Revista Científica DISCIPLINARES (2024). Vol. 3 (3)
ISSN: 2955-8905 (En línea)
https://iisunsa.com/index.php/Inicio/issue/archive

REVISIÓN SISTEMÁTICA

Revisión Sistemática de Modelos Educativos para la Capacitación en Buenas Prácticas de Ciberseguridad en Estudiantes y Empleados

Systematic Review of Educational Models for Training in Cybersecurity Best Practices for Students and Employees

Franco Andreé Julio Castillo Vera*

Unidad De Posgrado De La Facultad De Ingeniería De Producción Y Servicios

https://orcid.org/0009-0001-8921-6937

Wilder Francisco Castro Apaza

Unidad De Posgrado De La Facultad De Ingeniería De Producción Y Servicios

https://orcid.org/0009-0001-1689-3750

Lendy Shirley Pacho Quispe

Unidad De Posgrado De La Facultad De Ingeniería De Producción Y Servicios

https://orcid.org/0009-0002-4210-3086

Edwar Andres Velarde Allazo

Unidad De Posgrado De La Facultad De Ingeniería De Producción Y Servicios

https://orcid.org/0000-0002-6639-7632

Recibido: 16/12/2024
Revisado: 20/12/2024
Aceptado: 30/12/2024
Publicado: 31/12/2024

Correspondencia: *

Correo electrónico: fcastillove@unsa.edu.pe.

Resumen

El objetivo de esta Revisión Sistemática de Literatura (RSL) fue analizar modelos educativos efectivos para la capacitación en buenas prácticas de ciberseguridad en estudiantes y empleados, identificando enfoques que mejoren el conocimiento y las conductas relacionadas con la ciberseguridad.

Siguiendo las pautas PRISMA, se realizó una búsqueda sistemática en bases de datos como Scopus y ScienceDirect con términos clave relacionados con educación en ciberseguridad. Se seleccionaron 20 estudios tras aplicar criterios de inclusión y exclusión basados en el marco PICO, abarcando métodos de enseñanza, tecnologías utilizadas y los impactos de los programas formativos.

Los hallazgos destacan que métodos como la gamificación, simulaciones y aprendizaje basado en problemas son los más efectivos, ya que aumentan el compromiso de los usuarios y su capacidad para responder a ciber amenazas. Modelos educativos que integran personalización y tecnologías interactivas, como herramientas digitales y plataformas de aprendizaje, también mostraron mejoras significativas en las prácticas de ciberseguridad. En contraste, las campañas tradicionales de concienciación resultaron insuficientes para lograr cambios sostenibles.

Un modelo educativo integral que combine estrategias innovadoras y enfoques personalizados es clave para promover una cultura de ciberseguridad robusta. La integración de gamificación, simulaciones prácticas y evaluación continua contribuye a la mejora de la seguridad digital. Se sugiere realizar investigaciones futuras para validar estos enfoques en distintos contextos y medir su impacto a largo plazo en la reducción de vulnerabilidades.

Palabras clave: diseño educativo, marco instruccional, modelo de enseñanza, educación en ciberseguridad.

Abstract

The aim of this Systematic Literature Review (SLR) was to analyze the design of effective educational models for training in cybersecurity best practices among students and employees, in order to identify approaches that enhance knowledge and behaviors related to cybersecurity.

The PRISMA guidelines were followed for the collection and analysis of relevant studies. A systematic search was conducted in databases such as Scopus and ScienceDirect, using key

terms related to cybersecurity education. The selected articles were evaluated according to inclusion and exclusion criteria defined within the PICO framework. Ultimately, 20 studies were included, covering teaching methods, technologies used, and the impacts of training programs.

The review findings indicate that the most effective methods include gamification, simulations, and problem-based learning. These approaches enhance user engagement and improve the ability to identify and respond to cyber threats. Additionally, educational models integrating personalization and interactive technologies, such as digital tools and learning platforms, showed a positive impact on improving cybersecurity practices. However, traditional awareness campaigns are insufficient to generate sustainable changes.

Designing a comprehensive educational model that combines innovative strategies and personalized approaches is essential to fostering a strong cybersecurity culture. Integrating methods such as gamification and hands-on simulations, along with continuous assessment, contributes to improving digital security. Future research is recommended to validate these approaches in different contexts and measure their long-term impact on reducing vulnerabilities.

Key words: educational design, instructional framework, teaching model, cybersecurity education.

Introducción

La ciberseguridad se ha convertido en un desafío crítico para organizaciones de todos los tamaños, desde grandes corporaciones hasta pequeñas empresas e instituciones educativas. Los ciberataques, cada vez más sofisticados y frecuentes, explotan tanto las vulnerabilidades humanas como tecnológicas, generando pérdidas económicas significativas y daños reputacionales. Aunque las medidas técnicas de seguridad son fundamentales, la formación de los usuarios finales se reconoce como un aspecto clave para fortalecer la defensa cibernética de las organizaciones y minimizar los riesgos asociados a las ciberamenazas.

Estudios recientes han destacado que las campañas de concienciación tradicionales, basadas únicamente en la transmisión de información, no son suficientes para generar cambios de comportamiento duraderos. Los usuarios, a menudo, carecen de las habilidades y conocimientos necesarios para identificar y responder a las amenazas cibernéticas de manera efectiva. Ante esta situación, el desarrollo de modelos educativos personalizados y prácticos se presenta como una solución prometedora. A través de metodologías activas, como

simulaciones, juegos de rol y aprendizaje basado en problemas, estos modelos buscan equipar a los usuarios con competencias prácticas y conocimientos aplicables en situaciones reales,(Zhang-Kennedy & Chiasson, 2021).

Diversos enfoques han demostrado su efectividad al integrar tecnologías digitales y considerar las características específicas de diferentes perfiles de usuarios, como estudiantes y empleados. Por ejemplo, un marco conceptual propuesto para el ámbito académico resalta la importancia de combinar teorías de aprendizaje con prácticas interactivas para fomentar una cultura de ciberseguridad sostenible(Ayyash et al., 2024). De igual manera, revisiones sobre los métodos actuales de formación identifican la necesidad de vincular programas teóricos con simulaciones prácticas, tales como ejercicios de phishing, que refuercen el aprendizaje mediante experiencias tangibles (Bognár & Bottyán, 2024).(Khader et al., 2021)

Por otra parte, investigaciones como (Salau2 & Eshetu1, n.d.) subrayan la relevancia de factores culturales y sociales en la formación de actitudes hacia la ciberseguridad, mientras que otras como (Marshall et al., 2024) exploran cómo las dinámicas de confianza interpersonal influyen en la capacidad de los usuarios para adoptar prácticas seguras. En el ámbito laboral, se reconoce que un enfoque personalizado en la capacitación, alineado con los desafíos específicos de cada organización, es esencial para la sostenibilidad de las prácticas seguras a largo plazo.(Köhler & Meinel, 2024)

El presente trabajo propone una Revisión Sistemática de Literatura (RSL) para explorar el diseño de un modelo educativo que aborde las limitaciones de los enfoques tradicionales y fomente una cultura de ciberseguridad proactiva. Este modelo se centrará en:

El desarrollo de habilidades prácticas en ciberseguridad.

La personalización del aprendizaje para diferentes perfiles de usuarios.

La evaluación continua para medir el impacto y la eficacia de las intervenciones.

Preguntas de investigación

¿En qué medida el diseño de un modelo educativo mejora el aprendizaje de conceptos de ciberseguridad y reduce la vulnerabilidad frente a ciberamenazas?

¿Qué impacto tiene el desarrollo de un modelo educativo en el conocimiento de conceptos y buenas prácticas de ciberseguridad en estudiantes y empleados?

¿Cómo contribuye la implementación de un programa de capacitación en ciberseguridad a la reducción de ciberataques en usuarios de tecnología?

¿Qué estrategias educativas son más efectivas para mejorar la concienciación y la práctica segura en el uso de tecnología?

Objetivos del estudio

Esta revisión busca proporcionar una descripción integral sobre el panorama de la ciberseguridad en organizaciones e instituciones educativas, explorando las brechas existentes en el conocimiento y las prácticas actuales. Al integrar las evidencias más recientes (Alotibi, 2024; Elste & Croasdell, 2023; Fadli et al., 2024; Hijji & Alam, 2022), este trabajo contribuirá al desarrollo de un modelo educativo innovador que garantice la aplicación de buenas prácticas de ciberseguridad en la vida cotidiana de los usuarios. Además, se espera que las conclusiones de esta revisión sirvan como base para que instituciones educativas y empresas diseñen programas de capacitación más efectivos, fomentando la protección de información sensible y la confianza en el uso de tecnologías digitales.

Metodología

Para facilitar la transparencia y la integridad, se siguieron las pautas de Elementos de informes preferidos para revisiones sistemáticas y metaanálisis (PRISMA) para la presentación de informes de revisiones sistemáticas. Las directrices PRISMA proporcionan listas de verificación y protocolos para ayudar tanto en la preparación como en la facilitación de revisiones sistemáticas. Los elementos de una revisión sistemática que se deben considerar de acuerdo con las pautas PRISMA descritas en la nuestro grafico PRISMA incluyen elementos relevantes tanto para revisiones sistemáticas.

A. Criterios de Elegibilidad

Como se describió anteriormente, seguimos las pautas PRISMA para definir criterios de elegibilidad claros utilizando el marco PICO, que ayudó a proporcionar una estructura sistemática para la inclusión y criterios de exclusión. Este enfoque aseguró que el proceso de selección fuera riguroso y consistente, centrándose en estudios relevantes.

El marco PICO tiene cuatro componentes.

1. Población o Problema(P)

Personas con falta de conocimiento en buenas prácticas de ciberseguridad, como trabajadores, estudiantes o usuarios en tecnología en actividades diarias.

2. Intervención(I)

Diseño de un modelo educativo enfocado en el aprendizaje de conceptos y buenas prácticas de ciberseguridad.

3. Comparación(C)

En la investigación no se desarrolla una comparación explícita en el diseño de la investigación, puesto que la intervención busca evaluar el impacto directo del modelo educativo propuesto, sin contrastarlo con otros enfoques.

4. Resultado(o)

Incremento en el aprendizaje de conceptos de ciberseguridad y reducción de vulnerabilidades y prácticas inseguras, mitigación de riesgos de ciberataques.

Tabla 1.

Marco PICO - Inclusión y Exclusión

Criterio	*Inclusión*	*Exclusión*
Población	Estudios que incluyan estudiantes de nivel universitario o empleados de organizaciones públicas o privadas. Participantes con niveles básicos o intermedios de conocimiento en ciberseguridad.	Estudios enfocados exclusivamente en poblaciones altamente especializadas en ciberseguridad (por ejemplo, expertos o técnicos certificados). Investigaciones en estudiantes o empleados menores de edad sin relación con entornos educativos formales.
Intervención	Programas o modelos educativos enfocados en la capacitación en buenas prácticas de ciberseguridad. Intervenciones que utilicen métodos innovadores, como aprendizaje en línea, simulaciones, o aprendizaje activo.	Programas de capacitación que no estén relacionados con buenas prácticas de ciberseguridad (por ejemplo, formación en programación o gestión de TI sin relación con ciberseguridad). Estudios que no detallen claramente la intervención educativa utilizada.

Comparación	-	-
Resultado	Publicaciones que midan resultados como aumento en el conocimiento de ciberseguridad, mejora en prácticas seguras, o cambios en comportamiento frente a riesgos cibernéticos.	Publicaciones que no presenten resultados medibles o comparativos sobre el conocimiento o comportamiento en ciberseguridad. Estudios con resultados cualitativos no suficientemente detallados o aplicables.

Nota . Esta tabla muestra los criterios de inclusión y exclusión utilizados en el marco PICO.

B. Fuentes de información y estrategia de búsqueda

En diciembre de 2024 se realizó una búsqueda sistema tica de títulos y resúmenes utilizando Scopus y Science Direct, donde los términos de búsqueda utilizados fueron:

1) SCOPUS: educational design, instructional framework. teaching model education,

cybersecurity, cybersecurity education, digital security training, information security learning, knowledge improvement, cybersecurity awareness.

2) SCIENCE DIRECT: cybersecurity education, cybersecurity training, awareness, teaching methods, training programs.

En la siguiente Tabla podemos apreciar las fórmulas de búsqueda en nuestras bases de datos consultadas.

Tabla 2.

Fórmulas de Búsqueda y Resultados

Base de datos	Formula de Búsqueda	Resultados
Scopus	(TITLE-ABS-KEY ("educational design" OR "instructional framework" OR "teaching model" OR "education") AND TITLE-ABS-KEY ("cybersecurity" OR "cybersecurity education" OR "digital security training" OR "information security learning") AND TITLE-ABS-KEY ("employees" OR "students" OR "users" OR "workforce") AND TITLE-ABS-KEY ("learning outcomes" OR "knowledge improvement" OR "cybersecurity	53

	awareness")) AND PUBYEAR > 2019 AND PUBYEAR < 2025 AND (LIMIT-TO (OA , "all")) AND (LIMIT-TO (LANGUAGE , "English"))	
Science Direct	("cybersecurity education" OR "cybersecurity training") AND (students OR workers) AND ("skills" OR "awareness") AND ("teaching methods" OR "training programs")	41

C. **Proceso de recolección de data**

El proceso de recolección de datos incluye una serie de pasos claves para enfocarse en modelos de educación en ciberseguridad.

i. Selección de estudios y extracción de datos

La eliminación mediante los filtros que fueron obtener artículos de libre acceso y con una antigüedad no mayor a 5 años redujo el número de artículos de 257 a 94. Se redujo a 51 después de la revisión del título y el resumen.

Posteriormente se realizó una revisión de texto completo de los artículos utilizando los criterios de inclusión y exclusión descritos anteriormente, lo cual resulto en la inclusión de 20 artículos en la revisión.

En la Figura 3 Prisma se presenta una descripción general completa del procedimiento de selección de artículos.

Figura 1.

Publicaciones por año

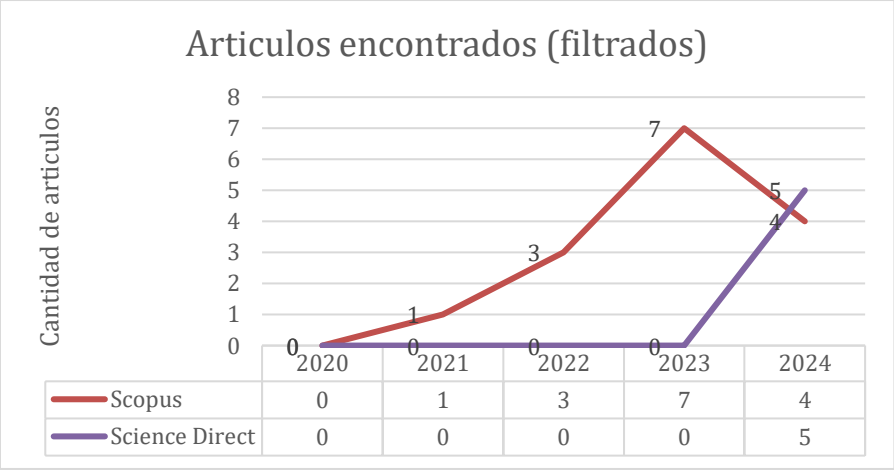


Figura 2.

Porcentaje de artículos por base de datos

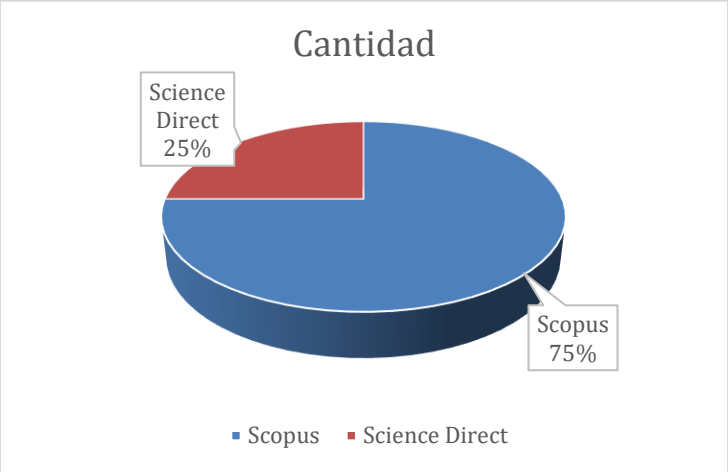
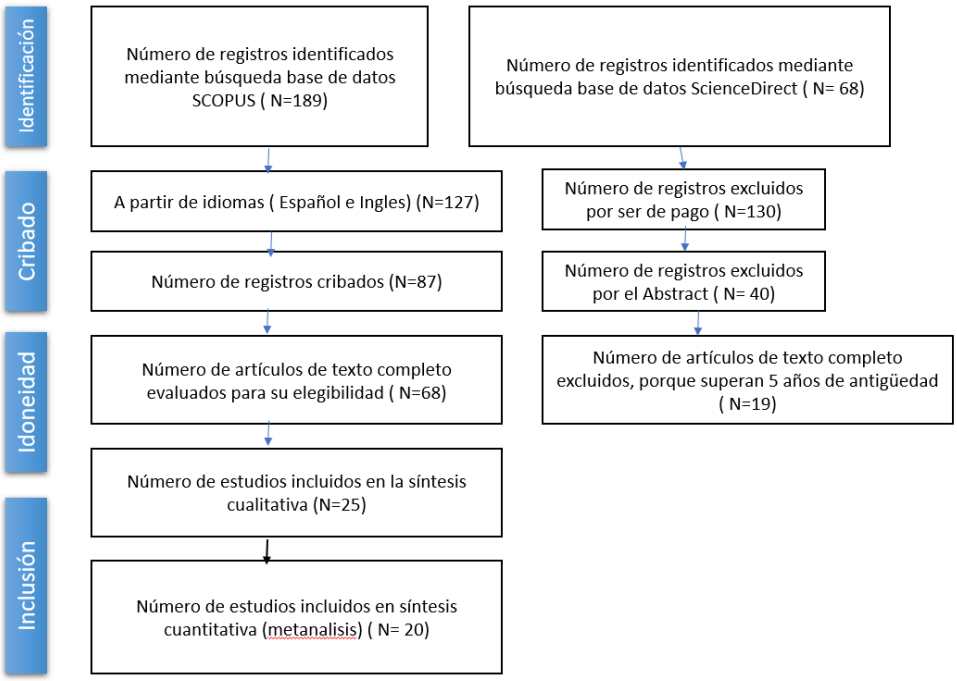


Figura 3.

PRISMA



Resultado

La presente Revisión Sistemática de Literatura (RSL) analiza las contribuciones recientes en el ámbito de la ciberseguridad educativa, centradas en el diseño de modelos efectivos para la capacitación en buenas prácticas de ciberseguridad dirigidos a estudiantes y empleados. Los

estudios revisados proporcionan información valiosa sobre métodos, marcos conceptuales y enfoques prácticos que abordan las principales brechas en el conocimiento y las vulnerabilidades humanas frente a ciber amenazas.

Diseño de Modelos Educativos en Ciberseguridad

Los hallazgos destacan que la falta de concienciación y educación en ciberseguridad es un factor crítico que aumenta la susceptibilidad a ciberataques, tanto en el ámbito educativo como laboral. Los modelos educativos propuestos integran estrategias como simulaciones, gamificación y enfoques basados en problemas para mejorar las competencias prácticas y promover cambios de comportamiento sostenibles en los usuarios. Por ejemplo, un marco conceptual diseñado específicamente para instituciones académicas (CAFA) propone la incorporación de módulos interactivos de ciberseguridad en los planes de estudio, empleando herramientas digitales como Moodle y Kahoot para maximizar la retención del conocimiento(Chaudhary, 2024).

La efectividad de estos modelos radica en la personalización del aprendizaje, adaptando las estrategias educativas a las necesidades y características específicas de los participantes. Los métodos gamificados y las simulaciones no solo aumentan el compromiso de los usuarios, sino que también mejoran la capacidad para identificar amenazas como el phishing y mitigar riesgos en entornos laborales y educativos (Herath et al., 2022; Taherdoost, 2024).

Cambios de Comportamiento y Factores Humanos

La implementación de programas de capacitación que fomenten cambios conductuales positivos es esencial para garantizar la adopción de buenas prácticas en ciberseguridad. Los estudios revisados identifican que el apoyo de la alta dirección, el establecimiento de normas sociales y el uso de incentivos desempeñan un papel crucial en la creación de una cultura de seguridad sostenible. Sin embargo, estas intervenciones requieren ser reforzadas continuamente para adaptarse a las amenazas emergentes y mantener su efectividad a largo plazo.

Un aspecto relevante es la incorporación de elementos psicológicos en el diseño de los programas educativos. Por ejemplo, la investigación sobre el factor humano en phishing resalta cómo las vulnerabilidades cognitivas, como la autoridad y la escasez, pueden ser abordadas mediante simulaciones y ejercicios prácticos que reflejen escenarios reales. Estos enfoques permiten a los usuarios reconocer patrones de ataque y responder de manera efectiva,

reduciendo significativamente las tasas de éxito de los atacantes(Gallo et al., 2024; Saeed, 2023).

Brechas Identificadas y Desafíos

Pese a los avances en el diseño de modelos educativos, las investigaciones destacan varias limitaciones. Entre ellas, se encuentra la falta de validación empírica en contextos reales y la necesidad de evaluar el impacto de estas iniciativas a largo plazo. Además, muchos de los estudios revisados emplean muestras pequeñas, lo que limita la generalización de los resultados. Estas brechas subrayan la importancia de desarrollar métricas estandarizadas para medir la efectividad de los programas y garantizar su aplicabilidad en diferentes sectores e industrias.

Asimismo, aunque los métodos tradicionales como la transmisión de información siguen siendo parte integral de los programas de capacitación, se requiere una mayor integración de tecnologías emergentes, como la inteligencia artificial y las simulaciones avanzadas, para personalizar aún más el aprendizaje y aumentar su impacto (Bailey et al., n.d.; Prümmer et al., 2024).

Propuesta Educativa para Estudiantes y Empleados

Con base en los hallazgos, se plantea el desarrollo de un modelo educativo que combine enfoques innovadores y probados, como la gamificación, el aprendizaje basado en problemas y las simulaciones prácticas. Este modelo debe:

- Integrarse en los currículos académicos y programas corporativos, garantizando que tanto estudiantes como empleados desarrollen competencias prácticas en ciberseguridad.

- Personalizarse según las necesidades del público objetivo, considerando factores como su nivel de conocimiento previo, contexto laboral o educativo, y características cognitivas.

- Incorporar tecnologías digitales interactivas para mejorar la experiencia de aprendizaje y aumentar la retención del conocimiento.

- Evaluarse continuamente mediante métricas claras que permitan medir tanto el cambio de comportamiento como la reducción de vulnerabilidades a largo plazo.

Los resultados de esta RSL evidencian que un enfoque educativo integral y adaptativo puede transformar la manera en que estudiantes y empleados enfrentan los desafíos de ciberseguridad. Al integrar prácticas innovadoras y considerar factores humanos, los programas de capacitación pueden fomentar una cultura de seguridad más sólida en organizaciones e instituciones educativas, reduciendo así la incidencia de ciberataques y fortaleciendo la confianza en el uso de tecnologías digitales.

Tabla 3.

Descripción de artículos

Nota. Dimensiones adaptadas del Inventario SISCO

Autor & Año	Tema	Metodología	Tipo de entrenamiento	Muestra	Recolección de datos	Año
(Zhang-Kennedy & Chiasson, 2021)	Ciberseguridad y educación	Ambiente Controlado	Gamificación /Practico	-	Cualitativa	2020
(Ayyash et al., 2024)	Ciberseguridad y educación	Texto	Encuestas	251	Cuantitativa	2024
(Bognár & Bottyán, 2024)	Ciberseguridad y educación	Texto	Cuestionario /Practico	638	Cuantitativa	2024
(Khader et al., 2021)	Ciberseguridad y educación	Ambiente Controlado	Practico / Teórico	-	Cualitativa	2021

Autor & Año	Tema	Metodología	Tipo de entrenamiento	Muestra	Recolección de datos	Año
(Salau2 & Eshetu1, n.d.)	Ciberseguridad y educación	Texto	Encuestas	-	Cuantitativas	2024
(Gallo et al., 2024)	Ciberseguridad y concienciación	Ambiente Controlado	Practico	500	Cuantitativo	2024
(Saeed, 2023)	Ciberseguridad y educación	Texto	Cuestionario	198	Cualitativo	2023
(Bailey et al., n.d.)	Ciberseguridad y educación	Ambiente Controlado / Texto	Encuesta / Cuestionario	25	Cualitativo	2023
(Marshall et al., 2024)	Ciberseguridad y concienciación	Texto	Capacitación	-	Cualitativo	2024
(Prümmer et al., 2024)	Ciberseguridad y educación	Texto	Capacitación	-	Cualitativo	2024

Autor & Año	Tema	Metodología	Tipo de entrenamiento	Muestra	Recolección de datos	Año
(Blažič & Blažič, 2022)	Ciberseguridad y educación	Texto / Ambiente Controlado	Encuestas / Juegos Serios	-	Cualitativo	2022
(Chaudhary, 2024)	Ciberseguridad y concienciación	Texto	Cuestionarios	39	Cuantitativo	2024
(Taherdoost, 2024)	Ciberseguridad y educación	Ambiente Controlado/ Texto	Juegos Serios	-	Cuantitativo / Cualitativo	2024
(Herath et al., 2022)	Ciberseguridad	Texto	Encuesta	-	Cualitativo	2022
(Hobbs, 2023)	Ciberseguridad y educación	Texto	Encuesta	3500	Cuantitativo	2023
(Elste & Croasdell, 2023)	Ciberseguridad y educación	Ambiente Controlado / Texto	Juegos Serios /	-	Cualitativo	2023
(Hijji & Alam, 2022)	Ciberseguridad y concienciación	Texto / Ambiente Controlado	Teoria / Practica	-	Cualitativo	2022

Autor & Año	Tema	Metodología	Tipo de entrenamiento	Muestra	Recolección de datos	Año
(Fadli et al., 2024)	Ciberseguridad y concienciación	Texto	Cuestionarios	180	Cuantitativo	2024
(Alotibi, 2024)	Ciberseguridad, educación y concienciación	Texto	Teoría	-	Cualitativo	2024
(Köhler & Meinel, 2024)	Ciberseguridad y Educación	Texto / Ambiente Controlado	Teoría / Multimedia / Juegos Serios	-	Cualitativo	2024

Discusión

En esta esta RSL se observó que la educación en ciberseguridad es un elemento clave para reducir los riesgos asociados al error humano que son provocados por los usuarios finales. Los artículos revisados muestran múltiples enfoques, desde marcos educativos estructurados hasta herramientas gamificadas y simulaciones interactivas. Por ejemplo, el modelo "Cybersecurity Awareness Framework for Academia (CAFA)" integra módulos de aprendizaje gamificado para abordar los riesgos en docentes y estudiantes universitarios (Khader et al., 2021). En la parte laboral, se observó que las capacitaciones basadas en simulaciones y gamificación logran cambios significativos en los comportamientos de los trabajadores (Prümmer et al., 2024; Taherdoost, 2024). Asimismo, enfoques como la gamificación y las simulaciones han demostrado ser más efectivas para mejorar la retención del aprendizaje y fomentar cambios duraderos en los usuarios (Chaudhary, 2024; Taherdoost, 2024). Herramientas multimedia como juegos digitales y comics han sido especialmente útiles para

estudiantes, mientras que los empleados responden mejor a simulaciones o capacitaciones interactivas (Zhang-Kennedy & Chiasson, 2021).

El contexto cultural y demográfico también tiene un impacto en la efectividad de los modelos educativos. Por ejemplo, el modelo saudí aborda las necesidades específicas de estudiantes en redes sociales, considerando características culturales y legales locales (Alotibi, 2024). Además, las diferencias en disciplinas académicas influyen: los estudiantes técnicos muestran mayor conciencia que los de ciencias sociales (Bognár & Bottyán, 2024). Sin embargo, solo algunos de los estudios revisados incluyen datos empíricos o evaluaciones a largo plazo, lo que limita el impacto real de las capacitaciones en ciberseguridad (Zhang-Kennedy & Chiasson, 2021).

Los hallazgos en la RSL demuestran que las iniciativas educativas reducen significativamente la susceptibilidad a amenazas como phishing y malware, siempre que sean diseñadas con un enfoque en teorías conductuales y motivacionales (Chaudhary, 2024; Gallo et al., 2024; Taherdoost, 2024). Los resultados de los artículos destacan, la importancia de desarrollar modelos educativos robustos que combinen enfoques gamificados, herramientas multimedia y marcos culturales adaptados tanto para estudiantes como para empleados. Integrar múltiples metodologías, como la gamificación y simulaciones, permite abordar una mayor diversidad de formas de aprendizaje (Khader et al., 2021; Zhang-Kennedy & Chiasson, 2021).

A pesar de los avances presentados en los artículos, se identifican algunas limitaciones. La mayoría de los estudios no miden la sostenibilidad de los cambios de comportamiento a largo plazo, lo que limita la comprensión de su impacto real(Zhang-Kennedy & Chiasson, 2021). Algunas iniciativas, como el modelo saudí, requieren ser modificados para ser aplicables en otros contextos culturales, mientras que herramientas tecnológicas avanzadas, como simulaciones, pueden no estar disponibles en entornos que tengan una brecha digital (Alotibi, 2024). Por otro lado, algunos estudios siguen utilizando métodos poco interactivos, como presentaciones y videos genéricos, que muestran menor impacto en el aprendizaje (Prümmer et al., 2024; Taherdoost, 2024).

Para futuras investigaciones, es crucial diseñar estudios que midan el impacto de las capacitaciones en comportamientos y conocimientos a lo largo plazo (Zhang-Kennedy & Chiasson, 2021). También se puede investigar cómo adaptar modelos educativos a diferentes culturas, disciplinas académicas y niveles educativos (Alotibi, 2024; Fadli et al., 2024). El impacto de tecnologías emergentes como la inteligencia artificial en programas interactivos y

personalizados es otra área prometedora (Zhang-Kennedy & Chiasson, 2021). Incorporar teorías conductuales, como la Teoría del Comportamiento Planeado, puede enriquecer el diseño de capacitaciones basadas en evidencia científica (Chaudhary, 2024; Taherdoost, 2024). Finalmente, desarrollar programas educativos accesibles y escalables para instituciones con recursos limitados, enfocándose en que sea sostenible y de bajo costo(Alotibi, 2024; Khader et al., 2021).

Discusión

En esta revisión de la literatura nos permite responder de manera fundamentada a las preguntas clave relacionadas con el diseño e implementación de un modelo educativo en ciberseguridad. En primer lugar, la pregunta principal

¿En qué medida el diseño de un modelo educativo mejora el aprendizaje de conceptos de ciberseguridad y reduce la vulnerabilidad frente a ciberamenazas?

Un modelo educativo bien diseñado, que integre fundamentos teóricos sólidos y estrategias interactivas como juegos serios, realidad virtual y aprendizaje personalizado, puede mejorar significativamente la comprensión de conceptos clave de ciberseguridad. Esto, a su vez, contribuye a reducir la vulnerabilidad de los usuarios frente a ciberamenazas al promover comportamientos más seguros y una mayor capacidad de respuesta ante riesgos digitales.

¿Qué impacto tiene el desarrollo de un modelo educativo en el conocimiento de conceptos y buenas prácticas de ciberseguridad en estudiantes y empleados?

La implementación de modelos educativos en ciberseguridad tiene un impacto positivo en el conocimiento de conceptos y prácticas seguras, como lo demuestran los resultados de múltiples estudios revisados. Los participantes muestran mejoras en su nivel de conocimiento, actitudes hacia la seguridad y, en algunos casos, en la intención de adoptar prácticas más seguras. Estos cambios pueden ser más profundos cuando el modelo incorpora personalización y retroalimentación continua.

¿Cómo contribuye la implementación de un programa de capacitación en ciberseguridad a la reducción de ciberataques en usuarios de tecnología?

Los programas de capacitación pueden desempeñar un papel fundamental en la reducción de ciberataques al abordar factores humanos que suelen ser puntos débiles en la seguridad digital. La formación efectiva incrementa la conciencia de los usuarios sobre amenazas como el

phishing y las amenazas internas, disminuyendo su susceptibilidad a este tipo de ataques. Sin embargo, la evaluación a largo plazo de su impacto sobre la incidencia de ciberataques es un área que requiere más atención en la investigación futura.

¿Qué estrategias educativas son más efectivas para mejorar la concienciación y la práctica segura en el uso de tecnología?

Las estrategias educativas más efectivas combinan métodos interactivos y adaptativos, como juegos serios, simulaciones en entornos virtuales y aprendizaje personalizado. Estas técnicas no solo aumentan el compromiso de los participantes, sino que también potencian la retención del conocimiento. Además, las campañas tradicionales, como carteles y boletines, deben considerarse complementarias y no sustitutivas de métodos más dinámicos.

En conclusión, el desarrollo de un modelo educativo integral para la capacitación en ciberseguridad, basado en la teoría del cambio de comportamiento y reforzado con métodos innovadores, puede tener un impacto significativo en la mejora del aprendizaje, la adopción de buenas prácticas y la reducción de vulnerabilidades ante ciber amenazas en estudiantes y empleados. Este enfoque representa una vía prometedora para fortalecer la seguridad digital en contextos educativos y laborales.

Referencias

Alotibi, G. (2024). A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks. Engineering, Technology and Applied Science Research, 14(2), 13787–13795. https://doi.org/10.48084/etasr.7123

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2024). Cybersecurity Education and Awareness Among Parents and Teachers: A Survey of Bahrain. IEEE Access, 12, 86596–86617. https://doi.org/10.1109/ACCESS.2024.3416045

Bailey, D., Kornegay, M., Partlow, L., Bowens, C., & Gareis, K. (n.d.). Utilizing Culturally Responsive Strategies to Inspire African Utilizing Culturally Responsive Strategies to Inspire African American Female Participation in Cybersecurity American Female Participation in Cybersecurity. http://docs.lib.purdue.edu/jpeer

Blažič, B. J., & Blažič, A. J. (2022). Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development

in Cybersecurity. Sustainability (Switzerland), 14(8). https://doi.org/10.3390/su14084763

Bognár, L., & Bottyán, L. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. Education Sciences, 14(6). https://doi.org/10.3390/educsci14060588

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. Computers and Security, 142. https://doi.org/10.1016/j.cose.2024.103858

Elste, J. R., & Croasdell, D. (2023). Cyber Teaching Hospitals: Developing Cyber Workforce Competence. International Conference on Information Systems Security and Privacy, 643–650. https://doi.org/10.5220/0011783800003405

Fadli, R., Surjono, H. D., Sari, R. C., Hidayah, Y., & Eliza, F. (2024). Assessing Cybersecurity Awareness Among Vocational Students in Office Administration. International Journal of Safety and Security Engineering, 14(4), 1115–1123. https://doi.org/10.18280/ijsse.140410

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. Computers and Security, 139. https://doi.org/10.1016/j.cose.2023.103671

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. In Journal of Cybersecurity and Privacy (Vol. 2, Issue 1, pp. 1–18). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/jcp2010001

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors, 22(22). https://doi.org/10.3390/s22228663

Hobbs, J. (2023). Cybersecurity awareness in higher education: a comparative analysis of faculty and staff. Issues in Information Systems, 24(1), 159–169. https://doi.org/10.48009/1_iis_2023_114

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information (Switzerland), 12(10). https://doi.org/10.3390/info12100417

Köhler, D., & Meinel, C. (2024). The Right Tool for the Job: Contextualization of Cybersecurity Education and Assessment Methods. International Conference on Information Systems Security and Privacy, 1, 234–241. https://doi.org/10.5220/0012457900003648

Marshall, N., Sturman, D., & Auton, J. C. (2024). Exploring the evidence for email phishing training: A scoping review. Computers and Security, 139. https://doi.org/10.1016/j.cose.2023.103695

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers and Security, 136. https://doi.org/10.1016/j.cose.2023.103585

Saeed, S. (2023). Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. Sustainability (Switzerland), 15(12). https://doi.org/10.3390/su15129426

Salau2, O., & Eshetu1, A. Y. (n.d.). Endris Abdu Mohammed1 y Ayodeji Acceso abierto INVESTIGACIÓN Reflejos Abstracto Revista de Big Data. https://doi.org/10.1186/s40537¬024¬00980¬z

Taherdoost, H. (2024). A Critical Review on Cybersecurity Awareness Frameworks and Training Models. Procedia Computer Science, 235, 1649–1663. https://doi.org/10.1016/j.procs.2024.04.156

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. In ACM Computing Surveys (Vol. 54, Issue 1). Association for Computing Machinery. https://doi.org/10.1145/3427920