

**Concientización en seguridad digital: Una Guía Teórica y Práctica basada en
Ciberseguridad Preventiva para fortalecer la protección de la identidad digital en
estudiantes universitarios**

Digital Security Awareness: A Theoretical and Practical Guide based on Preventive
Cybersecurity to strengthen the protection of digital identity in university students

Sandra Yasmin Samudio
Universidad de Cundinamarca
ssamudio@ucundinamarca.edu.co
ORCID: <https://orcid.org/0009-0008-4855-5693>

Marcia Catalina Pulido Córdoba
Universidad de Cundinamarca
mcpulido@ucundinamarca.edu.co
ORCID: <https://orcid.org/0000-0003-4602-8642>

Gina Paola Suárez Ávila
Universidad de Cundinamarca
gpsuarez@ucundinamarca.edu.co
ORCID: <https://orcid.org/0000-0002-7338-2121>

Recibido: 3 junio 2026 **Aceptado:** 19 junio 2026 **Publicado:** 1 julio 2026

Cómo citar: Samudio, S. Y., Pulido Córdoba, M. C., & Suárez Ávila, G. P. (2026). Concientización en seguridad digital: Una guía teórica y práctica basada en ciberseguridad preventiva para fortalecer la protección de la identidad digital en estudiantes universitarios. Revista Electrónica de Investigación de Tecnologías Educativas ITFIPVIRTUAL, 8(1), 43-74.

© 2026 Los autores. Este artículo se publica en acceso abierto bajo la licencia Creative Commons Atribución 4.0 Internacional (CC BY 4.0), que permite el uso, distribución, reproducción y adaptación del contenido en cualquier medio o formato, incluso con fines comerciales, siempre que se otorgue el reconocimiento adecuado a los autores y a la publicación original.

Licencia: <https://creativecommons.org/licenses/by/4.0/>

© 2026 The Authors. This article is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, reproduction, and adaptation in any medium, including commercial use, provided appropriate credit is given to the original authors and source.

License: <https://creativecommons.org/licenses/by/4.0/>

Resumen. La transformación digital ha incrementado significativamente la exposición de los usuarios a riesgos asociados con la protección de datos personales, el robo de identidad, la ingeniería social y otras amenazas derivadas de la interacción en entornos digitales. En este contexto, las instituciones de educación superior enfrentan el desafío de fortalecer las competencias relacionadas con la seguridad digital y la protección de la identidad digital de sus estudiantes. El objetivo de este estudio fue analizar el aporte de una estrategia de apropiación social del conocimiento basada en ciberseguridad preventiva al fortalecimiento de la sensibilización frente a riesgos digitales en estudiantes del programa de Ingeniería de Sistemas y Computación de la Universidad de Cundinamarca. Metodológicamente, se desarrolló una experiencia educativa de carácter descriptivo sustentada en tres fases: diagnóstico inicial de conocimientos, implementación del manual Concientización en Seguridad Digital: Una Guía Teórica y Práctica basada en Ciberseguridad Preventiva y evaluación posterior de percepciones y prácticas relacionadas con la seguridad digital. Participaron 55 estudiantes en la fase diagnóstica y 59 en la evaluación posterior. Los resultados evidenciaron que el 71,2 % de los participantes reconoce algún grado de vulnerabilidad frente a amenazas digitales, el 83,1 % identifica la relación entre la exposición de información personal y los ataques de ingeniería social, mientras que el 69,5 % consideró la estrategia pertinente o muy pertinente. Se concluye que las iniciativas de apropiación social del conocimiento constituyen mecanismos efectivos para fortalecer la

cultura de ciberseguridad preventiva y promover prácticas orientadas a la protección de la identidad digital en contextos universitarios.

Palabras clave: apropiación social del conocimiento, ciberseguridad preventiva, identidad digital, ingeniería social, seguridad digital.

Abstract. Digital transformation has significantly increased users' exposure to risks associated with personal data protection, identity theft, social engineering, and other threats derived from interactions in digital environments. In this context, higher education institutions face the challenge of strengthening students' competencies related to digital security and digital identity protection. The objective of this study was to analyze the contribution of a knowledge social appropriation strategy based on preventive cybersecurity to raising awareness of digital risks among students from the Systems and Computer Engineering program at the University of Cundinamarca. Methodologically, a descriptive educational experience was developed through three phases: initial knowledge assessment, implementation of the manual Digital Security Awareness: A Theoretical and Practical Guide Based on Preventive Cybersecurity, and a subsequent evaluation of perceptions and practices related to digital security. Fifty-five students participated in the diagnostic phase and fifty-nine in the post-intervention evaluation. The results showed that 71.2% of participants recognized some degree of vulnerability to digital threats, 83.1% identified the relationship between personal information exposure and social engineering

attacks, and 69.5% considered the strategy relevant or highly relevant. It is concluded that knowledge social appropriation initiatives are effective mechanisms for strengthening preventive cybersecurity culture and promoting practices aimed at protecting digital identity in university contexts.

Keywords: knowledge social appropriation, preventive cybersecurity, digital identity, social engineering, digital security.

Introducción

La transformación digital ha cambiado de manera significativa la forma en que las personas se comunican, acceden a la información, promueven su aprendizaje y participación social en redes sociales, generando nuevas oportunidades para la interacción y la construcción de conocimiento, la ciberseguridad y la identidad digital han adquirido una importancia cada vez mayor, especialmente porque el número de usuarios conectados continúa creciendo y, con ello, también aumentan los riesgos asociados al uso de entornos digitales, ahora, bien entre las principales amenazas se encuentra el phishing, ingeniería social, robo de identidad, malware y la exposición indebida de datos personales. Diversos estudios señalan las instituciones de educación superior

son particularmente vulnerables frente a este tipo de riesgos debido a la alta dependencia tecnológica de sus procesos académicos, administrativos (Afolalu et al., 2025).

En el ámbito universitario, la identidad digital adquiere una relevancia especial porque influye tanto en la vida académica como en el futuro profesional de los estudiantes, esta identidad está conformada por el conjunto de datos, interacciones y acciones que cada persona proyecta en internet y que construyen su reputación digital (Giones-Valls & Serrat-Brustenga, 2010). Estudios recientes evidencian que muchos estudiantes presentan dificultades para reconocer los riesgos relacionados con la exposición de información personal, el manejo seguro de contraseñas, la configuración de privacidad en redes sociales y la identificación de ataques basados en ingeniería social (Tomalá-Domínguez, 2024), estas debilidades aumentan la probabilidad de ser víctimas de amenazas que explotan principalmente factores humanos más que vulnerabilidades tecnológicas.

En respuesta a esta necesidad, la Universidad de Cundinamarca desarrolló el manual Concientización en Seguridad Digital: Una Guía Teórica y Práctica basada en Ciberseguridad Preventiva, concebido como una estrategia educativa orientada a fortalecer la cultura de seguridad digital en estudiantes universitarios, el manual pretende que cada creador de oportunidades de la Universidad de Cundinamarca comprenda que la ciberseguridad comienza en las pequeñas decisiones diarias y que cada persona puede convertirse en el primer “firewall” humano de su entorno digital, la apropiación social del conocimiento se convierte así en una estrategia

fundamental para fortalecer capacidades relacionadas con la prevención de riesgos, la protección de datos y el uso responsable de las tecnologías.

El presente estudio tuvo como objetivo analizar el aporte de una estrategia de apropiación social del conocimiento basada en ciberseguridad preventiva al fortalecimiento de la sensibilización frente a riesgos digitales y la protección de la identidad digital en estudiantes del programa de Ingeniería de Sistemas y Computación de la Universidad de Cundinamarca.

Materiales y métodos

Diseño del estudio

La presente investigación se desarrolló bajo un enfoque de Apropiación Social del Conocimiento (ASC) con alcance descriptivo y orientación aplicada, el estudio se estructuró como una experiencia educativa orientada al fortalecimiento de la cultura de ciberseguridad preventiva en estudiantes universitarios mediante la implementación de una estrategia de sensibilización basada en recursos educativos especializados, este enfoque reconoce la importancia de acercar el conocimiento científico y tecnológico a comunidades específicas, con intención de favorecer procesos de comprensión, apropiación y aplicación práctica para la solución de problemáticas del contexto (Ministerio de Ciencia, Tecnología e Innovación [MinCiencias], 2022).

La estrategia desarrollada en esta propuesta parte de la idea y necesidad de que la protección de la identidad digital no depende únicamente del uso de herramientas tecnológicas o sistemas de seguridad avanzados, sino también de la capacidad que tienen las personas para reconocer riesgos, tomar decisiones responsables y adoptar hábitos seguros en su vida digital, en este sentido, se consideró fundamental fortalecer procesos de formación y sensibilización orientados a que los estudiantes comprendieran cómo las amenazas de ingeniería social aprovechan principalmente el desconocimiento, la confianza y las prácticas inadecuadas de los usuarios.

La propuesta se apoyó en lo planteado por Barragán-Sánchez y Murta (2024), quienes señalan que la ciberseguridad debe entenderse como un proceso educativo y cultural permanente, donde la construcción de capacidades digitales resulta esencial para prevenir riesgos y promover comportamientos seguros en los entornos virtuales.

Contexto institucional

La experiencia se desarrolló en la Universidad de Cundinamarca, específicamente con estudiantes vinculados al programa de Ingeniería de Sistemas y Computación, la estrategia se articuló con las acciones institucionales orientadas al fortalecimiento de competencias digitales, la formación integral y la promoción de una cultura de uso responsable y seguro de las tecnologías de la información.

El proyecto se desarrolló durante un semestre académico y estuvo orientado a promover la reflexión crítica sobre los riesgos asociados a la exposición digital, la protección de la información personal y la adopción de buenas prácticas de ciberseguridad.

Participantes

La población objeto de estudio estuvo conformada por estudiantes del programa de Ingeniería de Sistemas y Computación de la Universidad de Cundinamarca.

Durante la fase diagnóstica participaron 55 estudiantes, quienes diligenciaron el instrumento inicial de caracterización de conocimientos relacionados con seguridad digital, seguido, en la fase de evaluación de resultados participaron 59 estudiantes, quienes respondieron el instrumento orientado a identificar percepciones, prácticas y niveles de sensibilización frente a riesgos digitales.

La participación fue voluntaria y se desarrolló bajo principios de confidencialidad y protección de datos personales.

Estrategia de apropiación social del conocimiento

La intervención se desarrolló mediante el manual denominado “Concientización en Seguridad Digital: Una Guía Teórica y Práctica basada en Ciberseguridad Preventiva”, diseñado como recurso educativo para fortalecer la cultura de seguridad digital en contextos universitarios, el documento integra contenidos conceptuales y prácticos relacionados con identidad digital, autenticación multifactor, protección de datos personales, gestión de contraseñas, seguridad en redes sociales, seguridad del correo electrónico, ingeniería social y ciberseguridad preventiva.

La estrategia contempló actividades de socialización, sensibilización y apropiación de contenidos, promoviendo la reflexión sobre situaciones reales de riesgo digital y el reconocimiento de prácticas orientadas a la protección de la información personal y académica.

Instrumentos de recolección de información

Diagnóstico inicial de conocimientos

Se diseñó un instrumento de caracterización orientado a identificar el nivel de conocimiento previo de los participantes respecto a conceptos fundamentales de seguridad digital y ciberseguridad preventiva.

El cuestionario incluyó preguntas relacionadas con:

- Concepto de identidad digital.
- Seguridad en redes sociales.
- Gestión de contraseñas.
- Ingeniería social.
- Autenticación multifactor.
- Seguridad del correo electrónico.
- Protección de datos personales.
- Riesgos asociados al entorno digital.

La información obtenida permitió establecer una línea base sobre los conocimientos de los estudiantes antes de la implementación de la estrategia educativa.

Evaluación posterior

Posteriormente se aplicó un segundo instrumento orientado a identificar percepciones, comportamientos y prácticas relacionadas con la seguridad digital después de la implementación de la estrategia de apropiación social del conocimiento.

Las variables analizadas incluyeron:

- Percepción de vulnerabilidad digital.
- Conciencia frente a riesgos de ingeniería social.
- Uso de autenticación multifactor.
- Gestión de contraseñas.
- Verificación de enlaces sospechosos.
- Revisión de permisos digitales.
- Valoración de la pertinencia de la estrategia educativa.

Procedimiento

La investigación se desarrolló en cuatro fases consecutivas:

Fase 1. Diagnóstico inicial

Se aplicó el instrumento de caracterización para identificar conocimientos previos relacionados con identidad digital, protección de datos y ciberseguridad preventiva.

Fase 2. Diseño e implementación de la estrategia

Se elaboró y socializó el manual Concientización en Seguridad Digital: Una Guía Teórica y Práctica basada en Ciberseguridad Preventiva, incorporando contenidos orientados a la prevención de riesgos digitales y fortalecimiento de capacidades para la protección de la identidad digital.

Fase 3. Sensibilización y apropiación del conocimiento

Los estudiantes participaron en actividades de reflexión y apropiación de contenidos relacionados con amenazas digitales, buenas prácticas de seguridad y mecanismos de protección de la información.

Fase 4. Evaluación posterior

Se aplicó el instrumento de evaluación para identificar percepciones, prácticas y niveles de sensibilización alcanzados tras la implementación de la estrategia educativa.

Consideraciones éticas

La investigación se clasificó como una actividad educativa sin riesgo, dado que no involucró intervenciones sobre la integridad física o psicológica de los participantes, la participación fue voluntaria y los creadores de oportunidades “estudiantes” fueron informados sobre los objetivos académicos de la estrategia.

Durante el proceso se registraron nombres y correos electrónicos institucionales únicamente con fines de control de participación, posteriormente, la información fue anonimizada para garantizar la confidencialidad de los datos durante el análisis y presentación de resultados.

El tratamiento de la información se realizó conforme a los principios establecidos en la Ley 1581 de 2012, relacionada con la protección de datos personales en Colombia (Congreso de Colombia, 2012), y en concordancia con los lineamientos nacionales de confianza y seguridad digital establecidos en el CONPES 3995 de 2020 (Consejo Nacional de Política Económica y Social [CONPES], 2020).

Plan de análisis de datos

La información recopilada fue consolidada y procesada mediante técnicas de estadística descriptiva.

Se calcularon frecuencias absolutas, porcentajes y distribuciones de respuesta para cada una de las variables analizadas. Los resultados obtenidos permitieron identificar tendencias relacionadas con la percepción de vulnerabilidad digital, la protección de la identidad digital, la adopción de prácticas seguras y la valoración de la estrategia de apropiación social del conocimiento.

Resultados y discusión

Caracterización de los participantes

La evaluación posterior contó con la participación de 59 estudiantes del programa de Ingeniería de Sistemas y Computación de la Universidad de Cundinamarca. Respecto al nivel de experiencia digital reportado por los participantes, se identificó un predominio de niveles intermedios y altos de familiaridad con herramientas tecnológicas y entornos digitales. Específicamente, el 50,8 % manifestó poseer un nivel intermedio de experiencia digital, el 35,6 % un nivel alto y el 8,5 % un nivel muy alto, mientras que únicamente el 5,1 % reportó un nivel bajo.

Tabla 1.

Nivel de experiencia digital de los participantes

Nivel de experiencia digital	Frecuencia	Porcentaje (%)
Bajo	3	5,1
Intermedio	30	50,8
Alto	21	35,6
Muy alto	5	8,5

Total	59	100
-------	----	-----

Nota. Elaboración propia a partir de los resultados de la evaluación posterior.

Los resultados evidencian que la mayoría de los participantes interactúa frecuentemente con tecnologías digitales. Sin embargo, diversos estudios han demostrado que la experiencia tecnológica no necesariamente se traduce en comportamientos seguros frente a amenazas cibernéticas, razón por la cual la alfabetización digital debe complementarse con procesos específicos de sensibilización en seguridad digital y protección de la información (Barragán-Sánchez & Murta, 2024).

Percepción de vulnerabilidad frente a amenazas digitales

Uno de los propósitos de la estrategia educativa consistió en fortalecer la conciencia sobre los riesgos asociados al entorno digital. Los resultados muestran que el 47,5 % de los participantes se considera moderadamente vulnerable frente a amenazas como phishing, malware o robo de identidad, mientras que el 23,7 % se percibe vulnerable o muy vulnerable.

Tabla 2
Percepción de vulnerabilidad frente a amenazas digitales

Nivel de vulnerabilidad	Frecuencia	Porcentaje (%)
Nada vulnerable	4	6,8
Poco vulnerable	13	22
Moderadamente vulnerable	28	47,5
Vulnerable	10	16,9
Muy vulnerable	4	6,8

Total	59	100
-------	----	-----

Nota. Elaboración propia.

En conjunto, el 71,2 % de los participantes reconoce algún grado de exposición a riesgos digitales. Este resultado coincide con investigaciones recientes que señalan que la percepción del riesgo constituye uno de los principales factores asociados a la adopción de comportamientos preventivos en materia de seguridad digital (Ahamed, 2024). La literatura especializada indica que los usuarios que reconocen su vulnerabilidad frente a amenazas digitales presentan una mayor disposición para implementar mecanismos de protección y adoptar prácticas seguras de navegación.

Conciencia sobre riesgos asociados a ingeniería social

La ingeniería social representa actualmente una de las principales amenazas para la seguridad de la información debido a que explota factores humanos más que vulnerabilidades tecnológicas. Al consultar a los participantes sobre la relación entre la exposición de información personal en redes sociales y la posibilidad de sufrir ataques de ingeniería social, el 83,1 % manifestó estar de acuerdo o totalmente de acuerdo con dicha afirmación.

Tabla 3.

Relación entre exposición de información personal e ingeniería social

Respuesta	Frecuencia	Porcentaje (%)
Neutral	9	15,3

De acuerdo	24	40,7
Totalmente de acuerdo	25	42,4
Total	58	100

Nota. Elaboración propia.

Este hallazgo evidencia una comprensión significativa sobre los riesgos derivados de la sobreexposición digital. Camacho et al. (2024) señalan que la falta de conciencia sobre la información compartida en entornos digitales constituye uno de los principales factores que facilitan ataques basados en phishing y manipulación psicológica. En consecuencia, los resultados sugieren que la estrategia educativa contribuyó a fortalecer la comprensión de los participantes sobre la importancia de proteger la información personal en plataformas digitales.

Gestión de contraseñas y protección de credenciales

La gestión adecuada de credenciales continúa siendo uno de los principales desafíos para la seguridad digital, los resultados muestran que el 71,2 % de los participantes reutiliza contraseñas al menos ocasionalmente en diferentes servicios digitales.

Tabla 4.
Frecuencia de reutilización de contraseñas

Frecuencia	Frecuencia	Porcentaje (%)
Nunca	6	10,2
Rara vez	11	18,6
Algunas veces	19	32,2
Frecuentemente	16	27,1

Siempre	7	11,9
Total	59	100

Nota. Elaboración propia.

Aunque los participantes evidencian niveles importantes de conocimiento sobre riesgos digitales, persiste una brecha entre la comprensión conceptual y la implementación efectiva de prácticas seguras, este resultado coincide con investigaciones desarrolladas en contextos universitarios que identifican la reutilización de contraseñas como una de las principales vulnerabilidades asociadas al factor humano (Goliath et al., 2024). La evidencia científica sugiere que las estrategias educativas deben orientarse no solamente a la transmisión de conocimientos, sino también a la transformación de hábitos y comportamientos relacionados con la seguridad digital.

Uso de autenticación multifactor

La autenticación multifactor es considerada uno de los mecanismos más efectivos para reducir el riesgo de accesos no autorizados, los resultados muestran que únicamente el 16,9 % de los participantes la utiliza de forma permanente.

Tabla 5.
Uso de autenticación multifactor

Frecuencia	Frecuencia	Porcentaje (%)
Nunca	2	3,4
Rara vez	8	13,6

Algunas veces	22	37,3
Frecuentemente	17	28,8
Siempre	10	16,9
Total	59	100

Nota. Elaboración propia.

Aunque el 82,9 % reportó utilizar este mecanismo al menos ocasionalmente, la adopción sistemática continúa siendo limitada; estudios recientes destacan que la autenticación multifactor constituye uno de los controles más eficaces para prevenir incidentes derivados de filtraciones de credenciales y ataques de ingeniería social (Prümmer et al., 2024). Por tanto, fortalecer su adopción representa una oportunidad de mejora para futuras estrategias institucionales de seguridad digital.

Verificación de enlaces sospechosos y prevención del phishing

Los resultados muestran que únicamente el 47,5 % de los participantes verifica enlaces sospechosos de manera frecuente o permanente antes de acceder a ellos.

Tabla 6.

Verificación de enlaces sospechosos

Frecuencia	Frecuencia	Porcentaje (%)
Nunca	1	1,7
Rara vez	10	16,9
Algunas veces	20	33,9
Frecuentemente	19	32,2
Siempre	9	15,3

Total	59	100
-------	----	-----

Nota. Elaboración propia.

La literatura especializada ha identificado el phishing como una de las amenazas más frecuentes en entornos académicos debido a la dependencia de plataformas digitales para la comunicación y gestión de información (Tomalá-Domínguez, 2024), en este sentido, los resultados evidencian avances en la sensibilización de los estudiantes, aunque persisten oportunidades para fortalecer prácticas preventivas relacionadas con la identificación de contenidos fraudulentos.

Valoración de la estrategia de apropiación social del conocimiento

Uno de los hallazgos más relevantes corresponde a la valoración otorgada por los participantes a la estrategia educativa implementada.

Tabla 7.

Valoración de la estrategia educativa

Valoración	Frecuencia	Porcentaje (%)
Nada pertinente	1	1,7
Poco pertinente	1	1,7
Moderadamente pertinente	14	23,7
Pertinente	25	42,4
Muy pertinente	16	27,1
Total	57	100

Nota. Elaboración propia.

Los resultados muestran que el 69,5 % calificó la estrategia como pertinente o muy pertinente, mientras que el 93,2 % emitió una valoración favorable al incluir la categoría moderadamente pertinente. Estos resultados respaldan el potencial de la apropiación social del conocimiento como mecanismo para fortalecer la cultura de ciberseguridad preventiva en educación superior. Diversos estudios coinciden en que los procesos educativos orientados a la sensibilización y apropiación de conocimientos contribuyen significativamente al desarrollo de comportamientos seguros y a la reducción de vulnerabilidades asociadas al factor humano (MinCiencias, 2022; Camacho et al., 2024), (Holman Reyes Puentes et al., 2026).

En conjunto, los hallazgos permiten afirmar que la estrategia implementada favoreció procesos de sensibilización relacionados con la protección de la identidad digital, el reconocimiento de amenazas asociadas a ingeniería social y la adopción de prácticas orientadas a la prevención de riesgos digitales, estos resultados evidencian la pertinencia de integrar iniciativas de apropiación social del conocimiento dentro de las estrategias institucionales de formación en seguridad digital, contribuyendo al fortalecimiento de comunidades académicas más conscientes, resilientes y preparadas frente a los desafíos de la transformación digital.

Conclusiones

Los resultados obtenidos evidencian que la transformación digital ha incrementado la necesidad de fortalecer capacidades relacionadas con la protección de la identidad digital y la prevención de riesgos asociados a la interacción en entornos virtuales; aunque los participantes reportaron niveles intermedios y altos de experiencia digital, los hallazgos muestran que esta familiaridad tecnológica no garantiza la adopción sistemática de prácticas seguras frente a amenazas como phishing, ingeniería social o robo de credenciales. Este resultado coincide con investigaciones recientes que destacan la existencia de brechas entre el conocimiento tecnológico y los comportamientos efectivos de ciberseguridad (Ahamed, 2024; Goliath et al., 2024).

La estrategia de apropiación social del conocimiento basada en el manual Concientización en Seguridad Digital: Una Guía Teórica y Práctica basada en Ciberseguridad Preventiva contribuyó al fortalecimiento de la sensibilización frente a riesgos digitales, favoreciendo la comprensión de conceptos relacionados con identidad digital, protección de datos personales, autenticación multifactor e ingeniería social, los resultados muestran que una proporción significativa de los participantes reconoce la relación entre la exposición de información personal y la posibilidad de sufrir ataques basados en manipulación psicológica, evidenciando avances en la construcción de una cultura de protección digital.

No obstante, persisten prácticas que incrementan la vulnerabilidad frente a incidentes de seguridad, especialmente aquellas relacionadas con la reutilización de contraseñas, la adopción limitada de mecanismos de autenticación multifactor y la verificación inconsistente de enlaces sospechosos, estos hallazgos reflejan la necesidad de fortalecer procesos continuos de formación que promuevan cambios de comportamiento y no únicamente la adquisición de conocimientos conceptuales sobre seguridad informática.

La apropiación social del conocimiento demostró ser una estrategia pertinente para acercar conceptos especializados de ciberseguridad a contextos educativos universitarios, la valoración positiva otorgada por los participantes evidencia que este tipo de iniciativas favorece la comprensión de amenazas digitales y fortalece la adopción de prácticas orientadas a la prevención y protección de la información personal (Carlomagno Sancho Noriega et al., 2026).

Asimismo, el estudio confirma la importancia de incorporar la ciberseguridad preventiva como componente transversal dentro de los procesos formativos de la educación superior, la protección de la identidad digital, la gestión segura de credenciales y la comprensión de riesgos asociados a ingeniería social constituyen competencias fundamentales para la formación de ciudadanos digitales responsables en escenarios caracterizados por una creciente dependencia tecnológica.

Finalmente, se concluye que las estrategias de apropiación social del conocimiento pueden contribuir significativamente al fortalecimiento de la cultura de ciberseguridad en las instituciones de educación superior, promoviendo comunidades académicas más conscientes, resilientes y preparadas para enfrentar los desafíos derivados de la transformación digital.

Limitaciones del estudio

La presente investigación presenta algunas limitaciones que deben considerarse para la interpretación de los resultados, en primer lugar, la experiencia se desarrolló con estudiantes pertenecientes a un único programa académico de una institución de educación superior, lo que limita la generalización de los hallazgos a otros contextos educativos.

En segundo lugar, los instrumentos aplicados durante las fases diagnóstica y de evaluación posterior tuvieron propósitos diferentes, mientras el diagnóstico inicial se orientó a identificar conocimientos relacionados con seguridad digital, la evaluación posterior se centró en percepciones y prácticas asociadas a la protección de la identidad digital, situación que restringe la realización de comparaciones estadísticas directas entre ambas mediciones.

Adicionalmente, la información analizada corresponde a respuestas autorreportadas por los participantes, lo que puede introducir sesgos asociados a la percepción individual o a la deseabilidad social, por esta razón, futuras investigaciones podrían incorporar metodologías

mixtas que permitan complementar los resultados cuantitativos con evidencia cualitativa relacionada con comportamientos y experiencias de los usuarios frente a amenazas digitales.

Implicaciones prácticas

Los resultados obtenidos permiten recomendar la incorporación de programas permanentes de sensibilización en ciberseguridad dentro de las instituciones de educación superior, especialmente en programas académicos que hacen uso intensivo de tecnologías digitales.

Asimismo, se recomienda fortalecer estrategias orientadas a promover el uso de autenticación multifactor, gestores de contraseñas, protección de la identidad digital y mecanismos de prevención frente a ataques de ingeniería social. Estas acciones pueden contribuir significativamente a la reducción de riesgos asociados al factor humano y al fortalecimiento de la cultura institucional de seguridad digital.

La experiencia desarrollada puede servir como referente para otras universidades interesadas en implementar procesos de apropiación social del conocimiento orientados a la promoción de buenas prácticas de ciberseguridad y protección de datos personales.

Agradecimientos

Las autoras expresan su agradecimiento a la Universidad de Cundinamarca y al Programa de Ingeniería de Sistemas y Computación por el apoyo brindado para el desarrollo de la estrategia

educativa y la implementación de las actividades de apropiación social del conocimiento en ciberseguridad preventiva.

Asimismo, agradecen a los estudiantes participantes por su disposición, compromiso y contribución al fortalecimiento de una cultura de protección digital en el contexto universitario.

Referencias bibliográficas

- Afolalu, O., et al. (2025). *Cybersecurity in higher education institutions: A systematic review. Future Internet*, 17(12), 575.
- Ahamed, B. (2024). *The role of cybersecurity attitude in the 4.0 industrial revolution: Examining knowledge, password security and awareness among university students. SAGE Open*, 14(1).
- Bal, E. (2024). *The implementation of a sustainable online course for digital citizenship in higher education. Sustainability*, 16(1), 445.
- Barragán-Sánchez, R., & Murta, L. M. (2024). La seguridad en Internet como parte de la competencia digital ciudadana: revisión sistemática. *Linguagem e Tecnologia*, 17, e51787.
- Camacho Coronel, A., Erazo Ayón, J. M., Salazar Tovar, C., & Pardo Centanaro, B. (2024). Ingeniería social: revisión sistemática de phishing y pretexting en plataformas académicas. *Revista Ibérica de Sistemas e Tecnologias de Informação*, E72, 122–136.
- Canham, M., et al. (2024). *Not all victims are created equal: Investigating differential phishing susceptibility*. National Institute of Standards and Technology (NIST).
- Congreso de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial de la República de Colombia.

- Consejo Nacional de Política Económica y Social (CONPES). (2020). *CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital*. Departamento Nacional de Planeación.
- Corradini, I. (2022). *Digital citizenship as a foundation for cybersecurity awareness. Journal of Education and Learning Technologies*.
- Dawkins, S. (2023). *The NIST Phish Scale and cybersecurity awareness*. National Institute of Standards and Technology (NIST).
- European Commission. (2022). *The Digital Competence Framework for Citizens (DigComp 2.2)*. Publications Office of the European Union.
- Giones-Valls, A., & Serrat-Brustenga, M. (2010). La gestión de la identidad digital: una nueva habilidad informacional y digital. *BiD: Textos Universitaris de Biblioteconomia i Documentació*, (24).
- Goliath, S., Tsibolane, P., & Snyman, D. (2024). *Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in higher education*.
- Ministerio de Ciencia, Tecnología e Innovación. (2022). *Lineamientos para la Apropiación Social del Conocimiento en Ciencia, Tecnología e Innovación*. Gobierno de Colombia.
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). *Política de Gobierno Digital*. Gobierno de Colombia.
- Mouwens-Singh, C. (2024). *A narrative review on enhancing cybersecurity in higher education. Expert Journal of Business and Management*, 12(1), 67–73.
- Prümmer, J., et al. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 139, 103756.
- Pulido Córdoba, M. C., Suárez Ávila, G. P., & Samudio López, S. Y. (2025). *Concientización en seguridad digital: Una guía teórica y práctica basada en ciberseguridad preventiva*. Universidad de Cundinamarca.

- Reyes Puentes, H. ., Herrán Cardoso, L. A. ., Feria Rodriguez , A. J., Sancho Noriega, C. ., Lara Vera, M. A. ., Castro Arana, J. L. ., Grimaldo Caviedes, C. ., Lara Meneses, C. E. ., Guayara Ramirez, H. H. ., Feria Cortes, A. J. ., Pava Cortes, A. ., Vásquez Gómez, D. S. ., Gómez Gómez, P. A. ., Salazar Diaz, N. H. ., Aragón Briñez, V. A. ., Parra Patiño, J. M. ., Otavo Morales, C. E. ., Palencia Quezada, J. J. ., Rodríguez Valdés, F. S. ., ... Vega Gomez, Y. . (Eds.). (2026). *Convergencias Académicas: Estudios Multidisciplinarios de Investigación*. Asociación Civil Científica Piensa Diferente. <https://doi.org/10.63526/3gmqgx21>
- Sancho Noriega, C. ., Rodríguez Fuentes, A. ., Feria Rodríguez, Álvaro J. ., Reyes Puentes, H. ., Sevilla Vallejo, S. ., & Sancho Vilchez, A. S. N. . (Eds.). (2026). *IV Congreso Iberoamericano del Pensamiento Transformacional*. Asociación Civil Científica Piensa Diferente. <https://universoliterario.editorialpiensadiferente.com/index.php/home/catalog/book/18>
- Tomalá-Domínguez, J. B. (2024). *Análisis de phishing y técnicas de ingeniería social: estrategias de concientización y prevención de ataques* (Tesis de maestría). Universidad Estatal Península de Santa Elena.
- Vera, M., et al. (2023). Gestión de la identidad digital en estudiantes universitarios: implicaciones para la ciudadanía digital y la protección de datos. *Revista Latinoamericana de Tecnología Educativa*.

Anexos

Conflicto de intereses

Las autoras declaran que no existe ningún conflicto de intereses relacionado con el desarrollo, análisis, interpretación o publicación de los resultados presentados en esta investigación.

Contribuciones de los autores

Sandra Yasmin Samudio López: Lideró la conceptualización de la investigación, el diseño metodológico, y el desarrollo del manual de concientización en seguridad digital y ciberseguridad preventiva como recurso educativo y estrategia de apropiación social del conocimiento, estructuró las estrategias pedagógicas, coordinó la recolección de datos e implementación metodológica, y, participó en la redacción, revisión y ajustes finales del artículo científico y del manual digital para su presentación y sometimiento.

Marcia Catalina Pulido Córdoba: Participó en la implementación de actividades de sensibilización y en la validación técnica del contenido del manual digital, apoyó en el diseño de instrumentos de recolección de datos, la revisión metodológica y la interpretación de

resultados, colaboró en la redacción del artículo, así como en la revisión y ajustes previos a su sometimiento.

Gina Paola Suárez Ávila: Contribuyó al diseño de contenidos educativos y al desarrollo del recurso digital, apoyó en la implementación de la estrategia de apropiación social del conocimiento y la organización de la información recolectada, participó en la sistematización de evidencias y resultados, y, en la revisión de ajustes finales del artículo y del manual para presentación y sometimiento.