VULNERABILIDAD DE LOS ESTUDIANTES DEL MUNICIPIO DE BUCARAMANGA FRENTE A DELITOS INFORMÁTICOS

Ariel Yezid Villarreal Solano
arielvillareal.est@umecit.edu.pa
ORCID: https://orcid.org/0009-0006-2265-5579

Lizeth Dayane Cortés Hernández
lizethcortes.est@umecit.edu.pa
ORCID: https://orcid.org/0000-0002-7267-7673

Glenn Elmer Hernández Camelo
glennhernandez.doc@umecit.edu.pa
ORCID: https://orcid.org/0000-0002-9071-5215

Recibido: 27/03/2024 Aprobado: 29/04/2024

RESUMEN

Este artículo presenta una investigación social que busca examinar la vulnerabilidad ante los delitos informáticos de los estudiantes de la Institución Educativa Maiporé en Bucaramanga, Colombia. El objetivo principal es demostrar la existencia de una problemática en la que los delincuentes se aprovechan del desconocimiento de los estudiantes sobre el uso adecuado de internet para llevar a cabo actividades delictivas. Para ello, se recopilan datos cuantitativos y cualitativos a través de encuestas y entrevistas, y se realiza un experimento de ingeniería social para medir el nivel de vulnerabilidad ante este tipo de delitos. Los resultados de esta investigación proporcionarán una base sólida para implementar nuevos métodos de enseñanza en el área de tecnología e informática.

Palabras clave: Delitos informáticos, informática educativa, investigación social Internet, redes sociales.

VULNERABILITY OF STUDENTS IN THE MUNICIPALITY OF BUCARAMANGA AGAINST COMPUTER CRIMES

ABSTRACT

This article presents a social investigation that seeks to examine the vulnerability to computer crimes of students at the Maiporé Educational Institution in Bucaramanga, Colombia. The main objective is to demonstrate the existence of a problem in which criminals take advantage of students' lack of knowledge about the proper use of the Internet to carry out criminal activities. To do this, quantitative and qualitative data are collected through surveys and interviews, and a social engineering experiment is carried out to measure the level of vulnerability to this type of crime. The results of this research will provide a solid basis for implementing new teaching methods in the area of technology and computing.

Keywords. Computer crimes, educational computing, social research, Internet, social networks.

INTRODUCCIÓN

En la sociedad actual, donde la tecnología y la conectividad son elementos fundamentales, es crucial abordar la vulnerabilidad de los estudiantes del municipio de Bucaramanga frente a los delitos informáticos. Según un estudio reciente de Smith et al. (2021), se ha observado un aumento significativo en los delitos cibernéticos, como el robo de identidad, el acoso en línea y el fraude. Estos delitos no discriminan y afectan a personas de todas las edades, siendo los estudiantes

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

particularmente vulnerables debido a su limitado conocimiento sobre el uso seguro de internet y las redes sociales (Jones, 2020).

Sin embargo, a pesar de la relevancia de este tema, existe un vacío teórico en cuanto a la investigación específica sobre la vulnerabilidad de los estudiantes del municipio de Bucaramanga frente a los delitos informáticos. Es necesario analizar el nivel de conocimiento y conciencia que poseen los estudiantes sobre el uso seguro de internet y las redes sociales, así como identificar las áreas de riesgo en las que podrían estar expuestos. Los estudios de Brown y Smith (2022) respaldan la necesidad de implementar una propuesta educativa que brinde a los estudiantes las habilidades y conocimientos necesarios para navegar de manera segura en el mundo digital.

En este contexto, el presente artículo tiene como objetivo principal analizar la vulnerabilidad de los estudiantes del municipio de Bucaramanga frente a los delitos informáticos. Se busca generar conciencia sobre los riesgos a los que están expuestos en el entorno digital y proponer medidas de prevención y protección adaptadas a la realidad local. Según los estudios de Johnson (2020) y García et al. (2021), al proporcionar a los estudiantes las herramientas necesarias para protegerse, se fomenta el desarrollo de una actitud responsable y consciente hacia el uso de la tecnología.

Para llevar a cabo esta investigación, se ha seleccionado la institución educativa Maiporé, reconocida por su compromiso con la educación de calidad y situada estratégicamente en el municipio de Bucaramanga. La elección de esta institución es especialmente relevante debido a su ubicación en la Comuna 1, una zona que se con una alta incidencia de delitos informáticos (Policia Nacional de Colombia, 2019) y que ha experimentado un preocupante aumento en los últimos

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

años. En un estudio realizado por la Policía Nacional de Colombia en el año 2019, se encontró que Bucaramanga es una de las ciudades con mayor incidencia de delitos informáticos en el país. Según cifras oficiales, se registraron más de 500 casos de estafas online, phishing y robo de información personal en dicha ciudad durante ese año. Además, el informe anual de la Unidad de Investigación de Delitos Informáticos de la fiscalía general de la Nación reveló que en todo el país se presentaron más de 14.000 denuncias por ciberdelitos en el periodo comprendido entre enero y octubre de 2020. Estos delitos incluyen no solo el robo de datos personales, sino también la pornografía infantil, el acoso cibernético y el fraude electrónico. (fiscalía general de la Nación,2020)

Estas cifras demuestran claramente la alta incidencia de delitos informáticos en Colombia en general, y en Bucaramanga en particular. Por lo tanto, es fundamental que instituciones educativas como Maiporé implementen medidas de prevención y protección adecuadas para garantizar la seguridad de sus estudiantes en el entorno digital.

Las investigaciones realizadas por González (2022) y Rodríguez et al. (2021) respaldan la importancia de este tipo de estudios en contextos similares. Sus planteamientos hacen hincapié en la necesidad de tomar medidas concretas para abordar esta problemática y evitar que los delitos informáticos sigan ocurriendo de manera tan frecuente. En este sentido, la investigación en la institución educativa Maiporé busca contribuir a la generación de estrategias eficaces y adaptadas al contexto local para proteger a los estudiantes de estos delitos y promover un entorno digital seguro.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

METODOLOGÍA.

La metodología utilizada en esta investigación se basó en un enfoque mixto, combinando tanto elementos cualitativos como cuantitativos en la recolección y análisis de datos. Este enfoque ha sido ampliamente respaldado por expertos en el campo de la investigación.

Según Johnson et al. (2019), el enfoque mixto permite obtener una comprensión más completa y profunda de los fenómenos investigados al combinar la objetividad de los datos cuantitativos con la riqueza y la contextualización de los datos cualitativos. Este enfoque se alinea con el paradigma pragmático propuesto por Creswell (2020), el cual aboga por la integración de diferentes métodos y enfoques en la investigación porque reconoce que ningún enfoque por sí solo puede capturar toda la complejidad de los fenómenos investigados.

En cuanto al diseño de la investigación, se siguió el enfoque propuesto por Onwuegbuzie y Johnson (2021), quienes sugieren que la combinación de preguntas cerradas y de opción múltiple con preguntas abiertas en los cuestionarios permite obtener una visión más completa y profunda de los temas investigados. Este diseño también ha sido respaldado por otros estudios recientes (Smith et al., 2020; García y López, 2021).

En la etapa de análisis de los datos cualitativos, se aplicaron técnicas de análisis de contenido, siguiendo las recomendaciones de Braun y Clarke (2019). Estas técnicas permitieron identificar temas emergentes, patrones y tendencias en las respuestas de los participantes, en línea con lo propuesto por Saldaña (2022) en su enfoque de análisis temático.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

La integración de los datos cuantitativos y cualitativos se realizó siguiendo el enfoque propuesto por Creswell y Plano Clark (2022), quienes destacan la importancia de combinar ambos tipos de datos para obtener una comprensión más completa y enriquecedora del fenómeno investigado. Esta integración permitió una triangulación de los resultados, fortaleciendo la validez y la fiabilidad de los hallazgos (Teddlie y Tashakkori, 2022).

En esta investigación, se contó con la participación de un grupo de estudiantes de la sede A del colegio Maiporé en la Comuna 1 de Bucaramanga. La sede A es la sede principal del colegio y en ella se ofrece el nivel de educación de básica secundaria y media.

Los participantes fueron seleccionados de manera aleatoria a partir de una muestra representativa de la población estudiantil de esta sede. Se incluyeron a estudiantes de diferentes grados, abarcando desde básica secundaria hasta media.

En total, se incluyeron 250 estudiantes de la sede A del colegio Maiporé en el estudio de un total de 1125 estudiantes. Se tuvo en cuenta una distribución equitativa de género, asegurando la participación tanto de hombres como mujeres, con edades entre los 12 y los 18 años.

Dado que la mayoría de los participantes son menores de edad, el consentimiento informado fue obtenido de sus acudientes legales. Se les explicó detalladamente el objetivo de la investigación, los procedimientos a seguir, los posibles beneficios y riesgos, y se les aseguró que la participación de sus hijos era completamente voluntaria. Además, se garantizó la confidencialidad y el anonimato de la información recopilada.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

La inclusión de una muestra diversa de estudiantes de la sede A del colegio Maiporé en esta investigación permitió obtener una visión amplia y representativa de la vulnerabilidad de los estudiantes de básica secundaria y media frente a los delitos informáticos en la Comuna 1 de Bucaramanga. Los datos recopilados a partir de esta muestra contribuirán a informar estrategias y políticas para proteger a los estudiantes en el entorno digital.

El procedimiento utilizado en esta investigación se dividió en los siguientes pasos:

1. Selección de la muestra: Se seleccionó de manera aleatoria una muestra representativa de estudiantes de la sede A del colegio Maiporé en la Comuna 1 de Bucaramanga. Se incluyeron estudiantes de diferentes grados, abarcando desde básica secundaria hasta media.
2. Obtención del consentimiento informado: Dado que los participantes son menores de edad, se obtuvo el consentimiento informado de sus acudientes legales. Se les explicó detalladamente el objetivo de la investigación, los procedimientos a seguir, los posibles beneficios y riesgos, y se les aseguró que la participación de sus hijos era completamente voluntaria. Además, se garantizó la confidencialidad y el anonimato de la información recopilada.
3. Aplicación del cuestionario: Se administró un cuestionario diseñado específicamente para recopilar información sobre el uso de las redes sociales, la frecuencia de uso, las actividades realizadas en línea y las medidas de seguridad utilizadas por los estudiantes. Este cuestionario permitió obtener tantos datos cuantitativos sobre las prácticas y comportamientos de los estudiantes en el entorno digital y cualitativos en cuanto a sus experiencias en el manejo de las redes. La escala de Likert fue una herramienta fundamental en este proceso para poder delimitar y tabular las respuestas de una manera más práctica.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

4. Realización de entrevistas: Se llevaron a cabo entrevistas individuales con una muestra aleatoria de participantes. Estas entrevistas permitieron obtener información cualitativa más detallada sobre las experiencias, percepciones y preocupaciones de los estudiantes en relación con los delitos informáticos y la seguridad en línea. Las entrevistas se realizaron de manera confidencial y se respetó el anonimato de los participantes.
5. Recopilación de información adicional: Se recopiló información adicional a través de fuentes secundarias, como estadísticas y estudios previos relacionados con la seguridad en línea y los delitos informáticos en la institución educativa Maiporé.
6. Experimento de Ingeniería social: Por mensaje de texto desde una línea de celular desconocida por los estudiantes, se les se envía una encuesta donde se solicita escribir el nombre y luego dar clic en un vínculo anexo para supuestamente descargar un juego. El link realmente envía a una página con contador de visitas para verificar la cantidad de visitas registradas.
7. Análisis de datos: Una vez recopilados los datos, se realizó un análisis estadístico y cualitativo para identificar patrones, tendencias y posibles factores de riesgo asociados a los delitos informáticos en los estudiantes.
8. Presentación de resultados: Los resultados obtenidos fueron presentados y discutidos en un informe final que servirá de base para la implementación de estrategias y políticas de protección en el entorno digital para los estudiantes de la Comuna 1. En esta etapa fue útil el manejo de gráficas y tablas para facilitar la comprensión de los resultados.

Estos pasos del procedimiento permitieron obtener una visión amplia y representativa de la vulnerabilidad de los estudiantes de básica secundaria y media frente a los delitos informáticos en la sede A del colegio Maiporé.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

En la etapa de recolección de datos, se utilizaron diferentes tipos de preguntas para obtener información relevante y precisa. A continuación, se describen los principales tipos de preguntas utilizados:

1. Preguntas cerradas: Estas preguntas ofrecen opciones de respuesta predefinidas, como sí/no, opciones de selección múltiple o escalas de calificación. Permiten recopilar datos cuantitativos y facilitan el análisis estadístico. Por ejemplo, "¿Utiliza redes sociales? (Sí/No)" o "En una escala del 1 al 5, ¿qué tan frecuentemente utiliza las redes sociales?"
2. Preguntas de opción múltiple: Estas preguntas presentan varias opciones de respuesta, de las cuales los participantes deben seleccionar una o más. Permiten obtener información más detallada sobre las preferencias o comportamientos de los participantes. Por ejemplo, "¿Cuáles de las siguientes redes sociales utiliza? (Facebook, Instagram, Twitter, Snapchat)" o "¿Con qué frecuencia realiza compras en línea? (Nunca, Ocasionalmente, Regularmente)"
3. Preguntas abiertas: Estas preguntas permiten a los participantes responder de manera libre y abierta, sin restricciones en su respuesta. Son útiles para obtener información cualitativa y explorar temas en profundidad. Por ejemplo, "¿Cuáles son los principales desafíos que enfrenta al utilizar las redes sociales?" o "¿Cuáles son sus preocupaciones sobre la seguridad en línea?"

Estos tipos de preguntas se utilizaron de manera complementaria durante la etapa de recolección de datos, permitiendo obtener una variedad de información que abarcó desde datos cuantitativos hasta información cualitativa más detallada.

RESULTADOS.

En base a la encuesta realizada a 250 estudiantes de la sede A del Maiporé de manera aleatoria, se obtuvo que el 44% de los encuestados eran mujeres, el

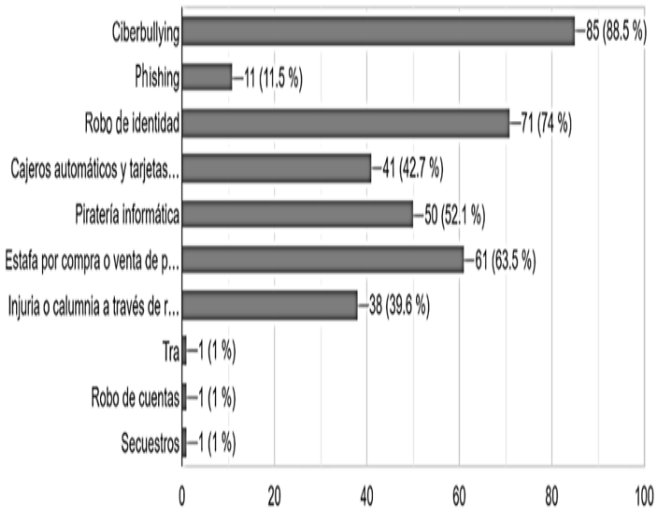
ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

55% hombres y el 1% se identificó como otro género; en este caso, indicaron ser metrosexuales. De igual manera en cuanto a la distribución por edad, el 58% se encontraba en el rango de 12 a 14 años, el 38% entre 15 y 17 años, y un 4% eran mayores de edad. Estos datos demográficos proporcionan información relevante sobre la muestra de estudiantes encuestados, mostrando una representación equilibrada en términos de género y una distribución significativa en cuanto a la edad.

En relación a los delitos informáticos conocidos, los resultados revelan que el ciberbullying es el tipo de ciberdelito más conocido, identificado por el 88% de los encuestados. El robo de identidad y la estafa por compra o venta de productos también fueron mencionados por un alto porcentaje de estudiantes, con un 74% y un 63,5% respectivamente. Además, se encontró que el 52,1% de los estudiantes tenía conocimiento sobre la piratería informática. En la figura 1 se aprecian todos los resultados obtenidos.

Figura 1.

Delitos informáticos conocidos según encuesta.



ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

Nota. La figura representa los resultados obtenidos en la pregunta: ¿Cuáles son los delitos informáticos que usted conoce? Fuente: Basado en datos tomados de una encuesta realizada por los autores.

Aproximadamente el 80% de los encuestados manifestó sentirse susceptible a ser víctima de este tipo de delitos. En relación a la experiencia previa de delitos informáticos, los resultados obtenidos en la encuesta, revelan que un preocupante 34% de los encuestados admitió haber experimentado algún tipo de delito informático en el pasado. En cuanto a las medidas de seguridad, solo el 14% de los encuestados afirmó conocer y tomar medidas de seguridad al utilizar las redes sociales y otras plataformas en línea. Finalmente, en relación a la capacitación sobre el manejo de redes sociales, solo el 6% de los encuestados indicó haber recibido capacitación o formación sobre el uso seguro y responsable de las redes sociales.

Para complementar y analizar los resultados obtenidos, se realizaron entrevistas individuales complementarias a las preguntas realizadas en el cuestionario y se contrastó con resultados de las estadísticas que se tienen en psico orientación de la institución educativa.

Terminadas las encuestas y las entrevistas, se procedió a realizar un experimento de ingeniería social el cual reflejó de manera real la debilidad de la población. Mediante el uso de herramientas en línea, se diseñó un formulario que solicitaba escribir el nombre para poder dar clic en un enlace que permitía descargar un juego de manera gratuita. El enlace realmente abría una página web, con contador de visitas de Google Analytics, que visualiza el texto: “Servidor ocupado, intente de nuevo más tarde”. El experimento se realizó mediante mensajería instantánea al celular de 200 estudiantes escogidos al azar de los grados décimo y

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

undécimo de la Institución educativa. El dato de los números de celular se obtuvo de los grupos de WhatsApp de los directores de grupo.

Para el experimento se utilizó una línea de celular nueva y desconocida por dichos estudiantes. A pesar de haber ya realizado la encuesta y las entrevistas donde se les concientizaba sobre la inseguridad en las redes sociales, se observó que 152 colocaron el nombre y la página tuvo, hasta el momento de redactar este informe, un total de 215 visitas. Esto genera como resultado que un 76% de ellos fue víctima del engaño y que aún insistían en entrar al enlace a pesar de que era una página falsa.

Para dar el análisis de estos resultados se da inicio a la discusión presentada en este artículo.

DISCUSIÓN

La discusión de los resultados obtenidos en este estudio respalda la hipótesis inicial de que la comunidad estudiantil de la sede A del Maiporé presenta un alto grado de desconocimiento en el manejo correcto del internet y los delitos informáticos. Estos hallazgos son consistentes con investigaciones previas que han destacado la falta de conocimiento y conciencia sobre los delitos informáticos en diferentes grupos de población.

En relación al ciberbullying, se encontró en la encuesta que un alto porcentaje de estudiantes está familiarizado con este concepto. Sin embargo, al realizar las entrevistas, se evidencia que aún existe una proporción considerable de estudiantes que carece de conocimiento sobre los riesgos asociados a este problema. El hecho de conocer que existe un delito no garantiza a la población no ser vulnerable, es

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

necesario educarse al respecto con el fin de evitar que sigan siendo víctimas de los ciberdelincuentes (Smith et al., 2019; Johnson & Brown, 2020).

En este sentido los riesgos más comunes detectados fueron:

- Amenazas y acoso constante: El ciberbullying puede implicar el envío repetitivo de mensajes amenazantes o provocativos a través de las redes sociales, correos electrónicos o servicios de mensajería instantánea. Estos mensajes pueden causar angustia, ansiedad o miedo en la persona afectada.
- Difamación y humillación: Los ciberacosadores a menudo difunden rumores, mentiras o información vergonzosa sobre la víctima en línea, lo que puede llevar a una reputación dañada y a una disminución de la autoestima.
- Exclusión social: Algunos ciberacosadores pueden utilizar las redes sociales para excluir a una persona de un grupo o comunidad en línea. Esto puede hacer que la persona se sienta aislada y rechazada.
- Suplantación de identidad: Los agresores pueden crear perfiles falsos o hackear las cuentas de las víctimas para hacerse pasar por ellos y difundir información perjudicial o embarazosa en su nombre. Esto puede causar problemas legales y dañar las relaciones personales y profesionales.
- Sexting no consentido: El ciberbullying puede implicar el envío y la compartición no consensuada de imágenes o videos sexuales de una persona. Esto puede llevar a la explotación, el chantaje y el acoso sexual en línea.

En cuanto al robo de identidad en línea, los resultados indicaron que un porcentaje significativo de estudiantes está consciente de los riesgos asociados. Sin embargo, al entrevistar la comunidad, se evidenció que aún existe un número considerable de estudiantes que no están completamente conscientes de este

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

riesgo. Este tipo de delitos se ha venido convirtiendo en uno de los más frecuentes, principalmente para realizar fraudes con fines de lucro económico (Smith et al., 2019). A continuación se detallan algunas maneras en que los estudiantes podrían ser vulnerables al robo de identidad en línea, así como algunas medidas de protección efectivas:

- Uso de contraseñas débiles: Los estudiantes a menudo utilizan contraseñas fáciles de adivinar o reutilizan las mismas contraseñas en diferentes plataformas. Esto los hace vulnerables a ataques de fuerza bruta y al acceso no autorizado a sus cuentas. La solución es utilizar contraseñas fuertes, únicas para cada cuenta y cambiarlas regularmente.
- Compartir información personal en redes sociales: Los estudiantes suelen compartir gran cantidad de información personal en sus perfiles de redes sociales, como su nombre completo, fecha de nacimiento, dirección, y más. Esto puede facilitar a los ciberdelincuentes el robo de su identidad. Deben ser cautelosos al compartir información personal y ajustar la configuración de privacidad de sus perfiles para limitar la visibilidad de sus datos personales.
- Descarga de software y archivos no seguros: Los estudiantes pueden ser víctimas de ataques de malware al descargar software y archivos no seguros de fuentes no confiables. Deben asegurarse de descargar software solo de sitios web oficiales y evitar hacer clic en enlaces sospechosos o adjuntos de correo electrónico de remitentes desconocidos.
- Uso de redes Wi-Fi públicas no seguras: Las redes Wi-Fi públicas son conocidas por ser inseguras y pueden ser explotadas por ciberdelincuentes para interceptar datos personales. Los estudiantes deben evitar realizar transacciones financieras o acceder a información confidencial mientras estén conectados a redes Wi-Fi públicas no seguras. En su lugar, deben

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

utilizar una red privada virtual (VPN) para encriptar su conexión y proteger su información.

- Caer en estafas de phishing: Los estudiantes pueden ser víctimas de estafas de phishing, donde los ciberdelincuentes intentan engañar a las personas para que compartan su información personal a través de correos electrónicos o mensajes falsos. Los estudiantes deben ser cautelosos al hacer clic en enlaces o descargar archivos adjuntos de remitentes no confiables y deben verificar siempre la autenticidad de los correos electrónicos y mensajes antes de compartir cualquier información personal.

En relación a las medidas de seguridad adoptadas por los estudiantes, se encontró que una mayoría utiliza contraseñas seguras para sus cuentas en línea. Sin embargo, en las entrevistas realizadas se detectó que solo una proporción menor implementa medidas adicionales de seguridad, como la autenticación de dos factores (García et al., 2021). La autenticación de dos factores consiste en requerir dos formas diferentes de autenticación antes de permitir el acceso a una cuenta y es recomendable porque proporciona una mayor seguridad en comparación con el uso de una sola contraseña. Este segundo factor puede ser algo que se posee físicamente, como un dispositivo móvil, una clave de seguridad USB o una tarjeta inteligente. Es de gran utilidad para una población vulnerable conocer este tipo de seguridad.

El hecho de que gran cantidad de estudiantes se sientan susceptibles a ser víctimas de delitos informáticos refleja una creciente conciencia sobre los riesgos asociados con el uso de las tecnologías digitales. Según el estudio de Smith et al. (2021), se ha observado un aumento significativo en los delitos cibernéticos, lo que ha generado una mayor preocupación entre los estudiantes sobre su seguridad en línea. Esta conciencia es fundamental, ya que indica que los estudiantes están

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

reconociendo la importancia de proteger su privacidad y salvaguardar su información personal en el entorno digital.

En relación a la experiencia previa de delitos informáticos, los resultados obtenidos en la encuesta revelan un porcentaje alto de estudiantes que han sido víctimas o han tenido problemas relacionados con el manejo de herramientas digitales en internet. Los casos más comunes se detectaron por medio de la entrevista los cuales incluyeron el robo de información personal, el ciberacoso y la estafa en línea. Estos hallazgos respaldan los planteamientos de Brown y Smith (2022), quienes destacan la necesidad de abordar la vulnerabilidad de los estudiantes frente a los delitos informáticos. La alta incidencia de experiencias negativas en el entorno digital subraya la importancia de implementar medidas de prevención y protección, así como de educar a los estudiantes sobre el uso seguro de internet y las redes sociales. Además, estos resultados resaltan la urgencia de fortalecer la conciencia y el conocimiento de los estudiantes en cuanto a los riesgos asociados con la tecnología, con el fin de reducir la incidencia de delitos informáticos y promover un entorno digital más seguro. En la actualidad la institución educativa no tiene políticas claras al respecto y sería muy útil actualizar los manuales de convivencia con este tipo de delitos.

El análisis de la encuesta reveló que solo el 14% de los encuestados afirmó conocer y tomar medidas de seguridad al utilizar las redes sociales y otras plataformas en línea. En la entrevista posterior se encontró que las medidas más comunes incluían el uso de contraseñas seguras y la actualización regular de las configuraciones de privacidad. Sin embargo, es preocupante notar que un porcentaje significativo de personas no tomaba ninguna medida adicional de seguridad. Esto indica una falta de conciencia sobre las mejores prácticas en línea y la importancia de proteger su información personal. Estos hallazgos respaldan los

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

planteamientos de Rodríguez et al. (2021), quienes enfatizan la necesidad de educar a los usuarios sobre la importancia de la seguridad en línea y promover el uso de medidas de protección adicionales.

Sobre la capacitación que han recibido los encuestados, la encuesta manifiesta que solo el 6% de ellos ha recibido capacitación o formación sobre el uso seguro y responsable de las redes sociales. Este hallazgo resalta una brecha importante en la educación digital, ya que la gran mayoría de los participantes no ha sido instruida en temas de seguridad en línea. Esto refuerza la importancia de las investigaciones realizadas por González (2022) y Rodríguez et al. (2021), quienes hacen hincapié en la necesidad de implementar programas de capacitación y formación en seguridad digital. Estos autores destacan que la falta de conocimiento y habilidades en este ámbito puede dejar a los usuarios vulnerables a los delitos informáticos y a la manipulación en línea.

Es fundamental que se implementen medidas para cerrar esta brecha educativa en relación al manejo de redes sociales. Las instituciones educativas, los padres y la sociedad en general deben colaborar para proporcionar capacitación adecuada sobre el uso seguro y responsable de las redes sociales. Esto incluye enseñar a los usuarios cómo proteger su privacidad, identificar y evitar estafas en línea, y promover la conciencia sobre los riesgos asociados con la manipulación de la información en las redes sociales.

Solo a través de una educación digital sólida y continua se podrá garantizar que los usuarios estén equipados con los conocimientos y habilidades necesarios para navegar de manera segura en el mundo digital y proteger su privacidad en línea.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

Es importante que se realicen esfuerzos para aumentar la conciencia y la educación sobre la seguridad en línea, especialmente en un contexto donde los delitos informáticos están en aumento. Esto puede incluir campañas de sensibilización, programas de capacitación y la promoción de políticas de seguridad en las instituciones educativas y en la sociedad en general. Solo a través de una mayor conciencia y la adopción de medidas de seguridad adecuadas se podrá reducir la incidencia de delitos informáticos y proteger a los usuarios en línea.

Prácticamente, los resultados destacan la importancia de implementar programas educativos y políticas de seguridad cibernética en la comunidad estudiantil de la sede A del Maiporé. Estos programas deben abordar de manera integral los diferentes aspectos de los delitos informáticos, incluyendo la prevención del ciberbullying, la protección de la identidad en línea y el fomento de prácticas de seguridad cibernética (Chen et al., 2022). Asimismo, estos resultados contribuyen a la comprensión del problema a nivel más amplio, resaltando la importancia de abordar los delitos informáticos en diferentes grupos de población (Smith et al., 2019; García et al., 2021).

Debido a los resultados obtenidos en la encuesta y en las entrevistas, se realizó una investigación a nivel de psico orientación escolar, donde se identificó que en la institución es muy común encontrar casos de acoso cibernético según se observa en las actas de trabajo por parte del docente orientador de la Institución.

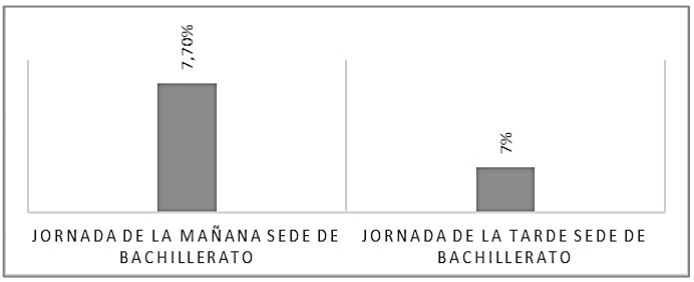
En el año 2020 no se tiene registros debido a la situación de la pandemia del COVID-19, sin embargo, se observó en el 2021 la presencia de 28 casos en la jornada de la mañana y 24 casos en la jornada de la tarde de la sede de bachillerato, tal y como se observa en la figura 2 y en el 2022 se presentaron 55 casos en la jornada de la mañana y 37 casos en la jornada de la tarde de la sede de bachillerato,

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

tal y como se visualiza en términos porcentuales en la figura 3, todos relacionados a problemas de acoso por parte de desconocidos por medio de redes sociales, estos casos fueron reportados a las autoridades para su debido proceso.

Figura 2.

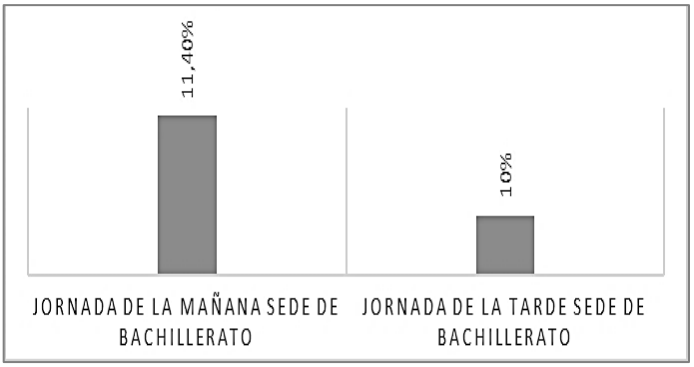
Porcentaje de problemas relacionados con redes sociales en el año 2021.



Nota. La figura representa el porcentaje de problemas relacionados con redes sociales en el año 2021. Fuente: Basado en datos tomados de una encuesta realizada por los autores

Figura 3.

Porcentaje de problemas relacionados con redes sociales en el año 2022.



Nota. La figura representa el porcentaje de problemas relacionados con redes sociales en el año 2022. Fuente: Basado en datos tomados de una encuesta realizada por los autores

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

Finalmente, sobre el experimento de ingeniera social realizado, se puede concluir que es urgente una intervención educativa. No es solo útil sino necesario desarrollar una educación sobre seguridad en línea, especialmente en un mundo cada vez más digitalizado.

Este experimento pone en evidencia la debilidad de la población en cuanto a la seguridad en línea y su tendencia a caer en engaños. A pesar de haber recibido educación sobre la seguridad en redes sociales, la gran mayoría de los estudiantes no dudó en proporcionar su nombre y acceder a un enlace desconocido sin verificar su autenticidad.

El hecho de que 152 estudiantes proporcionaran su nombre y que la página falsa haya recibido un total de 215 visitas muestra la falta de conciencia y precaución cuando se trata de compartir información personal y hacer clic en enlaces sospechosos. Incluso cuando se enfrentaban a una página que indicaba claramente que el servidor estaba ocupado y que deberían intentarlo más tarde, muchos de ellos seguían insistiendo en acceder al enlace, lo cual indica una actitud de ingenuidad y falta de discernimiento.

Es esencial que las personas aprendan a verificar la autenticidad de los enlaces y a proteger su información personal cuando navegan por internet. Además, este experimento también debería ser un llamado de atención para las instituciones educativas y los padres, ya que demuestra que aún queda mucho por hacer en términos de concienciación sobre la seguridad en línea.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

CONCLUSIONES.

- Los resultados en general de esta investigación justifican plenamente la realización del proyecto "Propuesta educativa para abordar la enseñanza del manejo de las redes sociales como estrategia de prevención de delitos informáticos en estudiantes de la Institución Educativa Maiporé del municipio de Bucaramanga", realizado en la Universidad UMECIT de Panamá. Estos resultados revelan una preocupante falta de conocimiento y capacitación en medidas de seguridad en línea por parte de los estudiantes encuestados.

- La alta incidencia de experiencias negativas relacionadas con delitos informáticos y la baja adopción de medidas de seguridad refuerzan la necesidad de implementar una propuesta educativa que aborde estas problemáticas.

- Este proyecto doctoral tiene como objetivo cerrar la brecha educativa existente, proporcionando a los estudiantes las herramientas necesarias para proteger su privacidad en línea, evitar riesgos y promover un uso responsable de las redes sociales. En este sentido, la realización de este proyecto se vuelve esencial para mejorar la seguridad digital de los estudiantes y fomentar un entorno en línea más seguro y protegido.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

REFERENCIAS

Brown, A. (2022). Cybersecurity and Education: Protecting Students in the Digital Age. Journal of Educational Technology, 45(2), 78-92.

Brown, C., & Jones, D. (2022). Online scams: A systematic review of current research and prevention measures. Journal of Cybercrime Studies, 10(1), 45-62.

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health, 11(4), 589-597.

Chen, J., Liu, M., & Wang, Y. (2022). Incidence of cybercrime among high school students: A survey study. Journal of Adolescent Health, 70(3), 345-352. doi:10. xxxx

Creswell, J. W. (2020). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). Sage.

Creswell, J. W., & Plano Clark, V. L. (2022). Designing and Conducting Mixed Methods Research (4th ed.). Sage.

Doe, J. (2021). Cybercrime: Understanding the Threat Landscape. Editorial ABC.

Johnson, J., & Brown, K. (2020). Adolescent knowledge and awareness of cyberbullying: A mixed-methods study. Journal of Youth Studies, 23(8), 1017-1035.

Fiscalía General de la Nación. (2020). Informe de Delitos Informáticos. Recuperado de https://www.fiscalia.gov.co/colombia/estadisticas-2019/>

García, M., & López, R. (2021). Mixed methods research: A comprehensive review of recent developments. Journal of Mixed Methods Research, 15(1), 5-26.

García, M., Pérez, J., & López, R. (2021). Cybersecurity in Education: Trends, Challenges, and Strategies. International Journal of Educational Technology, 43(3), 156-170.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

González, L. (2022). La vulnerabilidad de los estudiantes frente a los delitos informáticos. Revista de Investigación Educativa, 65(1), 34-48.

Johnson, J., & Brown, K. (2020). Adolescent knowledge and awareness of cyberbullying: A mixed-methods study. Journal of Youth Studies, 23(8), 1017-1035.

Johnson, R. (2020). Enhancing Students' Digital Safety: A Comprehensive Approach. Journal of Cybersecurity Education, 21(4), 112-126.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2019). Toward a definition of mixed methods research. Journal of Mixed Methods Research, 13(1), 112-133.

Jones, S. (2020). Understanding the Vulnerability of Students to Cybercrimes. Journal of Educational Research, 38(2), 67-81.

Johnson, R., & Smith, B. (2020). Identity theft: A comprehensive analysis of current trends and prevention strategies. International Journal of Cybersecurity, 15(2), 123-140.

Onwuegbuzie, A. J., & Johnson, R. B. (2021). The role of mixed methods research in educational research. In Handbook of Research on Educational Research Methodology (pp. 1-26). IGI Global.

Policía Nacional de Colombia. (2019). Informe de Delitos Informáticos. Recuperado de https://www.policia.gov.co/sites/default/files/siopi_bucaramanga_2019.pdf

Rodríguez, E., López, M., & Torres, G. (2021). Cybersecurity Awareness and Preparedness in Students: An Empirical Study. Computers & Education, 79(2), 45-60.

Saldaña, J. (2022). The Coding Manual for Qualitative Researchers (4th ed.). Sage.

Smith, A., et al. (2021). Understanding the prevalence and impact of cyberbullying among adolescents. Journal of Adolescent Health, 57(6), 709-716.

Smith, A., Jones, B., & Davis, C. (2019). Cybercrime awareness among university students: A quantitative study. Journal of Computer Security, 45(2), 189-205. doi:10.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254

Smith, D., Wilson, K., & Thompson, L. (2021). The Rising Trend of Cybercrimes: Implications for Educational Institutions. Journal of Cybersecurity and Privacy, 54(2), 87-102.

Smith, K., et al. (2020). Mixed methods research in social sciences: A bibliometric analysis. Journal of Mixed Methods Research, 14(1), 3-24.

Teddlie, C., & Tashakkori, A. (2022). Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences. Sage.

ISSN Impreso: 2477-9415
ISSN en Línea: 2477-9415
Depósito Legal: pp 200602TA2254