DOI: https://doi.org/10.56712/latam.v5i2.1910

Ciberseguridad enfocada en el futuro digital de los estudiantes

Cybersecurity focused on the digital future of students

Nathaly Jessenia Pinda Román
njpinda@pucesd.edu.ec
https://orcid.org/0009-0000-6233-7408
Pontificia Universidad Católica del Ecuador sede Santo Domingo
Santo Domingo de los Tsáchilas – Ecuador

Luis Alberto Moya Martínez
lmoya@pucesm.edu.ec
https://orcid.org/0009-0009-4264-6903
Pontificia Universidad Católica del Ecuador sede Manabí
Manabí – Ecuador

Artículo recibido: 15 de marzo de 2024. Aceptado para publicación: 01 de abril de 2024.
Conflictos de Interés: Ninguno que declarar.

Resumen

El presente artículo aborda la creciente importancia de la ciberseguridad en el contexto de protección del futuro digital de los estudiantes, debido al uso de las tecnologías de la información, necesario en el proceso educativo en razón de garantizar la seguridad de los estudiantes. Se examina los riesgos y desafíos específicos que enfrentan los estudiantes en el ciberespacio educativo y propone estrategias innovadoras para mitigar dichos riesgos. El objetivo fue fomentar procesos de prevención, comprensión y habilidades de defensa cibernética entre los estudiantes para instruirlos en el entorno digital en constante evolución, asegurando que estén equipados para enfrentar los desafíos de la integridad digital y contribuir de manera segura y ética al futuro digital, la metodología empleada fue cuali-cuantitativa y mediante la revisión bibliográfica. Los resultados obtenidos indican que es necesario garantizar un entorno digital seguro y útil capaz de proteger la información, para ello se requiere la concienciación y la capacitación continua para mitigar los riesgos cibernéticos en el ámbito educativo donde se ven involucrados los actores principales que son la institución educativa, personal docente y estudiantes. En este artículo se mencionan las responsabilidades de los planteles educativos, los profesores y la industria tecnológica para garantizar un entorno seguro y productivo para los estudiantes. Esto incluye enseñar habilidades críticas de pensamiento, promover el uso ético de la tecnología y la toma de decisiones acertadas en la resolución de problemas de la vida diaria. La investigación concluye destacando la necesidad de enseñar habilidades básicas de seguridad cibernética, como la creación de contraseñas seguras y la identificación de correos electrónicos de phishing y preparar adecuadamente a los estudiantes para los desafíos del futuro.

Palabras clave: protección de datos, informática educativa, cibernética, educación, plataforma digital

Abstract

This article delves into the escalating significance of cybersecurity in safeguarding the digital trajectory of students, prompted by the indispensable role of information technologies in modern education. Ensuring students' safety amidst the pervasive use of digital tools has become paramount

in educational endeavors. This article examines the specific risks and challenges faced by students in educational cyberspace and proposes innovative strategies to mitigate such risks. The objective of this initiative was to cultivate preventive measures, enhance understanding, and instill cyber-defense competencies among students. This aimed to prepare them for the dynamic digital landscape, ensuring they possess the necessary skills to navigate challenges concerning digital integrity responsibly and ethically. The methodology adopted encompassed qualitative and quantitative approaches, complemented by a comprehensive literature review. The results obtained indicate that it is necessary to ensure a safe and useful digital environment capable of protecting information, for this reason, awareness and continuous training is required to mitigate cyber risks in the educational environment where the main actors involved are the educational institution, teaching staff and students. This article discusses the responsibilities of schools, teachers and the technology industry to ensure a safe and productive environment for students. This includes teaching critical thinking skills, promoting the ethical use of technology and sound decision making in solving everyday problems. The research concludes by highlighting the need to teach basic cybersecurity skills, such as creating secure passwords and identifying phishing emails and adequately prepare students for future challenges.

Keywords: data protection, educational computing, cybernetics, education, digital platforms

Cómo citar: Pinda Román, N. J., & Moya Martínez, L. A. (2024). Ciberseguridad enfocada en el futuro digital de los estudiantes. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 5 (2), 701 – 714. https://doi.org/10.56712/latam.v5i2.1910*

INTRODUCCIÓN

La ciberseguridad en la educación es fundamental para garantizar la protección de información sensible, la integridad de los sistemas y la privacidad de los estudiantes y personal educativo. El futuro digital de la sociedad contemporánea cada día es más amplio, en la actualidad existen muchas herramientas tecnológicas digitales que los estudiantes deben utilizar en el proceso de enseñanza aprendizaje, en este contexto los estudiantes son capaces de prepararse en términos como la ciberseguridad, esta se define como la disciplina dentro del ámbito de las ciencias de la computación que se dedica a desarrollar e implementar los mecanismos destinados a resguardar la información y la infraestructura tecnológica (Cando & Medina, 2021).

La historia de la ciberseguridad en la educación es una narrativa que ha evolucionado junto con el crecimiento de la tecnología y la expansión del uso de sistemas informáticos en entornos educativos (Fernández, 2019). La evolución de las Tecnologías de la Información y Comunicación (TIC) plantea continuamente situaciones de riesgo que se van manifestando de manera constante. Si bien las tecnologías emergentes permiten el procesamiento de grandes volúmenes de datos, también facilitan su exposición (Díaz et al., 2019).

A medida que la tecnología educativa continúa avanzando, las instituciones deben adoptar medidas más sólidas para proteger el ambiente digital, cuidar la infraestructura tecnológica y los datos sensibles en el ámbito educativo. Las instituciones educativas enfrentan desafíos cibernéticos cada vez más sofisticados, que incluyen ransomware, phishing y amenazas persistentes avanzadas (López et al., 2022). La ciberseguridad en la educación se ha convertido en una prioridad, con enfoques en la formación de personal, la implementación de tecnologías de seguridad avanzadas y la concienciación continua.

Debido al notable avance tecnológico experimentado en la última década, impulsado por la nueva era digital y la globalización, se ha observado un desarrollo sin precedentes en el ámbito de la protección contra amenazas digitales. Este campo abarca una amplia gama de técnicas y herramientas diseñadas para hacer frente a los riesgos asociados con la tecnología y la comunicación (Cando & Medina, 2021). En este contexto, se destaca la importancia de considerar la seguridad informática como una inversión crucial, subrayando la necesidad de formar expertos en el campo, a quienes se les debería promover activamente su capacitación contra ataques informáticos. Un ataque informático se refiere a la realización de acciones por parte de un individuo o grupo con el propósito de afectar las propiedades de los activos de información de una organización o persona. El riesgo asociado a la seguridad de la información se define como la amenaza de una vulnerabilidad que podría ocasionar pérdida o daño a un activo de información (Bonilla, 2023).

Los dispositivos electrónicos más susceptibles en una red doméstica son las tabletas, teléfonos móviles inteligentes, ordenadores de sobremesa, portátiles y enrutadores, debido a una serie de factores que incluyen la filtración de información, la manipulación de datos, fallos en la interfaz de voz, seguimiento del comportamiento del usuario, interrupciones, y especialmente la autenticación de las cuentas de usuario. Esto se debe a la falta de medidas de seguridad adecuadas, con frecuencia utilizando métodos simples como contraseñas débiles o credenciales predeterminadas, como nombres o fechas de nacimiento (Chhetri & Motti, 2021). Tales prácticas pueden representar un riesgo considerable para la seguridad de la información confidencial por parte del usuario.

La transformación digital en la educación ha generado numerosos beneficios, pero también ha dado lugar a nuevas amenazas y vulnerabilidades, especialmente en lo que respecta a la seguridad de la información. Los estudiantes, que son usuarios activos de plataformas en línea, redes sociales y aplicaciones educativas, están expuestos a riesgos como el robo de identidad, el acoso cibernético y la pérdida de datos sensibles (Peña & García, 2014). Por ello es importante saber cómo la

ciberseguridad se convierte en un componente esencial para salvaguardar la integridad y privacidad de los estudiantes en el entorno digital (Goodman, 2001), por lo que se debe fomentar procesos de prevención, comprensión y habilidades contra ataques cibernéticos, disminuyendo amenazas y desafíos de seguridad informática que enfrentan los estudiantes en la era digital, así como las estrategias y mejores prácticas que deben adoptarse para mitigar estos riesgos (Ribble, 2015).

METODOLOGÍA

La investigación está orientada hacia un enfoque descriptivo que consiste en conocer la información relacionada con la ciberseguridad en entornos educativos, identificando, desafíos y mejores prácticas, para encontrar y precisar las características desde un punto de vista analítico (Díaz et al., 2019).

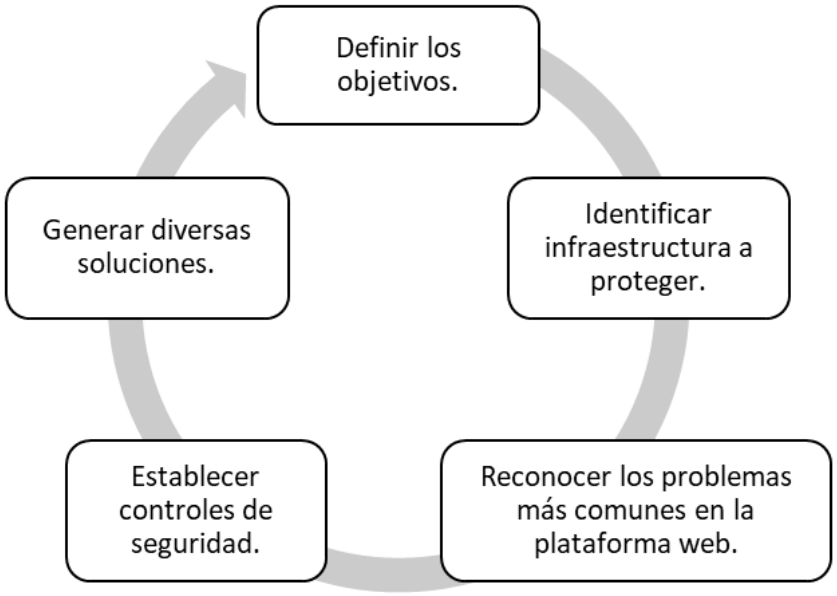
Se empleó la investigación cuali-cuantitativa, donde se analiza el objeto de estudio de manera integrada o completa tomando como referencia la Unidad Educativa Particular Pablo Palacios de Santo Domingo de los Tsáchilas - Ecuador, se pudo recolectar información, utilizando diferentes herramientas de búsqueda; revisión, análisis y síntesis bibliográfica. En donde se llevaron a cabo encuestas a una muestra de 81 personas mediante la aplicación del cálculo de la muestra para una población finita como se indica en la Ecuación 1 (Figueroa et al., 2019) donde se vieron involucrados estudiantes y educadores para comprender las percepciones y experiencias con respecto a la seguridad digital en el ámbito educativo con el objetivo de fomentar habilidades de ciberseguridad para analizar la seguridad de plataformas educativas comúnmente utilizadas, considerando aspectos como autenticación de usuarios y medidas contra malware. La investigación se llevó a cabo de manera virtual mediante un formulario de Google que permite la recopilación y análisis de datos.

RESULTADOS Y DISCUSIÓN

La ciberseguridad en las plataformas web educativas puede ser mejorada a través de un procedimiento que consta de distintos pasos que las unidades educativas deben considerar (Morales & Medina, 2021), tal como se muestra en la figura 1.

Figura 1

Fases del Procedimiento de Gestión



Nota: Este gráfico muestra las fases del procedimiento de gestión que se debe emplear para cuidar los datos de una institución.

Fuente: elaboración propia.

Definir los objetivos

Es importante establecer metas y objetivos a corto, mediano y largo plazo. Así como también elaborar estrategias y tácticas orientadas a la consecución de esos objetivos. De la misma forma crear un plan de acción detallado que incluya plazos y responsabilidades. Y finalmente implementar sistemas de comunicación interna que sean eficaces (Echeverría, 2021).

Identificar estructura a proteger

Se requiere fortalecer estructuras utilizadas y que son blancos de posibles ataques de robo de información tales como: redes, servidores, equipos informáticos y plataformas educativas (Chingo & Gómez, 2021).

Reconocer los problemas más comunes en la plataforma web

Algunos problemas comunes para el robo de información es el uso de contraseñas débiles, uso inadecuado de información confidencial y falta de autenticación de usuario.

Establecer controles de seguridad

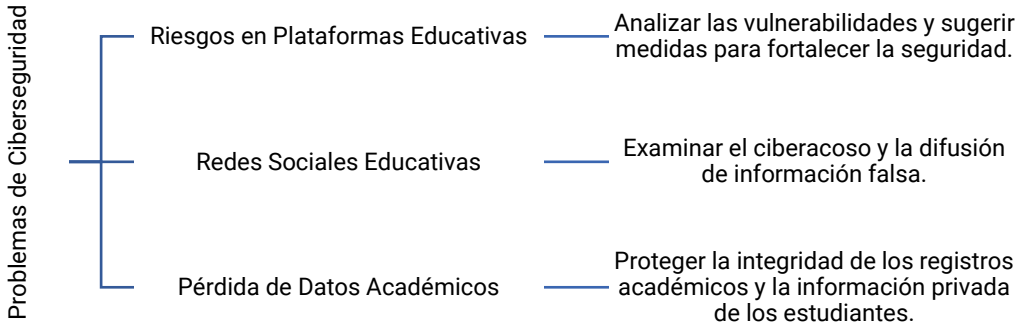
Es necesario configurar firewalls para controlar el tráfico de red y prevenir accesos no autorizados. Además, instalar y mantener actualizado un software antivirus en todos los dispositivos. Así también utilizar cifrado para proteger datos sensibles almacenados en dispositivos. Por último, implementar políticas de control de acceso para limitar la información a la que pueden acceder los usuarios (Pillajo & Avila, 2023).

Generar diversas soluciones

Para generar soluciones se debe fomentar una cultura de ciberseguridad a través de campañas de sensibilización y actividades educativas. También motivar el uso de contraseñas robustas y cambiarlas periódicamente (Echeverría, 2021). Además, establecer y comunicar claramente políticas de seguridad que aborden el uso adecuado de sistemas, dispositivos y datos. Los principales problemas de la ciberseguridad educativa se encuentran presentes en la ilustración 2 que se detalla a continuación (Morales & Medina, 2021).

Figura 2

Problemas de Ciberseguridad



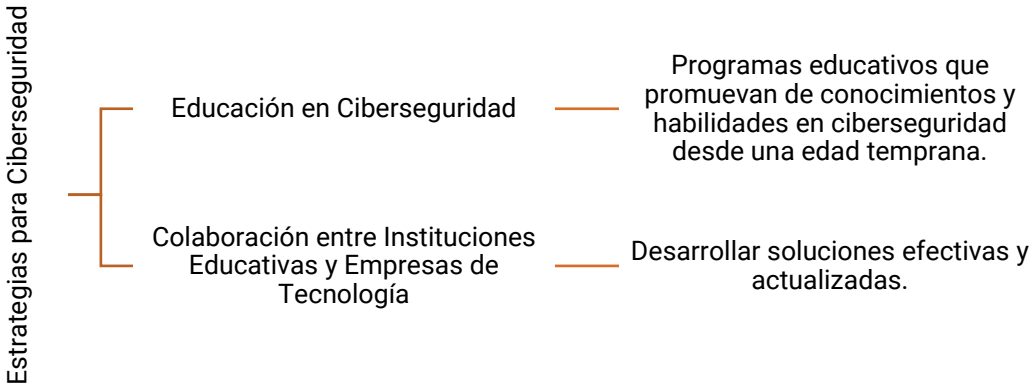
Nota: Este gráfico indica los principales problemas de ciberseguridad y posibles soluciones.

Fuente: elaboración propia.

Entre las principales estrategias innovadoras para la ciberseguridad educativa tenemos las que se nombran en la figura 3 debido a que forman parte de la protección que se requiere para cuidar los datos e información de los actores involucrados (Romero, 2023):

Figura 3

Estrategias para Ciberseguridad



Nota: Este gráfico presenta estrategias para proteger los datos vulnerables de los estudiantes en la web.

Fuente: elaboración propia.

Se necesita elaborar y aplicar políticas y normativas respecto al uso adecuado de la tecnología, la administración de contraseñas, la respuesta a incidentes de seguridad y la salvaguarda de la información personal de estudiantes y empleados, pues la implementación de políticas de seguridad bien estructuradas puede contribuir a reducir los riesgos y establecer criterios claros para todos los usuarios (Castillo, 2023).

Se utilizó la ecuación para muestra finita como se muestra.

$$n = \frac{N}{1+\frac{e^2(N-1)}{Z^2\ pq}} \qquad (1)$$

Donde:

n → Tamaño de la muestra que desea conocer.

N → Tamaño conocido de la población (100).

Z → Nivel de confianza (95%).

pq → Varianza de la población o variabilidad del fenómeno estudiado.

e → Índice de precisión o error muestral (5%).

Se obtuvo como resultado de la ecuación que la muestra es de 81 miembros de la comunidad educativa entre estudiantes y educadores.

Los resultados obtenidos en la encuesta realizada a la muestra entre alumnos y docentes de la Unidad Educativa Particular “Pablo Palacios” indican que el 63% de los encuestados fueron mujeres y el 37% hombres. A continuación, se presenta en la Tabla 1, los resultados relevantes obtenidos en la encuesta.

Tabla 1

Categorías y Resultados de la encuesta

Categorías	Sí %	No %
1. Capacitaciones sobre ciberseguridad.	28,4	71,6
2. Conocimiento de políticas y protocolos de seguridad informática en la institución.	44,4	55,6
3. Víctima de hackeo o robo de información.	24,7	75,3
4. Software antivirus instalado en su computadora.	64,2	32,3
5. La plataforma educativa cuenta con código de confirmación o verificación de usuario.	10	90
6. Significado y funcionalidad de Ransomware, phishing, malware y ciberseguridad.	28,4	71,6

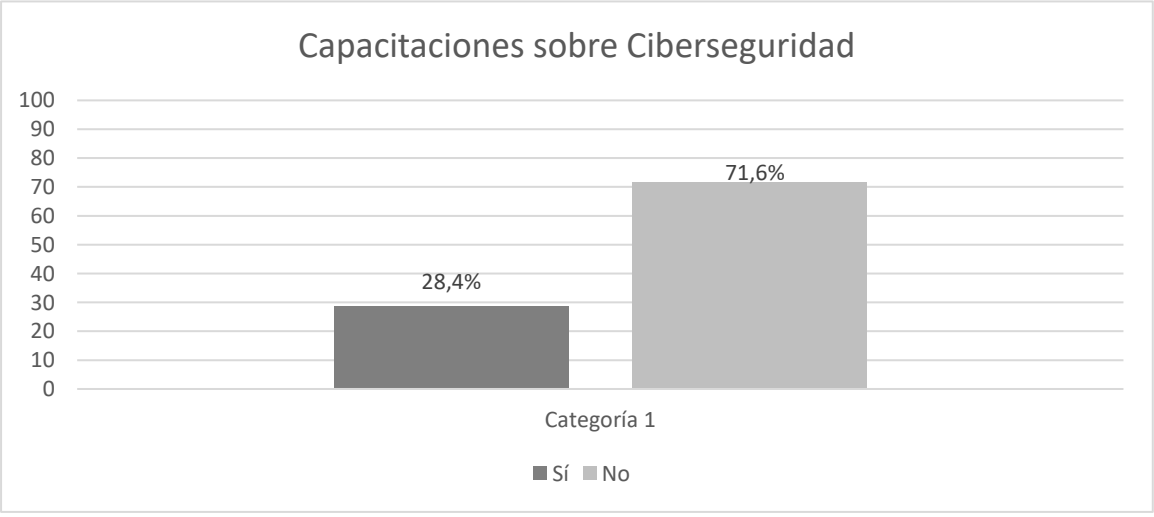
Nota: Esta tabla muestra los resultados obtenidos en porcentajes según la muestra de 81 personas entre estudiantes y docentes.

Fuente: elaboración propia.

Según los resultados obtenidos es evidente el poco conocimiento que los encuestados tienen sobre la ciberseguridad pues no reciben capacitaciones constantes sobre este tema, como se puede observar en la Tabla 1, en la categoría 1 se hace enfoque a que el 28,4 % de los actores involucrados recibe capacitaciones, pero el mayor porcentaje 71,6 % no han sido asesorados del tema, como se muestra en el gráfico 1.

Gráfico 1

Capacitaciones sobre ciberseguridad



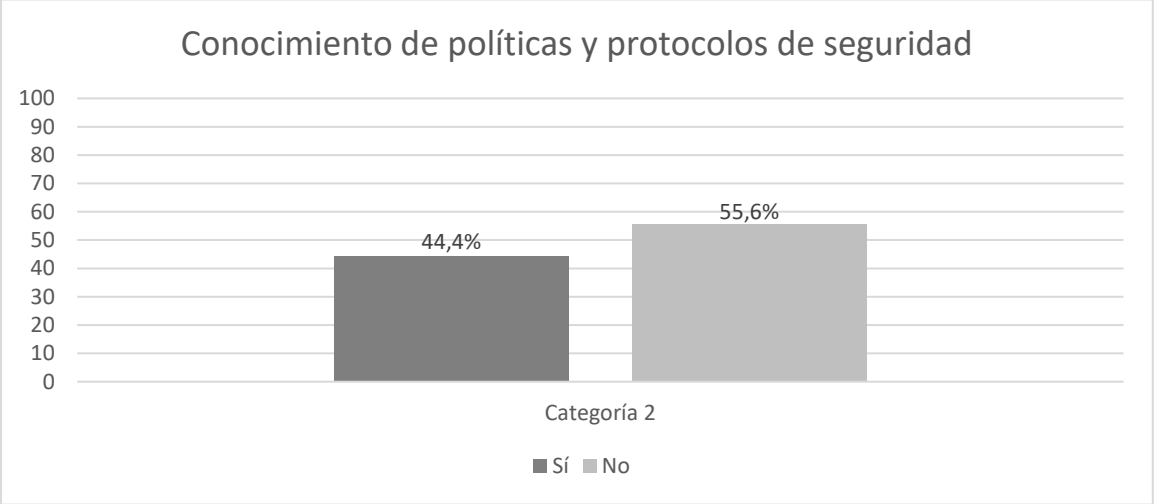
Nota: Este gráfico muestra los resultados de la encuesta en relación a las capacitaciones sobre ciberseguridad.

Fuente: elaboración propia.

Así también, el 55,6% de los encuestados no tiene conocimiento de las políticas y protocolos de seguridad informática que posee la institución educativa como se observa en el gráfico 2.

Gráfico 2

Conocimiento de políticas y protocolos de seguridad



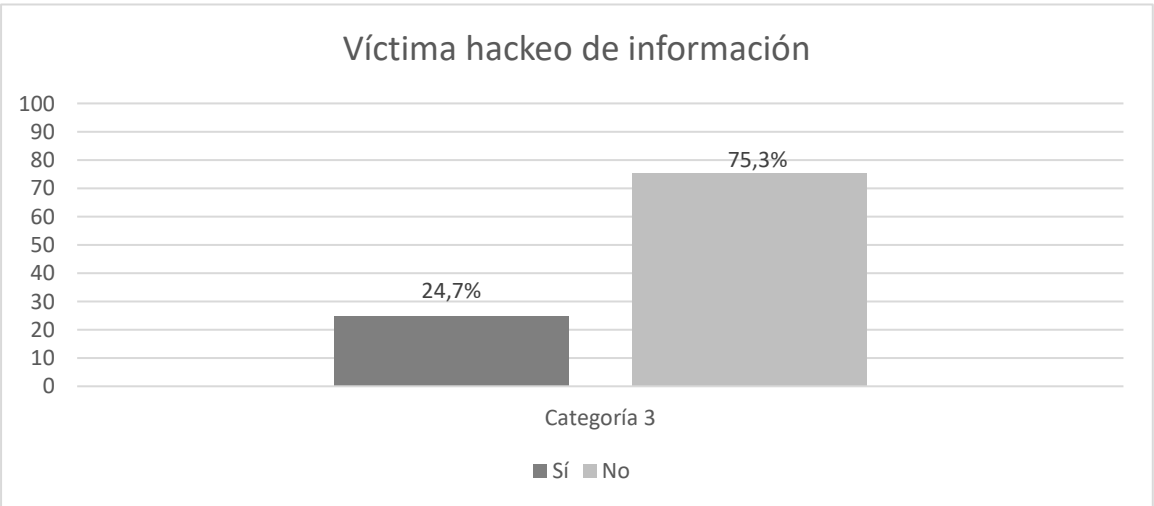
Nota: Este gráfico muestra los resultados obtenidos entre la población de muestra sobre el conocimiento de políticas y protocolos de seguridad.

Fuente: elaboración propia.

Existe un porcentaje de 75,3 % de la Ilustración 6 con relación a aquellos que manifiestan no haber sido víctimas de robo de información pues el otro 24,5 % en algún momento fue parte de un hacking cibernético y eso da cuenta de la necesidad de la protección de los datos.

Gráfico 3

Víctima de hackeo o robo de información



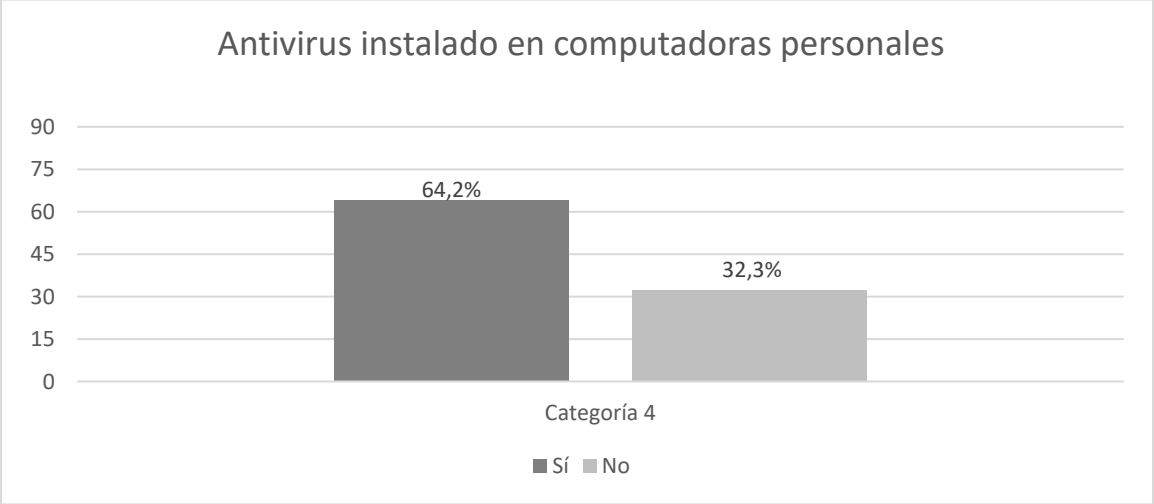
Nota: Este gráfico muestra los resultados obtenidos entre la población de muestra sobre el conocimiento de políticas y protocolos de seguridad.

Fuente: elaboración propia.

Como se observa a continuación en el gráfico 4 el 64,2% de la muestra indica que sí tienen instalado en sus computadoras un antivirus por lo que poseen mayor seguridad para sus aparatos electrónicos en comparación al 32,3% que no conoce o no ha visto la necesidad de tener uno instalado.

Gráfico 4

Computadoras con antivirus instalados



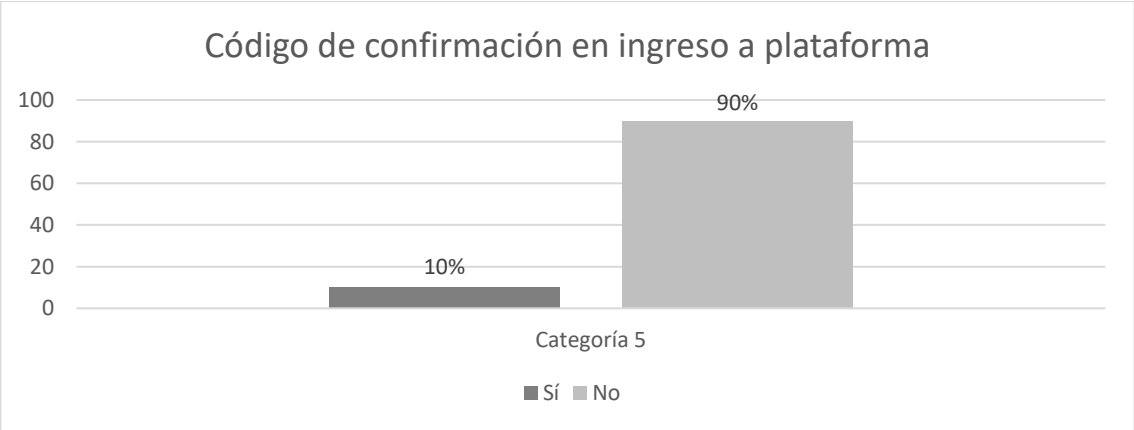
Nota: El gráfico indica el porcentaje de aquellos que tienen o no un antivirus en sus ordenadores.

Fuente: elaboración propia.

Se presenta una debilidad importante de la plataforma educativa, pues solo el 10% manifiesta que se le solicita código o correo de confirmación para ingresar a su plataforma, mientras que la mayor parte, es decir el 90% de la muestra indica todo lo contrario, poniendo en evidencia un problema importante, véase en el gráfico 5.

Gráfico 5

Confirmación de ingreso a plataforma educativa



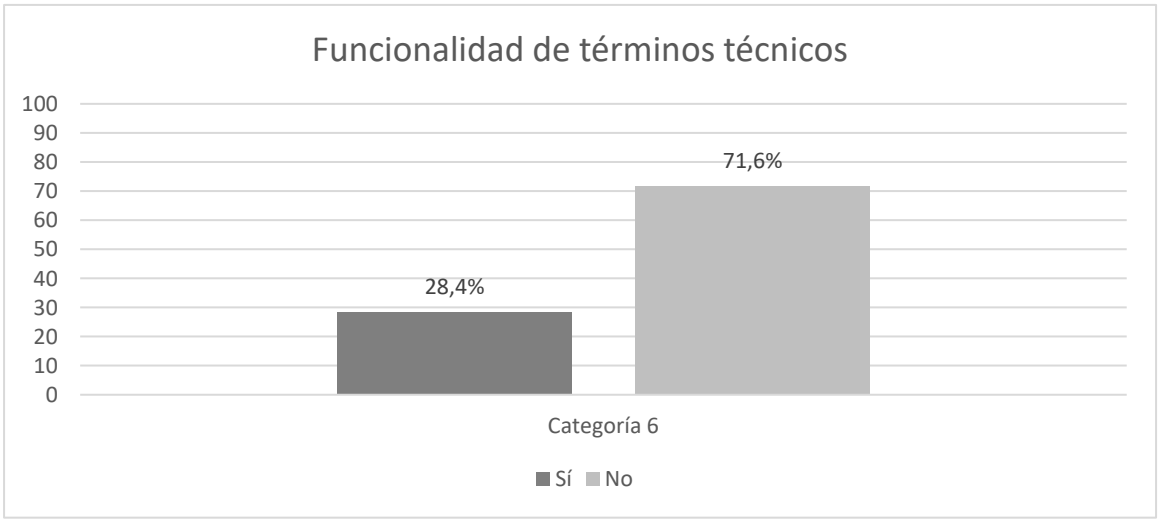
Nota: El gráfico indica el porcentaje de aquellos códigos de confirmación que se solicitan o no al ingresar a la plataforma educativa.

Fuente: elaboración propia.

La categoría 6 de la Tabla 1, hace énfasis en conocer si la muestra tomada en cuenta conoce sobre términos básicos que se ven involucrados en la seguridad y protección de datos de la comunidad educativa, como se observa en la Ilustración 9 el 71,6% no identifica el significado ni funcionalidad de Ransomware, phishing, malware y ciberseguridad, contrario al 28,4% que sí.

Gráfico 6

Conocimiento del significado y funcionalidad de Ransomware, phishing, malware y ciberseguridad



Nota: El gráfico indica el nivel de conocimiento sobre los programas Ransomware, phishing, malware y ciberseguridad.

Fuente: elaboración propia.

La discusión se centra en la necesidad de fortalecer la educación en ciberseguridad, mejorar la colaboración entre instituciones educativas y empresas tecnológicas, y desarrollar políticas más sólidas para proteger la información de los estudiantes en el futuro digital. El entorno digital está en constante evolución por lo que es necesario mejorar la protección de los datos en cuanto a la ciberseguridad en la educación del futuro.

Los resultados indican que los docentes y estudiantes muestran un alto desconocimiento, principalmente en relación a la información sobre seguridad informática, virus, suplantación de identidad, robo de información y filtración de datos.

CONCLUSIÓN

La ciberseguridad en el futuro digital de los estudiantes es un tema crítico que requiere atención inmediata. La implementación de estrategias innovadoras y la concienciación en ciberseguridad son fundamentales para proteger a los estudiantes en un entorno educativo cada vez más conectado.

La colaboración entre distintos actores, incluyendo instituciones educativas, gobiernos y empresas tecnológicas, es esencial para abordar de manera integral los desafíos emergentes en este ámbito pues la meta es que los involucrados estén en la capacidad de comprender y gestionar eficientemente los sistemas de ciberseguridad.

La ausencia de conocimiento y comportamientos seguros puede exponer a las personas a riesgos, resaltando así la relevancia de la enseñanza sobre seguridad cibernética y la incorporación de hábitos adecuados para resguardarse en el entorno digital actual. Se requiere una mayor investigación para profundizar en la comprensión de las amenazas emergentes y para crear soluciones innovadoras. La colaboración entre especialistas de diferentes disciplinas, como educación, psicología, tecnología y ciberseguridad, será esencial para abordar este desafío de manera efectiva.

REFERENCIAS

Bonilla, J. (2023). Importancia del uso de la ciberseguridad enfocada al hacking ético aplicados a las empresas: una revisión sistemática de la literatura. USAT, 7. http://hdl.handle.net/20.500.12423/6883

Cando, M., & Medina, P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. Dialnet, 10(2254–6529), 7. https://dialnet.unirioja.es/servlet/articulo?codigo=7888164

Castillo, J. (2023). Análisis de la ciberseguridad en espacios educativos pertenecientes a la Fuerza Aeroespacial Colombiana. Dialnet, 19 n., 137–151. https://doi.org/https://doi.org/10.18667/cienciaypoderaereo.803

Chhetri, C., & Motti, V. (2021). Identifying Vulnerabilities in Security and Privacy of Smart Home Devices. National Cyber Summit (NCS), 1271(NCS 2020). https://doi.org/https://doi.org/10.1007/978-3-030-58703-1_13

Chingo, R., & Gómez, O. (2021). Tecnología de contenedores y su aplicación en el aprendizaje de ciberseguridad: una revisión sistemática de literatura. Revista Electrónica De Computación, Informática, Biomédica Y Electrónica, 9(2). https://doi.org/https://doi.org/10.32870/recibe.v9i2.186

Díaz, F., Molinari, L., Venosa, P., & Macia, N. (2019). Investigación en ciberseguridad: nuevos desafíos para adaptarse a nuevos paradigmas. SEDICI, 5. https://sedici.unlp.edu.ar/handle/10915/77274

Echeverria, M. (2021). Cybersecurity in learning management system (LMS). Ecuadorian Science Journal, 5, 46–54. https://doi.org/https://doi.org/10.46480/esj.5.1.98

Fernández, L. (2019). Formación TIC (redes sociales, internet, ciberseguridad, big data, etc.) en casa, en el colegio, en la universidad y en la empresa: características, razón de ser y contenido. In Tecnología, Ciencia y Educación (TCyE, p. 110). https://doi.org/https://doi.org/10.51302/tce.2019.243

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2019). La seguridad informática y la seguridad de la información. Revista Científico-Académica Multidisciplinaria, 2550-682X. https://doi.org/10.23857/pc.v2i12.420

Goodman, M. (2001). Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. Semantic Scholar. https://www.semanticscholar.org/paper/Future-Crimes%3A-Inside-the-Digital-Underground-and-Goodman/72c1a613644e02e26bfdaae7abbe87beab218ebe#citing-papers

López, A., Roque, H., Ramón, V., Prieto, M., & Salazar, R. (2022). Hábitos y percepciones sobre Seguridad Informática en estudiantes universitarios pertenecientes a las generaciones Y, Z: Un estudio comparativo de dos universidades públicas en México. Dilemas Contemporáneos: Educación, Política y Valores, 9(3), 1. https://openurl.ebsco.com/EPDB%3Agcd%3A10%3A17177994/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A159643761&crl=c

Morales, P., & Medina, R. (2021). Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador. Dialnet, 10(2254–6529), 49–75. https://dialnet.unirioja.es/servlet/articulo?codigo=8091394

Peña, J., & García, L. (2014). La importancia del componente educativo en toda estrategia de Ciberseguridad. Estudios En Seguridad y Defensa, 9(18), 10. https://doi.org/https://doi.org/10.25062/1900-8325.9

Pillajo, P., & Avila, D. (2023). Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura. Revista Perspectivas, 5(e-ISSN: 2661-6688), 19–29. https://doi.org/https://doi.org/10.47187/perspectivas.5.1.179

Ribble, M. (2015). Digital Citizenship in Schools (Internatio). https://books.google.com.ec/books?id=z6WpCgAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Romero, A. (2023). La Ciberseguridad en el ámbito educativo para la Unidad Educativa Maryland de Villa Allende, Córdoba. Universidad Siglo 21, 62. https://repositorio.21.edu.ar/handle/ues21/28165