REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 9 – Número 2
Julio - Diciembre 2026
pp.171-179

Uso de Telegram como herramienta para difundir estrategias de ciberseguridad: Programa de Cibertips

Using telegram as a tool to disseminate cybersecurity strategies: the cybertips program

Roberto Daniel Gordon Graell
Universidad de Panamá, Centro Regional Universitario de Coclé, Panamá.
Correo: roberto.gordon@up.ac.pa https://orcid.org/0000-0001-8468-4910

Kerllys Valdés
Universidad de Panamá, Centro Regional Universitario de Coclé, Panamá.
Correo: kerllys.valdes@up.ac.pa. https://orcid.org/0009-0000-1406-2374

Recibido: 01-04-2026 Aprobado: 25-05-2026

DOI: https://doi.org/10.48204/j.faeco.v9n2.a9905

Resumen

En los últimos años, hemos evidenciado un crecimiento de alto valor en el uso de entornos digitales, permitiendo mayor interoperabilidad y automatizaciones. Sin embargo, a medida que estos entornos crecen, aparecen vulnerabilidades en ciberseguridad, poniendo en riesgo tanto la infraestructura del entorno como los datos en tránsito y reposo, proyectando los costos globales de la cibercriminalidad en B/. 10.5 billones de dólares anuales para 2025. Ante la ineficacia documentada de los modelos educativos unidireccionales para mitigar estos riesgos, esta investigación presenta y evalúa la implementación del Programa de Cibertips, una intervención educativa basada en la plataforma de mensajería Telegram. Se empleó un diseño de métodos mixto, utilizando encuestas y pruebas diagnósticas pre/post-estudio para la recopilación de datos cuantitativos, complementado con un análisis temático de las interacciones cualitativas. Los resultados cuantitativos demuestran un aumento estadísticamente significativo en el nivel de conocimiento, con un incremento del 30% al 75% de los participantes reportando un conocimiento básico a avanzado después de la intervención. Concluyendo queTelegram representa una solución pedagógica versátil y eficiente para la educación continua en ciberseguridad, facilitando la adopción de prácticas seguras y la construcción de una cultura digital resiliente.

Palabras clave: telegram, ciberseguridad, micro-aprendizaje, concienciación digital.

Abstract

In recent years, we have witnessed significant growth in the use of digital environments, enabling greater interoperability and automation. However, as these environments expand, cybersecurity vulnerabilities emerge, jeopardizing both the environment's infrastructure and data in transit and at rest. Global cybercrime costs are projected to reach $10.5 trillion annually by 2025. Given the documented ineffectiveness of one-way educational models in mitigating these risks, this research presents and evaluates the implementation of the Cibertips Program, an educational intervention based on the Telegram messaging platform. A mixed-methods design was employed, utilizing pre/post-study surveys and diagnostic tests for quantitative data collection, complemented by a thematic analysis of qualitative interactions. The quantitative results demonstrate a statistically significant increase in knowledge level, with the percentage of participants reporting basic to advanced knowledge rising from 30% to 75% after the intervention. In conclusion, Telegram represents a versatile and efficient pedagogical solution for continuing education in cybersecurity, facilitating the adoption of secure practices and the building of a resilient digital culture.

Keywords: Telegram, cybersecurity, microlearning, digital awareness

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 9 – Número 2
Julio - Diciembre 2026
pp.171-179

Introducción

La sociedad contemporánea se encuentra inmersa en un proceso de digitalización integral, donde las infraestructuras críticas, los sistemas empresariales y las interacciones personales dependen de la interconexión constante (Gartner, 2022). Esta dependencia tecnológica ha incentivado que la ciberseguridad ya no sea un tema más, sino un pilar imprescindible para resguardar el entorno, todo esto debido a las crecientes amenazas económicas relacionadas a los ataques de *phishing*, el *ransomware* y el *malware* que se han proliferado de manera significativa, alcanzando costos económicos de $10.5 billones de dólares anuales para el año 2025 (Cybersecurity Ventures, 2021).

A pesar de las cuantiosas inversiones en sistemas de *hardware* y *software* de defensa, la vulnerabilidad crítica persiste en el factor humano. Estudios han demostrado consistentemente que la mayoría de las brechas de seguridad se originan en errores humanos, ya sea por desconocimiento o por la omisión de prácticas seguras (García & Fernández, 2022). Específicamente, el *phishing*, una técnica de ingeniería social, es responsable de más del 80% de los incidentes de seguridad, mientras que el *ransomware* ha experimentado un crecimiento exponencial, evidenciando una brecha crítica en la conciencia y la capacitación del usuario final (López & Martínez, 2021).

La respuesta tradicional a esta crisis ha sido la implementación de seminarios anuales o módulos de formación masivos. Sin embargo, estos enfoques educativos unidireccionales son inherentemente limitados. Fallan en la retención del conocimiento debido a la sobrecarga informativa, carecen de la inmediatez necesaria para responder a amenazas emergentes y no logran fomentar un cambio conductual duradero (Martínez et al., 2023).

La ineficacia de estos modelos subraya la necesidad urgente de una innovación pedagógica que se adapte al ritmo acelerado de la evolución tecnológica y a los patrones de atención del usuario moderno (Miller, 2023).

Desde esta perspectiva, el micro-aprendizaje se presenta como una solución metodológica, caracterizada por la interactividad durante el aprendizaje con contenido específico y relevante. Asimismo, su aplicación se basa en sistemas automatizados que se integran a plataformas de comunicación ubicuas destacándose como herramientas útiles para superar las barreras de tiempo y fricción.

En ese sentido, la plataforma de mensajería instantánea Telegram se distingue de otras redes sociales por su enfoque en la privacidad, el cifrado robusto y las funcionalidades avanzadas para la difusión de información masiva. Sus características técnicas, como la creación de canales de alta capacidad, la automatización mediante *bots* interactivos y la facilidad para integrar contenido multimedia (video, infografías), la posicionan como un canal ideal para la distribución continua y dinámica de estrategias de ciberseguridad (Ruiz

& Martínez, 2023). Esta capacidad de interacción constante permite una formación "justo a tiempo," crucial para mantener la resiliencia digital (González & Pérez, 2021).

El presente estudio aborda la necesidad de innovación educativa mediante el diseño, implementación y evaluación del programa de Cibertips. Este programa surge con la intención de ayudar a muchos usuarios a mejorar su conocimiento sobre ciberseguridad en un momento crítico, donde las amenazas cibernéticas se siguen incrementando. El mismo consiste en pequeñas cápsulas de información, utilizando Telegram como plataforma para crear conciencia por medio de tips sobre cómo protegerse en el mundo digital. Su importancia radica en que nos encontramos ante un escenario de avances tecnológicos que a su vez enfrenta grandes desafíos relacionados a vulnerabilidades que en su mayoría inician desde el usuario que es considerado en cualquiera organización como la primera capa de defensa de cualquier infraestructura tecnológica. Es por ello que consideramos esencial informar y empoderar a todos los usuarios sobre la realidad del escenario actual que enfrenta nuestro entorno tecnológico y a su vez como protegerse ante este tipo de ataques y contar con herramientas adaptadas a las necesidades actuales.

El objetivo general de la investigación es analizar la efectividad del uso de Telegram, a través del Programa de Cibertips, para elevar el nivel de conocimiento, la comprensión y la adopción de prácticas seguras de ciberseguridad en la comunidad de usuarios.
Para lograr este fin, se plantea la Hipótesis de Trabajo sobre el uso de Telegram como plataforma de difusión de estrategias de ciberseguridad, a través de micro-contenidos (Ciber Tips) y *bots* interactivos, incrementa el nivel de concienciación y la adopción de prácticas seguras en los usuarios de la comunidad de manera estadísticamente significativa.

Materiales y Métodos

La investigación presenta un enfoque aplicado mediante un diseño mixto y concurrente de triangulación (CUAL-CUAN), fundamentado en las propuestas de González y Pérez (2021). Por otro lado, la vertiente cuantitativa aplicada se centró en medir la magnitud del impacto del programa en el conocimiento técnico, mientras que la cualitativa permitió una comprensión fenomenológica de las experiencias y actitudes de los usuarios. Bajo esta premisa, logramos obtener los datos para maximizar la profundidad de los hallazgos Posteriormente, se aplicó una triangulación, el cual nos permitió efectuar comparaciones que luego fueron analizados para su respectiva validación.

El estudio se llevó a cabo durante el año 2025 utilizando la plataforma Telegram como entorno experimental durante cinco meses (marzo-agosto). En cuanto a la población, se obtuvo un muestreo no probabilístico por conveniencia, atrayendo a usuarios interesados voluntariamente en la ciberseguridad.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 9 – Número 2
Julio - Diciembre 2026
pp.171-179

Para garantizar el rigor científico, se aplicaron criterios de inclusión estrictos: tener acceso activo a Telegram, interactuar con el contenido y, fundamentalmente, completar tanto la preevaluación como la post-intervención. Como resultado, la muestra final fue de 2,000 participantes. Además, se registraron variables de control como edad, nivel educativo y antecedentes formativos para mitigar potenciales efectos de confusión en el análisis estadístico.

El marco analítico se estructuró a partir de dos ejes principales:

- Variable Independiente (VI): Donde el Programa de "Ciber Tips", consistente en la difusión semanal de micro contenidos (infografías y videos) y soporte automatizado mediante un bot interactivo.
- Variable Dependiente (VD): Comprensión y Rendimiento en Ciberseguridad, medida a través de las puntuaciones en las pruebas diagnósticas y la escala de adopción de prácticas seguras.

Se diseñó un ecosistema digital de recolección de datos validado por juicio de expertos y pruebas de confiabilidad (Alfa de Cronbach = 0.85).

Tabla 1.

Matriz de Validez y Estructura de los Instrumentos

Instrumento	Objetivo	Método de Recolección	Evaluación de Validación
Ciber Tips	Difundir micro-contenidos	Platform: Telegram	Juicio de expertos, Alfa de Cronbach = 0.85
Pruebas Diagnósticas	Medir comprensión en ciberseguridad	Cuestionarios en Telegram	Revisión por expertos, confiabilidad verificada
Escala de Adopción	Evaluar la adopción de prácticas seguras	Encuestas post-intervención	Validación mediante análisis estadístico

Un aspecto crítico fue el diseño de las Pruebas Diagnósticas de Conocimiento (PDC). Donde se desarrollaron dos versiones equivalentes (formas paralelas) para evitar el sesgo de memoria, asegurando que la mejora en las puntuaciones se debiera al aprendizaje y no a la repetición de los reactivos.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 9 – Número 2
Julio - Diciembre 2026
pp.171-179

Tabla 2

Muestra de Reactivos y Criterios de Evaluación (PDC)

Reactivo	Tipo de Conocimiento	Criterio de Evaluación
Pregunta 1: ¿Qué es un phishing?	Conocimiento Básico	Respuesta correcta = 1 pt
Pregunta 2: Ejemplo de una práctica segura	Aplicación Práctica	Respuesta correcta = 1 pt
Pregunta 3: Identificar un riesgo online	Análisis	Respuesta correcta = 1 pt
Pregunta 4: Consecuencias del malware	Evaluación	Respuesta correcta = 1 pt
Pregunta 5: Estrategias de defensa	Síntesis	Respuesta correcta = 1 pt

La intervención se llevó a cabo en tres fases cronológicas: en la Fase 1, se realizó la Línea Base (Pre-intervención) a través de la aplicación de la Prueba de Diagnóstico inicial (PDC), que reveló que solo el 30% de los participantes poseía conocimientos básicos, lo que evidenció la necesidad de la intervención; en la Fase 2, se implementó la Intervención Educativa mediante la difusión constante de "Ciber Tips", fundamentados en principios de educación digital (Smith, 2020), enfocados en la brevedad y el impacto visual; finalmente, en la Fase 3, se realizó la Evaluación Final (Post-intervención) con la reaplicación de una versión paralela de la PDC y encuestas de percepción, cuyos resultados se compararon estadísticamente utilizando el Factor de Hake para medir la ganancia neta de aprendizaje.

Finalmente, los datos cuantitativos se procesaron en software especializado (SPSS/R) mediante análisis descriptivos y pruebas t de Student pareadas para determinar la significancia estadística ($p < 0.05$). Los datos cualitativos se sometieron a un análisis de contenido temático, cuya convergencia con los datos numéricos permitió validar la efectividad global del programa.

Resultados

La evaluación cuantitativa se centró en la participación de los usuarios y el rendimiento en las Pruebas Diagnósticas de Conocimiento.

Se registró un crecimiento sostenido de suscriptores, alcanzando más de 2,000 suscriptores al final del periodo. La métrica más relevante fue la Tasa de Participación Activa, definida como la interacción mensual (reacciones, comentarios, uso del *bot*).

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 9 – Número 2
Julio - Diciembre 2026
pp.171-179

Tabla 3

Tasa de Participación y Crecimiento del Canal

Métrica	Valoración	Observación
Suscriptores Totales Post-Estudio	> 2,000	Incremento del 150% desde el lanzamiento
Tasa de Participación Activa Mensual	65% promedio	Sugiere alta relevancia del contenido
Frecuencia de Interacción con el Bot	4.5 interacciones/usuario/mes	Indicador de la utilidad de la herramienta de consulta

Se compararon las puntuaciones medias obtenidas en las Pruebas Diagnósticas de conocimiento pre y post-intervención, normalizadas a una escala de 0 a 100 puntos.

Tabla 4.

Comparación de Puntuaciones Medias en la PDC (Nivel de Conocimiento)

Grupo	N	Puntuación Media Pre-Estudio (DE)	Puntuación Media Post-Estudio (DE)	Diferencia Media (IC 95%)	p-valor
Participantes Totales	2000	51.2 (10.5)	78.4 (9.1)	27.2 (26.1 - 28.3)	< 0.001
Conocimiento Básico (Pre)	1400	45.1 (8.9)	74.5 (8.5)	29.4 (28.2 - 30.6)	< 0.001

DE Desviación Estándar; IC 95%: Intervalo de Confianza del 95%. Los datos muestran un incremento significativo tras la intervención con Cibertips.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 9 – Número 2
Julio - Diciembre 2026
pp.171-179

Los resultados de la prueba t pareada mostraron una diferencia estadísticamente significativa entre las puntuaciones pre y post-estudio, lo que indica que el Programa de Cibertips tuvo un efecto causal positivo en el aumento del conocimiento. El porcentaje de usuarios que se autoclasificaron con un conocimiento básico pasó del 30% al 75% (aumento del 45%) después del estudio, sugiriendo un movimiento masivo hacia una comprensión más avanzada.

El análisis cualitativo realizado sobre los comentarios y el *feedback* recolectado del bot interactivo reveló tres categorías principales de hallazgos cualitativos.

En primer lugar, los participantes valoraron altamente la concisión y el formato de micro-contenido implementado. El uso estratégico de infografías y ejemplos extraídos de la vida real demostró ser crucial para la adecuada comprensión de conceptos complejos, como es el caso del *ransomware* (Davis & White, 2022). Esto se evidencia en comentarios como: "Los Ciber Tips son muy fáciles de entender, no parecen tan técnicos como otras informaciones que encuentro. El bot me ayudó mucho a entender lo del *ransomware*".

En segundo lugar, se constató que la mayor interacción y preocupación de los usuarios se centró en temas de aplicación práctica inmediata en su vida cotidiana. Específicamente, los usuarios mostraron gran interés en la protección de datos personales, la gestión segura de contraseñas y la identificación de diferentes modalidades de estafas, tales como el *phishing* y el *smishing*. Esto subraya una clara demanda de conocimiento que pueda ser aplicado directamente para mejorar la seguridad personal, como lo señalan García y Fernández (2022).

Finalmente, se observó un significativo cambio actitudinal, que transitó desde una postura inicial de temor o pasividad frente a las amenazas, hacia una actitud de mayor proactividad y confianza. Usuarios de la muestra reportaron sentirse "más seguros" o "más preparados" después de la intervención. Un indicador conductual muy relevante de la internalización del mensaje fue el aumento en la difusión de los Ciber Tips por parte de los usuarios con sus propios contactos, lo que sugiere el deseo de promover activamente una cultura de ciberseguridad más allá del canal experimental.

Discusión

La solidez de los resultados, tanto cuantitativos como cualitativos, proporciona un fuerte soporte empírico a la hipótesis de que Telegram es un vehículo educativo excepcionalmente eficaz para la difusión de estrategias de ciberseguridad (Ruiz & Martínez, 2023).

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 9 – Número 2
Julio - Diciembre 2026
pp.171-179

El incremento medio de 27.2 puntos en la PDC es una evidencia contundente de la eficacia pedagógica del modelo Ciber Tips. Este modelo aprovecha el principio de micro-aprendizaje, adaptándose a la curva de atención y los hábitos de consumo de contenido de los usuarios digitales (Davis & White, 2022). La integración de Telegram, una plataforma a la que los usuarios están inherentemente conectados reduce la fricción en el acceso a la formación. El formato de cápsulas informativas (*Ciber Tips*) aborda con éxito el desafío de la falta de conciencia y comprensión que perpetúa la vulnerabilidad digital (Martínez et al., 2023).

La complementariedad de los datos es clave. El hallazgo cuantitativo de un aumento en el conocimiento (Tabla 2) se valida y explica por el análisis cualitativo. La alta valoración cualitativa de la claridad y concisión del contenido explica por qué la intervención fue tan efectiva en la mejora de la comprensión, especialmente para aquellos participantes que inicialmente poseían conocimientos limitados. Este enfoque pedagógico inclusivo es fundamental para superar la intimidación generada por la terminología especializada, un problema común en la formación en ciberseguridad (Miller, 2023).

Más allá de la retención de datos, el impacto más significativo se observó en el plano actitudinal. El cambio de una actitud pasiva a una de proactividad y empoderamiento (autoeficacia) es crucial, ya que una actitud positiva se correlaciona directamente con la adopción de prácticas seguras y la resiliencia ante las amenazas. La capacidad del canal para generar un ambiente donde los usuarios se sienten cómodos y motivados a participar (65% de participación) demuestra que la plataforma fomentó un entorno de aprendizaje seguro y colaborativo.

Los resultados de las pruebas diagnósticas (PDC) permitieron la identificación de debilidades específicas en la muestra, como la gestión de riesgos y la identificación de vulnerabilidades. Esta información subraya la necesidad de un enfoque personalizado y adaptativo en la educación. La capacidad de Telegram para segmentar grupos (incluso implícitamente a través de la respuesta del *bot*) permite la futura implementación de contenido diferenciado, asegurando que el currículo cumpla con los estándares de aprendizaje y las demandas del mercado (NCSC, 2021).

El uso de Telegram capitaliza el potencial de la tecnología digital para transformar la educación en ciberseguridad, pasando de un modelo de cumplimiento pasivo a un modelo de concienciación activa y continua, lo cual es esencial en el panorama de amenazas actual.

Conclusiones

La implementación del Programa de Cibertips a través de Telegram ha demostrado ser una intervención educativa efectiva y escalable, significativamente mejorando el conocimiento y la adopción de prácticas de ciberseguridad entre los participantes. Los hallazgos cuantitativos reflejan un aumento notable en las puntuaciones de las pruebas de conocimiento, aumentando de 51.2 a 78.4, con un valor de $p < 0.001$. Este resultado subraya claramente el impacto positivo que ha tenido el programa en la formación de los usuarios. Además, el análisis cualitativo pone de manifiesto la utilidad y la claridad de los micro-contenidos, donde los participantes consideraron accesibles y valiosos. La capacidad de Telegram para promover la interactividad y facilitar el acceso a la información es un aspecto fundamental, especialmente en un contexto donde los métodos de aprendizaje tradicionales a menudo pueden ser insuficientes. Esto permite a los usuarios consumir información de manera ágil, lo que fomenta su aplicación práctica en situaciones cotidianas.

A la luz de estos resultados, es recomendable que tanto instituciones educativas como empresas consideren la adopción de modelos de micro-aprendizaje a través de plataformas de comunicación instantánea como una parte integral de su formación continua en ciberseguridad. La evolución de la educación en este ámbito es esencial, ya que no solo busca impartir conocimientos, sino también empoderar a los individuos para que se conviertan en defensores activos de su propia información, contribuyendo así a la creación de una cultura de seguridad digital colectiva.

Referencias Bibliográficas

Cybersecurity Ventures. (2021). Cybercrime costs - The world $10.5 trillion annually by 2025. https://cybersecurityventures.com/

Davis, R., & White, T. (2022). Using Telegram for interactive learning: A case study. Journal of Digital Learning, 10(4), 300–320.

Foro Económico Mundial. (2023). The global cybersecurity skills shortage.

García, R., & Fernández, J. (2022). Tendencias actuales en ciberseguridad: Un análisis de las amenazas emergentes. Revista de Ciberseguridad y Tecnología, 15(1), 45–67.

Gartner. (2022). Cybersecurity trends 2022.

González, A., & Pérez, M. (2021). Learning through interaction: A study on educational approaches in cybersecurity. Journal of Educational Technology, 15(3), 200–215.

López, A., & Martínez, P. (2021). Phishing: Una amenaza creciente en la ciberseguridad. Journal of Cybersecurity Research, 12(3), 22–39.

Martínez, S., Rodríguez, P., & Vera, T. (2023). La importancia de la formación continua en ciberseguridad en las organizaciones. Educación y Tecnología, 18(2), 88–102.

Miller, S. (2023). Cybersecurity education: Trends and innovations. Journal of Information Security, 22(1), 20–30.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 9 – Número 2
Julio - Diciembre 2026
pp.171-179

NCSC (Centro Nacional de Seguridad Cibernética). (2021). Principios de ciberseguridad.

Pérez, T., & Gómez, M. (2022). El impacto de la ciberseguridad en la reputación empresarial. Journal of Business Ethics, 14(4), 150–165.

Ruiz, J., & Martínez, C. (2023). Telegram como herramienta educativa en ciberseguridad: Un estudio de caso. Revista de Educación y Ciberseguridad, 10(1), 55–70.

Smith, J. (2020). Gamification in education: The future of learning. International Journal of Educational Research, 45(2), 150–165.

UNESCO. (2024). Educación y ciberseguridad: Recursos y estrategias para padres y estudiantes. Informe anual.