Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Artículo científico

DOI: http://doi.org/10.15517/revedu.v47i2.53905

Inclusión de la formación en prevención y atención de delitos informáticos en la educación policial

Inclusion of Prevention and Handle of Cybercrime in Police Education Training

Fredy Yesid Avila Niño
Escuela de Policía Rafael Reyes
Santa Rosa de Viterbo,
Colombia
segundo.avila@correo.policia.gov.co
https://orcid.org/0000-0002-4266-9621

Paola Maritza Rincón Núñez
Escuela de Policía Rafael Reyes
Santa Rosa de Viterbo,
Colombia
paola.rinconn@correo.policia.gov.co
https://orcid.org/0000-0002-9366-9218

Recepción: 22 de marzo 2023
Aprobación: 24 de mayo 2023

¿Cómo citar este artículo?

Avila-Niño, F. Y. y Rincón-Núñez, P. M. (2023). Inclusión de la formación en prevención y atención de delitos informáticos en la educación policial. Revista Educación, 47(2). http://doi.org/10.15517/revedu.v47i2.53905

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

RESUMEN

El objetivo de la investigación fue generar una estrategia que les permitiera a las aspirantes a patrulleras de la Escuela de Policía Rafael Reyes la obtención de conocimientos y la adopción de buenas prácticas, para evitar afectaciones por un delito informático, específicamente, phishing, vishing, smishing, suplantación o estafa. Lo anterior, orientado al fortalecimiento del servicio de Policía, con el propósito de que, desde el proceso de formación, se busque que las personas estudiantes adquieran las competencias básicas en este campo y se tenga conocimiento del procedimiento a seguir, en caso de ser víctima o de atender a la ciudadanía afectada por este tipo de delitos. Esta investigación empleó un enfoque mixto que combinó elementos cualitativos y cuantitativos. Inicialmente, se realizó a través de una encuesta aplicada a 220 personas estudiantes del técnico profesional en servicio de policía. Se identificaron los delitos informáticos más comunes, que han afectado a la comunidad académica. Adicionalmente, por medio del servicio del CAI Virtual: ciberincidentes, se conocieron cuáles fueron los delitos que más se denunciaron en el país durante el año 2022. Del mismo modo, se consultaron registros estadísticos de las conductas punibles registradas en el Sistema de Información Estadístico Delictivo y Contravencional de la Policía Nacional de Colombia – SIEDCO y se tomaron como referencia las 5 modalidades más denunciadas. Finalmente, se buscó generar competencias en las aspirantes a patrulleras frente a la atención de delitos informáticos, mediante el diseño de una aplicación móvil, en la cual se encuentra la información sobre estos delitos informáticos y las medidas de protección, además de herramientas en línea e indicaciones para realizar una denuncia. Para este caso de estudio, se logró evidenciar que las instituciones educativas, especialmente las de formación policial, la ciberseguridad debe ser una prioridad e incluirse en el plan de estudios temas de prevención y cuidado digital.

PALABRAS CLAVE: Delito informático, Prevención del crimen, Tecnología, Formación, Educación policial.

ABSTRACT

The objective of the research consisted of developing a strategy through which aspiring police officers of the Rafael Reyes Police School could acquire knowledge and adopt practices to prevent cybercrime, specifically, phishing, vishing, smishing, impersonation, and scamming. This strategy aimed to strengthen the police service by ensuring that students acquire basic competencies in this field and are familiar with the procedures to follow in the event of being a victim or assisting affected individuals. The research employed a mixed-method approach, combining qualitative and

quantitative elements. Initially, the researchers surveyed 220 students enrolled in the professional police service technician program to identify the most common cybercrimes that have affected the academic community. Additionally, by using the Virtual CAI (Cyber Incidents) service, the investigators identified the most reported crimes in the country during 2022. Moreover, statistical records of criminal activities registered in the Statistical Criminal and Contraventional Information System of the National Police of Colombia (SIEDCO) were also consulted, focusing on the five most frequently reported modalities. Finally, the authors sought to develop competencies in aspiring police officers to address cybercrimes by designing a mobile application that provides information on these felonies, protective measures, online tools, and instructions to file an official complaint. This case study highlighted the need for educational institutions, especially police training institutions, to prioritize cybersecurity and include topics of prevention and digital safety in their curriculum.

KEYWORDS: Cybercrime, Crime Prevention, Technology, Training, Police Education.

INTRODUCCIÓN

El objetivo de este artículo fue educar a las futuras patrulleras de la Policía Nacional en temas como la estrategia de prevención y atención de delitos informáticos. Esto parte de la educación en ciberseguridad, es decir, educar a las personas usuarias de tecnología (en este caso a las personas estudiantes) sobre los riesgos potenciales a los que se enfrentan al usar herramientas de comunicación en Internet, como lo son: redes sociales, chat, juegos en línea, correo electrónico y mensajería instantánea. Para esto, además de la sensibilización y capacitación en estos temas, se desarrolló una aplicación móvil que contiene consejos y buenas prácticas para evitar ser afectado por estos delitos, así como instrucciones sobre cómo denunciar y un apartado de preguntas frecuentes.

El desarrollo de este trabajo de investigación es importante y de impacto dentro de la Escuela de Policía Rafael Reyes y en la Policía Nacional de Colombia, esto en la medida en que es posible incluir la formación específica en temas de prevención frente a los delitos informáticos y se generan competencias en las aspirantes a patrulleras de la Policía Nacional, lo que favorecerá su perfil y capacidades para atender este tipo de situaciones cuando presten el servicio de Policía en las comunidades.

Es común que las personas sean víctimas de estos delitos por desconocimiento o por realizar malas prácticas en cuanto al manejo de los diferentes dispositivos y servicios de internet. Los delitos informáticos se presentan con mayor frecuencia en el país y es un desafío que debe enfrentar la Policía

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Nacional, ya que, para los delincuentes, resulta más beneficioso tratar de engañar o estafar a las personas a través de internet. Por tal motivo, es fundamental que las personas funcionarias de Policía cuenten con competencias básicas en cuanto a seguridad digital y tengan claro el procedimiento que se debe realizar cuando una persona ha sido víctima de un ataque cibernético.

Por otra parte, los funcionarios egresados de este centro de formación policial podrán contar con los conocimientos básicos en cuanto a la prevención de los delitos informáticos y será posible generar un impacto en el lugar de trabajo asignado a nivel nacional. Así, junto con la comunidad, se podrán desarrollar estrategias y planes para que la ciudadanía esté informada sobre cómo podría evitar estos riesgos, o en caso contrario, como actuar frente a una afectación de este tipo.

El artículo se estructura de la siguiente manera: se inicia con los antecedentes prácticos, contextualizando el tema de investigación y resaltando las necesidades y problemáticas existentes; luego, se presentan los referentes conceptuales, revisando teorías, enfoques y estudios previos para establecer una base sólida; por otro lado, se presenta la metodología empleada, en la cual se detallan los procedimientos y herramientas utilizados en el estudio; después, se presentan los resultados de manera clara, analizándolos con relación a los objetivos e información existente; por último, en las conclusiones, se resumen los hallazgos clave y su importancia, ofreciendo recomendaciones prácticas para futuras acciones. En conjunto, el artículo brinda una visión completa y coherente de la investigación, proporcionando información descriptiva e interpretativa para comprender y abordar el tema de manera efectiva.

Antecedentes prácticos

A medida que las tecnologías de la información y comunicación se integran cada vez más en nuestra sociedad, los delitos informáticos se han convertido en un peligro generalizado a escala mundial. Según cifras presentadas en el informe Digital 2022 April Global Statshot, hay 5000 millones de personas en línea en todo el mundo (We are social, 2022). Este es un escenario interesante para los ciber criminales, ya que la mitad de la población puede correr el riesgo de ser víctima de un delito cibernético. En el caso de Colombia, la población está compuesta por 51.39 millones de personas, donde el 82% vive en áreas urbanizadas, y existen 65.5 millones de teléfonos conectados a internet. Si este dato es comparado con la población, significa que, en proporción, cada colombiano tiene en promedio 1.2 teléfonos móviles y la cantidad de usuarios conectados a Internet equivale a 35.5 millones; o bien, el 69.1% de la población puede utilizar el servicio. En cuanto al uso de las

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

redes sociales, Colombia tiene 45.8 millones de usuarios activos, que corresponde al 81% de la población (Rosgaby, 2022).

La pandemia de COVID-19 ha generado una convergencia acelerada de los espacios físicos y cibernéticos, donde muchas de las tareas esenciales en el ámbito laboral y personal son cada vez más dependientes de la conectividad. Así es como la ciberdelincuencia ha tomado mayor fuerza y cada vez es más complejo identificar si un correo o mensaje es legítimo. Esto configura un gran desafío para las fuerzas del orden en todo el mundo y, específicamente para este caso de estudio, para la Policía Nacional de Colombia.

Al evaluar el rol que debe desempeñar la educación superior en el mantenimiento del orden, es imperativo que se tenga en cuenta qué tipo de agentes de policía la comunidad necesita (Bryant et al., 2014). Así, la sociedad requiere policías que estén capacitados y que tengan dominio de las nuevas tendencias delictivas. Por otra parte, los funcionarios de Policía no solo necesitan "saber cosas", sino ser capaces de promover buenas prácticas en cuanto al uso de las nuevas tecnologías y generar acciones preventivas frente a los delitos informáticos.

Los cuerpos de Policía alrededor del mundo no pueden permitir que su proceso formativo no cuente con temáticas relacionadas a la prevención y atención de delitos informáticos. Además, deben involucrarse y adaptarse a las sinergias emergentes entre la tecnología y el crimen. En el artículo *Educating the Technology Officer of the Future: A Needs Analysis*, se destaca la necesidad de contratar una fuerza laboral con conocimientos tecnológicos dentro del sector de la justicia penal. Del mismo modo, se plantean preguntas más amplias sobre el papel de la educación secundaria en la enseñanza de habilidades tecnológicas para aquellos que se convertirán en los agentes del orden (Wydra, 2015). Asimismo, en el Plan Estratégico de la Iniciativa Nacional para la Educación en Seguridad Cibernética, se sugiere que las TIC deben integrarse de manera más sistemática en la educación formal (National Initiative for Cybersecurity Education [NICE], 2016).

Para el desarrollo de esta investigación, se utilizaron como referencia algunos estudios que se han realizado en otros países, por ejemplo, uno llamado Formación policial en ciberdelincuencia: percepciones, pedagogía y política, donde se manifiesta que uno de los desafíos clave es comprender cuál es la mejor forma de impartir de manera efectiva habilidades y conocimientos relevantes sobre el delito cibernético en toda la organización, para permitir que los oficiales de policía reaccionen adecuadamente ante tales comportamientos ilícitos (Cockcroft et al., 2018).

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

En otro contexto, es importante tener en cuenta que este es un proceso de formación integral, donde se aporta al individuo desde diferentes perspectivas y se aprovecha lo manifestado en la carta de derechos humanos y principios para internet:

> Internet ofrece oportunidades sin precedentes para desarrollar los Derechos Humanos y desempeña un papel cada vez más importante en nuestra vida. Por lo tanto, es esencial que todos los agentes, tanto públicos como privados, respeten y protejan los Derechos Humanos en Internet. También se deben tomar medidas que garanticen que Internet funcione y evolucione de manera que cumpla y sea respetuosa con estos derechos (Internet Rights y Principles Coalition, 2019, p. 7).

Un enfoque interesante se muestra en el artículo El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito, el cual presenta una propuesta detallada de una ruta crítica para guiar la implementación de la innovación tecnológica en el cuerpo policial de Costa Rica. Esta propuesta busca facilitar la integración y la interconexión de tecnologías en la Fuerza Pública, teniendo en cuenta las mejores prácticas de estrategias policiales basadas en la innovación tecnológica en América Latina (Villalobos, 2020). Aquí toma relevancia el componente de capacitación en materia tecnológica, desarrollo de sistemas integrados de información y análisis de big data.

Por su parte, la Organización Internacional de Policía Criminal o Policía Internacional (INTERPOL) hace referencia a que la Policía debe seguir el ritmo de los avances tecnológicos y contar con la experiencia y las habilidades necesarias para responder a la evolución del delito digital a nivel nacional, regional e internacional. Por tal razón, ayudan a los países miembros a desarrollar habilidades cibernéticas, conocimientos y capacidades técnicas adaptadas a sus necesidades. Lo anterior, en el marco de programas, proyectos, herramientas y plataformas para la capacitación en habilidades cibernéticas, contribuyendo a que los funcionarios de policía en todas partes estén preparados para responder de manera efectiva al delito cibernético. Para lograr esto es fundamental que, en la etapa de formación básica del profesional de Policía, se incluyan los aspectos de conocimiento del delito informático y su prevención. La Oficina del Programa de Delitos Cibernéticos del Consejo de Europa indica que el uso delictivo de la tecnología está en constante evolución, con delitos cometidos en un volumen, velocidad y alcance cada vez mayores. Por lo tanto, las agencias de aplicación de la ley o cuerpos de Policía están bajo presión constante para mantenerse al día y renovar sus conocimientos y habilidades sobre ciberdelincuencia y pruebas electrónicas.

Como los desafíos son multifacéticos, se deben tomar numerosas acciones de manera simultánea, tales como: capacitación, reclutamiento, investigación, inversión en herramientas y

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

equipos, entre otras (INTERPOL, 2022). De esta forma, resulta relevante para el estudiantado de las Escuelas de formación policial y se deben incluir los temas relacionados con la prevención y atención de delitos informáticos, donde el proceso sea construido sobre la promoción y el respeto de los Derechos Humanos, ahora también en el contexto de Internet y las nuevas tecnologías.

Referentes conceptuales o marco teórico

Para el desarrollo del escrito fueron utilizadas teorías y referentes conceptuales clave, de los cuales es importante comprender su definición en términos generales, que ayudan a conocer algunas modalidades de delitos informáticos e identificar las necesidades en cuanto a la formación en estos aspectos. Además, es fundamental abordar el concepto de ciberseguridad.

La ciberseguridad consiste en salvaguardar las redes, dispositivos y datos para prevenir el acceso no autorizado o el uso indebido; se enfoca en asegurar la confidencialidad, integridad y disponibilidad de la información (Kaspersky, 2023). Los ataques cibernéticos, a menudo, tienen como objetivo el acceso, modificación o destrucción de información confidencial, extorsionar a usuarios o simplemente interrumpir los procesos que normalmente ejecuta una organización. Implementar medidas efectivas de ciberseguridad es particularmente desafiante hoy en día porque hay más dispositivos que personas y los atacantes son cada vez más innovadores (Cisco, 2022). Un enfoque de seguridad eficaz implica la implementación de diversas medidas de protección en diferentes niveles, abarcando redes, computadoras, aplicaciones, programas, información y datos que se desean resguardar. En las organizaciones, es fundamental que los procesos, las personas y la tecnología trabajen en conjunto para establecer una defensa sólida contra los ataques cibernéticos (Barbieri, 2021). Para el caso de estudio, se sigue un enfoque dirigido hacia el usuario común, que muchas veces tiene la percepción de que no tiene nada que ocultar o nada que perder en el mundo digital, pero olvida que sus datos personales representan un activo importante con el cual los ciber delincuentes pueden causar mucho daño.

Por otra parte, el cibercrimen o el delito cibernético puede definirse en un sentido estricto como cualquier delito dirigido a datos informáticos o, en un sentido muy amplio, como cualquier delito que involucre un sistema informático. En el primero, se corre el riesgo de ser demasiado restrictivo, ya que excluiría fenómenos que existen en el mundo físico, pero estos han ganado una calidad e impacto diferente a través del uso de computadoras como pornografía infantil, fraude o violaciones de los derechos de propiedad intelectual. En el segundo, sería demasiado amplio ya que la mayoría de los delitos hoy en día involucran una computadora de una forma u otra (Seger, 2012).

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

En este sentido, los ciber delincuentes cada vez son más sofisticados al momento de afectar a sus víctimas y aunque los ataques que usan no son novedosos, aún resultan efectivos, debido a que incluyen nuevas técnicas para que alguien muerda el anzuelo. Uno de los ataques más populares es el phishing. En el documento llamado Qué es el Phishing y cómo protegerse, este concepto se constituye como una de las modalidades de estafa preferida por los atacantes, con el fin de conseguir datos del usuario como su número de tarjeta de crédito o cualquier información que pueda ser utilizada de forma fraudulenta (Acens Technologies, 2020). Por su parte, el smishing está definido, en el artículo científico Seguridad por capas frenar ataques de smishing, como una combinación de las palabras phishing y SMS; es un nuevo tipo de técnica o variante del phishing que tiene como propósito robar la información de un usuario, mediante el uso del servicio de mensajería de texto (SMS) de un teléfono móvil (Martínez et al, 2018).

Otra modalidad que ha afectado a los usuarios con bastante frecuencia es el vishing (mezcla las de palabras voz y phishing). Se trata de una estafa telefónica en la que los delincuentes buscan engañar a la persona afectada con el objetivo de obtener información confidencial como datos personales, financieros o de seguridad, incluso, inducir a la víctima a realizar transferencias de dinero. Esta definición es presentada en el documento titulado Fraude del CEO (Europol, 2020).

Otra de las amenazas ampliamente usadas por los atacantes es el malware, ya que haciendo uso de este pueden generar una afectación aún mayor en los usuarios. Un malware no es más que un software maligno, habitualmente consiste en un código desarrollado por ciber atacantes, pensado y diseñado exclusivamente para causar daños, los cuales se enfocan en los datos y sistemas, con el propósito de obtener acceso no autorizado en una red. El malware suele ser distribuido a través de correo electrónico en forma de enlaces o archivos y su activación requiere que el usuario haga clic en el enlace o abra el archivo para ejecutarlo (Forcepoint, 2021).

Existe una característica que es común en los delitos mencionados anteriormente: los atacantes usan técnicas de ingeniería social, como la suplantación de identidad, para lograr engañar a las personas. Los ataques basados en suplantación de identidad pueden ser en gran medida perjudiciales para la reputación en línea de la víctima. A medida que los motores de búsqueda agregan cada vez más los datos en línea sobre las personas, dicha información es utilizada por los ciber delincuentes para una variedad de propósitos, incluida la evaluación de su idoneidad para el empleo. Los ataques de suplantación, particularmente aquellos que no se detectan, pueden tener serios efectos adversos consecuencias para las víctimas, incluso, en el mundo fuera de línea (Goga et al., 2021).

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Por otra parte, en algunos casos de grooming, puede producirse suplantación de identidad, ya que los perpetradores pueden utilizar identidades falsas o hacerse pasar por personas que no son con el fin de ganarse la confianza de los menores (UNICEF, 2017). Esta suplantación puede involucrar la creación de perfiles falsos en redes sociales, el uso de fotos o información personal engañosa, e incluso pueden adoptar identidades similares a las de los amigos o familiares de la víctima para generar una sensación de familiaridad y confianza. La suplantación de identidad es una táctica manipuladora utilizada en el proceso de grooming para establecer una relación y manipular a los menores. Es fundamental que los jóvenes mantengan una actitud de vigilancia constante y adopten medidas de seguridad para resguardar su identidad en el entorno digital. Además, es crucial que sean plenamente conscientes de los riesgos inherentes al entablar interacciones con individuos desconocidos en Internet.

El spoofing se usa para obtener la información de contacto, como los números de teléfono, correos electrónicos y sitios web; se manipula intencionalmente con el objetivo de engañar y aparentar ser legítima. Esta práctica se utiliza para diversos fines como realizar llamadas automáticas masivas, utilizando números de teléfono falsificados, enviar correos electrónicos de spam en masa mediante direcciones falsificadas y crear sitios web fraudulentos, que engañan y recopilan información personal. Estas acciones suelen estar relacionadas con otros tipos de delitos (Internet Crime Complaint Center, 2022).

La integración de los datos personales en las nuevas tecnologías abarca diversas etapas como la recopilación, el almacenamiento, el análisis, el procesamiento y la interpretación de volúmenes masivos de información, conocido como Big Data. Esto ha convertido al comercio electrónico en el impulsor principal de la economía del siglo XXI, donde los datos personales se han convertido en la moneda de la economía digital. Sin embargo, este escenario también plantea desafíos, ya que implica la interacción de múltiples actores y puede dar lugar a accesos indebidos o no autorizados a los datos, así como la divulgación de información a personas no autorizadas (Garzón y Cuero, 2023).

Retomando, la suplantación de sitios web, también conocida como phishing, es una técnica utilizada por ciberdelincuentes para engañar a los usuarios y obtener sus datos personales sensibles. Consiste en crear páginas web falsas que imitan a sitios legítimos, como los de bancos, redes sociales, tiendas en línea u otros servicios populares. El objetivo principal de la suplantación de sitios web es que los usuarios crean que están interactuando con una entidad confiable y legítima. Estas páginas falsas suelen tener un diseño y una apariencia muy similares a los originales, utilizando logotipos, colores y estructuras de navegación idénticas o similares. Una vez que los usuarios visitan el sitio

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

web falso, se les solicita ingresar su información personal, como nombres de usuario, contraseñas, números de tarjetas de crédito, direcciones y otros datos sensibles. Estos datos son luego capturados por los ciberdelincuentes y pueden ser utilizados para cometer fraudes financieros, robo de identidad u otros delitos.

La suplantación de sitios web, a menudo, se realiza a través de enlaces maliciosos enviados por correo electrónico, mensajes de texto, redes sociales u otras formas de comunicación electrónica. Los usuarios pueden ser redirigidos automáticamente al sitio falso o engañados para que accedan a él a través de técnicas de ingeniería social, como el uso de mensajes alarmantes o urgentes que los manipulan para tomar acciones rápidas sin verificar la autenticidad del sitio. Según datos de la Fiscalía General de la Nación, en el mes de abril de 2023, se han denunciado 512 casos relacionados con la suplantación de sitios web, con el objetivo de robar datos e información personal de los usuarios, como se puede evidenciar en la Figura 1.

Figura 1.

Suplantación de sitios web

Fuente: Fiscalía General de la Nación (2023).

Por otra parte, los bancos llevan a cabo actividades de concienciación y educación financiera de manera continua. En el caso específico de Colombia, varios actores, como la Policía Nacional, Incocrédito y Asobancaria realizan esfuerzos constantes para concienciar a los usuarios financieros sobre la importancia de proteger datos sensibles como contraseñas y claves de sus productos. Estas iniciativas tienen como objetivo promover la seguridad y la protección de la información personal y financiera de los usuarios (Ospina y Sanabria, 2023).

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Metodología

Apoyado en los referentes teóricos anteriormente expuestos, el proyecto se desarrolló como una investigación mixta, con el diseño y la aplicación de una encuesta al estudiantado de la Escuela de Policía Rafael Reyes, donde se forman funcionarios de Policía con el grado de Patrulleras y que obtienen el título de Técnico Profesional en Servicio de Policía. Para la recolección de la información se empleó la encuesta y como instrumento un cuestionario conformado por catorce preguntas, las cuales fueron sometidas a un proceso de validación por parte de conocedores del tema y la asesora metodológica del centro de formación policial. Estas respondieron a aspectos fundamentales para la investigación, tales como: identificar incidentes de seguridad ocurridos, conocimiento de ocurrencia de delitos informáticos a terceros, tratamiento dado al incidente, identificación de delitos informáticos, medidas de prevención, habilidades en el uso de herramientas tecnológicas y acceso a internet, conocimiento de aspectos legales y denuncia e información que se comparte en la red. La muestra fue de doscientas once personas estudiantes.

Posterior al análisis de los resultados obtenidos en la encuesta, se logró determinar las modalidades de los delitos informáticos que afectan a la comunidad educativa. Con el propósito de abordar la problemática que más afecta a la ciudadanía en general, se utilizó la información que suministra la herramienta del CAI Virtual ciberincidentes y los registros estadísticos de las conductas punibles registradas en el Sistema de Información Estadístico Delictivo y Contravencional de la Policía Nacional de Colombia – SIEDCO. En estas se muestran los casos que se han denunciado por parte de las personas que han sido víctimas. Adicionalmente, se clasificaron las modalidades más denunciadas, que a su vez generan mayor riesgo y se presentan con mayor frecuencia. Una vez realizado este procedimiento se enfocó el estudio a los siguientes delitos informáticos: phishing, smishing, vishing, suplantación de identidad y malware. Dentro de los resultados obtenidos se encontró que la estafa es una modalidad presente con mucha frecuencia, pero que se puede combatir si se adoptan buenas prácticas para prevenir los delitos mencionados, de tal forma que se aborda desde esta perspectiva o desde este vector de ataque.

A continuación, se efectuó un análisis frente a las actividades a desarrollar para generar las competencias en las aspirantes a patrulleras de la Escuela de Policía Rafael Reyes en cuanto a la prevención y atención de los delitos informáticos, de tal modo que surgieron diferentes espacios en los cuales fue posible compartir la información, a través de medios digitales, creación de material multimedia, socializaciones, exposiciones y representaciones. Finalmente, la información recopilada,

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

las buenas prácticas sugeridas y demás recomendaciones serán difundidas mediante una aplicación móvil. De esta manera, la estrategia de prevención y atención se presenta abarcando las modalidades que afectan a la comunidad. La siguiente etapa es la generación de conocimiento en cuanto a las buenas prácticas en el uso de dispositivos y servicios de internet y por último el medio de difusión de la información en forma digital.

El enfoque de la investigación fue mixto, debido a que se usaron elementos cualitativos y cuantitativos, donde se realizó un estudio y análisis de los delitos informáticos para obtener recomendaciones y buenas prácticas para evitar ser víctimas de los ciber delincuentes. Actualmente, las tecnologías de la información y la comunicación constantemente avanzan, los delincuentes han cambiado su modus operandi y logran afectar a la ciudadanía también en el ciberespacio, especialmente, en el robo de dinero o de identidad. Por otra parte, se presenta un enfoque analítico cuantitativo con relación a los registros estadísticos de las conductas punibles registradas en el Sistema de Información Estadístico Delictivo y Contravencional de la Policía Nacional de Colombia – SIEDCO.

Para seleccionar la población y muestra, se tomó como población a las 640 personas estudiantes del Técnico Profesional de Servicio de Policía, de la Escuela de Policía Rafael Reyes y como muestra a 220 encuestadas. Lo anterior, porque la muestra es representativa con relación a la población de interés, en este caso, se utilizó un 35% de las personas estudiantes del técnico profesional de servicio de Policía. Por otra parte, la selección de las 220 personas encuestadas se realizó de forma aleatoria, es decir, que todas las personas tuvieron la misma probabilidad de ser seleccionadas, lo cual evitó sesgos y contribuyó a asegurar que los resultados sean generalizables.

Resultados

En primera medida, la intención del estudio es conocer la problemática que afecta a las personas estudiantes del técnico profesional en servicio de policía, a través de la información y datos recopilados por medio de la encuesta. Las personas estudiantes manifestaron que, en su gran mayoría, no han sido víctimas de delitos informáticos y que conocen el procedimiento a seguir en caso de verse afectadas. Sin embargo, de acuerdo a las respuestas obtenidas en preguntas puntuales, se logró evidenciar que no aplican buenas prácticas en cuanto el uso de medios informáticos y que pueden verse inmersas en estos casos, porque, aun siendo parte de la Policía Nacional, son un blanco altamente buscado por la delincuencia. En estos casos, generalmente, las personas no reconocen que

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

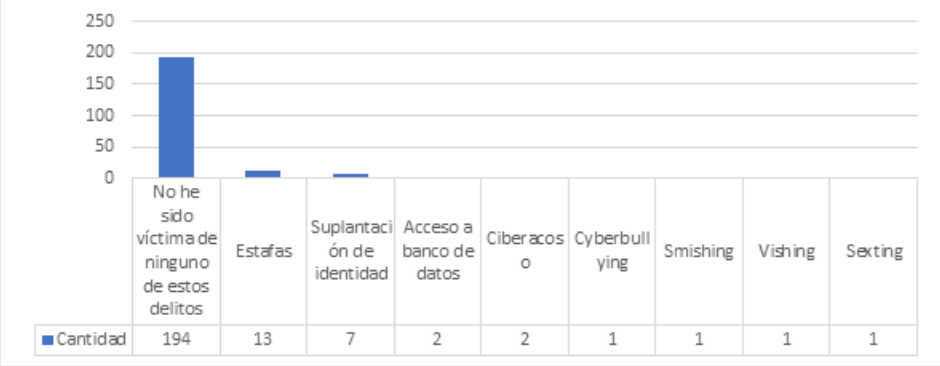
han sufrido afectaciones por alguna de las modalidades mencionadas, pues al analizar la situación detenidamente después de ocurrido el evento, se evidencia que el delincuente logró engañar y conseguir su objetivo. Por este mismo, motivo muchas veces ni siquiera se presenta la respectiva denuncia. Inicialmente, se preguntó a las personas estudiantes si han sido víctimas de un delito informático.

Posteriormente, se realizó la pregunta ¿ha sido víctima de un delito informático?, donde un 95% de las personas encuestadas respondieron negativamente y un 5% manifiesta que sí han sido afectadas. Se deduce que, mayoritariamente, las personas estudiantes no han tenido ningún tipo de problema con delitos informáticos, pero esto no es ninguna garantía de que en el futuro no puedan ser afectadas. Otro aspecto importante es conocer si alguien cercano ha sufrido afectación por estos delitos, para lo cual se preguntó ¿tiene conocimiento de una persona víctima de un delito informático? En este caso, se obtuvo que un 85% de la población encuestada admite no tener conocimiento alguno con respecto a la pregunta planteada, pero un 15% sí conoce algún caso de una persona cercana que ha sido víctima de un delito informático, lo cual da índices relevantes para el desarrollo de la investigación, puesto que esto corresponde a 33 casos.

Es fundamental conocer las modalidades delictivas que han afectado a las personas estudiantes. Así, en la Figura 2, se pueden evidenciar las elecciones sobre qué tipo de delito informático ha afectado a la población en estudio. Se pudo determinar que 194 personas (88%) manifestaron no haber sido víctima de ninguno de estos delitos, 13 seleccionaron la estafa, 7 la suplantación de identidad, 2 el acceso a banco de datos, 2 seleccionaron la opción ciberacoso y, finalmente, 1 persona por cada opción seleccionada: sexting, smishing, vishing y cyberbulling. Cabe mencionar que los demás delitos no han sido contemplados por ninguna de las personas encuestadas.

Figura 2.

¿De cuál o cuáles de los siguientes delitos informáticos ha sido víctima?



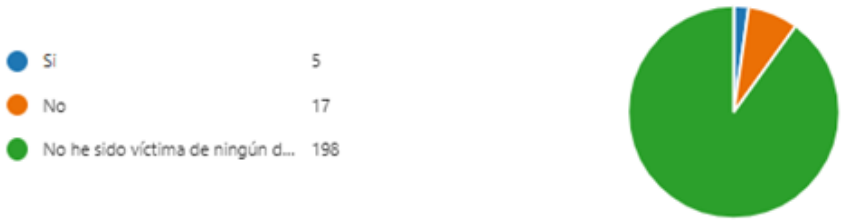
Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Fuente: Elaboración propia a partir de datos obtenidos de la encuesta aplicada al estudiantado.

En este apartado se requería conocer si aquellas personas afectadas realizaron la denuncia, de lo que se obtuvo:

Figura 3.

¿Se realizó el debido procedimiento (denuncia) para informar sobre el delito ocurrido?

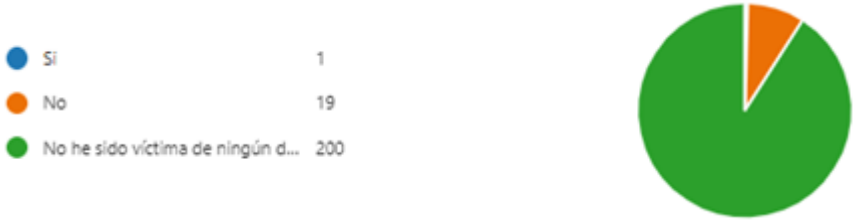


Fuente: Elaboración propia a partir de datos obtenidos de la encuesta aplicada al estudiantado.

La Figura 3 muestra que el 90% manifiesta no haber sido víctima de ningún delito, siendo esta la opción principal. Por otro lado, un 8% representa a aquellas personas que manifestaron “no” en este aspecto y un 2% afirma haber realizado la denuncia. Otro aspecto interesante por identificar es si posterior a la denuncia hubo consecuencias de algún tipo, a lo que respondieron:

Figura 4.

¿Al realizar la denuncia hubo consecuencias legales llevadas a cabo?



Fuente: Elaboración propia a partir de datos obtenidos de la encuesta aplicada al estudiantado.

En la Figura 4, se evidencian las respuestas obtenidas a la pregunta: ¿al realizar la denuncia hubo consecuencias legales llevadas a cabo? En este caso, el 1% (1 persona) afirma que sí hubo consecuencias legales, el 8.6% (19 personas) manifiesta que no las hubo y, finalmente, la mayoría de las personas encuestadas (90%, 200 personas estudiantes en total) manifiestan que no han sido víctimas de ningún tipo de delito cibernético, por lo que no han realizado denuncias.

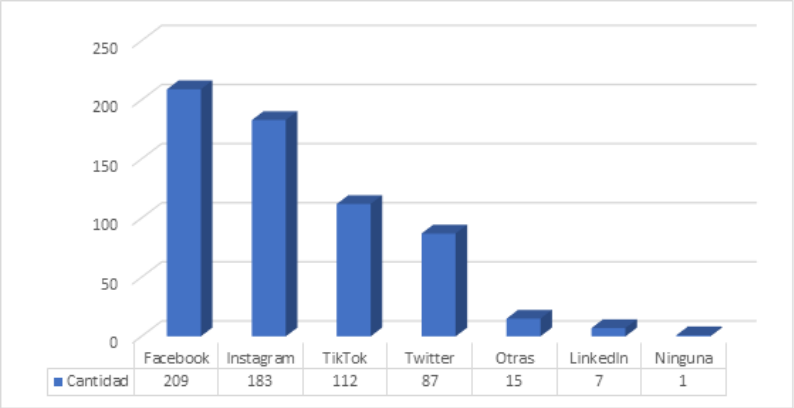
Con respecto a la pregunta ¿considera que toma precauciones para evitar ser víctima de alguno de estos delitos?, se pudo apreciar que el 94% de las encuestadas (la mayoría de la población correspondiente a 207 personas estudiantes en total) manifiesta que está de acuerdo con la pregunta planteada, pero un 6% (13) seleccionaron la opción No. Esto no representa a la mayoría, pero sí es

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

un número considerable de personas que se exponen a un delito informático. Es clave conocer las redes sociales que utilizan las personas encuestadas, por lo que se procedió a indagar en este aspecto.

Figura 5.

Seleccione las redes sociales que utiliza



Fuente: Elaboración propia a partir de datos obtenidos de la encuesta aplicada al estudiantado.

En la Figura 5, es posible evidenciar las redes sociales que utilizan las personas encuestadas, obteniendo los siguientes resultados: Facebook es la aplicación más votada con un total de 209 votos, es decir, el 95%; en segundo lugar, aparece Instagram con 183 (83%); en tercer lugar, se encuentra TikTok con 112 (50.9%); Twitter ocupa el cuarto lugar con 87 respuestas; por su parte,15 personas optaron por la opción “otras”; finalmente, se encuentra Linkedln con 7 votos, lo cual es interesante, ya que es una plataforma muy útil para aspectos profesionales. Estos datos permitieron identificar en cuales redes sociales se debe enfatizar sobre prevención y buenas prácticas, con el fin de evitar afectaciones a los usuarios por causa de un delito informático relacionado.

También, es fundamental para este estudio conocer si las aspirantes a patrulleras saben cómo realizar la denuncia, pues cualquier funcionario de policía debería estar bien informado al respecto, por lo que se preguntó: En caso de ser víctima de un delito informático, ¿conoce cómo se debe realizar la denuncia o a qué ente territorial debe acudir? Aquí, evidenciar que el 22.3% de las personas manifiesta que no tienen conocimiento sobre cómo realizar la denuncia o ante qué entidad se debe acudir, lo cual resulta preocupante, ya que ante esta modalidad delictiva cada vez más presente, los funcionarios de policía deben estar a la vanguardia y contar con los conocimientos y competencias suficientes, no solo para evitar ser víctimas de los delitos, sino también para orientar a la ciudadanía. Por otra parte, el aspecto legal es la base sobre la cual se debe fundamentar el procedimiento, por este

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

motivo es importante conocer la ley que aplica para este tema. Por esta razón, se indagó sobre el conocimiento de una ley en específico para Colombia y se obtuvo el siguiente resultado:

Figura 6.

¿Cuál es la ley de delitos informáticos en Colombia?

Fuente: Elaboración propia a partir de datos obtenidos de la encuesta aplicada al estudiantado.

En la Figura 6, se muestran tres opciones sobre la identificación de la ley de delitos informáticos en Colombia, de lo cual se obtuvo que un 93% (205 personas en total) reconocen la Ley 1273 de 2009; por lo cual el 7% de las personas encuestadas no conocen dicha ley.

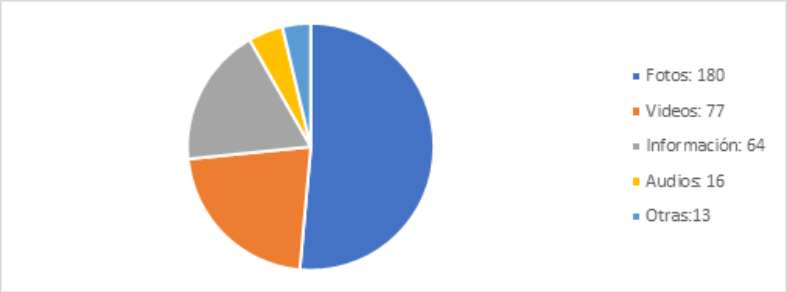
Anteriormente, se cuestionó sobre las precauciones que se deben tomar. Ahora se indaga sobre el conocimiento de un 2FA (factor de doble autenticación). Sobre esto, se logró evidenciar que, aunque la mayoría de las encuestadas habían respondido que aplicaban medidas de prevención, en esta pregunta se demuestra que el 47 % (103 personas) no sabe que es un factor de doble autenticación, siendo este considerado como el primer mecanismo para proteger las cuentas de correo o de redes sociales (identificadas en la pregunta 7), ya que incorpora un paso adicional de seguridad. Esto permitió deducir que las personas no tienen claridad sobre cuáles medidas de prevención deben aplicar ante un delito informático.

Para continuar con las medidas de prevención, es fundamental conocer qué tipo de información las personas estudiantes comparten en internet, pues una medida básica de prevención es no compartir información sensible o que pueda ser usada para otros fines. Con las siguientes preguntas se trató de identificar en qué medida evalúan el contenido que comparten en internet y son conscientes de que dicha información queda disponible para cualquier usuario en internet.

Figura 7.

¿Qué tipo de contenido comparte en la red?

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644



Fuente: Elaboración propia a partir de datos obtenidos de la encuesta aplicada al estudiantado.

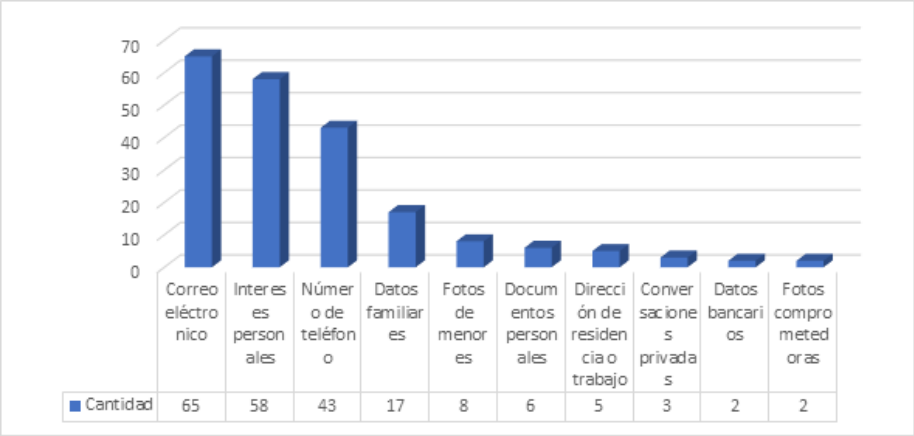
En la Figura 7, se indagó sobre el tipo de contenido que publican, obteniendo que el 51% (la mayor población encuestada) manifestó que las fotos son las más publicadas, un 22% seleccionó el ítem de videos, un 18% coincide en que lo más revelado es su información personal o profesional, lo cual es un aspecto al que se le debe prestar mayor atención. Posteriormente, 5% de las respuestas correspondieron a la opción de audios la selección de audios y un 4% la opción otros. Ante este interrogante, se cuestionó al estudiantado nuevamente sobre las precauciones antes de publicar este tipo de contenidos en la red con la pregunta ¿toma precauciones sobre lo que comparte en la red? Se obtuvo que el 96% (211 personas en total) opta por acciones preventivas frente a lo que exponen en la red y el 4% (9 personas) admite que no toma ningún tipo de prevención. Para esto, también es importante conocer si estas personas evalúan el riesgo de compartir datos o información en internet, de lo que se pudo apreciar la percepción que tiene el personal estudiantil en estudio con respecto a los riesgos que pueden presentarse al compartir cualquier tipo de información en el internet. Se evidencia que el 95% (208 personas encuestadas en total) manifestaron que sí evalúan el riesgo, mientras que el 5% no se toman el tiempo de valorar las condiciones inseguras al momento de compartir cualquier dato en internet.

Finalmente, se procedió a indagar el tipo de información que las personas estudiantes han compartido en internet. En la Figura 8, se puede evidenciar que las estas comparten en internet información sensible y que un ciber delincuente puede utilizar para causar afectaciones, tanto a la persona y como a sus familiares o amigos, pues puede suplantar su identidad. Al analizar estos resultados, se encontró que, aunque este grupo manifestó tomar medidas de prevención y que evalúan el riesgo de publicar información en internet, se evidencia que no es cierto y que comparten datos e información sensible en internet.

Figura 8.

De los siguientes, ¿Qué información suya está disponible en internet?

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644



Fuente: Elaboración propia a partir de datos obtenidos de la encuesta aplicada al estudiantado.

Posterior a esto, se realizó la consulta en el Sistema de Información Estadístico Delictivo y Contravencional de la Policía Nacional de Colombia – SIEDCO, con el propósito de validar cuáles son los principales delitos informáticos que se denuncian por parte de la ciudadanía. Esto permitió delimitar el estudio a 5 modalidades delictivas de este tipo.

Análisis y discusión de resultados

La Oficina de Seguridad del Internauta (OSI) y el Instituto Nacional de Ciberseguridad (INCIBE) lazaron una campaña que les indica a los usuarios siete datos que nunca deben compartir en Internet, dentro de los cuales se tiene:

1. Correo electrónico y número de teléfono: al compartir esta información, el usuario puede ser víctima de spam, phishing y cualquier ataque basado en ingeniería social.
2. Dirección y ubicación: no es posible conocer las intenciones de las personas que tengan acceso a nuestra dirección o ubicación.
3. Fotos de menores: no se tiene certeza de donde puedan terminar estas imágenes ni quien puede tener acceso a estas.
4. Fotos comprometedoras: este material puede ser usado para la sextorsión o el ciber acoso.
5. Documentos personales: publicando estos archivos es posible ser víctima de suplantación de identidad.
6. Opiniones, quejas, comentarios: esto puede ser usado por las personas que puedan sentirse ofendidas.

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

7. Conversaciones privadas: si la conversación es privada, no debe publicarse en internet, ya que puede contener información que la otra persona no desea divulgar.

Aunque en el anterior compilado no aparecen datos bancarios, datos familiares y los intereses personales, estos también representan un alto riesgo para los usuarios que comparten este tipo de información en internet. La información bancaria solamente debe interesar al titular, pues puede ser usada por los delincuentes para su beneficio personal. Los datos familiares son usados generalmente cuando se suplanta a una persona y los intereses personales se usan para los ataques de contraseñas, ya que con esta información el delincuente va probando posibles claves de los servicios de internet.

Ante estos datos obtenidos, se demostró que, aunque la mayoría de las personas encuestadas manifestaron tener precauciones, la aplicación de medidas de prevención y evaluar el riesgo de compartir información en internet no se demuestra y, probablemente, muchas ya están expuestas en la red. Puede que las medidas que tomaron no fueron efectivas o que simplemente tienen la percepción de que, como usan sus servicios de internet, actualmente lo están haciendo de forma segura.

Por esta razón, es necesaria la inclusión de la formación en prevención y atención de delitos informáticos en la educación policial. Sin embargo, no se debe limitar esto a la educación policial, ya que, por el riesgo que esto representa para todas las personas, también es una necesidad que en la educación básica y primaria se eduque a los usuarios. Esto con el fin de que, desde edades tempranas, se forje una cultura de seguridad de la información en las comunidades y se pueda mitigar este riesgo, así como crear conciencia sobre el uso responsable y seguro de internet.

Como resultado de esta investigación, se generó un compilado de buenas prácticas y recomendaciones para evitar ser víctima de los delitos informáticos más comunes identificados, así como el instructivo para realizar la denuncia en Colombia. Posteriormente, se integró toda esta información en una aplicación móvil, la cual permite tener fácil acceso a esta y se puedan incorporar estas acciones en la vida cotidiana. Asimismo, que las personas puedan orientarse de mejor manera a la ciudadanía. A continuación, se muestran algunos capturas de pantalla de la aplicación y una breve descripción de su contenido.

Figura 9.

Pantalla de inicio aplicación móvil

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Fuente: Aplicación móvil delitos informáticos.

En la Figura 9, se muestra la pantalla principal, donde se encuentran los accesos a la información relacionada a cada delito: phishing, smishing, vishing, grooming, suplantación y estafa. Así como el menú principal ubicado en la parte superior izquierda que da acceso a: cómo denunciar, herramientas online y una sección de preguntas frecuentes.

Figura 10.

Pantalla cómo denunciar

Fuente: aplicación móvil delitos informáticos.

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

En la Figura 10, se muestra el apartado donde se encuentra con detalle el paso a paso para realizar la denuncia, así como también la normativa.

Figura 11.

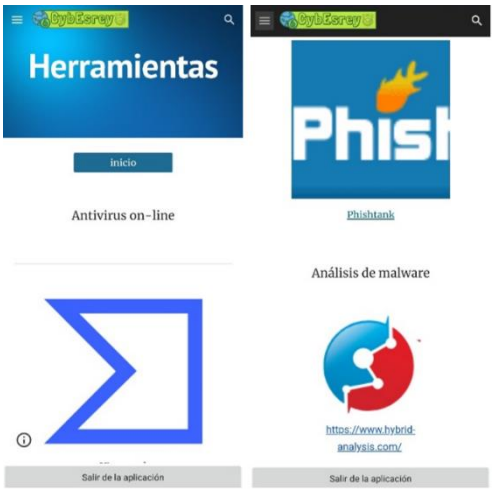
Pantalla redes sociales

Fuente: aplicación móvil delitos informáticos.

En la Figura 11, se encuentra la sección de redes sociales, donde el usuario puede encontrar las principales recomendaciones para proteger las cuentas, así como un video de estas mismas recomendaciones, para que la persona usuaria también cuente con otro formato.

Figura 12.

Pantalla herramientas



Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Fuente: aplicación móvil delitos informáticos.

Como se evidencia en la Figura 12, la persona usuaria puede encontrar enlaces a herramientas en línea como: antivirus, análisis de malware y verificador de enlaces.

Figura 13.

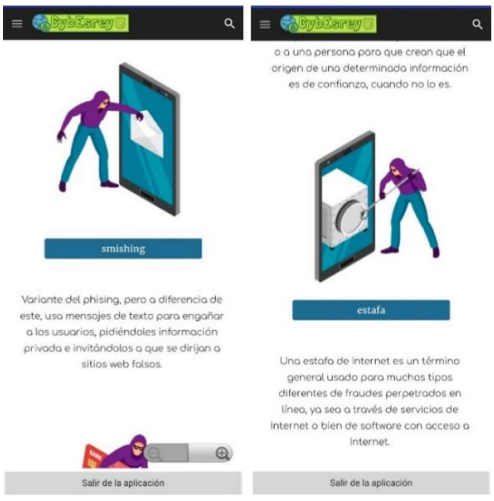
Pantalla casos reales

Fuente: aplicación móvil delitos informáticos.

En la Figura 13, se muestra que dentro de la aplicación se incluyó un apartado con testimonios de personas que fueron víctimas de un delito informático.

Figura 14.

Pantalla delitos informáticos



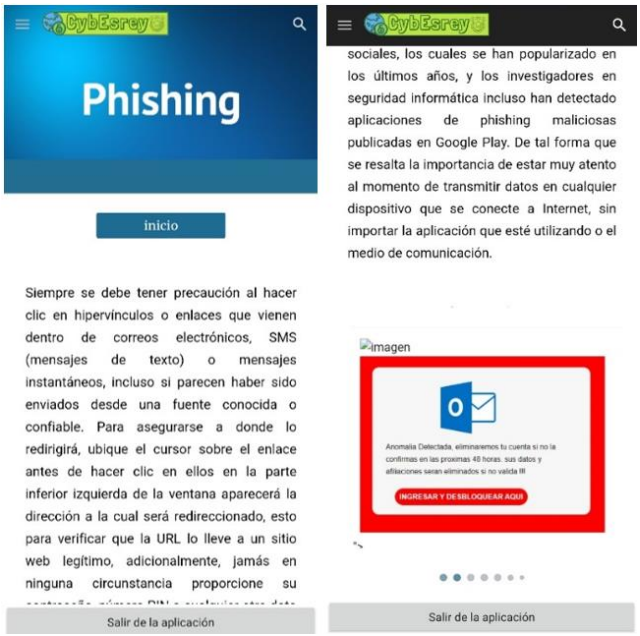
Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Fuente: aplicación móvil delitos informáticos.

En la Figura 14, se muestran algunos accesos a los delitos objeto de estudio.

Figura 15.

Pantalla phishing



Fuente: aplicación móvil delitos informáticos.

En la Figura 15, se muestra el contenido de la categoría phishing, en donde al final se muestra una galería de muestras de correos phishing, con el fin de que el usuario aprenda a identificar este tipo de correos.

Limitaciones

- Disponibilidad de datos: Puede haber limitaciones en la disponibilidad de datos relevantes y actualizados sobre la inclusión de la formación en prevención y atención de delitos informáticos en la educación policial. La información específica sobre los programas de formación y sus resultados puede no ser fácilmente accesible o estar sujeta a restricciones de confidencialidad.

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

- Sesgos en las respuestas: Existe la posibilidad de que los informantes proporcionen respuestas sesgadas o que no reflejen la realidad de la situación. Esto puede deberse a la presión social, deseos de mostrar resultados positivos o evitar revelar debilidades en los programas de formación.
- Generalización de los resultados: Dado que la educación policial puede variar entre países, regiones o instituciones, es importante considerar las limitaciones en la generalización de los resultados. Los hallazgos obtenidos en una determinada área geográfica o contexto educativo pueden no ser aplicables de manera directa a otros lugares o instituciones.
- Evolución tecnológica: La rápida evolución de la tecnología y las tácticas utilizadas por los delincuentes informáticos puede ser un desafío para la investigación. Los métodos y enfoques de formación que se consideren efectivos en el momento de la investigación podrían volverse obsoletos en un corto período de tiempo, debido a los avances tecnológicos.
- Limitaciones de tiempo y recursos: Los estudios de investigación pueden verse limitados por restricciones de tiempo y recursos. Realizar una investigación exhaustiva y abarcar diferentes aspectos de la inclusión de la formación en delitos informáticos en la educación policial puede requerir un tiempo y recursos considerables.

Conclusiones

Las instituciones educativas en general, y más aún las de formación policial, deben hacer de la ciberseguridad una prioridad e incluirse los temas de prevención y cuidado digital. Los delitos informáticos no son bajos en frecuencia o gravedad en Colombia. De hecho, como se ha podido evidenciar en el estudio, estas modalidades son ampliamente denunciadas y parecen estar ganando popularidad año tras año.

La educación en seguridad informática en un nivel básico proporciona a los usuarios conocimientos y habilidades necesarias para reconocer y prevenir posibles riesgos y ataques. Les enseña sobre la importancia de contraseñas seguras, actualizaciones de software, navegación segura, protección de datos personales y cómo identificar intentos de phishing o estafas en línea.

La seguridad en línea es una responsabilidad compartida, un objetivo común entre los funcionarios que promueven buenas prácticas para el uso responsable y seguro de medios TIC; también, parte de los usuarios finales quienes, al acatar las recomendaciones, minimizan el riesgo de ser víctimas de algún tipo de delito informático.

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Los delitos informáticos se refieren a la comisión de actos criminales usando una computadora o una red informática. Estos delitos pueden variar desde el uso ilegal de la información contenida en una computadora hasta el acceso no autorizado a los sistemas informáticos de otra persona.

Desde el servicio de Policía se debe prevenir y desde sus especialidades se debe detectar e investigar este tipo de delitos. Esto incluye la vigilancia en internet para detectar actividades sospechosas o incidentes de seguridad. El servicio de Policía también debe ofrecer servicios de educación y prevención para ayudar a las personas usuarias a evitar los delitos informáticos.

Como aporte para la educación policial se generó la aplicación móvil en su versión beta para contribuir a generar competencias y conocimiento, para generar buenas prácticas para prevención del delito informático.

Recomendaciones

Actualización del plan de estudio: es importante que las instituciones educativas policiales revisen y actualicen el plan de estudios, para incluir módulos específicos sobre delitos informáticos. Esto permitirá que los futuros funcionarios de policía adquieran los conocimientos necesarios para prevenir y responder adecuadamente a estos delitos.

Ejercicios prácticos y simulaciones: la formación en prevención y atención de delitos informáticos debe incluir ejercicios prácticos y simulaciones de situaciones reales. Estos ejercicios permiten practicar habilidades en un entorno controlado y desarrollar la capacidad de responder de manera efectiva a los delitos informáticos.

Actualización constante: dado que el panorama de los delitos informáticos evoluciona rápidamente, es esencial que la formación en esta área se mantenga constantemente actualizada Las instituciones educativas policiales deben establecer mecanismos para garantizar que el cuerpo docente, que orienta la asignatura “tecnologías aplicadas al servicio de policía”, y los funcionarios reciban capacitación periódica y estén al tanto de las últimas tendencias y técnicas utilizadas por los delincuentes informáticos. Esto puede incluir programas de educación continua, participación en conferencias y talleres, y acceso a recursos actualizados en línea.

Referencias

Acens Technologies. (2020). *Qué es el Phishing y cómo protegerse.* https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

Barbieri, C. (2021). *Tú y tu empresa están en peligro y no lo sabes*. https://oxfordusa.com/es/tu-y-tu-empresa-estan-en-peligro-y-no-lo-sabes/

Bryant, R., Cockcroft, T., Tong, S. y Wood, D. (2014). *The developing relationship between universities and police services: the past and present situation.* [La relación en desarrollo entre las universidades y los servicios policiales: la situación pasada y presente]. En J. Brown, *Police Training and Education: Past, present and future* (pp.383-397). https://www.researchgate.net/publication/315799908_Police_Training_and_Education_Past_present_and_future

Cisco. (2022). *What Is Cybersecurity?* [¿Qué es la ciberseguridad?] https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cockcroft, T., Shan-A-Khuda, M., Cliffe, Z., Trevorrow, P. (2018). *Police Cybercrime Training: Perceptions, Pedagogy and Policy* [Formación policial en ciberdelincuencia: percepciones, pedagogía y política]. *A Journal of policy and practice, 15(1), 15-33*. https://doi.org/10.1093/police/pay078

Europol. (2020). *Fraude del CEO*. https://www.europol.europa.eu/sites/default/files/documents/colombia_1.pdf

Fiscalía General de la Nación (2023). Estadística de denuncias por delitos. https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/

Forcepoint. (2021). *What is Malware? Malware Defined, Explained, and Explored* [¿Qué es el malware? Malware definido, explicado y explorado]. https://www.forcepoint.com/es/cyber-edu/malware

Garzón, J. O. y Cuero, K. S. (2023). Una mirada a la cibercriminalidad en Colombia y su asimilación con los delitos de impacto. *Revista Criminalidad*, *64*(3), 203-225. https://doi.org/https://doi.org/10.47741/17943108.373

Goga, O., Venkatadri, G. y Gummadi, K. (2021). *Exposing Impersonation Attacks* [Exposición de ataques de suplantación de identidad]. https://www.lix.polytechnique.fr/~goga/papers/impers_cosn14.pdf

Internet Rights y Principles Coalition. (2019). *Carta de derechos humanos y principios para internet. Internet Governance Forum* [Foro de Gobernanza de Internet]. https://drive.google.com/file/d/1REWtM5NmfClVDWcHBvEcHTyBGm7fgHd9/view

Interpol. (2022). *Guide for developing law enforcement training strategies on cybercrime and electronic evidence* [Guía para el desarrollo de estrategias de formación policial sobre

Revista Educación, 2023, 47(2), julio-diciembre, ISSN: 0379-7082 / e-ISSN 2215-2644

ciberdelincuencia y pruebas electrónicas]. https://rm.coe.int/guide-for-developing-training-strategies-final/1680a62c72

Internet Crime Complaint Center. (2022). *Internet Crime Report* [Reporte de crímenes en internet]. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Kaspersky. (2023). *¿Qué es la ciberseguridad?*. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Martínez, C., Cruz, Y., Cruz, T., Álvarez, M. (2018). Seguridad por capas frenar ataques de Smishing. *Dominio de las ciencias, 4*(1), 115-130. http://dominiodelasciencias.com/ojs/index.php/es/article/view/726

National Initiative for Cybersecurity Education [NICE]. (2016). *Strategic Plan. National initiative for cybersecurity education* [Plan estratégico. Iniciativa nacional para la educación en ciberseguridad]. NICE. https://www.nist.gov/system/files/documents/2020/10/26/2012_NICE-strategic-plan_withcover.pdf

Ospina, M. R. y Sanabria, P. E. (2023). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista criminalidad, 62*(2), *199-212.* https://dialnet.unirioja.es/servlet/articulo?codigo=7667839

Rosgaby, K. (2022). *Estadísticas de la situación digital de Colombia en el 2021-2022.* https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2021-2022/#:~:text=Por%20otro%20lado,%20el%20n%C3%BAmero,el%2081%25%20de%20la%20poblaci%C3%B3n.

Seger, A. (2012). *Cybercrime strategies* [Estrategias de ciberdelincuencia]. Council of Europe. https://rm.coe.int/16802fa3e1

Villalobos, H. (2020). El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito. *Revista de relaciones internacionales, estrategia y seguridad*. *15(1),* 79-97. https://revistas.unimilitar.edu.co/index.php/ries/article/view/4243

We are social. (2022). *Más de 5 mil millones de personas ya usan internet.* https://wearesocial.com/es/blog/2022/04/mas-de-5-mil-millones-de-personas-ya-usan-internet/#:~:text=Usuarios%20de%20Internet:%205.000%20millones,millones%20durante%20el%20%C3%BAltimo%20a%C3%B1o

Wydra, C. (2015). *Educating the Technology Officer of the Future: A Needs Analysis* [Educando al Oficial de Tecnología del Futuro: Un Análisis de Necesidades]. Revista *Issues in Information Systems, 16(4), 224-231*. https://iacis.org/iis/2015/4_iis_2015_224-231.pdf