593 Digital Publisher
CEIT
ISSN 2588-0705

La importancia de la educación en ciberseguridad para niños

The importance of cybersecurity education for children

Dayana Herrera-Shigua [1]
Universidad Tecnológica Indoamérica - Ecuador
Dherrera11@indoamérica.edu.ec

Teresa Mendoza-Solorzano [2]
Universidad Tecnológica Indoamérica - Ecuador
tmendoza2@indoamerica.edu.ec

Leidy León-Navarrete [3]
Universidad Tecnológica Indoamérica - Ecuador
lleon9@indoamerica.edu.ec

Maria Zambrano-Antón [4]
Universidad Tecnológica Indoamérica - Ecuador
Mzambrano53@indiamerica.edu.ec

Aracelly Núñez-Naranjo [5]
Universidad Tecnológica Indoamérica - Ecuador
fernandanunez@uti.edu.ec

doi.org/10.33386/593dp.2025.1-2.2952

V10-N1-2 (ene) 2024, pp 5-19 | Recibido: 19 de noviembre del 2024 - Aceptado: 25 de enero del 2025 (2 ronda rev.)
Edición Especial

1 Estudiante de la Licenciatura en Educación General Básica de la Universidad Tecnológica Indoamérica. ORCID: http://orcid.org/0009-0006-1853-5443
2 Estudiante de la Licenciatura en Educación General Básica de la Universidad Tecnológica Indoamérica. ORCID: http://orcid.org/0009-0000-6457-2655
3 Estudiante de la Licenciatura en Educación General Básica de la Universidad Tecnológica Indoamérica. ORCID: http://orcid.org/0009-0008-7230-9206
4 Estudiante de la Licenciatura en Educación General Básica de la Universidad Tecnológica Indoamérica. ORCID: http://orcid.org/0009-0002-0841-6118
5 Docente en Licenciatura en Educación General Básica de la Universidad Tecnológica Indoamérica. ORCID: http://orcid.org/0000-0001-7431-2339

Cómo citar este artículo en norma APA:

Herrera-Shigua, D., Mendoza-Solorzano, T., León-Navarrete, L., Zambrano-Antón, M., & Núñez-Naranjo, A., (2025). La importancia de la educación en ciberseguridad para niños. 593 Digital Publisher CEIT, 10(1-2), 5-x, https://doi.org/10.33386/593dp.2025.1-2.2952

Descargar para Mendeley y Zotero

RESUMEN

Introducción: La ciberseguridad es un tema crítico debido al aumento del uso de dispositivos digitales por parte de los niños. A menudo, acceden a Internet sin la supervisión adecuada, lo que los expone a amenazas como el ciberacoso y el robo de datos. Objetivo: El objetivo del estudio es analizar los riesgos que enfrentan los niños en línea y proponer estrategias educativas y regulatorias que garanticen su seguridad en el entorno digital. Metodología: Se utilizó una revisión sistemática de literatura y análisis de contenido para identificar las principales variables relacionadas con la educación en ciberseguridad, la diversidad cultural y la formación en competencias digitales. Resultados: Los hallazgos indican que la educación temprana en ciberseguridad fomenta habilidades críticas en los niños, permitiéndoles reconocer y manejar riesgos en línea. Además, se destaca la importancia de la colaboración entre instituciones educativas, familias y gobiernos para crear un entorno seguro. Conclusión: La ciberseguridad infantil requiere un enfoque integral que combine educación, supervisión y políticas públicas. Proteger a los niños en el entorno digital no solo es esencial para su seguridad inmediata, sino también para empoderarlos como ciudadanos digitales responsables en el futuro.

Palabras claves: ciberseguridad, educación, riesgos, protección, responsabilidad.

ABSTRACT

Introduction: Cybersecurity is a critical issue due to the increasing use of digital devices by children. They often access the Internet without proper supervision, exposing them to threats such as cyberbullying and data theft. Objective: The study aims to analyze the risks children face online and propose educational and regulatory strategies to ensure their safety in the digital environment. Methodology: A systematic literature review and content analysis were conducted to identify key variables related to cybersecurity education, cultural diversity, and the development of digital skills. Results: The findings indicate that early cybersecurity education fosters critical skills in children, enabling them to recognize and manage online risks. Moreover, the study highlights the importance of collaboration among educational institutions, families, and governments to create a secure environment. Conclusion: Child cybersecurity requires a comprehensive approach that combines education, supervision, and public policies. Protecting children in the digital environment is not only essential for their immediate safety but also for empowering them as responsible digital citizens in the future.

Keywords: cybersecurity, education, risks, protection, responsibility.

593 Digital Publisher CEIT ISSN 2588-0705

Introducción

La ciberseguridad para niños

La ciberseguridad se está convirtiendo en una preocupación creciente a medida que los niños utilizan cada vez más dispositivos digitales desde una edad temprana. Sin supervisión y conciencia de los riesgos, los niños pueden estar expuestos a amenazas como el ciberacoso, el robo de identidad y el robo de identidad. Según la investigación de (Villarroel-Molina et al., 2024) la edad promedio a la que los niños utilizan Internet por primera vez es de alrededor de 8 años, un período en el que los niños aún carecen de la madurez necesaria para tomar decisiones informadas sobre su seguridad en línea.

Es importante señalar que los ciberataques son cada vez más comunes y más graves a medida que incluso las grandes empresas, los gobiernos y los individuos están expuestos a las acciones de los ciberdelincuentes; Así pues, en los últimos años se ha generalizado la conciencia sobre este problema; destaca que en España se han detectado ataques de phishing que han provocado importantes costes (Olivares Ruiz et al., 2022). Ante una situación económica difícil, los ciberdelincuentes están cambiando sus métodos para atacar a los grupos más vulnerables, como los niños, porque no tienen la madurez suficiente para distinguir hábitos de uso de Internet socialmente inapropiados.

Los niños deben ser conscientes de las consecuencias del mal uso de las nuevas tecnologías desde una edad temprana, porque aún no son conscientes de todos los peligros que supone iniciar sesión en las redes sociales y hacer un mal uso de estas plataformas. Según (Bustillos Ortega et al., 2023) Cuando un niño interactúa en línea, es más probable que entable conversaciones con extraños, haga clic en enlaces inseguros o descargue malware para robar información que cualquier otro miembro de su familia.

En el mundo digital, el contacto con extraños plantea grandes riesgos, especialmente para los niños, que pueden convertirse en víctimas del Grooming, una táctica utilizada por los ciberdelincuentes para apoderarse de su dinero con malas intenciones. La tendencia de los niños a compartir información personal también contribuye a estas situaciones peligrosas. Según *Internet Watch Foundation* (Martín-Ramallal & Ruiz-Mondaza, 2022) el número de incidentes de Grooming ha aumentado significativamente en los últimos años, lo que proporciona una fuerte justificación para implementar medidas de protección en familias e instituciones educativas. Por ejemplo, se debe informar a los niños que no es seguro revelar información personal a usuarios desconocidos en Internet.

El ciberbullying es otro problema social que parece afectar cada vez más a los niños en línea. Las redes sociales y la mensajería instantánea también se han convertido en medios para que los menores sean acosados o intimidados por amigos o desconocidos en forma de burlas, insultos e incluso mensajes amenazantes (D. Fernández, 2019). Este tipo de acoso no sólo es perjudicial para la autoestima del niño, sino que también puede ser destructivo y provocar otros problemas como aislamiento social o bajo rendimiento académico.

Los niños enfrentan problemas de robo de identidad y privacidad debido a la falta de conocimiento sobre las medidas de seguridad básicas, esto cuando instalan aplicaciones o juegos sin comprobar la fuente y pueden quedar expuestos a malware que puede recopilar ilegalmente información personal y financiera, lo que aumenta los riesgos tanto para los niños como para sus familias. El número de ciberdelincuentes que atacan a los niños ha aumentado en los últimos años, lo que pone de relieve la necesidad urgente de tomar medidas preventivas, como establecer contraseñas seguras y mantenerse alejado de redes Wi-Fi públicas no seguras y evitar compartir información personal en línea (Trujillo-Torres et al., 2024).

La exposición a contenidos inapropiados en línea plantea riesgos importantes para los niños y puede afectar su desarrollo emocional y psicológico. Es sumamente importante tomar medidas de protección y educativas para

garantizar su seguridad y bienestar en el entorno digital. Según el trabajo de (Chérrez et al., 2021) un informe de la *Unión Internacional de Telecomunicaciones* encontró que un número significativo de niños están expuestos a contenidos nocivos en Internet, lo que puede afectar negativamente el desarrollo emocional y mental de los niños. Las plataformas digitales deberían tomar medidas más estrictas para proteger a los menores, como mejorar la moderación de contenidos y proporcionar herramientas que permitan a los padres monitorear sus actividades en línea.

En el entorno digital, los niños corren el riesgo de sufrir abusos, como la publicación no autorizada de contenidos privados, chantajes, acoso y distribución ilegal de contenidos. La falta de control en las plataformas y el desconocimiento de los menores sobre sus actividades online los convierte en víctimas potenciales, lo que puede tener graves consecuencias psicológicas. Es de vital importancia tomar medidas para proteger a los menores en Internet y capacitarlos para que utilicen la tecnología digital de manera segura y responsable (M. R. Fernández et al., 2022). Por tanto, es importante enseñarles a valorar su privacidad, fomentar el uso responsable de las redes sociales y garantizar regulaciones digitales más estrictas para proteger a los grupos vulnerables.

La ciberseguridad en los niños requiere una educación digital temprana y responsable. Los padres y educadores deben enseñarles sobre ciberamenazas, prevención y comportamiento en línea, y supervisar su tiempo en Internet. Una educación adecuada en ciberseguridad no solo protege a los niños, sino que también los prepara para ser usuarios responsables de la tecnología en el futuro (Aznar-Martínez et al., 2024). De esta manera se promueve una cultura de seguridad en Internet que puede trascender generaciones.

Las políticas públicas y la legislación son fundamentales para proteger a los menores en el entorno digital. Los gobiernos y organismos internacionales deben establecer normativas que obliguen a las empresas tecnológicas a implementar medidas de seguridad estrictas y transparentes, como controles parentales, eliminación de contenido perjudicial y persecución de ciberdelincuentes. Según la *Unión Internacional de Telecomunicaciones*, los países con legislaciones robustas en ciberseguridad infantil han logrado reducir significativamente los incidentes de riesgos digitales en esta población (Macías-Lara et al., 2022).

El objetivo de este estudio es crear un marco integral de ciberseguridad infantil que combine educación, tecnología y regulación, para garantizar la seguridad y bienestar de los menores en el entorno digital. El estudio analiza los principales riesgos y estrategias para proteger a los niños en línea, utilizando una metodología de revisión sistemática de literatura y análisis de contenidos lo que permite identificar las principales variables relacionadas con la educación inclusiva, la diversidad cultural y la formación en competencias digitales.

Desarrollo

Riesgos y amenazas en línea para los niños

Las amenazas y peligros relacionados con Internet son cada vez más preocupantes debido al acceso temprano y frecuente de los niños a dispositivos conectados a Internet. Según un estudio reciente que analiza las observaciones de 12.000 adultos, 5.123 padres y 11.516 niños, el 45% de los padres admitió que dedican poco tiempo a monitorear las actividades en línea de sus hijos y a preguntarse si deberían hacer más para protegerlos (Guerrero-vega et al., 2024). Esta realidad se ve agravada por el hecho de que el 24% de los padres encontraron fotos de sus hijos publicadas en línea sin su consentimiento, cifra significativamente superior al 15% reportado entre los adultos.

Sin embargo, más de la mitad de los padres confían ciegamente en que sus hijos saben cómo protegerse en línea, lo que refleja una brecha entre las percepciones de seguridad y los riesgos reales que enfrentan los niños en línea. Aunque muchos padres creen que sus hijos pueden bloquear a extraños o evitar interacciones sospechosas, estas medidas no son suficientes

593 Digital Publisher CEIT ISSN 2588-0705

para mantenerlos seguros en un entorno digital complejo y en constante evolución (Trejos-Gil & Vélez, 2023). Los niños, especialmente aquellos entre 5 y 16 años, son un grupo particularmente vulnerable debido a su falta de experiencia y comprensión de las amenazas en línea.

El informe encontró que el 85% de los niños utilizan Internet a diario o casi a diario, lo que aumenta su exposición a amenazas como el ciberacoso, el acoso y el acceso a contenidos inapropiados. A pesar de esta visión, muchos padres no dan prioridad a mantenerse informados sobre los avances en ciberseguridad, lo que limita su capacidad para educar y proteger eficazmente a sus hijos. Uno de los problemas más graves es la falta de conciencia sobre la importancia de la privacidad en Internet. Muchos niños comparten información personal, fotografías o detalles sobre su vida diaria sin comprender las posibles consecuencias (Villarroel-molina et al., 2024). Este comportamiento puede dar lugar a la divulgación no autorizada de datos confidenciales, lo que aumenta el riesgo de robo de identidad, chantaje o acoso.

Las investigaciones muestran que la responsabilidad de educar a los niños en estas áreas recae principalmente en los padres, quienes reconocen la importancia de esta educación adicional, pero no siempre la implementan de manera efectiva. La falta de tiempo o de conocimientos de los adultos perpetúa una cultura de incertidumbre y vulnerabilidad en el entorno digital; otro desafío grave es el rápido desarrollo de las amenazas en línea, que obliga a padres e hijos a actualizar constantemente sus conocimientos sobre seguridad en línea (Quirumbay Yagual et al., 2022). Pero muchos adultos no se toman el tiempo para aprender sobre estos temas, lo que pone a los niños en situaciones que podrían evitarse con la supervisión adecuada.

Aunque los padres son conscientes de su papel en la protección de sus hijos, está claro que muchos todavía confían demasiado en la capacidad de sus hijos para afrontar situaciones difíciles. La educación temprana y continua sobre temas como la privacidad, el respeto en línea y el uso seguro de la tecnología es fundamental para reducir la vulnerabilidad de los niños en línea; también es importante que los adultos asuman la responsabilidad de mantenerse informados y proteger proactivamente a sus familias de las amenazas en línea (Herrero-Martín et al., 2022).

Beneficios de la educación en ciberseguridad para niños

Educar a los niños sobre ciberseguridad es fundamental para garantizar su desarrollo seguro en el entorno digital que cada vez está más presente en sus vidas. Investigaciones recientes muestran que la capacitación temprana en mejores prácticas digitales fomenta el pensamiento crítico, lo que permite a los niños identificar riesgos y tomar decisiones informadas en línea. Al comprender conceptos como privacidad, gestión de identidad y seguridad en las redes sociales, los niños desarrollan habilidades que no solo los protegen a corto plazo, sino que son esenciales en su transición a la edad adulta (Olivares Ruiz et al., 2022). La alfabetización digital fortalece su autonomía y los prepara para interactuar responsablemente en un mundo conectado. Otro beneficio importante de la educación en ciberseguridad es la prevención del ciberbullying y el acoso, que son amenazas comunes en el ciberespacio.

Las investigaciones sobre el comportamiento en línea han demostrado que los niños educados en seguridad digital tienen más probabilidades de reconocer comportamientos inapropiados y buscar ayuda en situaciones peligrosas. Además, al fomentar la comunicación abierta entre padres, profesores y niños, se crea un ambiente de confianza, facilitando la intervención temprana ante posibles problemas, esto reduce el impacto psicológico y emocional que estas amenazas pueden tener en los niños (D. Fernández, 2019). La educación en ciberseguridad también mejora la relación de los niños con la tecnología al enseñarles a verla como una herramienta poderosa cuando se usa de manera ética y responsable.

Este enfoque ayuda a los niños a desarrollar una perspectiva equilibrada sobre

el uso de Internet, evitando la adicción o el uso excesivo de dispositivos digitales. También fomenta la creatividad y el aprendizaje independiente porque los niños pueden explorar recursos educativos en línea de forma segura. Según la UNESCO, la formación en habilidades digitales es clave para cerrar la brecha digital y empoderar a las nuevas generaciones en un mundo impulsado por la tecnología (A. F. Núñez-Naranjo, 2024). Un aspecto importante es que la educación en ciberseguridad no solo beneficia a los niños sino también a sus familias y comunidades.

Los conocimientos adquiridos por los niños suelen tener un efecto positivo en quienes los rodean, transmitiendo prácticas de seguridad a otros familiares o amigos. Además, integrar programas de ciberseguridad al sistema educativo promoverá una cultura de seguridad digital con impacto social, esto es especialmente cierto en el contexto global, donde los ciberataques son cada vez más frecuentes y sofisticados, y la defensa colectiva es esencial para garantizar un entorno digital más seguro (Criollo et al., 2023).

Siendo así la educación en ciberseguridad prepara a los niños para convertirse en ciudadanos digitales responsables, conscientes de los derechos y responsabilidades asociados con el uso de Internet. Al aprender la importancia de respetar la privacidad y el bienestar de los demás, los niños adquieren valores fundamentales que ayudan a crear comunidades virtuales más respetuosas y cooperativas. Además, esta formación les ayuda a convertirse en participantes activos en la promoción del uso ético de la tecnología, contribuyendo al cambio positivo en la sociedad (A. Núñez-Naranjo & Chancusig-Toapanta, 2022). De esta manera, la educación en ciberseguridad no solo protege a los niños, sino que también les ayuda a liderar transformaciones significativas en el futuro digital.

Herramientas y recursos educativos en ciberseguridad

Las herramientas y recursos educativos en ciberseguridad son esenciales para enseñar a los niños prácticas seguras en el entorno digital. Actualmente, existen plataformas interactivas y aplicaciones diseñadas para introducir conceptos básicos de seguridad en línea de manera didáctica y accesible; ya que estas herramientas incluyen juegos educativos que simulan escenarios de riesgo, guías interactivas para identificar amenazas como el *phishing*, y programas diseñados para enseñar el manejo de contraseñas seguras (Miranda, 2014). Estas estrategias no solo facilitan el aprendizaje, sino que también refuerzan la retención del conocimiento al involucrar a los niños en actividades prácticas y dinámicas.

Entre los recursos más destacados se encuentran los programas educativos ofrecidos por instituciones internacionales como la Agencia Europea de Ciberseguridad (ENISA) y organizaciones sin fines de lucro que promueven la alfabetización digital. Estas entidades desarrollan contenidos específicos adaptados a diferentes edades, como vídeos explicativos, fichas didácticas y talleres interactivos. Por ejemplo, iniciativas como *CyberSmart* han demostrado ser efectivas en la enseñanza de principios fundamentales de seguridad digital, logrando que los menores interioricen buenas prácticas mientras exploran el entorno digital (Trejos-Gil & Vélez, 2023). La integración de estos recursos en los planes de estudio escolares asegura un alcance amplio y una enseñanza uniforme en temas de ciberseguridad.

Los simuladores de riesgos en línea son otro recurso valioso que permite a los niños experimentar situaciones hipotéticas de forma segura. Estas herramientas recrean interacciones reales con ciberdelincuentes, como intentos de robo de información o manipulación en redes sociales, para enseñarles a reconocer y reaccionar adecuadamente ante estas amenazas (Chérrez et al., 2021). Al participar en estas simulaciones, los menores adquieren habilidades prácticas que los preparan para enfrentar riesgos en la vida real.

593 Digital Publisher CEIT ISSN 2588-0705

Además, estos simuladores suelen incluir guías posteriores que explican los errores cometidos y refuerzan el aprendizaje mediante ejemplos concretos.

Finalmente, los padres y educadores juegan un papel crucial en la utilización efectiva de herramientas y recursos educativos en ciberseguridad. Es importante que estas iniciativas sean acompañadas de un diálogo constante y supervisión activa para resolver dudas y reforzar los conceptos aprendidos (Taco, 2022). Al combinar recursos tecnológicos con un enfoque pedagógico personalizado, se fomenta un aprendizaje integral que empodera a los niños para navegar con confianza y seguridad en el entorno digital. Estas herramientas, junto con una educación continua, contribuyen a formar usuarios responsables y conscientes de los desafíos de la era digital.

Formas de navegación segura en el internet

Navegar de forma segura en Internet es una habilidad esencial que debe inculcarse desde la infancia, en actividades educativas tanto en el aula como en el hogar, ya que, son herramientas clave para sensibilizar a los niños sobre los riesgos de los contenidos inapropiados y los peligros asociados con el uso excesivo de dispositivos conectados (Villa Ramírez et al., 2023). Los menores, movidos por la curiosidad natural de su edad, tienden a explorar sin considerar las posibles amenazas, como la exposición a material nocivo o la interacción con desconocidos y enseñarles a identificar y evitar estos peligros es una prioridad que requiere la colaboración entre educadores y familias.

Un problema recurrente es la tendencia de los niños a descargar archivos como juegos, música o aplicaciones sin supervisión adecuada. Este comportamiento aumenta el riesgo de infectar los dispositivos con malware o compartir información personal sin querer. Para mitigar este riesgo, es fundamental enseñarles a discernir entre sitios seguros y potencialmente peligrosos. Actividades como verificar la autenticidad de una página web o identificar extensiones de archivo sospechosas pueden ser integradas en su educación tecnológica (Barbarita Álava Zambrano et al., 2022).

Para fomentar una navegación segura, es esencial el uso de herramientas y configuraciones diseñadas específicamente para este propósito. Aplicaciones educativas que simulan riesgos reales, junto con sistemas de navegación segura que bloquean contenido malicioso, son recursos accesibles y efectivos. Estas soluciones no solo protegen a los niños de amenazas inmediatas, sino que también promueven el desarrollo de habilidades críticas, como el reconocimiento de intentos de phishing y el manejo adecuado de información personal (Tatiana et al., n.d.). Estas herramientas deben combinarse con un enfoque pedagógico que motive a los niños a adoptar medidas de autoprotección.

Los educadores y padres tienen un rol fundamental en la enseñanza de prácticas responsables para navegar en Internet. Más allá de proporcionar herramientas tecnológicas, es importante acompañar a los menores en el aprendizaje de buenas prácticas. Por ejemplo, actividades interactivas que involucren escenarios reales, como crear contraseñas seguras o evitar clics en enlaces sospechosos, pueden reforzar conceptos clave (Hernández Prados et al., 2021). Además, mantener un diálogo abierto y constante sobre los riesgos y beneficios del entorno digital fomenta una relación de confianza que permite a los niños compartir sus inquietudes y dudas.

En definitiva, la implementación de un decálogo de navegación segura, que combine educación, herramientas tecnológicas y supervisión activa, es esencial para proteger a los niños en el entorno digital ya que, con reglas claras, como no compartir información personal, evitar descargas de fuentes desconocidas y consultar siempre con un adulto en caso de duda, forman una base sólida para un uso responsable de Internet (Olivares Ruiz et al., 2022). Estas prácticas, al ser promovidas tanto en el hogar como en la escuela, contribuyen a una experiencia digital enriquecedora y segura, empoderando a los niños para enfrentar los desafíos de la era tecnológica.

Consejos prácticos para padres y tutores sobre la educación en ciberseguridad

Mantener la privacidad es esencial para mantener a los niños seguros en el entorno digital, ya que se debe comprender que no deben compartir información personal como nombre, dirección, número de teléfono o fotografías con personas que no conocen o en plataformas en las que no confían plenamente. Los padres y tutores deben enseñar a sus hijos que incluso datos aparentemente inofensivos pueden ser utilizados por terceros con fines maliciosos, exponiéndolos a riesgos como el robo de identidad, el chantaje y el acoso (Garmendia et al., 2012). Para lograrlo, es importante promover el hábito de consultar a los adultos antes de proporcionar cualquier información en línea y fomentar el uso de herramientas que ayuden a identificar sitios web y aplicaciones seguras.

El uso adecuado de la tecnología requiere establecer límites claros para equilibrar el tiempo dedicado a actividades digitales con otras responsabilidades y momentos de relajación fuera de línea. Los niños necesitan saber que la tecnología es una herramienta valiosa, pero su uso excesivo puede causar problemas físicos, emocionales y sociales. Los padres y tutores pueden establecer horarios y rutinas que incluyan tiempo supervisado de estudio, juego y comunicación en línea (Domínguez Castillo et al., 2019). Es sumamente importante monitorear el contenido que consumen y sus interacciones con él, especialmente en las redes sociales, donde pueden encontrar contactos desconocidos o contenido inapropiado. El diálogo continuo entre adultos y niños ayuda a reforzar la importancia de estas medidas. Animar a los niños a pensar críticamente es una estrategia importante para mantenerlos seguros en línea. Se debe enseñar a los niños a cuestionar la autenticidad de la información que encuentran en Internet y a no confiar en mensajes o enlaces que parezcan sospechosos.

Los padres pueden trabajar con sus hijos para enseñarles a reconocer señales de advertencia en correos electrónicos, mensajes de texto o sitios web que puedan estar relacionados con estafas de phishing o malware. Esta enseñanza debe estar respaldada por conversaciones abiertas sobre las experiencias en línea de los niños, creando una atmósfera de confianza en la que puedan expresar dudas e inquietudes. De esta manera, los niños estarán mejor preparados para tomar decisiones acertadas y evitar situaciones de riesgo (Cruz Lucas et al., 2022). Crear un entorno digital más seguro es un esfuerzo de colaboración entre padres, cuidadores y los propios niños. Herramientas como controles parentales, filtros de contenido y navegadores dedicados son aliados importantes para minimizar las amenazas en línea. Sin embargo, la tecnología por sí sola no es suficiente; Esto debe complementarse con educación y apoyo de los adultos.

Los padres deben ser conscientes de las amenazas más comunes y de las soluciones disponibles para enseñar eficazmente a sus hijos a utilizar Internet de forma responsable. Además, es importante que los niños se sientan cómodos al hablar sobre cualquier situación incómoda o sospechosa que encuentren para que se puedan tomar medidas preventivas y promover una educación integral en ciberseguridad garantiza que los niños desarrollen hábitos sólidos para protegerse en línea (Herrero-Martín et al., 2022). Esto incluye enseñarles a crear contraseñas seguras, evitar compartir información confidencial y reconocer intentos de phishing.

Las escuelas también desempeñan un papel importante en la integración de contenidos de ciberseguridad en el plan de estudios, utilizando recursos interactivos y ejemplos de la vida real para reforzar este conocimiento. Al mismo tiempo, los padres deben reforzar estas lecciones en casa asegurándose de que los niños comprendan la importancia de una navegación segura (Hernández Prados et al., 2021). Al adquirir estas habilidades, los niños no sólo se convierten en usuarios más seguros sino también en personas más conscientes y responsables en el entorno digital.

593 Digital Publisher
CEIT
ISSN 2588-0705

Estrategias para promover la conciencia y responsabilidad digital

Son pocos los docentes que enseñan a los pequeños sobre ciberseguridad, pero más allá de resguardarse de los peligros de internet, es necesario fomentar en ellos una actitud de cuidado de su entorno digital, promoviendo la responsabilidad y conciencia digital. Todos los profesores que son inmigrantes digitales basan sus formaciones en una perspectiva que mira exclusivamente el control, la cautela y la prevención de los peligros del mundo digital (Quirumbay Yagual et al., 2022). Una actitud que no les permite integrar en sus estrategias otro tipo de prácticas más positivas provenientes del mundo digital, una actitud conservadora que puede llegar a ser peligrosa tanto para el progreso como para el futuro de sus estudiantes, desconociendo su realidad y necesidades, pero también para su bienestar.

Pero los peligros digitales existen y puede que no esté de más haber una materia o área curricular específica progresiva, basada en la progresión y adaptada al alumnado. Por lo que deberíamos informar, educar y asesorar sobre los riesgos digitales al alumnado desde edades tempranas. Pero también, a través de una pedagogía basada en la experiencia y abierta a la exploración, la toma de conciencia, la reflexión crítica y la autorregulación sobre los peligros que conlleva navegar en un mundo no del todo seguro (Catalina García et al., 2014).

Y, sobre todo, en cualquier caso, desde una perspectiva de progreso, de fomento de los valores y el desarrollo personal, no del individualismo ni el miedo al otro. Como docentes es importante fomentar en los alumnos una actitud de cuidado y responsabilidad de su entorno digital, además de hacer lo posible para que funcionar en el mundo digital no sea patrimonio de los más listos, poderosos y buenos, sino también de cualquier persona que así lo desee, independientemente de su identidad social, de género, condición, situación, etc. (Bustillos Ortega et al., 2023).

Estudios de caso y ejemplos inspiradores

Existen diferentes casos donde se evidencia como la enseñanza en la ciberseguridad ayuda a los niños, padres y docentes en el control y cuidado de los niños, un equipo de capacitadores creó un curso básico con el objetivo de prevenir que niños sean víctimas de acoso, grooming, suplantación de identidad, sextorsión y otros tipos de delitos (Medina Pérez & Vargas Ipaz, 2024). Es un tema que, hasta ahora, nadie había incluido dentro del currículo escolar; sin embargo, cada día más y más niños acceden a los dispositivos electrónicos y a Internet. muchos de ellos, pequeños, explican en la descripción del curso. Pero no es el único sitio profesional que ha incorporado cursos de ciberseguridad para chicos. Recientemente, se presentó una escuela de ciberseguridad gratuita y orientada a niños desde los diez años. Los temas que se están tratando dentro de esta iniciativa son variados: desde cómo funciona Internet hasta seguridad de los dispositivos.

De igual forma se encuentra el caso de *Social DiGi Kids* que es una innovadora propuesta creada para promover un entorno digital seguro, orientado a la prevención, el uso responsable de las redes sociales y el fortalecimiento de valores como la autoprotección. Inicialmente concebida como un programa de formación para padres, la iniciativa se transformó en un espacio virtual de intercambio de buenas prácticas, sensibilización y formación. Dirigida a niños de entre 6 y 12 años, ofrece programas como Cuida tu privacidad, Navego seguro y Soy cuidadoso, que combinan juegos interactivos, animaciones y consejos prácticos para educadores, brindando herramientas efectivas para un aprendizaje dinámico y compartido (Pinto et al., 2023).

El papel de las escuelas en la educación en ciberseguridad

El papel de las escuelas en la educación en ciberseguridad resulta fundamental, especialmente en un contexto donde las Nuevas Tecnologías ocupan un lugar central en la vida de los menores. Aunque tradicionalmente se ha atribuido a las familias la responsabilidad

de educar sobre el uso adecuado de estas herramientas, las instituciones educativas han asumido un rol cada vez más activo. Esto responde a la creciente necesidad de orientar a los niños y niños en un entorno donde los riesgos, como el sexting, son una realidad (Pillajo-García & Avila-Pesantez, 2023). Muchas víctimas de estas prácticas no recurren a sus padres o tutores, sino que buscan el apoyo de sus pares, quienes perciben como más comprensivos. Por ello, las campañas de concienciación suelen centrarse en actividades escolares, como talleres, charlas de sensibilización y eventos educativos, que buscan ofrecer espacios seguros para abordar estas problemáticas.

Las escuelas se han convertido en espacios donde los estudiantes pueden reflexionar sobre el uso responsable de las Tecnologías de la Información y la Comunicación (TIC), especialmente fuera del horario escolar. A través del trabajo conjunto con los Departamentos de Orientación, los centros educativos desarrollan estrategias que buscan no solo supervisar las actividades digitales de los menores, sino también fomentar la convivencia digital (Morales-Paredes & Medina-Chicaiza, 2021). Estas iniciativas pretenden mitigar los riesgos asociados al mal uso de las TIC, como la pérdida de habilidades prosociales o los problemas de convivencia, que pueden derivar en situaciones de ciberacoso o conflictos interpersonales entre los alumnos. La gestión de estas problemáticas ha llevado a las escuelas a reconocer la importancia de promover la ciberconvivencia como un componente esencial de su misión educativa.

En respuesta a estos desafíos, muchas instituciones han implementado buenas prácticas de ciberconvivencia que integran protocolos de actuación para abordar conflictos digitales. Estas medidas, incluidas en los Planes de Convivencia, buscan prevenir y gestionar situaciones que surjan de la interacción digital entre iguales. Además, fomentan un entorno donde las relaciones virtuales sean una extensión positiva del aprendizaje y no una fuente de conflictos. La educación en ciberseguridad, desde esta perspectiva, no solo se centra en la prevención, sino también en el desarrollo de habilidades que permitan a los estudiantes interactuar de manera ética y responsable en el ámbito digital (Mosquera Ayala, 2019).

De esta manera, las escuelas trascienden su papel tradicional como espacios exclusivamente académicos y se posicionan como agentes clave en la formación integral de los estudiantes. Su función no se limita a enseñar contenidos curriculares, sino que incluye la preparación de los menores para enfrentar los retos de un mundo digital en constante evolución (Aguilar Antonio, 2021). Esto implica no solo protegerlos de los riesgos, sino también empoderarlos para que puedan desenvolverse con confianza y responsabilidad en un entorno virtual que forma parte inseparable de su realidad cotidiana.

Colaboraciones y alianzas en ciberseguridad infantil

Las colaboraciones y alianzas en el ámbito de la ciberseguridad infantil son fundamentales para proteger a los menores en el entorno digital. Un ejemplo destacado es la participación de AESAND en la Alianza para la Ciberseguridad de la Comisión Europea. Esta organización establece que el acceso a los datos personales procesados en sitios web de entidades públicas debe estar restringido, siguiendo lo dispuesto en su normativa (Morales-Paredes & Medina-Chicaiza, 2021). Dicho acceso solo puede realizarse mediante un registro con usuario y contraseña, y no se permite de forma gratuita, salvo en casos específicos, como cuando los datos son requeridos por organismos de seguridad o las propias personas interesadas. Este enfoque subraya la importancia de garantizar que los datos sensibles de los menores sean gestionados con altos estándares de seguridad.

Por otro lado, la Agencia de Certificación para Delitos en Telecomunicaciones ha desarrollado un video titulado *Protegiendo a los niños a través de Internet*. Este material resalta cómo la red puede ser una herramienta valiosa para el aprendizaje y la comunicación de los menores, pero también advierte sobre los peligros asociados a su uso (Beltran Muñoz, 2020). Uno de cada cinco niños se siente amenazado

593 Digital Publisher CEIT ISSN 2588-0705

en el entorno digital. Sin embargo, muchos riesgos pueden prevenirse si los padres adoptan ciertas medidas simples, como supervisar las actividades en línea de sus hijos y fomentar un uso responsable de la tecnología. La participación activa de los padres resulta clave para mitigar los riesgos y garantizar una experiencia más segura en Internet.

Otro esfuerzo importante es el programa educativo para la prevención del ciberacoso, una iniciativa conjunta de Europol e INSAFE a través del programa *Safer Internet*. Este proyecto tiene como objetivo sensibilizar a los estudiantes sobre su papel en la prevención y el abordaje del ciberacoso. A través de recursos complementarios, como películas, caricaturas y dramatizaciones, se busca educar a los niños y jóvenes sobre qué es el ciberacoso y cómo actuar en caso de ser afectados (Bustillos Ortega et al., 2023). Este enfoque práctico y pedagógico permite a los menores desarrollar habilidades para enfrentar este problema de manera efectiva.

Estas colaboraciones y recursos educativos reflejan el compromiso de diversas instituciones internacionales en la protección de los menores en el ámbito digital. Desde el control del acceso a datos personales hasta la creación de programas de sensibilización y prevención, estas iniciativas representan un esfuerzo colectivo por garantizar que los niños puedan aprovechar los beneficios de Internet sin estar expuestos a riesgos innecesarios. La combinación de medidas técnicas, educativas y familiares es esencial para construir un entorno digital más seguro para los menores (Pillajo-García & Avila-Pesantez, 2023).

Desafíos y oportunidades futuras en la educación en ciberseguridad para niños

Los desafíos y oportunidades en la educación en ciberseguridad para niños reflejan la complejidad y rapidez con la que evoluciona nuestra sociedad. Aunque ya se han destacado varios aspectos cruciales en este trabajo, el panorama futuro promete ser aún más dinámico, impulsado no solo por avances tecnológicos, sino también por transformaciones sociopolíticas que redefinirán los entornos digitales. Esta evolución plantea la necesidad de una reflexión profunda sobre cómo abordar de manera efectiva la formación en ciberseguridad, asegurando que los niños estén preparados para enfrentarse a los retos emergentes y aprovechar las oportunidades que la tecnología les ofrece (Bustillos Ortega et al., 2023).

A pesar de los esfuerzos actuales para ofrecer soluciones formativas que mitiguen problemas como el vandalismo digital y la suplantación de identidad, los niños continúan enfrentando conflictos en sus interacciones en línea. Estas experiencias subrayan la urgencia de perfeccionar los contenidos educativos destinados a fomentar una convivencia digital segura y pacífica (Cruz Lucas et al., 2022). Los menores, aunque considerados nativos digitales, no están exentos de los riesgos que conlleva el mundo virtual, lo que exige a la sociedad y a la comunidad educativa un compromiso renovado para formarlos como ciudadanos responsables en un entorno digital en constante cambio.

Las oportunidades futuras en este ámbito son inmensas. La incorporación de nuevas metodologías pedagógicas y el uso de tecnologías innovadoras, como la inteligencia artificial y la realidad aumentada, podrían transformar la manera en que se enseña ciberseguridad, haciéndola más interactiva y accesible (Olivares Ruiz et al., 2022). Además, la colaboración entre instituciones educativas, familias, empresas tecnológicas y gobiernos será clave para desarrollar estrategias integrales que respondan a las necesidades de los menores. Estos esfuerzos conjuntos pueden contribuir a que los niños no solo sean usuarios informados, sino también defensores activos de un entorno digital ético y seguro.

Sin embargo, los retos no deben subestimarse. Entre ellos, destaca la brecha en la formación de docentes en temas de ciberseguridad, la resistencia a integrar estos contenidos en los currículos escolares y la dificultad para adaptar las soluciones a contextos diversos y con esto superar estos obstáculos requerirá un enfoque flexible y adaptativo, que

permita abordar las realidades específicas de cada comunidad, al tiempo que se fomenta una cultura digital global orientada hacia el respeto y la seguridad (Macías-Lara et al., 2022).

En este sentido, la educación en ciberseguridad para niños se posiciona como un campo de enorme relevancia, no solo para protegerlos de los riesgos actuales, sino también para empoderarlos como ciudadanos digitales del futuro. La integración de valores como la responsabilidad, la convivencia y la conciencia ética en este ámbito será fundamental para que las próximas generaciones puedan desenvolverse en un entorno digital más seguro, equitativo y enriquecedor.

Conclusiones.

En conclusión, se destaca la urgente necesidad de abordar los riesgos que enfrentan los niños en el entorno digital. Cuando los niños acceden a Internet a una edad más temprana, son vulnerables a diversas amenazas, como el ciberacoso, la exposición a contenidos inapropiados y el robo de identidad. Los resultados muestran que, aunque los niños son considerados nativos digitales, todavía carecen de las habilidades necesarias para navegar de forma segura en un mundo en constante cambio. Por lo tanto, es extremadamente importante que tanto los profesores como los padres asuman un papel activo en la enseñanza de prácticas responsables en línea. Esto incluye no sólo proporcionar herramientas tecnológicas sino también fomentar el diálogo abierto sobre los riesgos y beneficios del entorno digital. La educación en ciberseguridad debe ser integral y estar dirigida no solo a prevenir amenazas sino también a inculcar un sentido de responsabilidad y conciencia digital en los niños.

Además, el artículo enfatiza la importancia de las políticas públicas y la colaboración entre diferentes actores como gobiernos, instituciones educativas y empresas de tecnología para crear un entorno seguro para los niños en línea. Se necesitan leyes estrictas de seguridad cibernética para niños para establecer leyes que protejan a los menores y obliguen a las empresas a implementar medidas de seguridad efectivas. Sin embargo, estas iniciativas deben ir acompañadas de campañas de información dirigidas a padres y educadores, principales responsables de la seguridad de los niños. En conclusión, la educación en ciberseguridad es importante no solo para proteger a los niños de las amenazas actuales, sino también para capacitarlos para que se conviertan en ciudadanos digitales responsables del futuro mediante la promoción de una cultura de respeto y seguridad en el entorno digital.

Referencias.

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*, *53*(198), 169. https://doi.org/10.5354/0719-3769.2021.57067

Aznar-Martínez, B., Casarramona-Basany, A., Grané-Morcillo, J., Lorente-De-Sanz, J., Prats-Fernández, M.-À., & Ballester-Brage, L. (2024). Uso responsable de Internet y seguridad digital: revisión sistemática de programas educativos. *Estudios Sobre Educación*, 125–152. https://doi.org/10.15581/004.47.006

Barbarita Álava Zambrano, K., Eduardo Basurto Vidal, W., Ronaldo Tóala Vera, R., Superior Politécnica Agropecuaria de Manabí, E., & Félix Lopez, M. (2022). Vulnerabilidades En Los Sistemas Informáticos Owasp Top 10: Revisión Bibliográfica Vulnerabilities in Computer Systems Owasp Top 10: Bibliographic Review. *Journal Business Science*, *3*, 1–8.

Beltran Muñoz, A. (2020). Educar y proteger: análisis de la educación en ciberseguridad para combatir la ciberdelincuencia. *Journal GEEJ*, *7*(2). https://doi.org/10.1344/REYD2024.30.44082

Bustillos Ortega, O., Rojas Segura, J., & Murillo Gamboa, J. (2023). Ciberseguridad y desarrollo de

habilidades digitales: propuesta de alfabetización digital en edades tempranas. *Interfases*, *018*, 185–205. https://doi.org/10.26439/interfases2023.n018.6626

Catalina García, B., López de Ayala López, M. C., & García Jiménez, A. (2014). The risks faced by adolescents on the Internet: Minors as actors and victims of the dangers of the Internet. *Revista Latina de Comunicación Social*, *69*, 462–485. https://doi.org/10.4185/RLCS-2014-1020

Chérrez, M., Eduardo, W. I., Pesantez, Á., & Fernando I, D. I. (2021). Ciberseguridad en las redes sociales: una revisión teórica Cybersecurity in social media: a theoretical review. *Journal Article*, *8*, 06.

Criollo, E., Flores, C., Flores, C., Santacruz, J., & Ron, M. (2023). Diagnóstico y línea base de los activos de información e infraestructura crítica de ciberseguridad del estado ecuatoriano. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *7*, 101–119. https://doi.org/10.29018/issn.2588-1000vol7iss49.2023pp101-119

Cruz Lucas, G. I., Delgado Tejena, L. E., Ponce Solorzano, B. R., & Marcillo Merino, M. J. (2022). Riesgos de seguridad de los datos en la web. *Journal TechInnovation*, *1*(2), 43–49. https://doi.org/10.47230/journal.techinnovation.v1.n2.2022.43-49

Domínguez Castillo, J. G., Cisneros Cohernour, E. J., & Quiñonez Pech, S. H. (2019). Vulnerabilidad ante el uso del Internet de niños y jóvenes de comunidades mayahablantes del sureste de México. *RIDE Revista Iberoamericana Para La Investigación y El Desarrollo Educativo*, *10*(19). https://doi.org/10.23913/ride.v10i19.531

Fernández, D. (2019). *Formación TIC, características, razón de ser y contenido*. *12*, 16–27. https://doi.org/10.51302/tce.2019.243

Fernández, M. R., Soria, I. N., Collado-Valero, J., Lavigne-Cervan, R., & Domenech, B. D. (2022). Ciberacoso y Funciones Ejecutivas en niños y adolescentes una revisión sistemática. *Revista de Educacion*, *2022*(397), 67–92.

Garmendia, M., Garitaonandia, C., Mart\'\inez, G., & Casado, M. A. (2012). Los menores en internet. Usos y seguridad desde una perspectiva europea. *Quaderns Del CAC*, *38*(1), 37–44.

Guerrero-vega, R. N., Revista, E. A., Forenses, C., & Desde, E. (2024). Nuevo paradigma de la investigación : Oportunidades y desafíos del uso de las herramientas de inteligencia artificial para la elaboración y publicación de productos científicos. *Revista de Criminología y Ciencias Forenses: Ciencia, Justicia y Sociedad*, *3*(5), 0–3.

Hernández Prados, M. Á., López Vicent, P., & Gamboa Gil de Sola, G. (2021). Análisis documental sobre los riesgos y las posibilidades de internet para los menores. Pautas educativas dirigidas a familias. *Revista Interuniversitaria de Investigación En Tecnología Educativa*, 9–22. https://doi.org/10.6018/riite.430341

Herrero-Martín, J., Rodríguez-Merino, C., Valdivielso, R., & Amo, D. (2022). *Formación en ciberseguridad y educación. Variables de sensibilidad y cambio en la formación del profesorado.* 6–8. https://doi.org/10.4995/inred2022.2022.15855

Macías-Lara, R. A., Boné Andrade, M. F., Quiñonez Angulo, F., Mendoza Loor, J. J., Estupiñan-Troya, G., & Rodríguez Vizuete, J. D. (2022). Frequent cases, criminalization and prevention of computer crimes in Ecuador: a brief systematic review. *Sapienza*, *3*(2), 231–243. https://doi.org/10.51798/sijis.v3i2.324

Martín-Ramallal, P., & Ruiz-Mondaza, M. (2022). Child protection agents and social networks. The TiKToK dilemma. *Revista Mediterranea de Comunicacion*,

13(1), 31–48. https://doi.org/10.14198/MEDCOM.20776

Medina Pérez, V. H., & Vargas Ipaz, E. F. (2024). Desafíos de la Enseñanza en Línea Durante la Pandemia Desencadenada por Covid-19en la Educación Básica. Revisión Bibliográfica. *Ciencia Latina. Revista Científica Multidisciplinar*, *8*(3). https://doi.org/10.37811/cl_rcm.v8i3.11957

Miranda, R. (2014). La infancia y la adolescencia en la era digital: Nuevos retos para la garantía de sus derechos. *Revista Relações Internacionais Do Mundo Atual Unicuritiba*, *4*(42), 465–489. https://doi.org/10.21902/Revrima.v4i42.6449

Morales-Paredes, P. I., & Medina-Chicaiza, P. (2021). La Provincia De Tungurahua-Ecuador Cybersecurity for Learning Platforms in Higher Education Institutions in Tungurahua Province of Ecuador. *Ed*, *10*(2), 49–75. https://doi.org/10.17993/3ctic.2021.102.49-75

Mosquera Ayala, A. M. (2019). Tendencias investigativas en educación en Colombia: revisión documental. *Sophia*, *15*(1), 1–4. https://doi.org/10.18634/sophiaj.15v.1i.908

Núñez-Naranjo, A., & Chancusig-Toapanta, A. (2022). Technological tools as a trend in secondary education in times of COVID-19: Theoretical review. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2022*(Special Issue E50), 142–154.

Núñez-Naranjo, A. F. (2024). Analysis of the determinant factors in university dropout: a case study of Ecuador. *Frontiers in Education*, *9*(October), 1–14. https://doi.org/10.3389/feduc.2024.1444534

Olivares Ruiz, N. A., Ostos Cruz, C. E., Suárez Jasso, E., & Pale Oropeza, K. D. (2022). Ciberseguridad: Análisis de riesgos en menores de edad en tiempos de pandemia (Caso de Estudio: Teocelo, Veracruz). *Interconectando Saberes*, *14*, 41–53. https://doi.org/10.25009/is.v0i14.2767

Pillajo-García, P., & Avila-Pesantez, D. (2023). Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura. *Revista Perspectiva*, *5*, 19–20. https://doi.org/10.47187/perspectivas.5.1.179

Pinto, B., Duarte, A., & Dias, P. (2023). La influencia de los YouTubers en los niños (8-12 años): actualidad y marcas. *Doxa Comunicación. Revista Interdisciplinar De Estudios De Comunicación Y Ciencias Sociales*, *36*, 321–340. https://doi.org/10.31921/doxacom.n36a1638

Quirumbay Yagual, D. I., Castillo Yagual, C., & Coronel Suárez, I. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE*, *9*(1), 57–65. https://doi.org/10.26423/rctu.v9i1.671

Taco, A. (2022). Dispositivos wearables y los riesgos a la privacidad: Una revisión de la literatura. *Interfases*, *16*, 213–229.

Tatiana, M., Mata, A., & Estrada, U. L. (n.d.). *Y NUEVAS TECNOLOGÍAS EN NIÑOS Y RISKS IN THE USE OF SOCIAL NETWORKS AND NEW*.

Trejos-Gil, C. A., & Vélez, Y. P. (2023). Cybercrimes with Minors in the Facebook Social Network: Systematic Literature Review. *Nuevo Derecho*, *19*(32), 1–18. https://doi.org/10.25057/2500672X.1493

Trujillo-Torres, J.-M., Rodríguez-Jiménez, C., Alonso-García, S., & Berral-Ortiz, B. (2024). Revisión sistemática de la literatura sobre la seguridad digital en estudiantes de educación superior. *Información Tecnológica*, *35*(4), 1–12. https://doi.org/10.4067/s0718-07642024000400001

Villa Ramírez, J. N., Mesa Méndez, C. M., Garzón Santos, J. L., & Urueña Sanabria, R. (2023). Redes Sociales: Riesgos y desafíos para la comunidad académica de los colegios de la Policía. *Revista Logos Ciencia & Tecnología*, *15*(3), 112–128. https://doi.org/10.22335/rlct.v15i3.1857

Villarroel-molina, R., Guaña-moya, J., Iván, W., & Paredes, S. (2024). Análisis de

Vulnerabilidades de Ciberseguridad
Mediante Técnicas de Ciencia de Datos.
VICTEC, *5*(8), 95–104.