Fecha de presentación: mayo, 2024, **Fecha de Aceptación**: junio, 2024, **Fecha de publicación**: septiembre, 2024

22

EVALUACIÓN DE LA EFECTIVIDAD DE PROGRAMAS EDUCATIVOS EN CIBERSEGURIDAD PARA REDUCIR EL FRAUDE DIGITAL ENTRE USUARIOS FINANCIEROS EN ECUADOR

EVALUATION OF THE EFFECTIVENESS OF EDUCATIONAL PROGRAMS IN CYBERSECURITY TO REDUCE DIGITAL FRAUD AMONG FINANCIAL USERS IN ECUADOR

Carlos Wilman Maldonado Gudiño[1*]
E-mail: ui.carlosmaldonado@uniandes.edu.ec
ORCID: https://orcid.org/0000-0001-8784-211X
Adrián Fernando Sánchez Puga [1]
E-mail: adriansp93@uniandes.edu.ec
ORCID: https://orcid.org/0009-0007-0170-7314
Alba Karina Vaca Morales [1]
E-mail: albavm31@uniandes.edu.ec
ORCID: https://orcid.org/0009-0004-9872-8290
Daniela Marilin Núñez Taboada [1]
E-mail: ca.danielamnt58@uniandes.edu.ec
ORCID: https://orcid.org/0009-0006-7373-1121
*Autor para correspondencia
[1] Universidad Autónoma Regional de Los Andes, Ibarra. Ecuador.

Cita sugerida (APA, séptima edición)

Maldonado Gudiño, C. W., Sánchez Puga, A. F., Vaca Morales, A. K., y Núñez Taboada, D. M. (Año). Evaluación de la efectividad de programas educativos en ciberseguridad para reducir el fraude digital entre usuarios financieros en Ecuador. ***Revista Conrado, 20***(100), 186-192.

RESUMEN

Este estudio tuvo como objetivo evaluar la efectividad de programas educativos en ciberseguridad para reducir la incidencia de fraude digital entre usuarios financieros en Ecuador. La investigación se centró en identificar las principales vulnerabilidades y áreas de desconocimiento entre los usuarios, y en desarrollar un programa educativo adaptado a sus necesidades. Se realizó una encuesta inicial a una muestra de 40 usuarios financieros ecuatorianos. A partir de los resultados, se diseñó y aplico un programa educativo mediante la utilización de tres métodos educativos diferentes: talleres presenciales y virtuales, cursos en línea autoguiados y campañas de sensibilización. Los resultados mostraron que los talleres presenciales y virtuales fueron los más efectivos, seguidos por los cursos en línea y las campañas de sensibilización. Los participantes mejoraron significativamente su conocimiento sobre ciberseguridad y adoptaron prácticas más seguras en línea. Las conclusiones destacaron la importancia de métodos educativos interactivos y personalizados para maximizar la efectividad en la educación en ciberseguridad. Este estudio subraya la necesidad de una educación continua y accesible para proteger a los usuarios contra las amenazas digitales emergentes en un entorno cada vez más conectado. Además, sugiere que una combinación de enfoques puede ser clave para mejorar las prácticas de seguridad digital y reducir el fraude entre los usuarios financieros.

Palabras clave:

Ciberseguridad, Educación Financiera, Fraude Digital, Vulnerabilidades, Seguridad en Línea.

ABSTRACT

This study aimed to evaluate the effectiveness of educational programs in cybersecurity to reduce the incidence of digital fraud among financial users in Ecuador. The research focused on identifying the main vulnerabilities and areas of lack of knowledge among users, and on developing an educational program adapted to their needs. An initial survey was carried out on a sample of 40 Ecuadorian financial users. Based on the results, an educational program was designed and implemented using three different educational methods: in-person and virtual workshops, self-guided online courses and awareness campaigns. The results showed that in-person and virtual workshops were the most effective, followed by self-guided online courses and awareness campaigns. Participants significantly improved their cybersecurity knowledge and adopted safer online practices. The findings highlighted the

importance of interactive and personalized educational methods to maximize effectiveness in cybersecurity education. This study highlights the need for continuous and accessible education to protect users against emerging digital threats in an increasingly connected environment. Furthermore, it suggests that a combination of approaches may be key to improving digital security practices and reducing fraud among financial users.

Keywords:

Cybersecurity, Financial Education, Digital Fraud, Vulnerabilities, Online Security

INTRODUCCIÓN

La inclusión financiera es un concepto multidimensional que abarca tanto la oferta como la demanda de productos y servicios financieros. Sus dimensiones incluyen el acceso, el uso, la calidad y el impacto sobre el bienestar financiero de las familias y las empresas. Según la Comisión Económica para América Latina y el Caribe (CEPAL), la inclusión financiera es un impulsor clave de siete de los diecisiete Objetivos de Desarrollo Sostenible: (ODS1) Fin de la pobreza, (ODS2) Hambre cero, (ODS3) Salud y bienestar, (ODS5) Igualdad de género, (ODS8) Trabajo decente y crecimiento económico, (ODS9) Industria, innovación e infraestructura, y (ODS10) Reducción de las desigualdades (Vargas, 2021).

Asimismo, el acelerado avance de la era electrónica a nivel mundial ha sido intensificado por la pandemia de COVID-19, extendiéndose su uso en todos los aspectos de la humanidad y afectando significativamente la gestión empresarial (Bellido y Bartolo, 2023). El comercio electrónico ha alcanzado su punto máximo de crecimiento, siendo el comercio en línea completamente natural en un mercado global donde las tiendas virtuales ofrecen masivamente sus bienes y productos a través de redes, páginas web y otros mecanismos electrónicos (González, 2020).

En tal contexto, las transacciones en línea son una práctica común en los negocios, lo que ha incrementado exponencialmente el riesgo de fraudes financieros con la proliferación de métodos y herramientas para ello (Alvarez, 2020). El término fraude se origina del latín "***fraus***" y se define como la realización de una acción incorrecta o deshonesta en perjuicio de una persona u organización (Cárdenas Gómez et al., 2021). El fraude es siempre intencional, y es crucial entender que la búsqueda de beneficios constituye su eje central. Este puede manifestarse de diversas formas, afectando principalmente dos elementos vulnerables: la información y el dinero, los cuales pueden ser robados, transferidos u ocultados. (Rivera, 2020)

El concepto de fraude es amplio, pero esencialmente se refiere a un acto intencional perpetrado con fines ilícitos, buscando una ventaja personal o para un grupo específico. Este tipo de actos tiene un impacto considerable en los estados financieros, distorsionando la información financiera, afectando principalmente el Estado de Resultados y el Balance General (Fortea et al., 2020). El fraude es un fenómeno mundial que se encuentra interconectado con la contabilidad y la ley, por lo que es necesario comprender el fraude desde una perspectiva contable y legal (Hernández et al., 2022). Por otro lado, Martorell (2019) define el fraude financiero como la conducta intencionada o descuidada, ya sea por acción u omisión, que resulta en la distorsión de los estados financieros.

Durante la pandemia de COVID-19, el fraude financiero digital se manifestó de manera significativa en los canales de información económica y financiera, adquiriendo un rol destacado en empresas e instituciones. Esto creó un entorno propicio para la perpetración de actividades ilícitas corporativas, dirigidas hacia los sistemas de información institucionales, resultando en pérdidas económicas, humanas y financieras (Albanese y Rivera, 2021). El empleo de tecnología con el propósito de atacar estos sistemas organizacionales incrementó considerablemente los riesgos de fraudes de índole tecnológica, económica y financiera durante la pandemia. (Muñoz et al., 2020)

En un contexto cada vez más digitalmente conectado, las transacciones financieras en línea se han vuelto indispensables en la vida diaria tanto en Ecuador como a nivel mundial (Heredia y Villarreal, 2022). Sin embargo, esta conveniencia también ha suscitado nuevas preocupaciones en relación con la seguridad, especialmente en lo que concierne al fraude en transacciones digitales. Este fenómeno ha captado una atención creciente tanto de individuos como de instituciones.

En el entorno digital contemporáneo, la ciberseguridad se ha vuelto una preocupación crucial debido al aumento significativo de los delitos cibernéticos, especialmente el fraude digital. Este fenómeno no solo afecta a individuos, sino también a organizaciones y entidades financieras que enfrentan constantes amenazas de ciberataques sofisticados (Aparicio, 2022). Según informes recientes, la incidencia de fraude digital entre clientes ha mostrado una tendencia al alza, impulsada por la creciente sofisticación de los métodos utilizados por los delincuentes cibernéticos para acceder a información personal y financiera.(Campos-Freire et al., 2017)

La literatura científica destaca la importancia de programas educativos en ciberseguridad como una medida preventiva efectiva para mitigar el riesgo y reducir la incidencia de fraude digital en diversos escenarios (Peña y Segura, 2014). Estos programas no solo buscan informar a los usuarios sobre las diversas formas de fraude y las medidas de seguridad disponibles, sino también educarlos sobre buenas prácticas en el manejo seguro de información sensible en entornos digitales. Investigaciones anteriores han señalado que la educación en ciberseguridad puede fortalecer la conciencia y la capacidad de

respuesta de los clientes frente a las amenazas digitales, contribuyendo así a la protección de sus activos financieros y personales.(González et al., 2024)

En este marco, el propósito de este estudio es evaluar la efectividad de diferentes métodos educativos para la implementación de un programa educativo en ciberseguridad para reducir la incidencia de fraude digital entre clientes. El objetivo principal es analizar cómo estos métodos impactan en el conocimiento, comportamiento y actitudes de los clientes hacia la ciberseguridad. La relevancia de esta investigación radica en su potencial para proporcionar evidencia empírica que oriente el diseño y la implementación de estrategias educativas efectivas en ciberseguridad, tanto para entidades financieras como para usuarios individuales, en un contexto globalizado y digitalmente interconectado.

MATERIALES Y MÉTODOS

Este estudio se llevó a cabo utilizando una metodología estructurada para garantizar el logro de los objetivos planteados. Inicialmente, se realizó una encuesta inicial para identificar el nivel de conocimiento y las áreas de mayor vulnerabilidad entre los usuarios financieros ecuatorianos. Para ello, se consideró una muestra de 40 usuarios, incluyendo clientes de bancos, tarjetahabientes, comerciantes en línea y profesionales del sector financiero de la ciudad de Quito. La encuesta inicial fue diseñada para que los usuarios participantes pudieran proporcionar información sobre sus hábitos de transacciones en línea, preocupaciones sobre fraude, experiencias pasadas y percepciones sobre medidas de seguridad. Las encuestas fueron diseñadas para diagnosticar las características de la muestra en cuanto a preferencias y percepciones sobre ciberseguridad. Las encuestas iniciales constituyeron la base sobre la cual se realizó y desarrolló un programa educativo enfocado en prácticas seguras en línea y ciberseguridad para los usuarios.

El grupo de usuario seleccionado para el estudio, fue dividido en tres grupos para la aplicación diferenciada del programa educativo elaborado. Se utilizaron talleres presenciales y virtuales (grupo 1), cursos en línea autoguiados (grupo 2) y aplicación de campañas de sensibilización (grupo 3) como métodos educativos diferenciados para evaluar su impacto final en los usuarios. La organización y desarrollo de los métodos se realizó como se muestra:

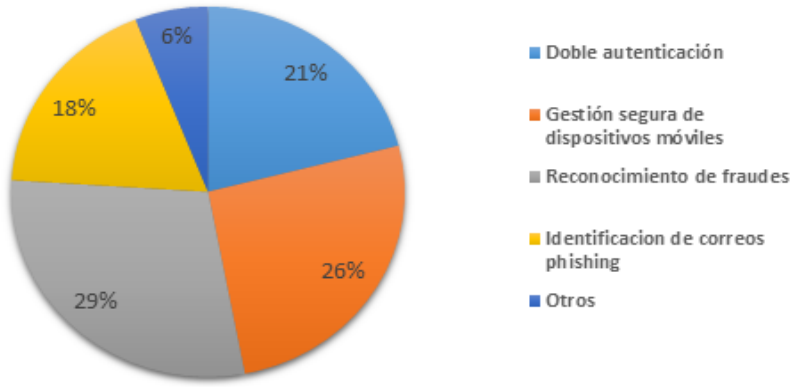
- **Talleres Presenciales y virtuales (Grupo 1)**: Se organizaron talleres interactivos en formato presencial y virtual para adaptarse a diferentes preferencias. Estos talleres incluyeron demostraciones en vivo de técnicas de fraude y métodos para prevenirlos, fomentando la participación a través de preguntas y respuestas, estudios de caso y simulaciones de escenarios de fraude.
- **Cursos en Línea Autoguiados (Grupo 2)**: Se desarrollaron cursos en línea que los participantes pudieron completar a su propio ritmo. Estos cursos cubrieron desde conceptos básicos hasta avanzados de ciberseguridad, con módulos de aprendizaje y evaluaciones para medir la comprensión.
- **Campañas de Sensibilización (Grupo 3)**: Se implementaron campañas a través de correos electrónicos, redes sociales y aplicaciones móviles bancarias. Estas campañas utilizaron infografías y videos educativos para explicar riesgos de fraude y prácticas seguras, junto con mensajes periódicos para mantener la conciencia sobre seguridad digital.

Esta diversificación en los métodos de enseñanza permitió evaluar la efectividad relativa de cada enfoque en la mejora del conocimiento y cambio de comportamiento hacia prácticas más seguras en línea. Se estableció un sistema de seguimiento continuo para monitorear la participación y evaluar el impacto del programa educativo. Se realizaron encuestas de seguimiento periódicas para medir el cambio en el conocimiento y comportamiento de los participantes, además de analizar incidentes reportados de fraude para evaluar cualquier reducción correlativa en su incidencia. Se compararon los resultados obtenidos antes y después de la aplicación del programa educativo, utilizando métodos estadísticos para determinar la efectividad relativa de los diferentes enfoques educativos en la reducción del fraude digital entre los participantes. Este enfoque metodológico aseguró la robustez del estudio al permitir una evaluación sistemática y comparativa de la efectividad de los programas educativos en ciberseguridad.

RESULTADOS-DISCUSIÓN

El análisis de los datos recopilados en la encuesta inicial reveló que el 63% de los encuestados mostró un conocimiento básico en ciberseguridad. Esto incluye la comprensión de conceptos fundamentales como la importancia de contraseñas seguras, la identificación de correos electrónicos de phishing y el uso de software antivirus. Sin embargo, este nivel de conocimiento básico indica que, aunque los usuarios están conscientes de las amenazas cibernéticas más comunes, podrían carecer de habilidades más avanzadas para mitigar riesgos más complejos. Por otro lado, el 37% restante reportó tener un conocimiento limitado o insuficiente sobre conocimientos o familiaridad con prácticas esenciales de seguridad, tales como la doble autenticación, la gestión segura de dispositivos móviles y el reconocimiento de fraudes más sofisticados. Esta brecha de conocimiento indicó una mayor vulnerabilidad a ser víctimas de fraude digital entre este grupo. Figura 1.

Fig. 1: Prácticas de seguridad menos conocidas o dominadas por los usuarios



Fuente: Elaboración propia

El análisis de los datos recopilados en la encuesta inicial reveló que el 63% de los encuestados mostró un conocimiento básico en ciberseguridad, mientras que el 37% restante reportó tener un conocimiento limitado o insuficiente. Este hallazgo inicial indicó una disparidad significativa en el nivel de entendimiento de prácticas seguras en línea entre los usuarios financieros ecuatorianos.

Simultáneamente, las áreas de mayor vulnerabilidad identificadas en la encuesta incluyeron preocupaciones específicas sobre el uso de contraseñas débiles, falta de familiaridad con medidas de autenticación multifactor, no utilización de softwares antivirus o antimalware, gestión inadecuada de datos sensibles, entre otras. En este caso, casi el 90% de los encuestados pudo identificar al menos una de las vulnerabilidades principales mencionados sin saber cómo enfrentarse a ello o que acciones tomar. La Tabla 1 muestra las principales vulnerabilidades detectadas durante el diagnóstico inicial.

Asimismo, la alta tasa de intentos de fraude reportados por los participantes (68%) indica que más de la mitad de los usuarios financieros han sido directamente afectados por actividades fraudulentas y al menos el 30% ha sido víctima de ello. Esto demuestra que el fraude digital es un problema latente en la sociedad ecuatoriana y un mal recurrente, lo cual justifica la necesidad de medidas preventivas más efectivas.

Tabla 1: Principales vulnerabilidades detectadas

Vulnerabilidades detectadas	%
Vulnerabilidad a correos electrónicos fraudulentos.	61%
Susceptibilidad a sitios web falsificados que imitan entidades legítimas.	26%
Falta de conocimientos sobre cómo identificar enlaces sospechosos y remitentes no confiables.	64%
Contraseñas cortas y fácilmente adivinables	80%
Reutilización de contraseñas en múltiples cuentas	92%
Baja tasa de adopción de aplicaciones de autenticación	93%
No utilización de software antivirus o antimalware	34%
Conexiones a redes Wi-Fi públicas sin precauciones de seguridad	84%
Almacenamiento de información personal y financiera en ubicaciones no seguras	76%
Falta de concienciación sobre nuevas amenazas y tendencias en ciberseguridad	64%
Uso de plataformas de comercio electrónico sin verificar su autenticidad y seguridad	88%
Falta de conocimiento sobre la verificación de certificados de seguridad en sitios web	88%

Fuente: Elaboración propia

A partir de los resultados obtenidos en la encuesta inicial, se diseñó un programa educativo con el fin de abordar las principales deficiencias, preocupaciones y vulnerabilidades identificadas en los usuarios encuestados. La Tabla 2 presenta un resumen de las actividades y temáticas clave que se abordarán para mitigar los problemas detectados.

Tabla 2: Programa educativo planificado.

Semana	Temáticas	Actividades	Objetivo
1 Introducción a la ciberseguridad y concienciación general	Conceptos básicos de ciberseguridad. Importancia de la ciberseguridad en el contexto financiero. Tipos de amenazas digitales y sus impactos.	Talleres presenciales y Virtuales: Organización de sesiones interactivas tanto presenciales como virtuales. Incluyen demostraciones en vivo de técnicas de fraude y métodos de prevención. Fomento de la participación mediante preguntas, estudios de caso y simulaciones de escenarios. Cursos en línea autoguiados: Desarrollo de cursos modulares en línea que abarcan los temas propuestos. Incluyen módulos de aprendizaje y evaluaciones para reforzar la comprensión. Campañas de sensibilización: Implementación de infografías, videos educativos y mensajes periódicos a través de correos electrónicos, redes sociales y aplicaciones móviles bancarias para concienciar sobre los temas propuestos.	Proveer una base sólida sobre ciberseguridad y crear conciencia sobre la importancia de protegerse contra amenazas digitales.
2 Seguridad en el uso de contraseñas	Importancia de contraseñas fuertes y seguras. Estrategias para crear y gestionar contraseñas complejas. Peligros de reutilizar contraseñas en múltiples cuentas.		Asegurar que los usuarios comprendan la importancia de utilizar contraseñas fuertes y únicas, y brindarles herramientas para gestionar sus contraseñas de manera efectiva.
3 Protección contra phishing y sitios web falsificados	Reconocimiento de correos electrónicos fraudulentos. Identificación de sitios web falsificados y enlaces sospechosos. Verificación de la autenticidad de plataformas de comercio electrónico.		Capacitar a los usuarios para reconocer y evitar intentos de phishing y sitios web fraudulentos, aumentando su capacidad de protección personal.
4 Medidas avanzadas de seguridad y buenas prácticas	Uso de autenticación multifactor y aplicaciones de autenticación. Importancia del software antivirus y antimalware. Prácticas seguras al conectarse a redes wi-fi públicas. Almacenamiento seguro de información personal y financiera. Verificación de certificados de seguridad en sitios web.		Proveer a los participantes con conocimientos y habilidades avanzadas para protegerse contra una amplia gama de amenazas cibernéticas y aplicar buenas prácticas de seguridad en su vida diaria.

Fuente: Elaboración propia

Al finalizar la cuarta semana correspondiente a la impartición del programa educativo en ciberseguridad, se aplicaron encuestas de seguimiento para verificar el comportamiento en cuanto al nivel de conocimientos y percepciones de los usuarios respecto a las vulnerabilidades detectadas inicialmente. Los resultados obtenidos se resumen en la Tabla 3, proporcionando una visualización clara y concisa de la información recolectada.

Tabla 3: Cambios mostrados tras la aplicación del programa educativo

Grupo	Participantes	Cambio en Conocimiento (%)	Cambio en Percepciones (%)
Talleres presenciales y virtuales	12	+26%	+33%
Cursos en línea autoguiados	15	+22%	+28%
Campañas de sensibilización	13	+18%	+24%

Fuente: Elaboración propia

Los resultados mostraron que el primer grupo de usuarios un aumento del 26% en el conocimiento sobre los temas de seguridad en ciberseguridad y un incremento del 33% en las percepciones de seguridad. En tal sentido, se puede destacar que, la aplicación de los talleres, permitieron una interacción directa entre los instructores y los participantes, facilitando la resolución inmediata de dudas y la personalización del contenido según las necesidades específicas de los usuarios. Este enfoque práctico y participativo resultó altamente efectivo para mejorar tanto el conocimiento como la percepción de seguridad entre los participantes. Por su parte, el segundo grupo experimentó un aumento del 22% en el conocimiento y del 28% en las percepciones de seguridad. Este método permitió a los usuarios aprender a su propio ritmo, lo que resultó en una buena absorción de conocimientos. Sin embargo, la falta de interacción directa pudo haber limitado la capacidad de los participantes para resolver dudas en tiempo real, lo que se reflejó en una menor mejora en comparación con los talleres presenciales y virtuales.

Finalmente, el tercer grupo, mostró un incremento del 18% en cuanto al conocimiento y un aumento del 24% en cuanto a las percepciones de seguridad. Las campañas de sensibilización se centraron en la difusión de información clave a través de diversos medios y en este caso, aunque este método fue menos intensivo que los anteriores, logró una mejora notable en la concienciación general sobre ciberseguridad. No obstante, la falta de profundidad en el contenido educativo y la ausencia de interacción directa pudieron haber limitado el impacto en el conocimiento y las percepciones de los usuarios.

De manera general, los talleres presenciales y virtuales demostraron ser el método más efectivo para mejorar tanto el conocimiento como las percepciones de seguridad entre los participantes. Este hallazgo es consistente con estudios previos que han destacado la importancia de la interacción directa y la personalización del aprendizaje en la educación en ciberseguridad (Roca et al., 2002). Paralelamente, los cursos en línea también mostraron mejoras significativas, aunque ligeramente menores en comparación con los talleres. El empleo de este método proporcionó flexibilidad a los participantes para aprender a su propio ritmo, pero la falta de interacción directa podría haber limitado la profundidad del aprendizaje y la resolución de dudas en tiempo real. (Salinas et al., 2018)

Finalmente, las campañas de sensibilización, aunque efectivas para aumentar la concienciación general sobre ciberseguridad, mostraron los cambios más modestos en términos de conocimiento y percepciones. Esto sugiere que, si bien la difusión de información es importante, métodos más interactivos y detallados pueden ser necesarios para un impacto más profundo (Chisag et al., 2017).

Estos resultados subrayan la importancia de adaptar los métodos educativos en seguridad financiera digital según las necesidades y preferencias de los usuarios. Las empresas y organizaciones pueden beneficiarse de implementar programas que combinen múltiples enfoques educativos.

CONCLUSIONES

El estudio realizado permitió evaluar la efectividad de diferentes métodos educativos para la implementación de un programa educativo en ciberseguridad entre usuarios financieros ecuatorianos. A través de las encuestas iniciales se identificaron las principales vulnerabilidades y áreas de desconocimiento, lo cual reveló una significativa necesidad de mejorar el conocimiento y las prácticas de seguridad digital entre los participantes. Los resultados indicaron que un considerable porcentaje de usuarios carecía de conocimientos avanzados en ciberseguridad, especialmente en áreas críticas como la gestión de contraseñas, la identificación de amenazas como el phishing y los sitios web falsificados. Para abordar estas deficiencias, se diseñó un programa educativo adaptado que combinó talleres presenciales y virtuales, cursos en línea y campañas de sensibilización. Estos métodos fueron implementados con el objetivo de educar a los participantes sobre prácticas seguras en línea y mejorar su capacidad para reconocer y prevenir los riesgos cibernéticos.

Los resultados mostraron que los talleres presenciales y virtuales fue el método más efectivo en aumentar tanto el conocimiento como las percepciones de seguridad de los implicados. Los cursos en línea también demostraron ser eficaces, aunque con resultados ligeramente menores, mientras que las campañas de sensibilización tuvieron un impacto más limitado. Las conclusiones de este estudio sugieren que la combinación de enfoques interactivos y personalizados puede ser clave para mejorar las prácticas de seguridad digital y reducir la incidencia de fraude entre los usuarios financieros. Se recomienda la realización de futuras investigaciones que logren explorar cómo adaptar estos programas a diferentes grupos demográficos y culturales, así como evaluar

la sostenibilidad a largo plazo de los conocimientos adquiridos por los participantes.

REFERENCIAS BIBLIOGRÁFICAS

Albanese, D. y Rivera, C. (2021). Auditoría de estados financieros en contexto de pandemia por COVID-19: un análisis de la normativa argentina. ***Escritos Contables y de Administración, 12***(1), 103–123. https://ojs.uns.edu.ar/eca/article/view/2250

Álvarez, F. (2020). Machine Learning en la detección de fraudes de comercio electrónico aplicado a los servicios bancarios. ***Ciencia y Tecnología, 20***, 81–95. https://dspace.palermo.edu/ojs/index.php/cyt/article/view/4310

Aparicio, V. V. (2022). Delitos informáticos en Ecuador según el COIP: un análisis documental. ***Sapienza: International Journal of Interdisciplinary Studies, 3***(1), 1057–1063. https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/284

Bellido, G. M. y Bartolo, E. E. J. (2023). Billeteras electrónicas: una herramienta para el emprendimiento en la era digital. ***Interconectando Saberes, 15***, 9–21. https://is.uv.mx/index.php/IS/article/view/2776

Campos-Freire, F., Yaguache, J., y Ulloa, N. (2017). Tendencias de la industria de los medios de América del Sur en la transición digital. Revista de Comunicación, 16(2), 33–59. https://revistadecomunicacion.com/article/view/986

Cárdenas Gómez, R., Ruiz Malbarez, M. C., y Pozo Ceballos, S. (2021). Proyección de la contabilidad y la auditoría forense ante el fraude financiero. ***Cofin Habana, 15***(1). http://scielo.sld.cu/scielo.php?pid=S2073-60612021000100003&script=sci_arttext

Chisag, J. C. C., Lagla, G. A. F., Alvarez, G. S. V., Moreano, J. A. C., Pico, O. A. G., y Chicaiza, E. M. I. (2017). Utilización de recursos didácticos interactivos a través de las TIC´ S en el proceso de enseñanza aprendizaje en el área de matemática. ***Boletín Redipe, 6***(4), 112–134. https://dialnet.unirioja.es/servlet/articulo?codigo=6119349

Fortea, J. I., Galán, Á., y Gelabert, J. E. (2020). ***Siete siglos de fraude fiscal en Europa***. Ediciones Universidad Cantabria. https://media.timtul.com/media/web_aehe/_wp-content_uploads_2020_12_Siete-Siglos-de-Fraude-Fiscal-en-Europa.pdf

González, H. R., Montesino, R., y Pérez, M. T. (2024). Superación profesional en ciberseguridad, análisis y experiencias en la Universidad de las Ciencias Informáticas. ***Jornadas Nacionales de Investigación en Ciberseguridad (JNIC) (9a. 2024)***. Sevilla) (2024), pp. 141-148. https://idus.us.es/handle/11441/159886

González, J. (2020). Comercio electrónico en China y México: surgimiento, evolución y perspectivas. ***México y la cuenca del Pacífico, 9***(27), 53–84. https://www.scielo.org.mx/scielo.php?pid=S2007-53082020000300053&script=sci_arttext

Heredia, D. E. y Villarreal, F. L. (2022). El comercio electrónico y su perspectiva en el mercado ecuatoriano. ***ComHumanitas: Revista Científica de Comunicación, 13***(1), 1–33. https://comhumanitas.org/index.php/comhumanitas/article/view/333

Hernández, L., Jimenez, A. V, Lemus, J. A., y Gutiérrez, F. (2022). La Prospectiva de los mecanismos en la detección de fraudes financieros. ***Revista Decisión Gerencial, 1***(1), 31–41. https://decisiongerencial.ucacue.edu.ec/index.php/decisiongerencial/article/view/6

Martorell, E. E. (2019). Auditores Externos. Nuevos vientos, traen nuevas responsabilidades. ***Revista Enfoques, 9***, 72–79. https://www.consejosalta.org.ar/wp-content/uploads/Auditores-externos.-_Nuevos-vientos_-traen-nuevas-responsabilidades.pdf

Muñoz, H., Canabal, J., Galindo, S. G., Zafra, B. S., y Benítez, Y. J. (2020). Informática forense y auditoría forense: Nuevas perspectivas en tiempos de COVID-19. ***Revista Espacios, 41***(42). https://revistaespacios.com/a20v41n42/a20v41n42p32.pdf

Peña, J. C. y Segura, L. A. G. (2014). La importancia del componente educativo en toda estrategia de Ciberseguridad. ***Estudios en Seguridad y Defensa, 9***(18), 5–13. https://esdegrevistas.edu.co/index.php/resd/article/view/9

Rivera, D. V. (2020). La auditoría forense como herramienta en la detección de delitos. ***Dilemas Contemporáneos: Educación, Política y Valores, VII***(Edición Especial). https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/2115

Roca, J. S., Castillo, M. A., y Marzo, L. (2002). La educación emocional y la interacción profesor/a-alumno/a. ***Revista Electrónica Interuniversitaria de Formación del Profesorado, 5***(3), 1. https://dialnet.unirioja.es/servlet/articulo?codigo=1034495

Salinas, J., De Benito, B., Pérez, A., y Gisbert, M. (2018). Blended learning, más allá de la clase presencial. ***RIED-Revista Iberoamericana de Educacion a Distancia, 21***(1), 195–213. https://repositori.uib.es/xmlui/handle/11201/164657

Vargas, A. H. (2021). La inclusión financiera en el Perú. ***Gestión En El Tercer Milenio, 24***(47), 129–136. https://revistasinvestigacion.unmsm.edu.pe/index.php/administrativas/article/view/20591