Fecha de presentación: agosto, 2024, **Fecha de Aceptación**: septiembre, 2024, **Fecha de publicación**: octubre, 2024

07

CAMPAÑA INFORMATIVA SOBRE LA SEGURIDAD CIBERNÉTICA PARA ESTUDIANTES DE UNA UNIDAD EDUCATIVA

INFORMATION CAMPAIGN ON CYBER SECURITY FOR STUDENTS OF AN EDUCATIONAL UNIT

Luis Javier Molina Chalacán [1*]
Email: uq.luismolina@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-3755-2717
Edmundo José Jalón Arias [1]
Email: uq.edmundojalon@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-3060-736X
Luis Orlando Albarracín Zambrano[1]
Email: uq.luisalbarracin@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-3164-5229
*Autor para correspondencia
[1] Universidad Regional Autónoma de Los Andes, Quevedo. Ecuador.

Cita sugerida (APA, séptima edición)

Molina Chalacán, L. J., Jalón Arias, E. J., y Albarracín Zambrano, L. O. (2024). Campaña informativa sobre la seguridad cibernética para estudiantes de una unidad educativa. *Revista Conrado, 20*(S1), 60-67.

RESUMEN

La investigación ha abordado la creciente vulnerabilidad de los estudiantes de la Unidad Educativa Particular frente a ataques cibernéticos, dado su uso intensivo de tecnología y su falta de conocimientos en ciberseguridad. El objetivo principal fue evaluar y mejorar el conocimiento y las prácticas de ciberseguridad entre estos estudiantes mediante una campaña informativa. La metodología empleada combinó enfoques cuantitativos y cualitativos con un diseño descriptivo, utilizando encuestas para recopilar datos sobre las prácticas y percepciones de los estudiantes en relación con la ciberseguridad. Se analizaron teorías relacionadas con la ciberseguridad y se evaluaron los conocimientos actuales de los estudiantes. Los instrumentos de recolección de datos incluyeron hojas de observación, listas de verificación, cuestionarios y grabadoras de voz, utilizando Google Forms y la escala de Likert para obtener respuestas homogéneas. Los resultados más destacados mostraron que una mayoría significativa de estudiantes no implementaba regularmente medidas de ciberseguridad, como el uso de contraseñas seguras y la realización de copias de seguridad. Las principales conclusiones y recomendaciones incluyeron la necesidad de una mayor concienciación y educación en ciberseguridad, sugiriendo la integración de estos contenidos en los programas educativos. Se propuso una campaña informativa dirigida a los estudiantes de la UEPAC para fortalecer sus habilidades y conocimientos en ciberseguridad. Este trabajo destacó la urgencia de fomentar una cultura de protección de datos y la colaboración entre instituciones educativas, empresas y gobiernos para construir un entorno digital más seguro.

Palabras clave:

Estudiantes, seguridad, protección de datos, ciberdelincuencia.

ABSTRACT

The research addressed the growing vulnerability of students at educative center to cyberattacks, given their intensive use of technology and lack of cybersecurity knowledge. The main objective was to evaluate and improve the cybersecurity knowledge and practices among these students through an informational campaign. The methodology employed combined quantitative and qualitative approaches with a descriptive design, using surveys to collect data on student's practices and perceptions regarding cybersecurity. Theories related to cybersecurity were analyzed, and student's current knowledge was assessed. Data collection instruments included observation sheets, checklists, questionnaires, and voice recorders, using Google Forms and the Likert scale to obtain homogeneous responses. The most notable results showed that a significant majority of students did not regularly implement cybersecurity measures, such as using secure passwords and performing backups. The main conclusions and recommendations included the need for greater awareness and education in cybersecurity, suggesting the integration of these contents into educational programs. An informational campaign aimed at UEPAC

students was proposed to strengthen their cybersecurity skills and knowledge. This work highlighted the urgency of promoting a culture of data protection and collaboration between educational institutions, businesses, and governments to build a safer digital environment.

Keywords:

Students, security, data protection, cybercrime.

INTRODUCCIÓN

Ecuador se sitúa en la sexta posición en América Latina respecto al compromiso con la seguridad cibernética. El país dispone de una Estrategia Nacional de Ciberseguridad que incluye seis pilares de acción: gobernanza, resiliencia cibernética, prevención y lucha contra la ciberdelincuencia, ciberdefensa, habilidades y capacidades en ciberseguridad, y cooperación internacional. No obstante, los ciberataques han incrementado en las últimas décadas, impactando tanto a instituciones públicas como privadas (Méndez, 2021).

Las decisiones para establecer un entorno digital seguro son vitales en un mundo cada vez más interconectado y dependiente de la tecnología (Fernández y Herrera, 2020). Entre estas medidas se encuentra la implementación de sistemas de firewall para prevenir accesos no autorizados y la instalación de software antivirus que detecte y elimine programas maliciosos (Taherdoost, 2022). Además, la seguridad de la red es fundamental para proteger la integridad y confidencialidad de la información que se transmite. Es también vital educar a los usuarios sobre la identificación de correos electrónicos de phishing y la importancia de utilizar contraseñas seguras y cambiarlas periódicamente (Cando-Segovia y Chicaiza, 2021).

Tipos de Ciberseguridad:

La seguridad de la red: protege la infraestructura contra accesos no autorizados, ataques y abusos mediante firewalls, sistemas de detección y prevención de intrusos (IDS/IPS) y VPNs, monitoreando el tráfico en tiempo real para detectar y responder a amenazas.

La seguridad de la información: se centra en proteger la confidencialidad, integridad y disponibilidad de la información mediante cifrado, gestión de accesos y políticas de control de datos, asegurando que solo personas autorizadas tengan acceso.

La seguridad de aplicaciones: protege las aplicaciones durante todo su ciclo de vida mediante análisis de vulnerabilidades, pruebas de seguridad y desarrollo seguro de software, incluyendo prácticas de parcheo y actualización continua (Aguilar Antonio, 2021).

La seguridad de endpoints: protege dispositivos individuales como ordenadores, smartphones y tablets utilizando antivirus, antimalware y soluciones de gestión de dispositivos móviles (MDM), monitoreando y protegiendo contra amenazas que puedan comprometer los dispositivos.

La seguridad en la nube: protege datos y aplicaciones en servicios de nube mediante controles de acceso, cifrado de datos y cumplimiento con normativas, asegurando la gestión de identidades y accesos (IAM) y la seguridad de la infraestructura cloud.

La seguridad de Internet de las Cosas (IoT): protege los dispositivos IoT y sus redes mediante autenticación segura, cifrado y actualizaciones regulares de firmware, monitoreando y gestionando el tráfico de datos de los dispositivos IoT para prevenir ataques.

La seguridad operacional: asegura los procesos y procedimientos para manejar y proteger datos mediante políticas de seguridad, auditorías regulares y gestión de riesgos, incluyendo la formación y concienciación del personal sobre buenas prácticas de seguridad.

La seguridad física: protege los equipos y las instalaciones mediante controles de acceso físico, cámaras de vigilancia y sistemas de alarma, asegurando que solo el personal autorizado pueda acceder a los equipos y datos sensibles. Cada tipo de ciberseguridad es necesaria para proteger los sistemas informáticos y la información, garantizando un entorno digital seguro y confiable (Aguilar Antonio, 2021; Concepción Donoso, 2022; Suárez et al., 2024).

La seguridad en la nube debe ser priorizada, asegurando que los datos almacenados en servicios de computación en la nube estén protegidos contra accesos no autorizados. Asimismo, la actualización regular de software y sistemas operativos cierra vulnerabilidades explotables por atacantes. Estas acciones combinadas crean una defensa fuerte y segura contra las ciberamenazas, promoviendo un entorno digital más seguro y confiable (Villacís, 2022). En este contexto, es necesario fomentar una cultura de protección de datos e implementar políticas claras y específicas en todos los niveles, tanto gubernamentales como privados. Además, es esencial integrar la ciberseguridad en los programas educativos (Astorga-Aguilar y Schmidt-Fonseca, 2019).

En la Unidad Educativa Particular Abdón Calderón, los estudiantes de tercer año de bachillerato utilizan la tecnología para diversos procesos, tanto educativos como

personales, incluyendo juegos, lo que los expone a los peligros de ataques en línea. Sin embargo, se sabe empíricamente que sus conocimientos en materia de seguridad contra ataques informáticos son escasos o nulos, lo que los convierte en objetivos fáciles para diversos delitos cibernéticos desde el internet. Este estudio tiene como objetivo llevar a cabo un análisis detallado de las políticas de protección de datos, las medidas de prevención de amenazas cibernéticas, en una institución educativa.

Para desarrollar la investigación se proponen los siguientes objetivos específicos:

- Analizar las teorías relacionadas con la ciberseguridad y la creación de un entorno digital seguro.
- Evaluar el nivel de conocimientos actuales que tienen los estudiantes sobre ciberseguridad.
- Desarrollar una campaña informativa sobre ciberseguridad dirigida a los estudiantes de bachillerato de la Unidad Educativa Particular Abdón Calderón (UEPAC) para mejorar su comprensión y habilidades en este campo.

MATERIALES Y MÉTODOS

Se empleó un enfoque de investigación cuantitativo-cualitativo, con un diseño descriptivo, para recopilar datos a través de encuestas y proceder a su análisis e interpretación. Este enfoque permitió cuantificar, analizar y determinar la falta de conocimientos en ciberseguridad presentes en el alumnado, obteniendo datos estadísticos de la muestra encuestada. Detallando a quienes afecta, el número de personas afectadas y en qué magnitud incide la ciberseguridad en los estudiantes de tercer año de bachillerato de la UEPAC en el año 2023.

Según (Alban et al., 2020), la investigación descriptiva es un tipo de investigación que tiene como objetivo explicar las características fundamentales de un conjunto homogéneo de fenómenos. Utiliza criterios que preservan la estructura y el comportamiento de los fenómenos involucrados en el estudio y proporciona información que puede compararse con otras fuentes. Este tipo de investigación permitió recopilar datos detallados sobre las prácticas de seguridad cibernética de los estudiantes, sus percepciones de las amenazas en línea y su nivel de conocimiento en esta área. Estos datos descriptivos actuaron como una base sólida para identificar patrones, áreas problemáticas y puntos de partida para futuras intervenciones.

La investigación de campo permitió usar técnicas de recolección de datos como encuestas y estudios. La investigación bibliográfica proporcionó información sobre el contexto de la ciberseguridad, así como sobre las prácticas y estrategias en este ámbito. La investigación histórica proporcionó información sobre la historia de la ciberseguridad y su relación con los estudiantes y un entorno digital seguro.

El método deductivo-inductivo se utilizó para investigar por qué los estudiantes de tercer año de bachillerato en la UEPAC en 2023 carecían de conciencia sobre ciberseguridad y determinar las consecuencias que enfrentaban. La investigación utilizó un enfoque inductivo para identificar los aspectos más comunes y profundamente arraigados de la ciberseguridad entre esta población estudiantil. El método analítico-sintético permitió reconocer la importancia de esta problemática, identificar a los actores involucrados y entender la relación entre la ciberseguridad y un entorno seguro.

Se emplearon diversas técnicas para la recopilación de información en la investigación: la observación, la encuesta y la entrevista. La observación implicó registrar sistemáticamente información visual de forma objetiva. Las encuestas recopilaron datos descriptivos a través de un cuestionario estructurado y las entrevistas implicaron discusiones cara a cara para comprender las perspectivas de los estudiantes sobre ciberseguridad.

Se utilizaron varios instrumentos para la recopilación de datos: la hoja de observación, que fue fundamental para recopilar datos cualitativos sobre el comportamiento de los estudiantes en el entorno digital; el cuestionario, que proporcionó información valiosa sobre las actitudes y prácticas de los estudiantes en relación con la ciberseguridad y la técnica de la hoja de encuesta, que proporcionó información estandarizada para la comparación y el análisis estadístico de las respuestas. En las encuestas, se utilizó Google Forms y la escala de Likert para recolectar respuestas homogéneas a las preguntas realizadas.

Población y muestra:

Los alumnos de tercer año de bachillerato cuya población total es de 82, quedando la misma cantidad de individuos en la muestra. Tabla 1

Tabla 1: Población y muestra

Curso/Paralelo	Estudiantes
3ero BGU “A”	27
3ero BGU “B”	29
3ero BGU “C”	26
Total	82

Fuente: matrícula de la institución. Nota: elaboración propia

RESULTADOS

Una vez realizadas las encuestas a los estudiantes, se ha considerado según la escala de Likert que para calcular el porcentaje de encuestados que están de acuerdo, se suman los porcentajes de "Indeciso", "De acuerdo" y "Totalmente en acuerdo". Para los que están en desacuerdo, se sumaron los porcentajes de "Totalmente en desacuerdo" y "En desacuerdo". Con esta aclaración se han presentado los siguientes resultados:

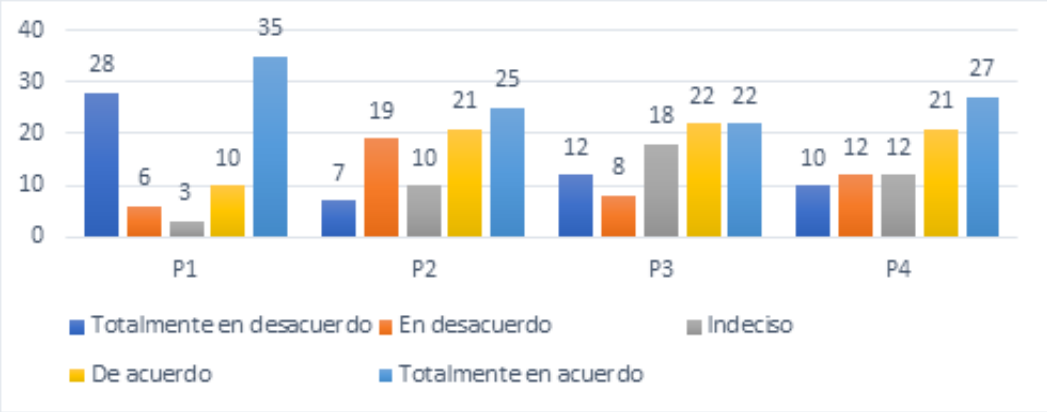
Categoría 1: Conocimientos sobre Ciberseguridad Tabla 1. Figura 1

Tabla 2: Preguntas Categoría 1

Repuestas	Preguntas							
	P1	P2	P3	P4	P1%	P2%	P3%	P4%
Totalmente en desacuerdo	28	7	12	10	34,15	8,54	14,63	12,20
En desacuerdo	6	19	8	12	7,32	23,17	9,76	14,63
Indeciso	3	10	18	12	3,66	12,20	21,95	14,63
De acuerdo	10	21	22	21	12,20	25,61	26,83	25,61
Totalmente en acuerdo	35	25	22	27	42,68	30,49	26,83	32,93
Total	82	82	82	82	100	100	100	100

Fuente: Elaboración propia

Fig. 1: Categoría 1 y sus preguntas



Fuente: Respuestas de la encuesta. Nota: elaboración propia

Pregunta 1: ¿La implementación de contraseñas seguras es una medida efectiva para proteger los datos personales en línea?

El 58.54% de los encuestados están de acuerdo o indecisos respecto a la efectividad de la implementación de contraseñas seguras para proteger los datos personales en línea. Este resultado sugiere que existe una cierta confianza o al menos una consideración de la importancia de utilizar contraseñas seguras. Sin embargo, el 41,46% de los encuestados expresaron desacuerdo o total desacuerdo con esta afirmación, lo que indica que hay una parte significativa de la muestra que puede cuestionar la eficacia de esta medida de seguridad.

Pregunta 2: ¿Los ataques de phishing representan una amenaza significativa para la seguridad informática?

El 68.29% de los encuestados están de acuerdo o indecisos respecto a la amenaza significativa que representan los ataques de phishing para la seguridad informática. Esta alta proporción de acuerdo sugiere un reconocimiento generalizado de la seriedad y el impacto de los ataques de phishing en la seguridad cibernética. Solo alrededor del 31.71% de los encuestados expresaron desacuerdo o total desacuerdo con esta afirmación, lo que indica que la mayoría reconoce la importancia de abordar este tipo de amenazas.

Pregunta 3: ¿La ciberseguridad se enfoca en proteger sistemas y redes informáticas contra amenazas y ataques cibernéticos?

El 75.61% de los encuestados están de acuerdo o indecisos respecto a que la ciberseguridad se enfoca en proteger sistemas y redes informáticas contra amenazas y ataques cibernéticos. Este resultado sugiere un fuerte consenso sobre el propósito principal de la ciberseguridad. Solo alrededor del 24.39% de los encuestados expresaron desacuerdo o total desacuerdo con esta afirmación, lo que indica que la gran mayoría reconoce el objetivo central de la ciberseguridad.

Pregunta 4: ¿Cuán efectivos consideras que son tus conocimientos sobre ciberseguridad en proteger tus dispositivos y datos personales?

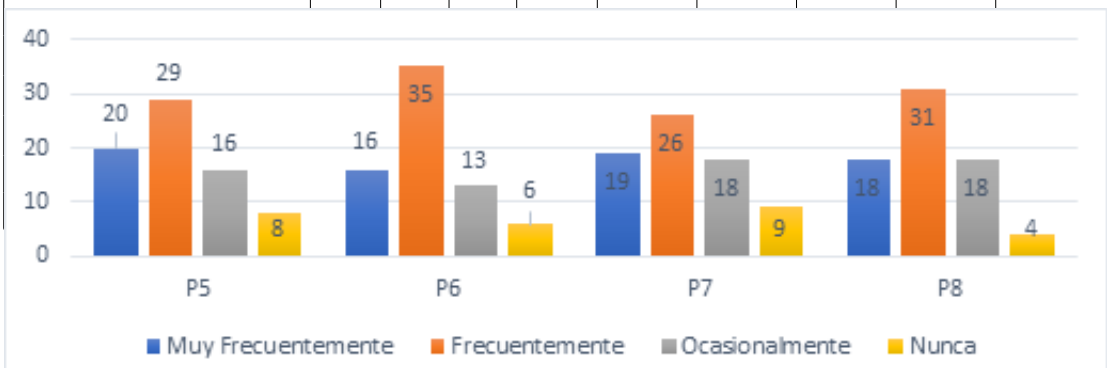
El 73.17% de los encuestados están de acuerdo o indecisos respecto a la efectividad de sus conocimientos sobre ciberseguridad para proteger sus dispositivos y datos personales. Este resultado sugiere una cierta confianza o al menos una consideración de la importancia de contar con conocimientos sólidos en ciberseguridad para proteger la información personal. Sin embargo, aproximadamente un 26.83% de los encuestados expresaron desacuerdo o total desacuerdo con esta afirmación, lo que indica que una proporción significativa de la muestra puede no estar segura de la eficacia de sus conocimientos en este ámbito.

En conclusión, la encuesta muestra percepciones diversas sobre la seguridad cibernética, desde la efectividad de las medidas de protección hasta la comprensión general del tema. Aunque hay acuerdo en algunos puntos, también hay diferencias de opinión, subrayando la necesidad de educación continua y concienciación en ciberseguridad.

Categoría 2: Uso de la Ciberseguridad Tabla 3, Figura 2

Tabla 3: Categoría Uso de la Ciberseguridad

Repuestas	Preguntas							
	P5	P6	P7	P8	P5%	P6%	P7%	P8%



Fuente: Respuestas de la encuesta. Nota: elaboración propia

Pregunta 5: ¿Siempre implementa medidas de ciberseguridad para proteger sus dispositivos y datos?

El 37.80% de los encuestados están de acuerdo o indecisos respecto a si suelen utilizar contraseñas fuertes y cambian regularmente sus contraseñas. Esto indica que hay una proporción significativa de encuestados que pueden no estar siguiendo prácticas recomendadas en cuanto a la gestión de contraseñas. Además, el 62.20% restante expresó que no suelen seguir estas prácticas, lo que resalta la importancia de la concienciación y la educación en seguridad de contraseñas.

Pregunta 6: ¿Suele utilizar contraseñas fuertes y cambia regularmente sus contraseñas?

El 37.80% de los encuestados están de acuerdo o indecisos respecto a si suelen utilizar contraseñas fuertes y cambian regularmente sus contraseñas. Esto indica que hay una proporción significativa de encuestados que pueden no estar siguiendo prácticas recomendadas en cuanto a la gestión de contraseñas. Además, el 62.20% restante expresó que no suelen seguir estas prácticas, lo que resalta la importancia de la concienciación y la educación en seguridad de contraseñas.

Pregunta 7: ¿Con qué frecuencia realizas análisis de antivirus y escaneos de malware en tus dispositivos como estudiante?

El 45.12% de los encuestados están de acuerdo o indecisos respecto a la frecuencia con la que realizan análisis de antivirus y escaneos de malware en sus dispositivos. Esto sugiere que hay una variedad de prácticas entre los encuestados en cuanto al mantenimiento de la seguridad de sus dispositivos. Sin embargo, el 54.88% restante expresó que no realizan estos análisis con la frecuencia recomendada, lo que podría aumentar su vulnerabilidad a amenazas cibernéticas.

Pregunta 8: ¿Con qué frecuencia realizas copias de seguridad de tus datos importantes como proyectos académicos y documentos personales?

El 40.24% de los encuestados están de acuerdo o indecisos respecto a la frecuencia con la que realizan copias de seguridad de sus datos importantes. Esto indica que hay una proporción considerable de encuestados que podrían no estar dando prioridad a la protección de sus datos mediante la realización de copias de seguridad regulares. Además, el 59.76% restante expresó que no realizan copias de seguridad con la frecuencia recomendada, lo que podría aumentar el riesgo de pérdida de datos en caso de un incidente de seguridad.

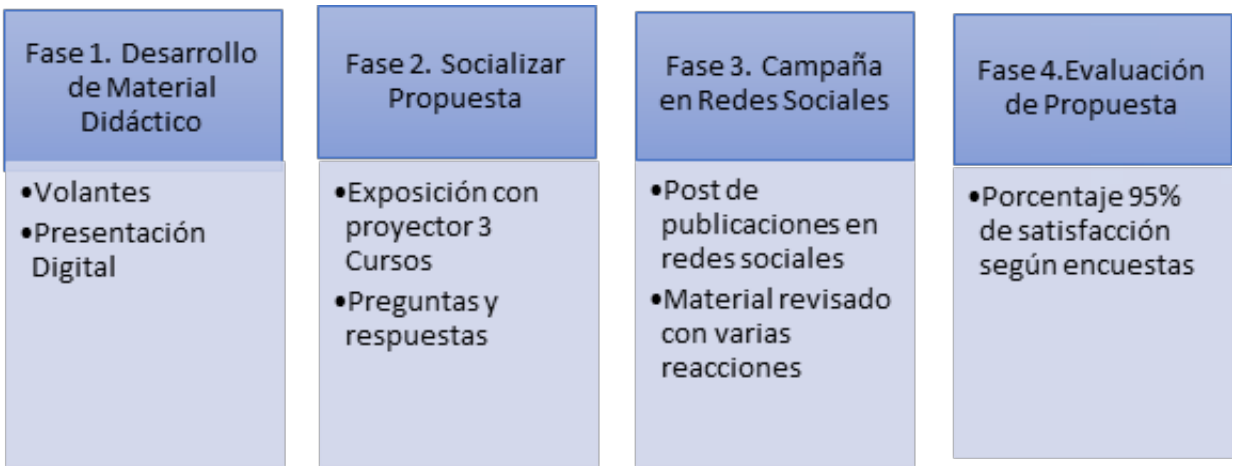
Estos resultados indican áreas de mejora en las prácticas de seguridad cibernética, como la aplicación constante de medidas de seguridad, el uso de contraseñas seguras y la realización regular de copias de seguridad y análisis de antivirus. Las entrevistas revelan la necesidad de incluir ciberseguridad en los contenidos académicos, mantenerse al día con las últimas tendencias en ciberseguridad, y ofrecer consejos a estudiantes interesados en carreras en el campo. Además, se destacan medidas implementadas por la UEPAC para proteger datos sensibles, como sistemas de seguridad avanzados, talleres, y políticas de gestión de contraseñas. Finalmente, se propone un programa integral de concienciación en ciberseguridad para toda la comunidad académica.

Propuesta

Título: Campaña informativa sobre la ciberseguridad para los estudiantes de la UEPAC, con el fin de fortalecer sus conocimientos y habilidades en este ámbito.

Objetivo general: desarrollar una campaña informativa sobre la ciberseguridad, a través de redes sociales y exposiciones presenciales, con el fin de fortalecer los intelectos y habilidades de los estudiantes de la UEPAC ubicada en el cantón Quevedo, 2023. Figura 3

Figura 3: Fases de la Campaña informativa



Fuente: autores de la investigación. Nota: elaboración propia

DISCUSIÓN

La implementación de medidas de ciberseguridad es un aspecto fundamental en la protección de los datos personales en línea y en la prevención de ataques informáticos (Mendivil Caldentey et al., 2022). En los resultados de la encuesta, los estudiantes han mostrado una percepción variada en cuanto a la efectividad de estas medidas, lo que

sugiere la necesidad de un análisis más profundo sobre las prácticas de seguridad en el entorno digital.

En primer lugar, respecto a la implementación de contraseñas seguras, la mayoría de los encuestados (55.87%) han expresado su acuerdo total o parcial sobre su efectividad. Sin embargo, es preocupante que un porcentaje considerable (41.47%) haya manifestado estar en desacuerdo o totalmente en desacuerdo con esta afirmación. Esto indica una posible falta de conciencia sobre la importancia de utilizar contraseñas seguras y la necesidad de promover una mejor educación en este sentido.

Por otro lado, en cuanto a la percepción sobre la amenaza representada por los ataques de phishing, los resultados son igualmente mixtos. Aunque una parte significativa de los encuestados (56.10%) ha reconocido la gravedad de esta amenaza. Un número considerable (31.71%) ha mostrado cierta indecisión o incluso desacuerdo. Esto refleja la necesidad de una mayor sensibilización sobre los riesgos asociados con el phishing y la importancia de adoptar medidas proactivas para prevenirlo.

En relación con la ciberseguridad en general, los resultados muestran una división entre aquellos que reconocen su importancia (53.66%) y aquellos que expresan dudas o desacuerdo (35.39%). Este hallazgo destaca la necesidad de mejorar la comprensión sobre los conceptos fundamentales de la ciberseguridad y su relevancia en la protección de sistemas y datos.

Es importante destacar que estos resultados están en línea con hallazgos de otros estudios realizados en Ecuador y Latinoamérica. Investigaciones previas han identificado una brecha significativa en la conciencia y la práctica de la ciberseguridad en la región, lo que ha llevado a un aumento en los incidentes de ciberataques y violaciones de datos.

Para abordar estos desafíos, es necesario implementar estrategias integrales de educación en ciberseguridad tanto a nivel educativo como empresarial. Esto incluye la inclusión de contenidos relacionados con la ciberseguridad en los programas de estudio, la realización de campañas de sensibilización y la promoción de buenas prácticas de seguridad digital en todos los niveles de la sociedad.

Aunque existen percepciones divergentes sobre la efectividad de las medidas de ciberseguridad, es evidente la necesidad de una mayor conciencia y acción para proteger la información personal y los sistemas en línea. La colaboración entre instituciones educativas, empresas y organismos gubernamentales es fundamental para abordar estos desafíos y construir un entorno digital más seguro y protegido en Ecuador y en toda América Latina.

ONCLUSIONES

La ciberseguridad es un aspecto fundamental en el mundo digital actual, especialmente en entornos educativos como la UEPAC en Ecuador, donde la falta de conciencia y conocimientos entre los estudiantes expone a la comunidad estudiantil a riesgos significativos como ataques cibernéticos y pérdida de datos personales.

La implementación de medidas proactivas, como campañas informativas sobre ciberseguridad, resulta fundamental para abordar la brecha de conocimientos y conciencia identificada en el estudio. Estas iniciativas no solo buscan fortalecer los intelectos y habilidades de los estudiantes en materia de ciberseguridad, sino también crear un entorno digital más seguro y protegido en la institución educativa y más allá.

La colaboración entre instituciones educativas, empresas y entidades gubernamentales es esencial para promover una cultura de seguridad digital y desarrollar estrategias integrales de educación en ciberseguridad. Esta colaboración permitirá abordar los desafíos identificados en el estudio y construir un futuro digital más resiliente y protegido para la sociedad en general.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. ***Estudios internacionales (Santiago)***, ***53***(198), 169-197. https://www.scielo.cl/pdf/rei/v53n198/0719-3769-rei-53-198-00169.pdf

Alban, G. P. G., Arguello, A. E. V., y Molina, N. E. C. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). ***RECIMUNDO***, ***4***(3), 163-173. https://www.recimundo.com/index.php/es/article/view/860

Astorga-Aguilar, C. y Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. ***Revista electrónica educare***, ***23***(3), 339-362. https://www.scielo.sa.cr/pdf/ree/v23n3/1409-4258-ree-23-03-339.pdf

Cando-Segovia, M. R., & Chicaiza, R. P. M. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. ***3 c TIC: cuadernos de desarrollo aplicados a las TIC***, ***10***(1), 17-41. https://dialnet.unirioja.es/servlet/articulo?codigo=7888164

Concepción Donoso, M. (2022). ¿ Cuán importante es la seguridad cibernética para lograr la seguridad hídrica? ***Revista de Ciencias Ambientales***, ***56***(1), 284-297. https://www.scielo.sa.cr/pdf/rca/v56n1/2215-3896-rca-56-01-284.pdf

Fernández, E. E. C. y Herrera, R. d. J. G. (2020). Prevención de riesgos por ciberseguridad desde la auditoría forense: Conjugando el talento humano organizacional. ***NOVUM, revista de Ciencias Sociales Apliacadas***, *1*(10), 61-80. https://www.redalyc.org/journal/5713/571361695004/571361695004.pdf

Méndez, A. E. L. (2021). Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano. ***Polo del Conocimiento: Revista científico-profesional***, *6*(3), 1229-1250. https://dialnet.unirioja.es/servlet/articulo?codigo=7926828

Mendivil Caldentey, J., Sanz Urquijo, B., & Gutierrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. ***Pixel-Bit: Revista de Medios y Educación, 63, 197-225.*** https://idus.us.es/handle/11441/145488

Suárez, G., Starnari, B. F., Venosa, P., & Queiruga, C. (2024). Acercando la ciberseguridad a la escuela secundaria desde una perspectiva lúdica. ***Electronic Journal of SADIO (EJS)***, *23*(2), 132-149. https://ojs.sadio.org.ar/index.php/EJS/article/view/861

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. ***Electronics***, *11*(14), 2181. https://www.mdpi.com/2079-9292/11/14/2181

Villacís, R. P. C. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. ***Revista Tecnológica Ciencia y Educación Edwards Deming***, *6*(1). https://revista-edwardsdeming.com/index.php/es/article/view/88