W. (2022). Cybersecurity behavior among government employees: The role of Protection Motivation Theory and responsibility in mitigating cyberattacks. *Information*, *13*(17), 9528. https://doi.org/10.3390/su13179528

Taborda, M. A., Collazos, F. A., Marulanda, C. A., y Villalba, K. M. (2021). Dynamic cybersecurity model based on ISO standards for higher education institutions in Colombia. *Ingeniería Solidaria*, *17*(3). https://doi.org/10.16925/2357-6014.2021.03.05

Torten, R., Reaiche, C., y Boyle S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79. https://doi.org/10.1016/j.cose.2018.08.007

Tsai, H. Y., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., y Cotten , S. R. (2016). Understanding online safety behaviors: A Protection Motivation Theory perspective. *Computers & Security*, *59*, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Ulven, J. B., y Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2). https://doi.org/10.3390/fi13020039

Valiente-Lopez, N., y Tejera-Reyte, C. C. (2022). Information and communication technologies as teaching-learning means. *Luz*, *21*(1), 28-37.

Vance, A., Siponen, M., y Pahnila, S. (2012). Motivating is security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Vrhovec, S., y Mihelic, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computer & Security*, *106*, 102309. https://doi.org/10.1016/j.cose.2021.102309

Cómo citar este artículo:

Morales Sáenz, F. I., Medina Quintero, J. M., y Abrego Almazan, D. (2025). Ciberseguridad en instituciones de educación superior: un análisis desde la perspectiva de la teoría de la motivación de protección. *IE Revista de Investigación Educativa de la REDIECH*, *16*, e2271. https://doi.org/10.33010/ie_rie_rediech.v16i0.2271

Todos los contenidos de *IE Revista de Investigación Educativa de la REDIECH* se publican bajo una licencia de Creative Commons Reconocimiento-NoComercial 4.0 Internacional, y pueden ser usados gratuitamente para fines no comerciales, dando los créditos a los autores y a la revista, como lo establece la licencia.