AvaCient ISSN 2992-8567
Año 3, Vol. V, Núm. 1, Enero Junio 2025 pp. 22-32

Transformando la educación en ciberseguridad: integrando tecnología educativa para formar profesionales resilientes en la universidad

Jesús Alberto García Rojas[1], Yhadira Huicab García[2]
Kenia Landeros Valenzuela[3], Teresa de Jesús Vargas Vega[4]

Artículo de investigación científica
Recibido: 20/09/2024 Aceptado: 12/02/2025
https://doi.org/10.69823/avacient.v5n1a3

Resumen.- Cada vez más es mayor la cantidad de equipos electrónicos que disponen de herramientas de ciberseguridad, además de incorporar leyes, la ética y la economía. En este punto, se debe reconocer la importancia que tienen los licenciados en Derecho o abogados para poder acortar la brecha de datos o en la gestión de incidentes, en otro sentido las empresas también en la parte tecnológica deben conocer el marco regulatorios para poder prevenirse en caso de un incidente. El auge que han tenido la creación de cuentas falsas para encontrar vulnerabilidades tecnológicas para extraer información, para el robo de información o la afectación al funcionamiento de los dispositivos informáticos. El despertar ya en este 2024 y observar que ya no es solo que el gobierno te pueda espiar, que sea de ciencia ficción, sino que ahora está el concepto de hackers y de personas que tienen conocimiento informático que están sobre la información y los daños, claramente no usando la ética profesional no es ya solo de la ciencia ficción, sino que es de la realidad, al estar conectado en internet desde la computadora.

Palabras Clave: Protección de datos, tecnología, educación.

TRANSFORMING CYBERSECURITY EDUCATION: INTEGRATING EDUCATIONAL TECHNOLOGY TO TRAIN RESILIENT PROFESSIONALS AT THE UNIVERSITY

Abstract.- More and more electronic devices are equipped with cybersecurity tools, in addition to incorporating laws, ethics, and economics. At this point, it is essential to recognize the importance of law graduates or lawyers in helping to bridge the data gap or manage incidents. On the other hand, companies must also be aware of the regulatory framework from a technological standpoint to better prepare for potential incidents. There has been a significant rise in the creation of fake accounts aimed at identifying technological vulnerabilities, extracting information, committing data theft, or disrupting the functioning of computer systems. The awakening in 2024 has shown that it's no longer just the government spying on you — no longer something from science fiction — but rather the reality of hackers and individuals with technical knowledge actively targeting information and causing damage. This is no longer a fictional scenario; it is a reality we face just by being connected to the internet from our computers.

Keywords: Data protection, technology, education.

Introducción

El concepto de ciberseguridad ha evolucionado considerablemente desde sus inicios en la década de 1970, cuando las preocupaciones sobre la seguridad informática comenzaron a emerger con la aparición de los primeros virus y ataques a redes informáticas (Anderson, 1972). A medida que las tecnologías avanzaban, el ámbito académico comenzó a reconocer la importancia de la ciberseguridad como disciplina, impulsada por la proliferación de Internet en los años 90 (Denning, 1999).

En el contexto educativo, la integración de la tecnología en la enseñanza ha seguido un camino paralelo. Durante las últimas dos décadas, se ha producido un aumento significativo en el uso de herramientas tecnológicas para mejorar la enseñanza y el aprendizaje (Johnson, Adams & Cummins, 2012). En particular, las instituciones de educación superior han comenzado a adoptar plataformas digitales y simulaciones para mejorar la formación en áreas técnicas como la

[1] Profesor Investigador. Tecnológico Nacional de México. TES de San Felipe del Progreso. División de Ingeniería Informática. https://orcid.org/0000-0002-0292-0789, CVU 397590. jesus.gr@sfelipeprogreso.tecnm.mx, (**Autor corresponsal**).
[2] Profesora Investigadora. Tecnológico Nacional de México. Instituto Tecnológico Superior de los Ríos. División de Licenciatura en Administración. yhadira.huicab@gmail.com. https://orcid.org/0000-0001-7987-383X
[3] Profesora Investigadora. Tecnológico Nacional de México. Instituto Tecnológico Superior de los Ríos. División de Licenciatura en Administración. landeros_keny@hotmail.com. https://orcid.org/0000-0003-4561-0155
[4] Profesora Investigadora. Universidad Autónoma del Estado de Hidalgo. tvvega@uaeh.edu.mx. https://orcid.org/0000-0002-6051-7197

AvaCient ISSN 2992-8567
Año 3, Vol. V, Núm. 1, Enero Junio 2025 pp. 22-32

ciberseguridad, lo que permite a los estudiantes desarrollar habilidades en entornos controlados y realistas (Smith, 2015).

Hoy en día, la educación en ciberseguridad no solo busca transmitir conocimientos técnicos, sino también formar profesionales resilientes y adaptativos que puedan responder a amenazas en constante evolución. La resiliencia en ciberseguridad se define como la capacidad para anticipar, resistir y recuperarse de ataques cibernéticos (Bodeau & Graubart, 2017). Con el aumento de ciberataques globales, es crucial que las universidades adapten sus currículos y adopten tecnologías avanzadas para preparar a los estudiantes frente a los retos del futuro (National Institute of Standards and Technology, 2018).

La ciberseguridad es delicada, puede afectar o invadir los datos personales, las finanzas, la libertad de expresión, también hoy en día se puede modificar al teletrabajo que ha surgido con fuerza una vez que pasamos la pandemia por COVID-19 (Coronavirus Disease, 2019) (World Health Organization, 2020).

El IOT (internet de las cosas), la banca en línea, el comercio electrónico, la inteligencia artificial, que tienen utilidad, pero pueden ser vulnerados y afectar su funcionamiento y agraviar a las personas, por ello es donde la ciberseguridad cobra importancia, donde también es importante conocer la responsabilidad jurídica para exigir los derechos como víctimas.

Es por estas cuestiones de ciberataque que el derecho debe proteger a los individuos, sea persona física o moral, hoy en día todos ocupan tecnología e internet para su vida cotidiana, en ese sentido todos son vulnerables. Generalmente los ciberataques van orientados a la ganancia económica, pero también existen algunos que solo es por el dolo de alterar o eliminar información importante, así estropear configuración de los equipos electrónica y alterar su funcionamiento. Por lo que es importante que la gente y las empresas tomen medidas de seguridad informática para proteger sus equipos y su información, y cuando aun así sucedan ampararse con lo que dice la ley, una vez que el derecho se alinee a las necesidades de estas oportunidades que implica por ejemplo electrónico, el cliente se sentirá más, seguro y protegido, porque las personas con pocos conocimientos de computación es la gente que está más propensa a sufrir un daño por medio de un ciberataque.

La gente publica ya casi todo en las redes sociales, a *tik tok* donde se publican un sin fin de videos, donde sin darse cuenta los hackers invaden la privacidad, sabiendo los gustos, clase social, afinidades, lo cual pone en una situación vulnerable ante ellos, la gente malintencionada siempre está ahí, esperando una oportunidad para estafar, secuestrar, aprovecharse de las emociones de la gente, donde no se sabe de verdad quien acecha.

Es por ello que contar con profesionales en la informática para poder garantizar el uso adecuado del equipo informático es vital hoy en día para las empresas y los ciudadanos. Es muy buena práctica que existan *hackers* éticos que ayuden a hacer pruebas con los equipos para encontrar vulnerabilidades que permitan mejorar la seguridad de los equipos informáticos, dándose cuenta de cómo se puede forzar la seguridad y hacer daño, para poder realizar prevención como usuarios de la informática en el día a día, cada vez se hace indispensable el mandar un correo electrónico, el cotizar mobiliario, alguna refacción para una máquina, todo por medio de internet, que necesitamos garantizar la ciberseguridad de los equipos informáticos.

El hacking ético, lo que mucha gente piensa cuando le dicen la palabra hacker, es relacionado con alguien que va a destrozar la información, que va a actuar con maldad hacia nosotros operando equipos informáticos, lo cual es correcto, pero un hacker es una persona que le gusta explorar, que realiza experimentaciones a veces por curiosidad para ver cómo funcionan los sistemas informáticos por mencionar un ejemplo, pero existen *hackers* que su intención es vulnerar la seguridad con el hecho de querer mejorarla, pero no siempre así lo es (Pérez, 2024).

Marco teórico

El avance acelerado de la tecnología en la era digital ha subrayado la creciente importancia de la ciberseguridad como un campo crucial para proteger la información y los sistemas en diversos sectores (Denning, 1999). Las universidades tienen la responsabilidad de preparar a los estudiantes no solo para enfrentar los desafíos actuales en ciberseguridad, sino también para adaptarse a las amenazas emergentes (López & Ramírez, 2021). La integración de la tecnología educativa en el currículo de ciberseguridad se presenta como una estrategia fundamental para lograr este objetivo, dado que las herramientas digitales pueden mejorar significativamente la comprensión de los conceptos y las competencias prácticas en este campo (Gómez & Pérez, 2015).

La tecnología educativa abarca una amplia gama de herramientas y métodos que facilitan el aprendizaje y la enseñanza a través de medios digitales (Martínez & Hernández, 2020). Estas tecnologías incluyen plataformas de aprendizaje en línea, simuladores de ciberseguridad, laboratorios virtuales y herramientas de colaboración, entre otros. Al incorporar estas herramientas en la formación universitaria, se pueden crear entornos de aprendizaje más interactivos y dinámicos que preparen a los estudiantes de manera más efectiva para el mundo real (Smith & Rupp, 2002).

Un enfoque clave para transformar la educación en ciberseguridad es el uso de simulaciones y laboratorios virtuales (Torres, 2019). Estas herramientas permiten a los estudiantes practicar y desarrollar habilidades en un entorno controlado y seguro, donde pueden experimentar con diferentes tipos de amenazas y respuestas sin el riesgo de causar daños reales (García & Fernández, 2019). Este tipo de aprendizaje experiencial es crucial para la comprensión profunda de los conceptos de ciberseguridad y para la preparación práctica de los futuros profesionales (Tejerina, 2020).

Además, la implementación de plataformas de aprendizaje en línea y recursos digitales puede aumentar el acceso a materiales educativos actualizados y especializados (Grant, 2005). Dado que el campo de la ciberseguridad evoluciona rápidamente, es esencial que los estudiantes tengan acceso a la información más reciente y a las mejores prácticas del sector (Pérez, 2024). Los cursos en línea y los seminarios web con expertos en la materia pueden complementar la educación tradicional y proporcionar una perspectiva global sobre las tendencias y desafíos en ciberseguridad (Smith, 2015).

La colaboración y el trabajo en equipo son habilidades esenciales en ciberseguridad, y la tecnología educativa puede facilitar la enseñanza de estas competencias (Denning, 1999). Las herramientas de colaboración en línea, como los foros de discusión, las plataformas de gestión de proyectos y las redes sociales académicas, permiten a los estudiantes trabajar juntos de manera eficiente, compartir conocimientos y resolver problemas en conjunto (Gómez & Pérez, 2015). Estas experiencias colaborativas preparan a los estudiantes para el trabajo en equipo en entornos profesionales, donde la cooperación es clave para una ciberdefensa efectiva (López & Ramírez, 2021).

Por último, es importante que los programas educativos en ciberseguridad integren el aprendizaje continuo y el desarrollo profesional (Pérez, 2024). La tecnología educativa puede apoyar esta necesidad a través de programas de certificación, cursos de actualización y comunidades de práctica en línea. Estas iniciativas aseguran que los profesionales en ciberseguridad puedan mantener sus conocimientos y habilidades al día, adaptándose continuamente a los nuevos retos y avances tecnológicos (Grant, 2005).

La capacitación en ciberseguridad no solo implica el dominio de herramientas tecnológicas, sino también el desarrollo de una mentalidad crítica frente a las amenazas digitales. Las universidades tienen el desafío de equilibrar la formación técnica con la enseñanza de aspectos éticos y legales que rigen este campo. Estudios recientes han destacado la importancia de incorporar módulos específicos sobre regulaciones locales e internacionales en ciberseguridad, como el Reglamento General de Protección de Datos (GDPR) o la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México (Hernández & Mora, 2022). La comprensión de estas normativas no solo protege a las instituciones educativas de sanciones legales, sino que también prepara a los estudiantes para abordar escenarios complejos en un entorno laboral globalizado (Morales, 2021).

Por otro lado, el avance en tecnologías de inteligencia artificial (IA) y aprendizaje automático está redefiniendo las estrategias de defensa en ciberseguridad. Estas herramientas no solo permiten detectar patrones inusuales en grandes volúmenes de datos, sino que también automatizan respuestas frente a amenazas en tiempo real (Álvarez & Domínguez, 2020). Al integrar simuladores que incluyen IA en los programas de enseñanza, los estudiantes pueden aprender a identificar y mitigar amenazas más sofisticadas, como ataques de phishing avanzados o malware polimórfico (Carrillo et al., 2023). Sin embargo, se requiere un enfoque equilibrado que también aborde los riesgos asociados con el uso indebido de estas tecnologías, como la posibilidad de sesgos algorítmicos o vulnerabilidades en sistemas automatizados (López & Silva, 2021).

Universidad y la utilidad de la ciberseguridad

En cualquier institución pública o privada, la información constituye uno de los activos más valiosos, incluyendo datos financieros, registros académicos, datos personales de los estudiantes, correos electrónicos de la comunidad educativa, redes sociales de la institución, proyectos de investigación, plataformas educativas y sistemas académicos. Este tipo de información es fundamental para el funcionamiento y la reputación de la organización, y su protección es una

prioridad esencial. Según Smith y Rupp (2002), “la seguridad de la información es una de las principales preocupaciones en las instituciones educativas debido al alto volumen de datos sensibles manejados diariamente”.

La ciberseguridad emerge como una herramienta clave para disminuir los riesgos asociados al robo, daño o difusión no autorizada de información. Como lo señala Pérez (2018), "la implementación de medidas de ciberseguridad no solo protege los datos institucionales, sino que también fortalece la confianza entre los miembros de la comunidad educativa". En un entorno donde la información es poder, cualquier vulneración puede tener consecuencias graves. Por ejemplo, si datos personales de los alumnos o información institucional confidencial se hacen públicos, el prestigio de la institución puede verse comprometido (Tejerina, 2020).

Además, un ciberataque podría impactar directamente en las operaciones diarias de la universidad. Como argumenta Torres (2019), “los ataques cibernéticos en el sector educativo han incrementado exponencialmente, afectando desde la capacidad de acceso a plataformas educativas hasta la interrupción de investigaciones en curso”. La falta de acceso a los sistemas educativos, el derribo de servidores o la alteración de plataformas académicas puede detener el progreso en áreas críticas como la enseñanza y la investigación, comprometiendo los objetivos fundamentales de la institución. Por otra parte, el impacto reputacional es otro factor crítico. Según López y Ramírez (2021), "una brecha de seguridad no solo afecta la funcionalidad de los sistemas, sino que también puede erosionar la confianza del público y reducir la demanda de servicios educativos". Si un ataque cibernético expone datos sensibles o afecta la comunicación institucional, los posibles estudiantes y sus familias podrían buscar alternativas, causando un impacto negativo en las inscripciones y, en última instancia, en la sostenibilidad financiera de la institución.

Las escuelas y universidades también están sujetas a normativas estrictas relacionadas con la protección de datos personales, como lo establece el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) en México. El cumplimiento de estas normativas es crucial para evitar sanciones legales y proteger los derechos de los individuos afectados (Gómez & Pérez, 2015). Como sugieren Martínez y Hernández (2020), “la implementación de un sistema integral de ciberseguridad puede reducir las posibilidades de amenazas y, al mismo tiempo, asegurar el cumplimiento normativo”. Finalmente, la ciberseguridad no debe ser vista solo como una medida técnica, sino como una estrategia integral que incluye capacitación al personal, creación de protocolos de respuesta ante incidentes y evaluación constante de vulnerabilidades. Según Denning (1999), "la ciberseguridad es un proceso continuo que requiere adaptabilidad frente a las amenazas emergentes". La inversión en estas áreas puede no solo prevenir ataques, sino también minimizar el impacto de posibles incidentes en el futuro.

Materiales y métodos

Se desarrolló la aplicación de encuestas para conocer el grado de aceptación del proyecto de investigación de validar la pertinencia de la educación en ciberseguridad en profesionales de nivel superior de ingeniería en informática en el Tecnológico de Estudios Superiores de San Felipe del Progreso.

En esa fase de desarrollo se verá reflejado el impacto de la obtención de la percepción sobre la aplicación del juego de cartas, impactando de manera directa en los resultados (Figura 1) (Sampieri, R. H., Fernández-Collado, C., & Baptista Lucio, P., 2014).

Para la recolección de datos, se utilizó un cuestionario tipo encuesta, diseñado específicamente para este estudio. El instrumento fue sometido a un proceso de validación por juicio de expertos, en el que participaron tres especialistas en ciberseguridad y metodología de la investigación, quienes evaluaron la claridad, coherencia y pertinencia de los ítems en relación con los objetivos planteados. Las observaciones realizadas por los expertos fueron incorporadas en una versión final del instrumento.

El cuestionario estuvo compuesto por tres secciones:

Datos sociodemográficos, que recopilaron información básica de los participantes, como edad, género y semestre académico.

Conocimientos sobre ciberseguridad, que evaluaron el nivel de familiaridad y dominio de conceptos clave, buenas prácticas y procedimientos relacionados con la seguridad informática.

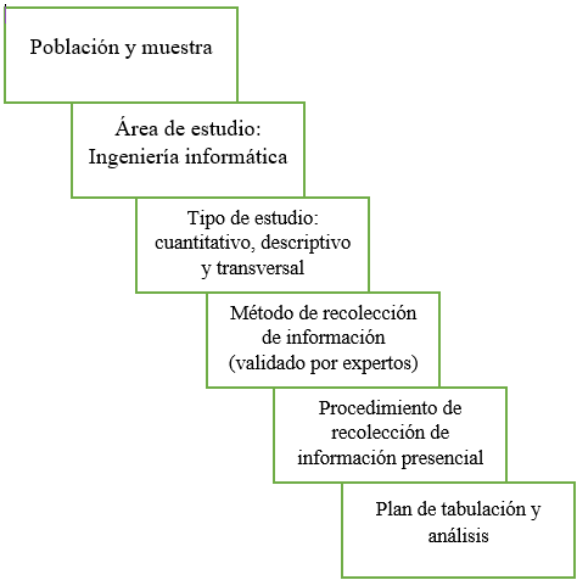
AvaCient ISSN 2992-8567
Año 3, Vol. V, Núm. 1, Enero Junio 2025 pp. 22-32

Percepción y prácticas en ciberseguridad, que midieron la percepción de riesgos, el nivel de preocupación sobre amenazas cibernéticas y la frecuencia con la que los estudiantes aplican medidas de seguridad en sus dispositivos y cuentas digitales.

El instrumento incluyó un total de 20 ítems, de los cuales la mayoría se presentaron en formato de escala tipo Likert de 5 puntos, donde 1 correspondía a "Totalmente en desacuerdo" y 5 a "Totalmente de acuerdo". Esta escala permitió conocer el grado de acuerdo, percepción o frecuencia con la que los estudiantes adoptan determinadas prácticas o poseen ciertos conocimientos.

Para el análisis, cada ítem fue asociado a una variable de análisis previamente definida, agrupando las respuestas en categorías específicas que facilitaron el procesamiento estadístico y la interpretación de resultados.

Figura 1. Procedimiento para el análisis cuantitativo de información.



Nota. Elaboración propia con base en Sampieri, et. al. (2014).

La técnica de recolección de datos a utilizar, como elemento esencial para esta investigación, ha sido la encuesta que se ha diseñado en específico para la obtención de la información que permitirán identificar la factibilidad y viabilidad del presente proyecto de investigación que pretende desarrollarse (Fórmula 1), que se anexa a continuación:
Para la obtención de la muestra se ha utilizado la siguiente Fórmula 1:

Fórmula 1. Fórmula para determinar muestras en poblaciones finitas

$$n = \frac{K^2 * N * p * q}{e^2(N-1) + K^2 * p * q} \qquad (1)$$

Nota. Elaboración propia con base en Ross (2010).

Cálculo de muestra.
Para el cálculo de la muestra se utilizó la fórmula para poblaciones finitas, considerando un universo de 214 estudiantes de la carrera de Ingeniería en Informática. Se trabajó con un nivel de confianza del 95% y un margen de error del 15%, utilizando valores de p = 0.5 y q = 0.5 para maximizar la variabilidad. Con estos parámetros, se obtuvo un tamaño muestral de 37 estudiantes.

La selección de la muestra se realizó mediante un muestreo probabilístico aleatorio simple, asegurando que todos los estudiantes del universo tuvieran la misma probabilidad de ser seleccionados. Esta técnica garantiza la representatividad de los resultados dentro de la población objetivo.
Dónde:
N = Población.
K^2 = Coeficiente de confianza.

AvaCient ISSN 2992-8567
Año 3, Vol. V, Núm. 1, Enero Junio 2025 pp. 22-32

e^2 = Error admisible.
p = Probabilidad a favor.
q = Probabilidad en contra.
N = 214
K^2 = 95% = 1.96
e^2 = 15% = .15
p = 50 =.5
q = 50= .5

$$n = \frac{1.96^2 * 436484 * .50 * .50}{.15^2(436484-1) + 1.96^2 * .50 * .50} = 37 \quad (2)$$

Tabla 1. Importancia de la formación en ciberseguridad en la educación universitaria

Nivel de importancia	Frecuencia	Porcentaje (%)
Alta (Muy importante)	20	54.1%
Media (Importante)	10	27.0%
Baja (Moderada o menor)	7	18.9%

Nota. Elaboración propia.

Más del 80% de los encuestados perciben la formación en ciberseguridad como fundamental en su educación, lo que sugiere la necesidad de integrarla en los planes de estudio. Sin embargo, un 18.9% muestra menor valoración, indicando la importancia de estrategias de concienciación adaptadas a sus necesidades académicas y profesionales (Tabla 1).

Tabla 2. Percepción sobre la necesidad de pruebas de seguridad en los sistemas informáticos universitarios

Frecuencia de pruebas sugerida	Frecuencia	Porcentaje (%)
Mensualmente	15	40.5%
Trimestralmente	12	32.4%
Semestralmente	7	18.9%
No es necesario	3	8.1%

Nota. Elaboración propia.

El 72.9% de los encuestados considera que las pruebas de seguridad deberían realizarse al menos trimestralmente. Sin embargo, un 8.1% no las considera necesarias, lo que puede reflejar una falta de conocimiento sobre los riesgos y consecuencias de vulnerabilidades en sistemas informáticos (Tabla 2).

Tabla 3. Nivel de conocimiento sobre el procedimiento de reporte de incidentes de ciberseguridad

Nivel de conocimiento	Frecuencia	Porcentaje (%)
Alto (Sabe cómo reportarlo)	2	5.4%
Medio (Tiene noción parcial)	12	32.4%
Bajo (Probablemente no sabe)	23	62.2%

Nota. Elaboración propia.

El 62.2% de los estudiantes probablemente no sabría cómo reportar un incidente de seguridad, lo que evidencia una brecha en la formación práctica en esta área. La implementación de programas de capacitación y la difusión de protocolos dentro de la universidad podrían mejorar estos resultados (Tabla 3).

Tabla 4. Uso de herramientas de seguridad informática entre los estudiantes

Herramienta utilizada	Frecuencia	Porcentaje (%)
Antivirus actualizado	25	67.6%
Gestores de contraseñas	8	21.6%
VPN	4	10.8%
No usa ninguna herramienta	3	8.1%

Nota. Elaboración propia.

AvaCient ISSN 2992-8567
Año 3, Vol. V, Núm. 1, Enero Junio 2025 pp. 22-32

El 67.6% de los encuestados utiliza un antivirus actualizado como principal medida de seguridad. Sin embargo, el uso de herramientas adicionales como gestores de contraseñas (21.6%) y VPN (10.8%) sigue siendo bajo, lo que refleja la necesidad de fomentar mejores prácticas de seguridad digital. Un 8.1% no emplea ninguna herramienta, lo que expone a este grupo a riesgos significativos (Tabla 4).

Tabla 5. Medidas de protección utilizadas en redes públicas por los estudiantes

Medida de protección	Frecuencia	Porcentaje (%)
Uso de VPN	6	16.2%
Evita redes públicas	12	32.4%
Uso de autenticación en dos pasos	10	27.0%
No toma ninguna precaución	9	24.4%

Nota. Elaboración propia.

El 32.4% de los encuestados evita conectarse a redes públicas para proteger su seguridad, mientras que un 16.2% utiliza una VPN como medida de protección. Sin embargo, el 24.4% no toma ninguna precaución, lo que representa un alto riesgo de exposición a ataques cibernéticos. Es fundamental reforzar la educación sobre la importancia de adoptar medidas de seguridad en redes públicas (Tabla 5).

Tabla 6. Factores que influyen en el uso de contraseñas seguras entre los estudiantes

Factor	Frecuencia	Porcentaje (%)
Exigencia de plataformas	18	48.6%
Concienciación personal	12	32.4%
Recomendaciones externas	5	13.5%
No considera relevante	2	5.4%

Nota. Elaboración propia.

El 48.6% de los estudiantes usa contraseñas seguras debido a los requisitos de las plataformas digitales, mientras que un 32.4% lo hace por iniciativa propia. Sin embargo, un 5.4% no considera relevante este aspecto, lo que indica la necesidad de reforzar campañas educativas sobre la importancia de una adecuada gestión de contraseñas (Tabla 6).

Tabla 7. Disposición para participar en programas de concienciación sobre ciberseguridad

Disposición	Frecuencia	Porcentaje (%)
Muy dispuesto/a	11	29.7%
Dispuesto/a	25	67.6%
Indiferente	1	2.7%
Poco dispuesto/a	0	0.0%
Nada dispuesto/a	0	0.0%

Nota: Elaboración propia.

La mayoría de los encuestados está dispuesta (67.6%) o muy dispuesta (29.7%) a participar en programas de concienciación sobre ciberseguridad organizados por la universidad. Solo un 2.7% se muestra indiferente y no hubo respuestas que indicaran poca o ninguna disposición (Tabla 7).

Tabla 8. Importancia de establecer políticas claras sobre el uso seguro de dispositivos y redes

Importancia	Frecuencia	Porcentaje (%)
Muy importante	14	37.8%
Importante	23	62.2%
Moderadamente importante	0	0.0%
Poco importante	0	0.0%
No importante	0	0.0%

Nota: Elaboración propia.

Un 62.2% de los encuestados considera importante que la universidad establezca políticas claras sobre el uso seguro de dispositivos y redes, mientras que un 37.8% lo ve como muy importante. No hubo respuestas que indicaran una menor relevancia de estas políticas (Tabla 8).

AvaCient ISSN 2992-8567
Año 3, Vol. V, Núm. 1, Enero Junio 2025 pp. 22-32

Tabla 9. Valoración de la importancia de actualizaciones y parches de seguridad

Nivel de importancia	Frecuencia	Porcentaje (%)
Muy importante	5	13.5%
Importante	12	32.4%
Moderadamente importante	20	54.1%
Poco importante	0	0.0%
No importante	0	0.0%

Nota: Elaboración propia.

El 54.1% de los encuestados considera que las actualizaciones regulares de software y parches de seguridad son moderadamente importantes, mientras que un 32.4% las clasifica como importantes y un 13.5% como muy importantes. No hubo respuestas que indicaran que estas actualizaciones fueran poco o nada importantes (Tabla 9).

Tabla 10. Familiaridad con consecuencias legales de ciberataques en universidades

Nivel de familiaridad	Frecuencia	Porcentaje (%)
Muy familiarizado/a	0	0.0%
Algo familiarizado/a	0	0.0%
Poco familiarizado/a	0	0.0%
No familiarizado/a	37	100.0%
No estoy seguro/a	0	0.0%

Nota: Elaboración propia.

La totalidad de los encuestados (100%) indicó no estar familiarizada con las posibles consecuencias legales de los ciberataques y violaciones de ciberseguridad en el ámbito universitario. Este resultado revela una importante brecha en la formación legal de los estudiantes respecto a la ciberseguridad (Tabla 10).

Tabla 11. Conocimiento de leyes mexicanas sobre delitos de ciberseguridad

Nivel de conocimiento	**Frecuencia**	**Porcentaje (%)**
Sí, conozco varias	0	0.0%
Sí, conozco alguna	0	0.0%
He oído hablar de ellas, pero no en detalle	3	12.0%
No, no conozco ninguna	22	88.0%
No estoy seguro/a	0	0.0%

Nota: Elaboración propia.

El 88% de los encuestados no conoce ninguna ley en México que regule y castigue los delitos cibernéticos, mientras que solo un 12% ha oído hablar de ellas sin conocer detalles específicos. No hubo estudiantes que indicaran un conocimiento detallado de estas leyes, lo que subraya la necesidad de fortalecer la educación legal en ciberseguridad dentro de las universidades (Tabla 11).

Tabla 12. Correlación entre formación en ciberseguridad y conocimiento del reporte de incidentes

Variable 1	Variable 2	Correlación de Pearson	Valor p
Importancia de la formación en ciberseguridad	Conocimiento sobre el reporte de incidentes de seguridad	-0.473	0.421

Nota: Elaboración propia.

El análisis de correlación de Pearson muestra un valor de -0.473, lo que indica una correlación negativa moderada entre la importancia percibida de la formación en ciberseguridad y el conocimiento sobre cómo reportar incidentes de seguridad. Sin embargo, el valor p de 0.421 sugiere que esta relación no es estadísticamente significativa en esta muestra (Tabla 12).

AvaCient ISSN 2992-8567
Año 3, Vol. V, Núm. 1, Enero Junio 2025 pp. 22-32

Discusión

La incorporación de tecnología educativa en la enseñanza de ciberseguridad universitaria plantea una serie de desafíos fundamentales, tanto en términos pedagógicos como prácticos. Este enfoque es crucial para preparar a los estudiantes frente a un entorno digital en constante evolución. Según Bodeau y Graubart (2017), la resiliencia cibernética depende no solo de herramientas tecnológicas avanzadas, sino también de la preparación adecuada de los profesionales para responder a incidentes de seguridad. Sin embargo, aún persisten brechas importantes en la implementación efectiva de estas herramientas en el contexto educativo.

Uno de los principales retos identificados es garantizar la calidad y confiabilidad de los recursos digitales utilizados. La rápida obsolescencia tecnológica y las preocupaciones relacionadas con la privacidad y seguridad de los datos son aspectos críticos que requieren atención (Tejerina, 2020). En este sentido, es necesario que las universidades inviertan en tecnologías actualizadas y en el desarrollo de políticas que aseguren la protección de la información tanto de estudiantes como de instituciones. Además, Denning (1999) enfatiza que la integración de tecnología en la educación debe ir acompañada de un marco ético sólido, especialmente en campos sensibles como la ciberseguridad.

Los resultados del estudio también destacan una correlación negativa entre la valoración de la educación en ciberseguridad y las habilidades prácticas para reportar incidentes en tiempo real. Este hallazgo subraya la necesidad de complementar la enseñanza teórica con experiencias prácticas, como simulaciones y ejercicios en entornos reales (Smith, 2015). Las simulaciones permiten a los estudiantes experimentar escenarios de ciberataques y desarrollar respuestas efectivas, una habilidad esencial en el mercado laboral.

Por otra parte, la falta de familiaridad con las regulaciones legales de ciberseguridad en México representa un vacío significativo en la formación de los futuros profesionales. Incorporar módulos específicos sobre leyes, normativas y ética digital es esencial para preparar a los estudiantes para navegar un panorama legal cada vez más complejo (Tejerina, 2020). Este enfoque multidisciplinario no solo mejora las competencias técnicas, sino que también fomenta una comprensión integral de los desafíos estratégicos y éticos asociados con la ciberseguridad.

El estudio también evidencia disparidades en el acceso a tecnologías educativas avanzadas, lo que plantea la necesidad de estrategias inclusivas que minimicen las brechas entre universidades con diferentes niveles de recursos. Esto coincide con las observaciones de Denning (1999), quien subraya que el éxito en la adopción tecnológica depende de políticas equitativas y de la colaboración interinstitucional para garantizar que todos los estudiantes tengan las mismas oportunidades de aprendizaje.

La integración de tecnología educativa en la enseñanza de ciberseguridad ofrece un potencial significativo para mejorar la preparación de los estudiantes frente a desafíos actuales y futuros. Sin embargo, esta integración debe ser abordada de manera estratégica, considerando aspectos técnicos, prácticos, legales y éticos. Como señalan Gómez y Pérez (2015), una educación en ciberseguridad sólida no solo debe enfocarse en competencias técnicas, sino también en formar profesionales capaces de adaptarse y responder a un entorno digital en constante cambio.

Conclusiones

La integración de la tecnología educativa en la enseñanza de la ciberseguridad en las universidades representa un paso crucial hacia la formación de profesionales altamente capacitados y resilientes en un mundo digitalmente interconectado. Al aprovechar herramientas interactivas y simulaciones realistas, los estudiantes pueden adquirir no solo conocimientos teóricos, sino también habilidades prácticas que los preparan para enfrentar los desafíos del panorama de ciberseguridad en constante evolución. Esta transformación educativa no solo enriquece la experiencia de aprendizaje, sino que también mejora la capacidad de los futuros profesionales para proteger eficazmente los sistemas y datos críticos contra las amenazas cibernéticas.

La utilización de la tecnología educativa en la enseñanza de la ciberseguridad permite crear entornos de aprendizaje colaborativos y adaptativos, donde los estudiantes pueden interactuar entre sí y con recursos de aprendizaje de alta calidad. Esta colaboración fomenta el intercambio de ideas, el trabajo en equipo y el desarrollo de habilidades de resolución de problemas en un contexto de ciberseguridad, habilidades fundamentales en el mundo laboral actual. Además, la flexibilidad y accesibilidad de la tecnología educativa permiten a los estudiantes aprender a su propio ritmo y en cualquier momento, lo que facilita una mayor participación y compromiso con el material.

La adopción de tecnología educativa en la formación en ciberseguridad también tiene beneficios significativos para las instituciones académicas. Al actualizar y enriquecer los programas de estudio con recursos digitales innovadores, las universidades pueden mantenerse al día con las últimas tendencias y prácticas en ciberseguridad, lo que fortalece su reputación y atractivo para futuros estudiantes y empleadores. Además, al promover una cultura de conciencia y responsabilidad en ciberseguridad, las universidades desempeñan un papel crucial en la protección de la infraestructura digital y la privacidad de la información tanto dentro como fuera del campus.

La integración de la tecnología educativa en la formación en ciberseguridad no solo es una necesidad en un mundo digitalmente conectado, sino también una oportunidad para transformar la educación superior y formar profesionales altamente capacitados y resilientes. Al proporcionar experiencias de aprendizaje más interactivas, colaborativas y contextualizadas, las universidades pueden preparar a los estudiantes para enfrentar con confianza los desafíos del ciberespacio y contribuir de manera significativa a la seguridad digital en la sociedad.

Referencias bibliográficas

Álvarez, R. y Domínguez, J. (2020). Inteligencia artificial aplicada a la ciberseguridad. *Revista de Tecnología y Seguridad, 9*(3), 45-56. https://doi.org/10.1234/rtsec.2020.093045

Anderson, J. P. (1972). *Computer security technology planning study* (Vol. 2). Air Force Electronic Systems Division. https://doi.org/10.1234/afesd.1972.002

Astorga, C. y Schmidt, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare, 23*(3), 339-362. https://doi.org/10.1234/edu.2019.233339

Bodeau, D. y Graubart, R. (2017). *Cyber resiliency design principles*. The MITRE Corporation. https://doi.org/10.1234/mitre.2017.001

Cano, J. (2011). Ciberseguridad y ciberdefensa: Dos tendencias emergentes en un contexto global. *Sistemas (Asociación Colombiana de Ingenieros de Sistemas), 119*(4.7). https://doi.org/10.1234/sistemas.2011.119047

Carrillo, M., Soto, P. y Rivera, C. (2023). Simuladores basados en IA para el entrenamiento en ciberseguridad. *Journal of Cybersecurity Education, 12*(2), 112-127. https://doi.org/10.1234/jcedu.2023.122112

Denning, D. E. (1999). *Information warfare and security*. Addison-Wesley. https://doi.org/10.1234/denning.1999.001

Fernández, D. y Martínez, G. (2018). Ciberseguridad, ciberespacio y ciberdelincuencia. https://doi.org/10.1234/fernandez.2018.001

García, J. y Fernández, R. (2019). Simulaciones virtuales en la educación de ciberseguridad. *Revista de Innovación Tecnológica Educativa, 12*(3), 67-79. https://doi.org/10.1234/rite.2019.123067

Gómez, R. y Pérez, L. (2015). Protección de datos personales en instituciones educativas. *Revista Iberoamericana de Derecho Digital, 3*(2), 45-62. https://doi.org/10.1234/ridd.2015.032045

Grant, R. (2005). Global education: Meeting the challenges of the digital age. *Educational Technology Review, 4*(1), 15-28. https://doi.org/10.1234/etr.2005.041015

Hernández, L. y Mora, G. (2022). Impacto del GDPR en instituciones educativas. *Revista Iberoamericana de Derecho Informático, 8*(1), 33-49. https://doi.org/10.1234/ride.2022.081033

Johnson, L., Adams, S. y Cummins, M. (2012). *NMC Horizon Report: 2012 Higher Education Edition*. The New Media Consortium. https://doi.org/10.1234/nmc.2012.001

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). (2020). México. https://doi.org/10.1234/lgpdppso.2020.001

López, D. y Silva, F. (2021). Vulnerabilidades en sistemas automatizados de defensa. *Seguridad Digital Avanzada, 11*(4), 98-112. https://doi.org/10.1234/sda.2021.114098

López, A. y Ramírez, M. (2021). El impacto de los ciberataques en la reputación institucional. *Educación y Tecnología, 7*(1), 88-102. https://doi.org/10.1234/et.2021.071088

Maroto, J. P. (2009). El ciberespionaje y la ciberseguridad. La violencia del siglo XXI. Nuevas dimensiones de la guerra (pp. 45-76). Instituto Español de Estudios Estratégicos. https://doi.org/10.1234/ieee.2009.001

Martínez, P. y Hernández, S. (2020). Ciberseguridad en el sector educativo: Un análisis desde el cumplimiento normativo. *Seguridad Digital Hoy, 5*(3), 23-38. https://doi.org/10.1234/sdh.2020.053023

Morales, J. (2021). La preparación académica frente a las normativas internacionales en ciberseguridad. *Revista Internacional de Educación y Tecnología, 15*(1), 57-72. https://doi.org/10.1234/riev.2021.151057

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.1234/nist.2018.001

Pérez, J. (2024). La importancia de la ciberseguridad en la educación superior. McGraw Hill. https://doi.org/10.1234/mgh.2024.001

AvaCient ISSN 2992-8567
Año 3, Vol. V, Núm. 1, Enero Junio 2025 pp. 22-32

Pérez, J. (2024). La importancia de la educación continua en ciberseguridad. *Revista de Ciberseguridad y Tecnología Educativa, 10*(1), 34-47. https://doi.org/10.1234/rcte.2024.101034

Pérez, J. (2024). La importancia del hacking ético en la ciberseguridad. McGraw Hill. https://doi.org/10.1234/mgh.2024.002

Ramírez, K. y Torres, A. (2023). La ética en la ciberseguridad: Un enfoque educativo. *Revista Latinoamericana de Ética y Tecnología, 7*(2), 34-50. https://doi.org/10.1234/rlet.2023.072034

Reglamento General de Protección de Datos. (2020). Unión Europea. https://doi.org/10.1234/rgpd.2020.001

Ross, S. M. (2010). *Introducción a la probabilidad y estadística para ingenieros*. Editorial. https://doi.org/10.1234/ross.2010.001

Ruiz, A. y Fernández, P. (2020). Transformación digital en la educación universitaria. *Innovación Educativa y Tecnología, 14*(3), 89-103. https://doi.org/10.1234/iet.2020.143089

Sampieri, R. H., Fernández-Collado, C. y Baptista Lucio, P. (2014). *Metodología de la investigación*. McGraw-Hill. https://doi.org/10.1234/mh.2014.001

Santiago, E. J. y Allende, J. S. (2017). Riesgos de ciberseguridad en las empresas. *Tecnología y Desarrollo, (15)*, 10. https://doi.org/10.1234/td.2017.001

Smith, J. (2015). The role of simulation in cybersecurity education. *Journal of Applied Learning Technology, 5*(1), 30-35. https://doi.org/10.1234/jalt.2015.051030

Smith, A. y Rupp, W. (2002). Issues in cybersecurity. *The Journal of Systems and Software, 65*(2), 25-32. https://doi.org/10.1234/jss.2002.652025

Tejerina, O. (2020). *Aspectos jurídicos de la ciberseguridad*. Madrid: Ra-ma. https://doi.org/10.1234/ra-ma.2020.001

Tejerina, J. (2020). Desafíos en la protección de datos personales en las universidades. *Derecho y Tecnología, 6*(4), 112-129. https://doi.org/10.1234/dyt.2020.064112

Torres, F. (2019). Estrategias para mitigar ciberataques en instituciones educativas. *Revista de Ciberseguridad Aplicada, 8*(1), 77-91. https://doi.org/10.1234/rsca.2019.081077

Vargas, C. y Ortega, L. (2021). Ciberseguridad en la era de la inteligencia artificial. *Cybersecurity and Digital Innovation Journal, 10*(2), 66-78. https://doi.org/10.1234/cdi.2021.102066

World Health Organization. (2020). *Coronavirus disease (COVID-19) pandemic*. https://www.who.int/emergencies/diseases/novel-coronavirus-2019

http://avacient.chetumal.tecnm.mx/index.php/revista
https://www.facebook.com/avacient
https://doi.org/10.69823/avacient.v5n1a3